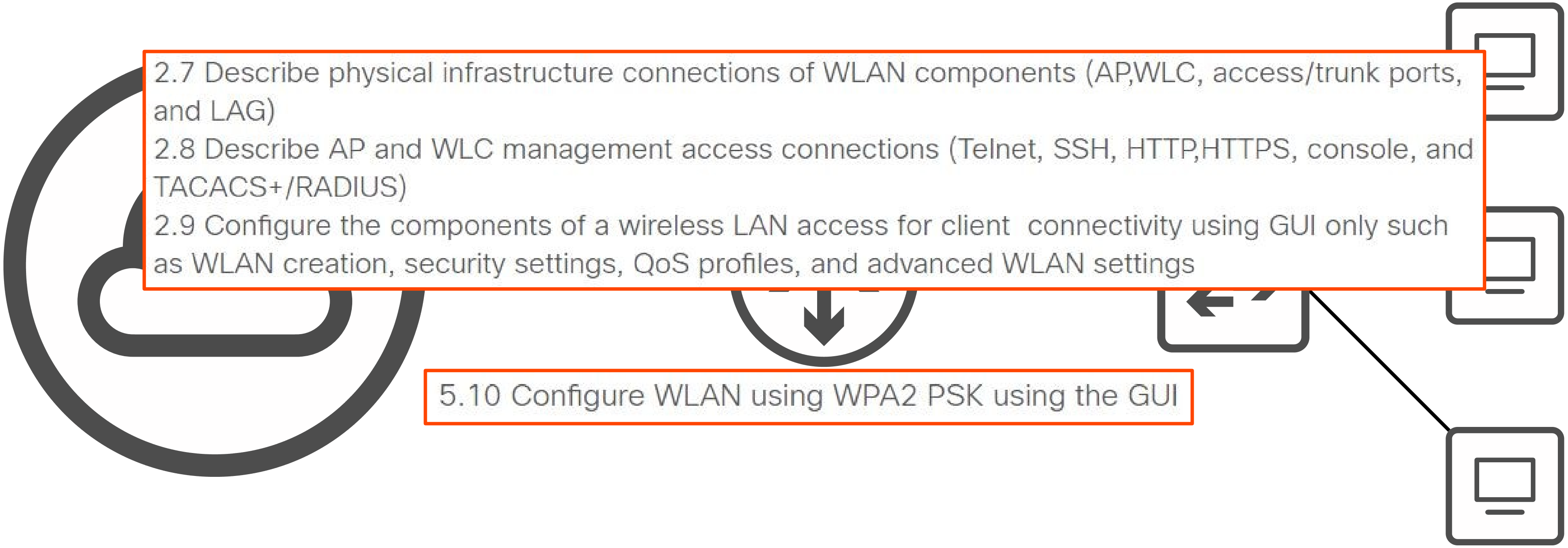
CCNA Day 58

Wireless Configuration



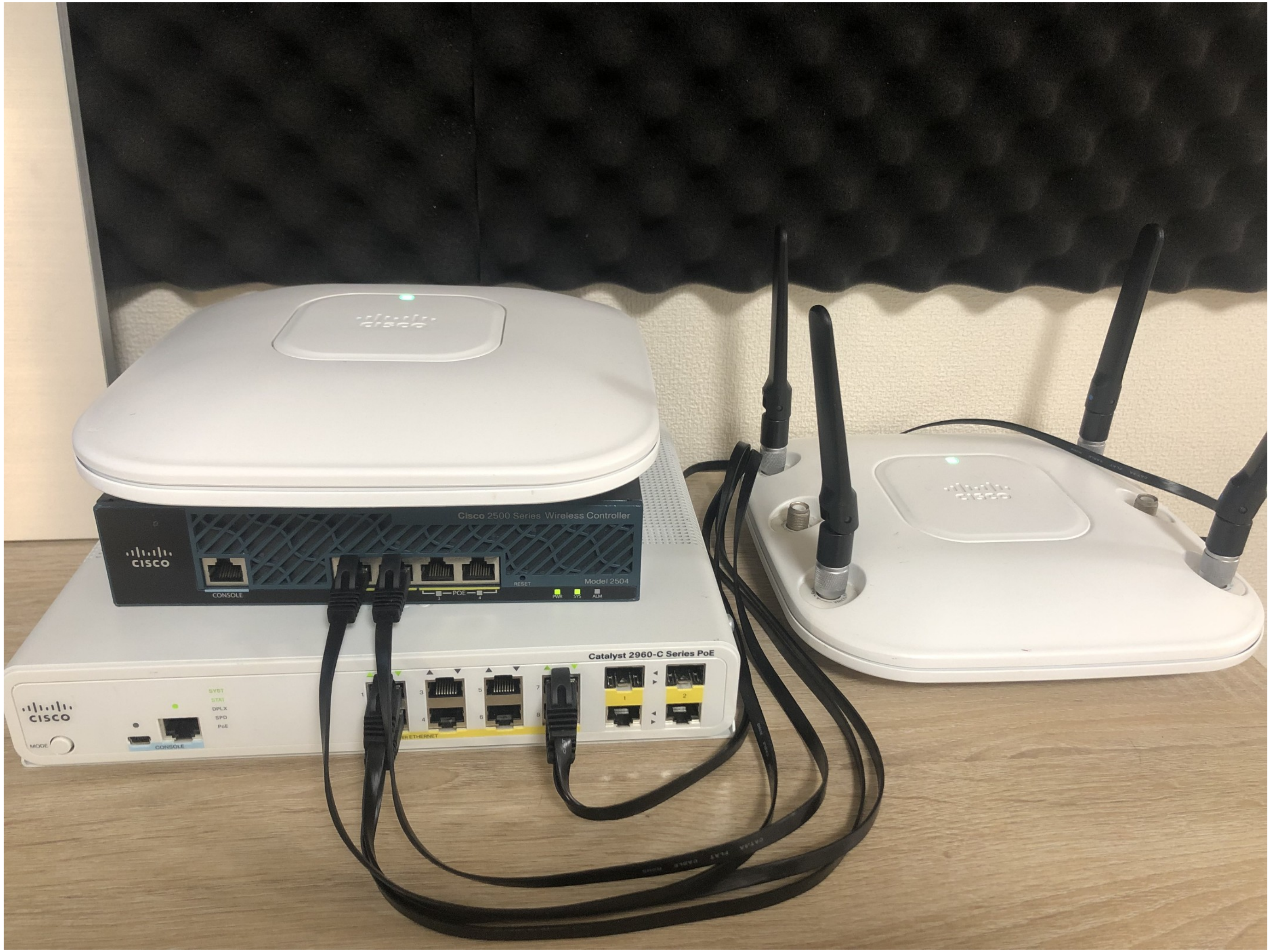
2.7 Describe physical infrastructure connections of WLAN components (AP,WLC, access/trunk ports, and LAG)
2.8 Describe AP and WLC management access connections (Telnet, SSH, HTTP,HTTPS, console, and TACACS+/RADIUS)
2.9 Configure the components of a wireless LAN access for client connectivity using GUI only such as WLAN creation, security settings, QoS profiles, and advanced WLAN settings

5.10 Configure WLAN using WPA2 PSK using the GUI

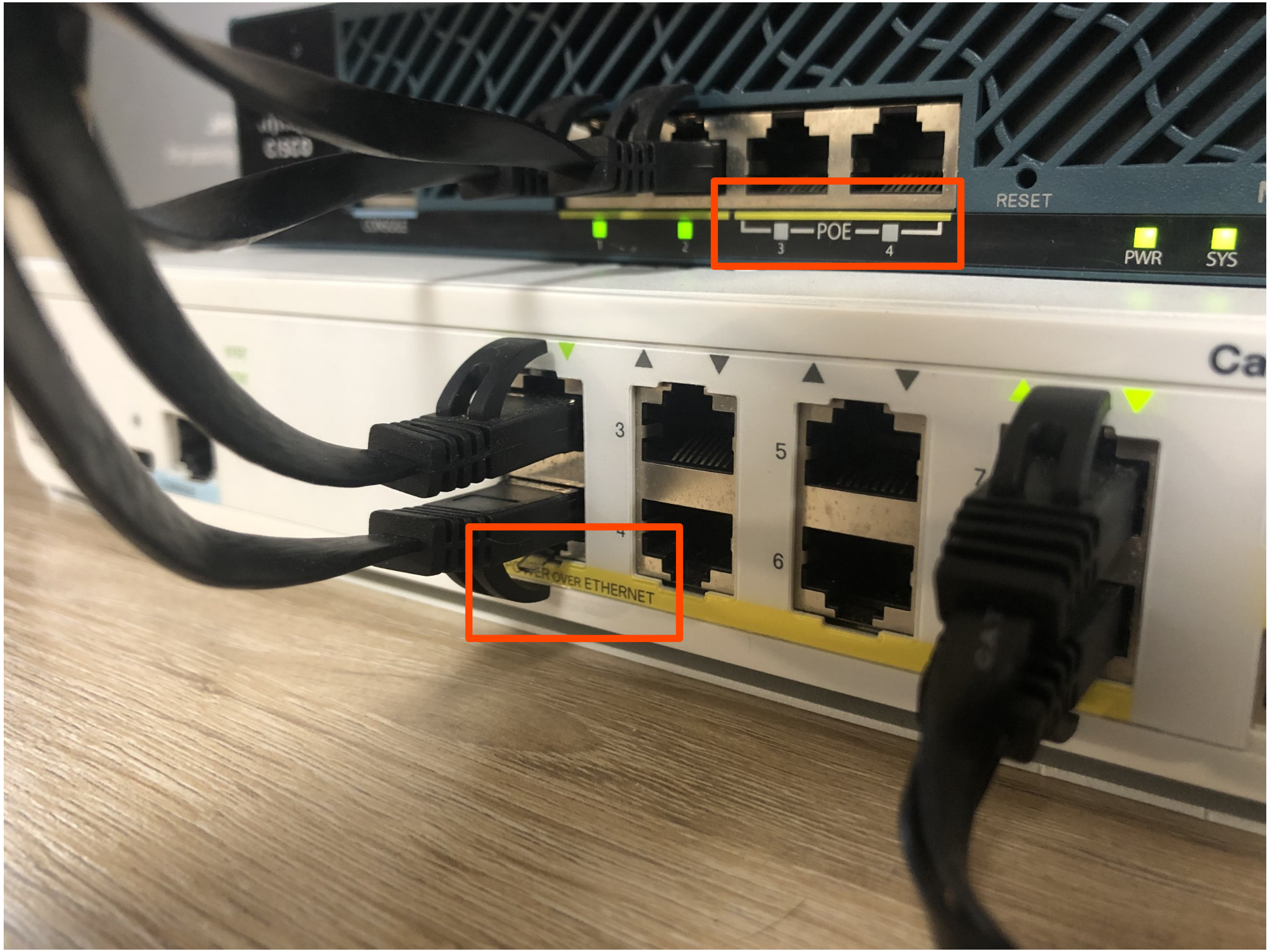
Things we'll cover

- Topology introduction
- Switch configuration
- WLC setup
- WLC interface configuration
- WLAN configuration
- Additional WLC features

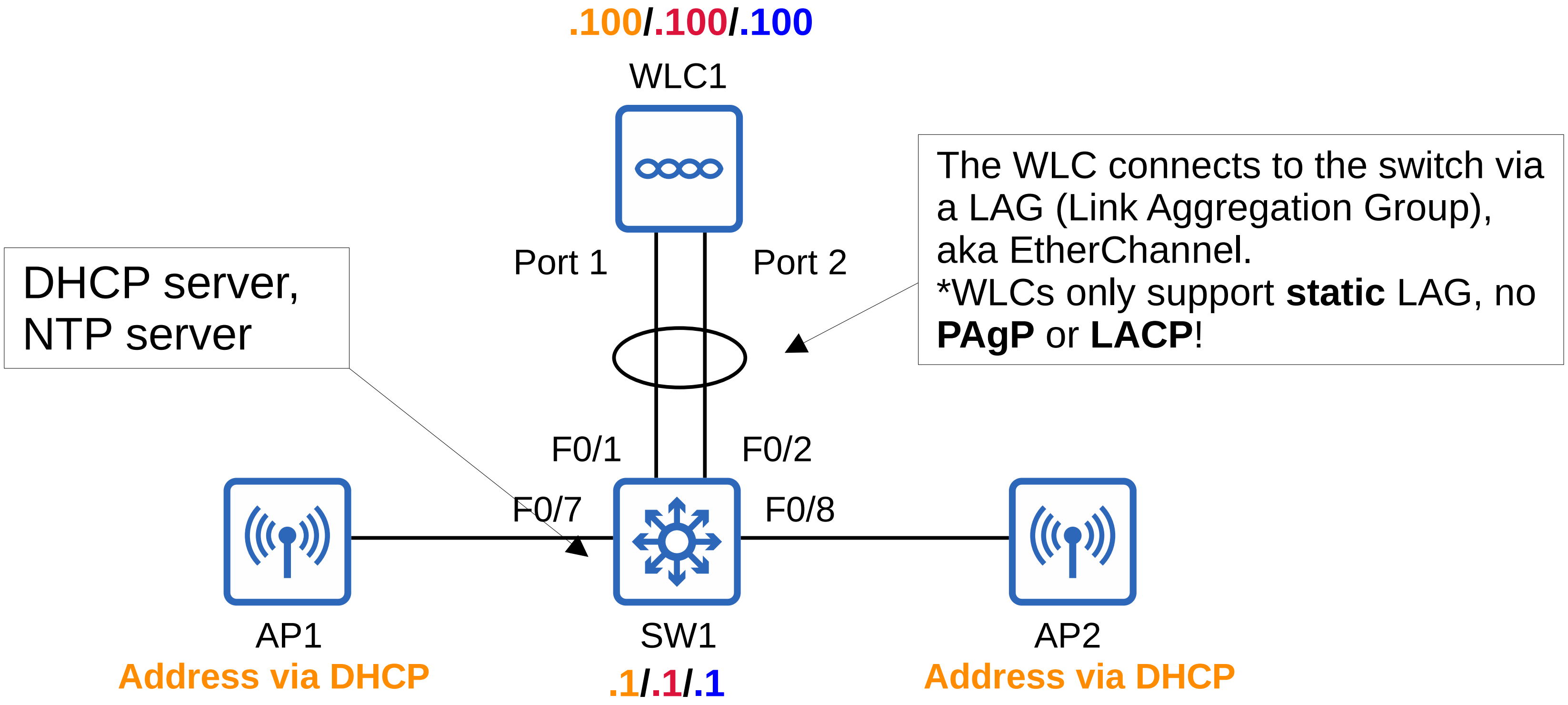
Network Topology



Network Topology



Network Topology

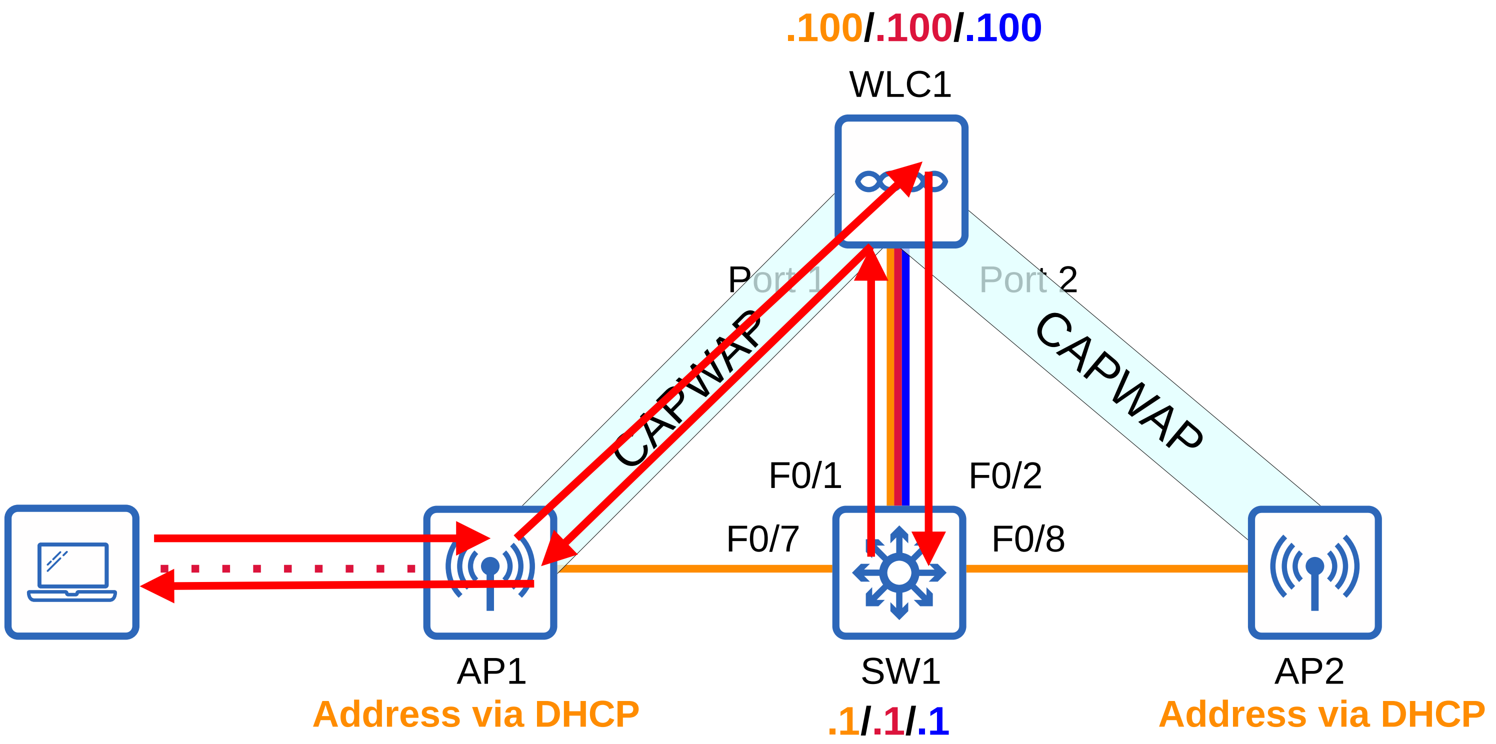


DHCP server,
NTP server

The WLC connects to the switch via a LAG (Link Aggregation Group), aka EtherChannel.
*WLCs only support **static** LAG, no **PAgP** or **LACP**!

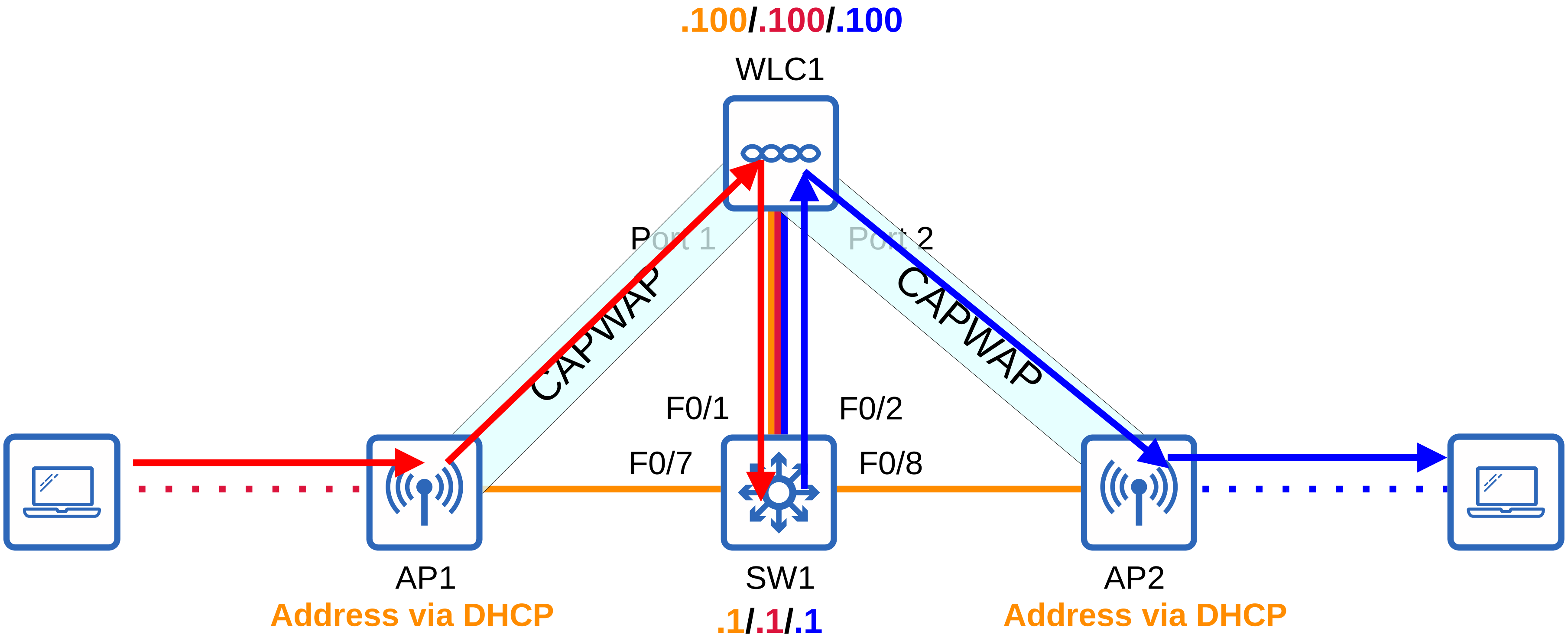
WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24

Network Topology



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24

Network Topology



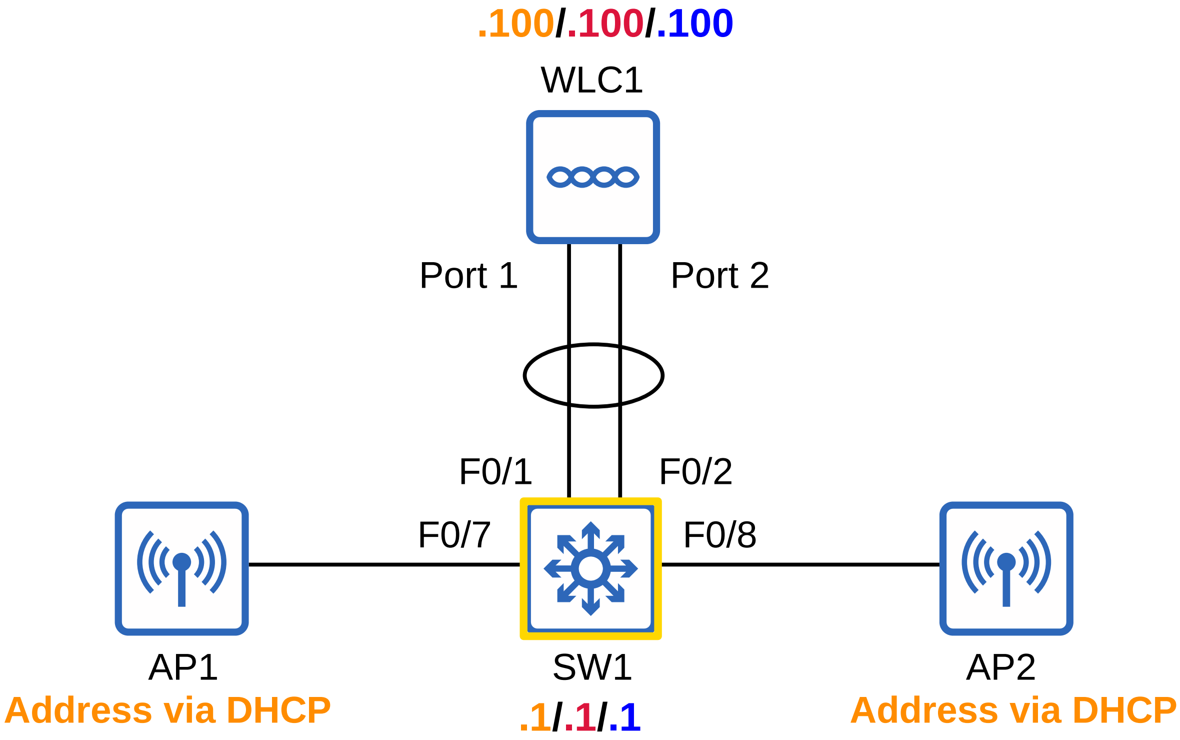
WLANs/VLANs

VLAN 10: Management, 192.168.1.0/24

VLAN 100: Internal, SSID: Internal, 10.0.0.0/24

VLAN 200: Guest, SSID: Guest, 10.1.0.0/24

Network Topology



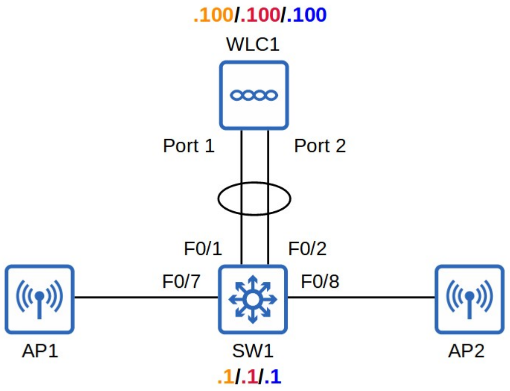
WLANs/VLANs

VLAN 10: Management, 192.168.1.0/24

VLAN 100: Internal, SSID: Internal, 10.0.0.0/24

VLAN 200: Guest, SSID: Guest, 10.1.0.0/24

Switch Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24

```
SW1(config)#vlan 10
SW1(config-vlan)#name Management
SW1(config-vlan)#vlan 100
SW1(config-vlan)#name Internal
SW1(config-vlan)#vlan 200
SW1(config-vlan)#name Guest
```

```
SW1(config)#int range f0/6 - 8
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#spanning-tree portfast
```

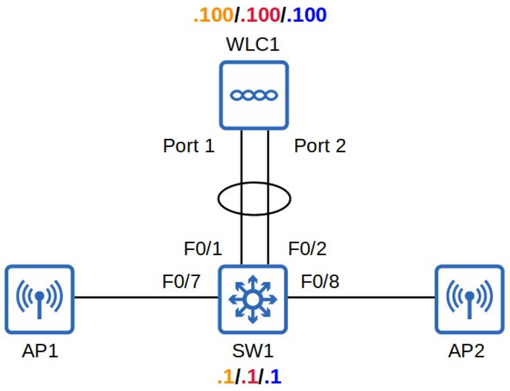
I included F0/6 because I will connect my PC to F0/6 to gain access to WLC1's GUI.

```
SW1(config-if-range)#interface range f0/1 - 2
SW1(config-if-range)#channel-group 1 mode on
```

Remember that WLCs only support static LAG, no PAgP or LACP.

```
SW1(config-if-range)#interface port-channel 1
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allowed vlan 10,100,200
```

Switch Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24

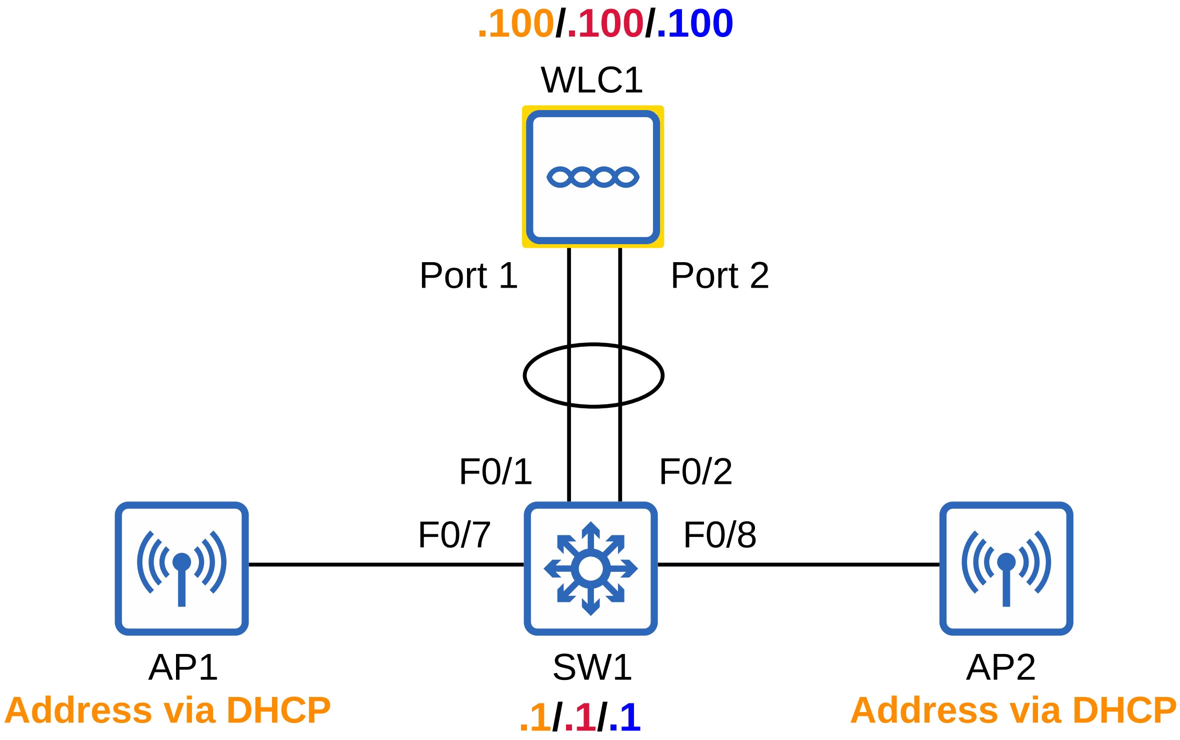
```
SW1(config)#interface vlan 10
SW1(config-if)#ip address 192.168.1.1 255.255.255.0
SW1(config-if)#interface vlan 100
SW1(config-if)#ip address 10.0.0.1 255.255.255.0
SW1(config-if)#interface vlan 200
SW1(config-if)#ip address 10.1.0.1 255.255.255.0
```

```
SW1(config)#ip dhcp pool VLAN10
SW1(dhcp-config)#network 192.168.1.0 255.255.255.0
SW1(dhcp-config)#default-router 192.168.1.1
SW1(dhcp-config)#option 43 ip 192.168.1.100

SW1(config)#ip dhcp pool VLAN100
SW1(dhcp-config)#network 10.0.0.0 255.255.255.0
SW1(dhcp-config)#default-router 10.0.0.1

SW1(config)#ip dhcp pool VLAN200
SW1(dhcp-config)#network 10.1.0.0 255.255.255.0
SW1(dhcp-config)#default-router 10.1.0.1
```

```
SW1(config)#ntp master
```

Option 43 can be used to tell the APs the IP address of their WLC.
*this is not necessary in this case because the APs and WLC are in the same subnet. The WLC will hear the APs broadcast CAPWAP *discovery* messages.

Network Topology



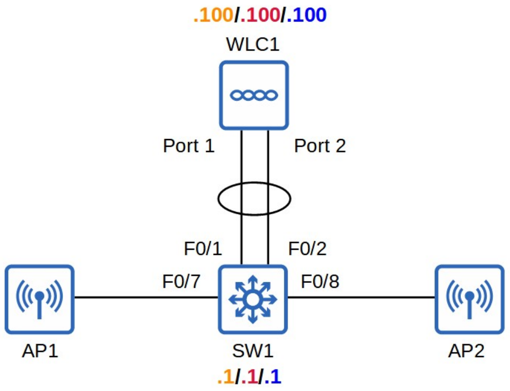
WLANs/VLANs

VLAN 10: Management, 192.168.1.0/24

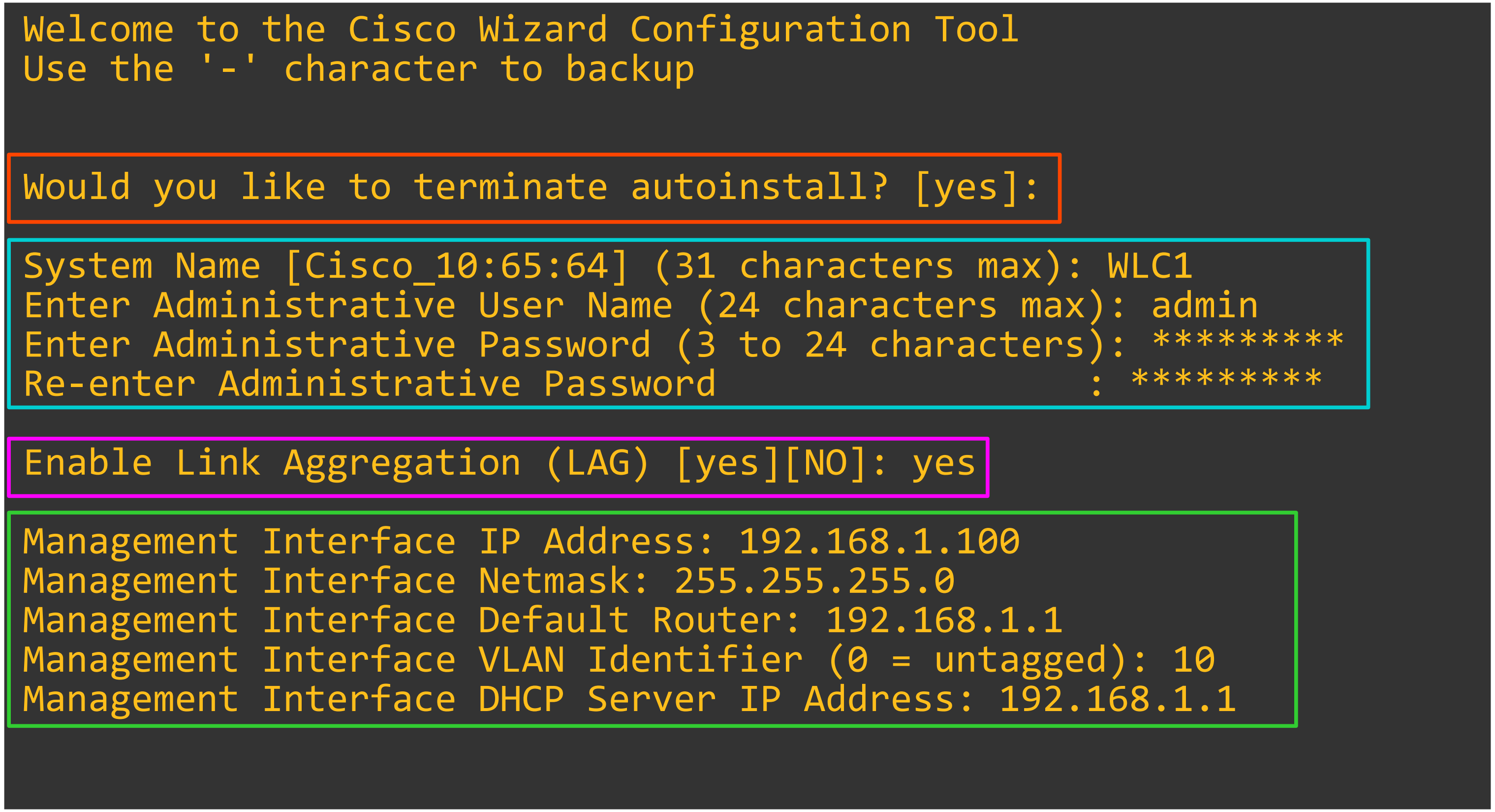
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24

VLAN 200: Guest, SSID: Guest, 10.1.0.0/24

WLC Initial Setup

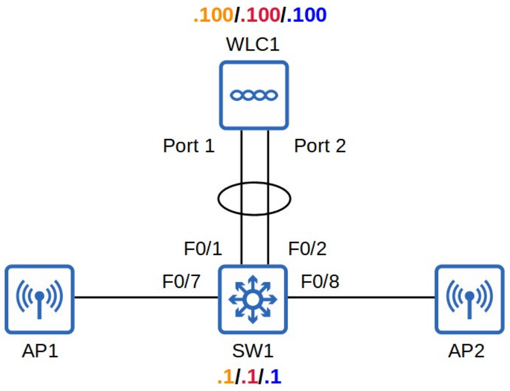


WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24

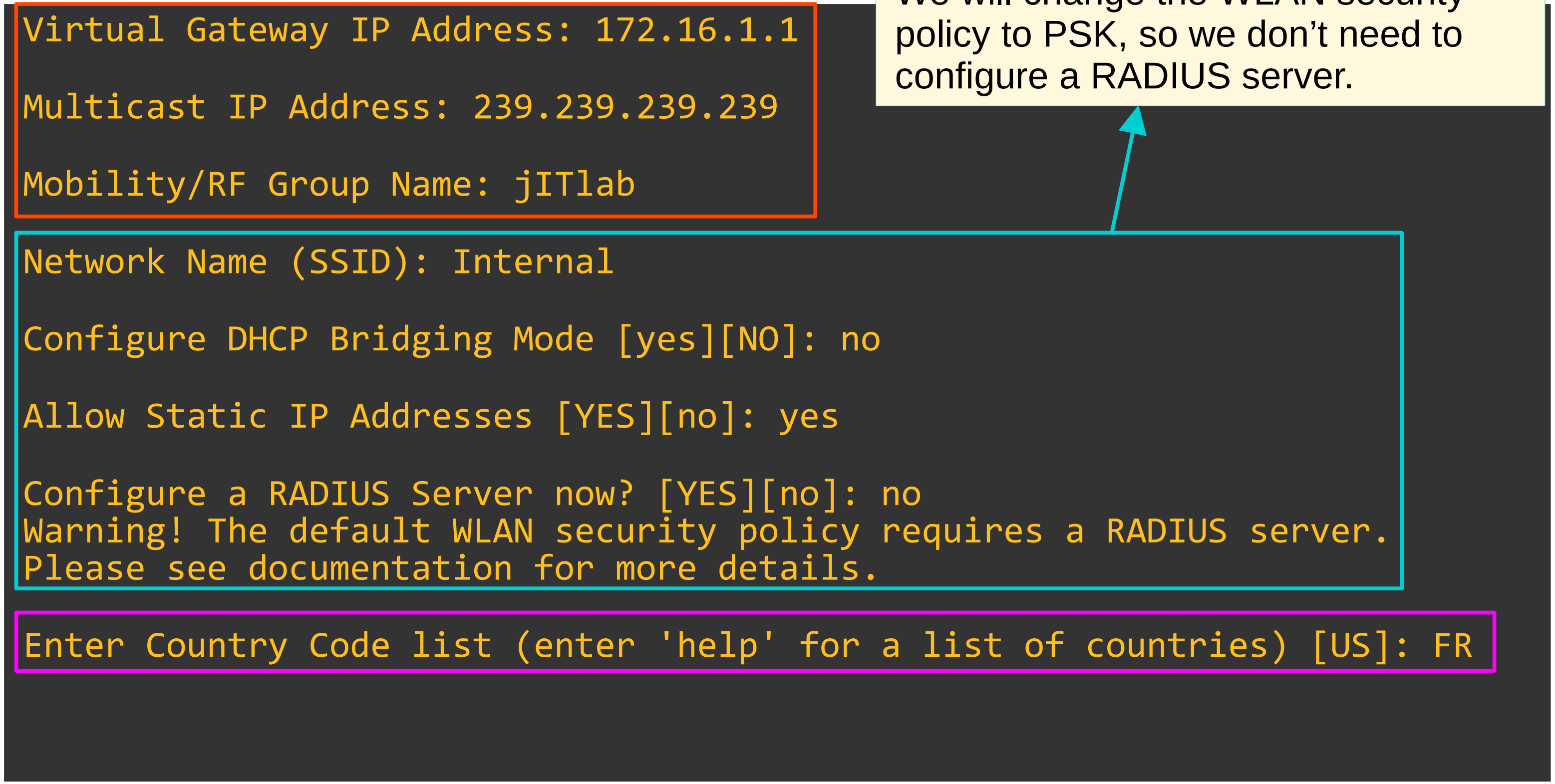


```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup


Would you like to terminate autoinstall? [yes]:

System Name [Cisco_10:65:64] (31 characters max): WLC1
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (3 to 24 characters): *********
Re-enter Administrative Password                 : *********

Enable Link Aggregation (LAG) [yes][NO]: yes

Management Interface IP Address: 192.168.1.100
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 192.168.1.1
Management Interface VLAN Identifier (0 = untagged): 10
Management Interface DHCP Server IP Address: 192.168.1.1
```

WLC Initial Setup



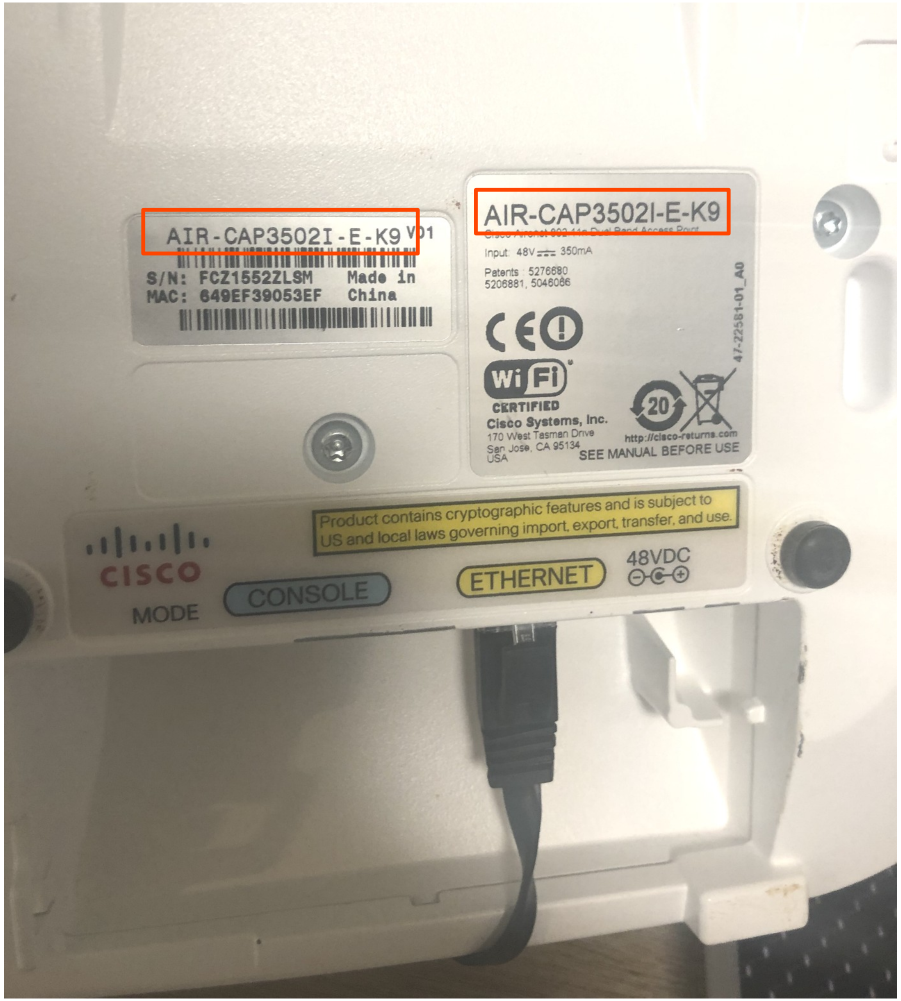
WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



```
Virtual Gateway IP Address: 172.16.1.1

Multicast IP Address: 239.239.239.239

Mobility/RF Group Name: jITlab

Network Name (SSID): Internal

Configure DHCP Bridging Mode [yes][NO]: no

Allow Static IP Addresses [YES][no]: yes

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]: FR
```

We will change the WLAN security policy to PSK, so we don't need to configure a RADIUS server.

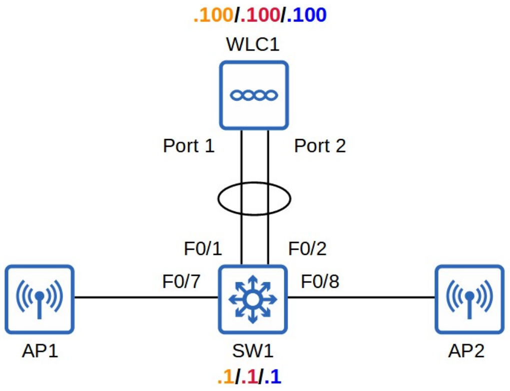
WLC Initial Setup



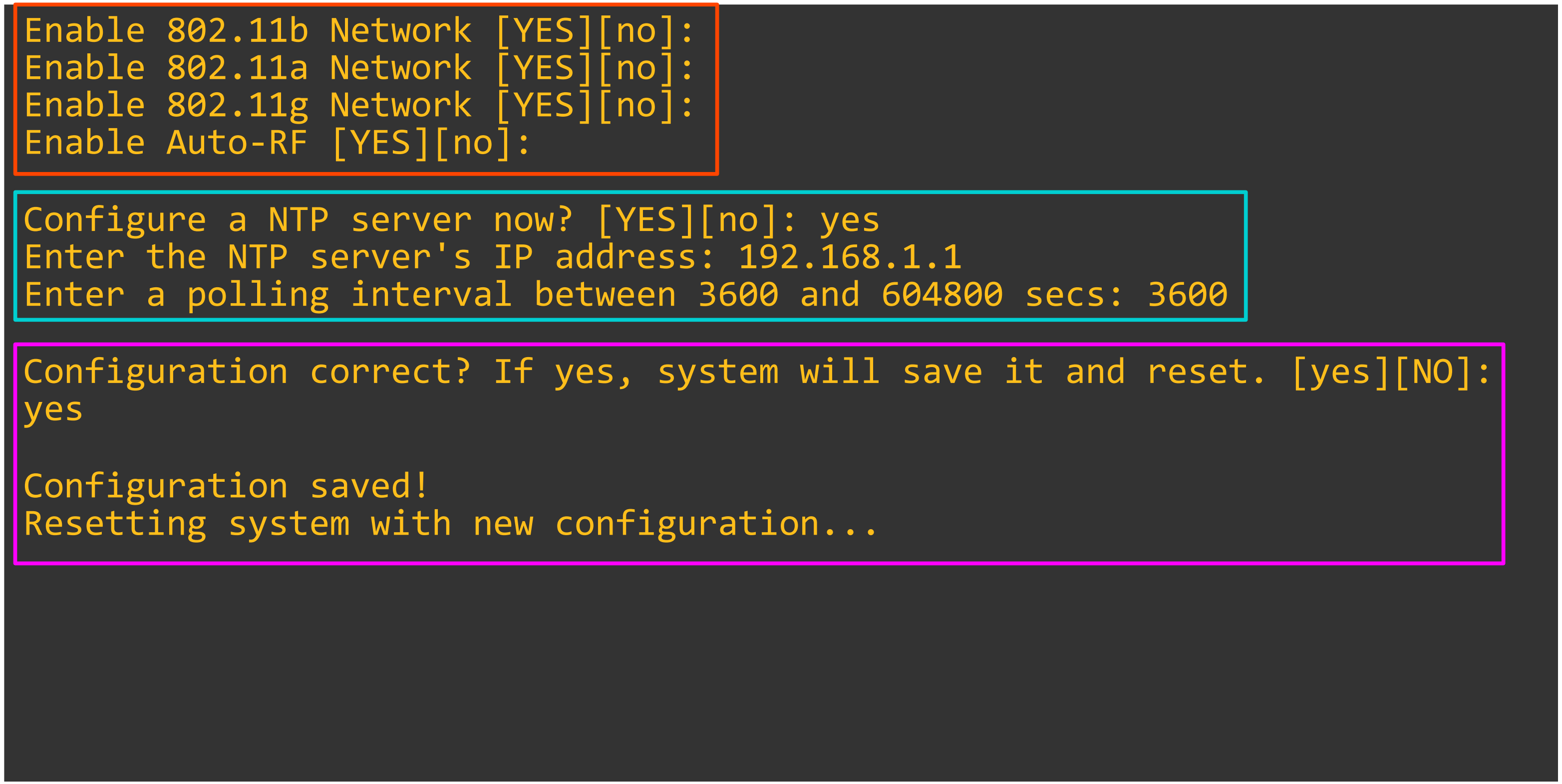
AIR-CAP3502I-E-K9

- -E is the *regulatory domain* of the device.
- -E indicates Europe.
- If the regulatory domain of the country specified in the WLC configuration doesn’t match the regulatory domain of the AP, the AP won’t be able to join the WLC.
- https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html to check the regulatory domain of each country.

WLC Initial Setup



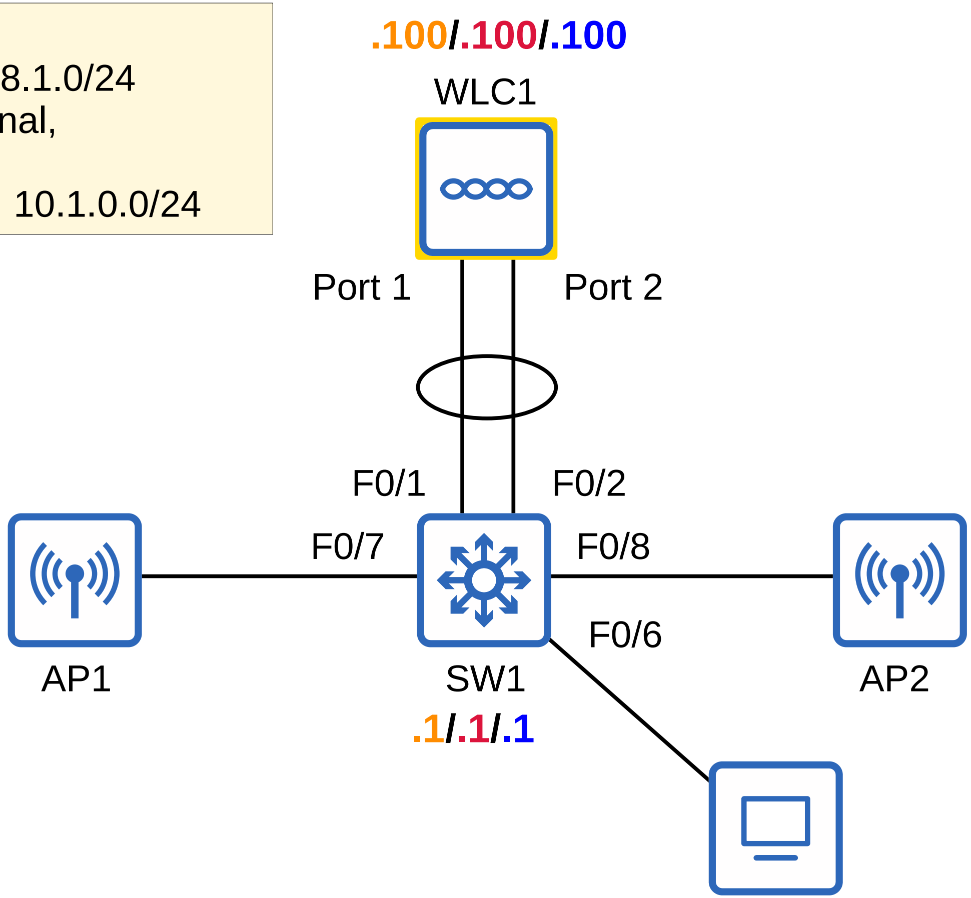
WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



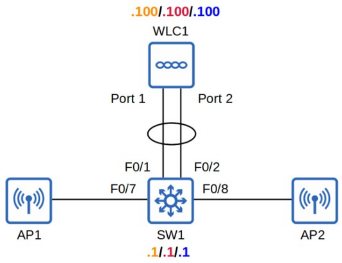
```
Enable 802.11b Network [YES][no]:
Enable 802.11a Network [YES][no]:
Enable 802.11g Network [YES][no]:
Enable Auto-RF [YES][no]:

Configure a NTP server now? [YES][no]: yes
Enter the NTP server's IP address: 192.168.1.1
Enter a polling interval between 3600 and 604800 secs: 3600

Configuration correct? If yes, system will save it and reset. [yes][NO]:
yes

Configuration saved!
Resetting system with new configuration...
```

Network Topology

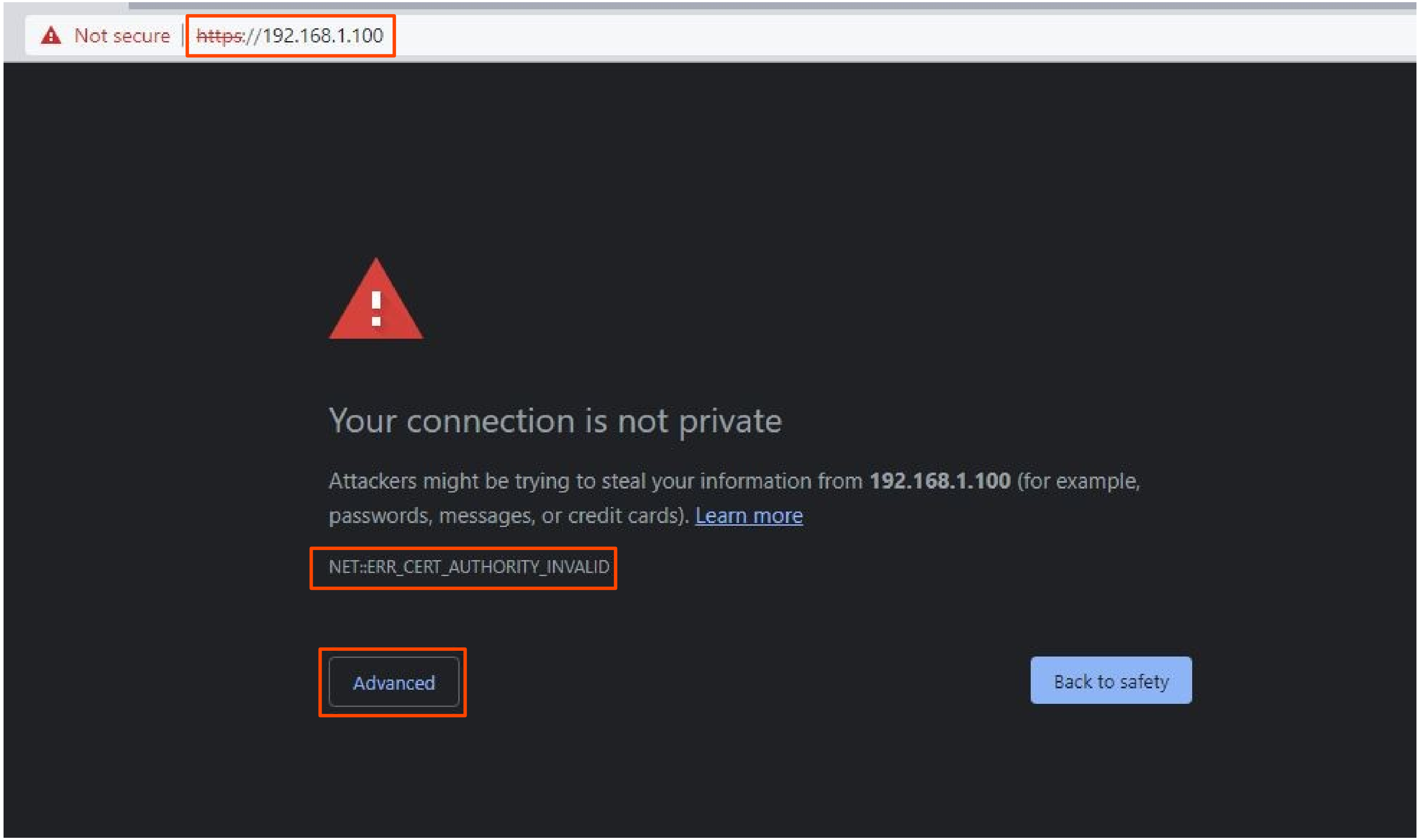
WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



Accessing the GUI



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



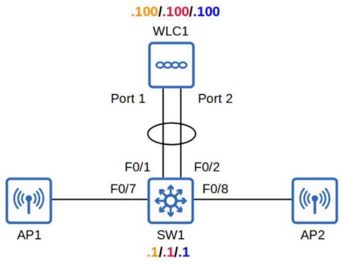
Not secure | ~~https~~://192.168.1.100

Your connection is not private

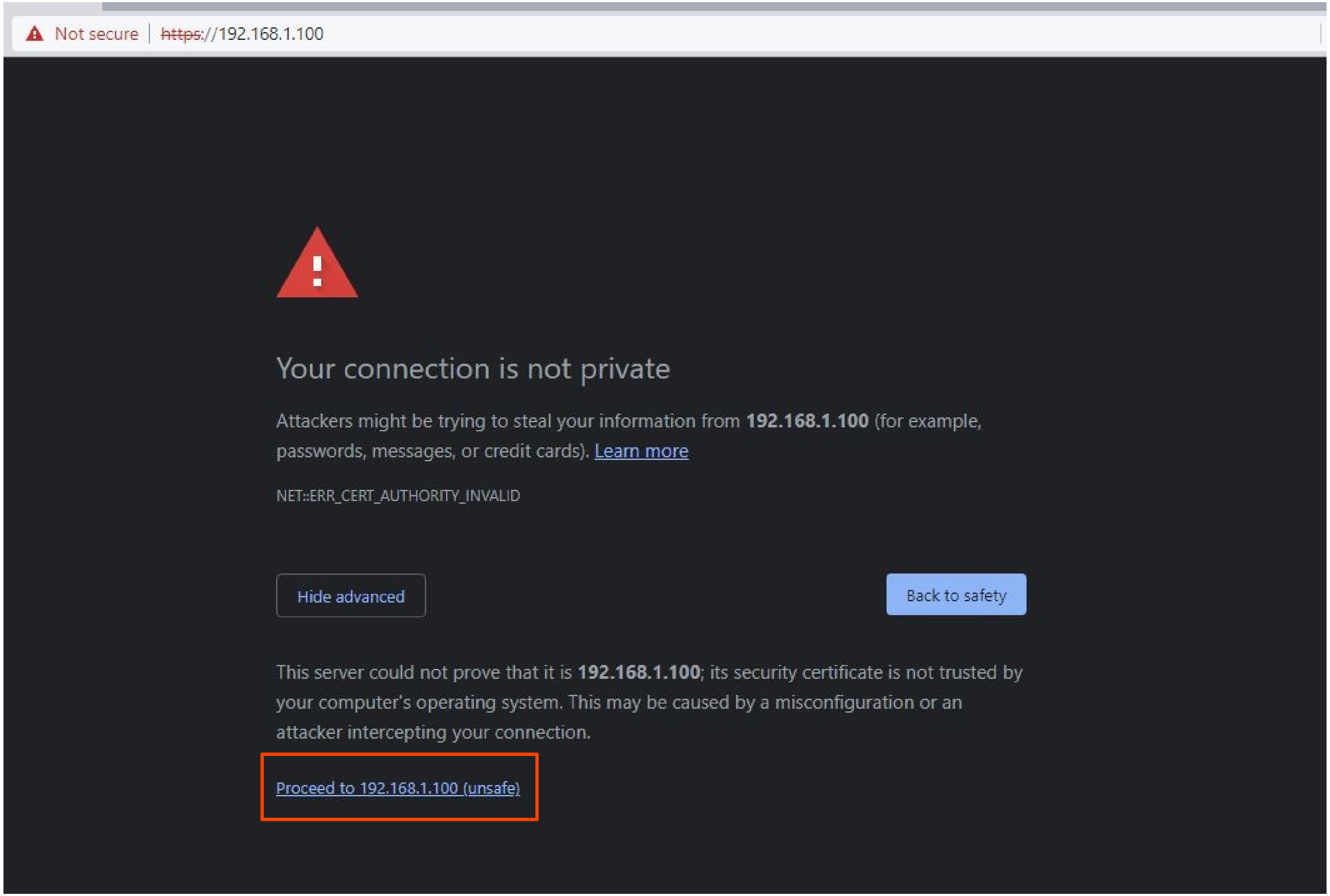
Attackers might be trying to steal your information from **192.168.1.100** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

Accessing the GUI



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



Not secure | ~~https~~://192.168.1.100

Your connection is not private

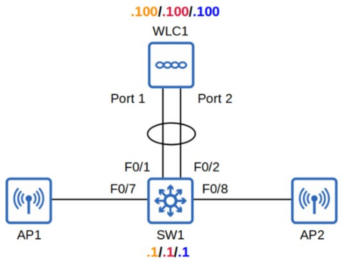
Attackers might be trying to steal your information from **192.168.1.100** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

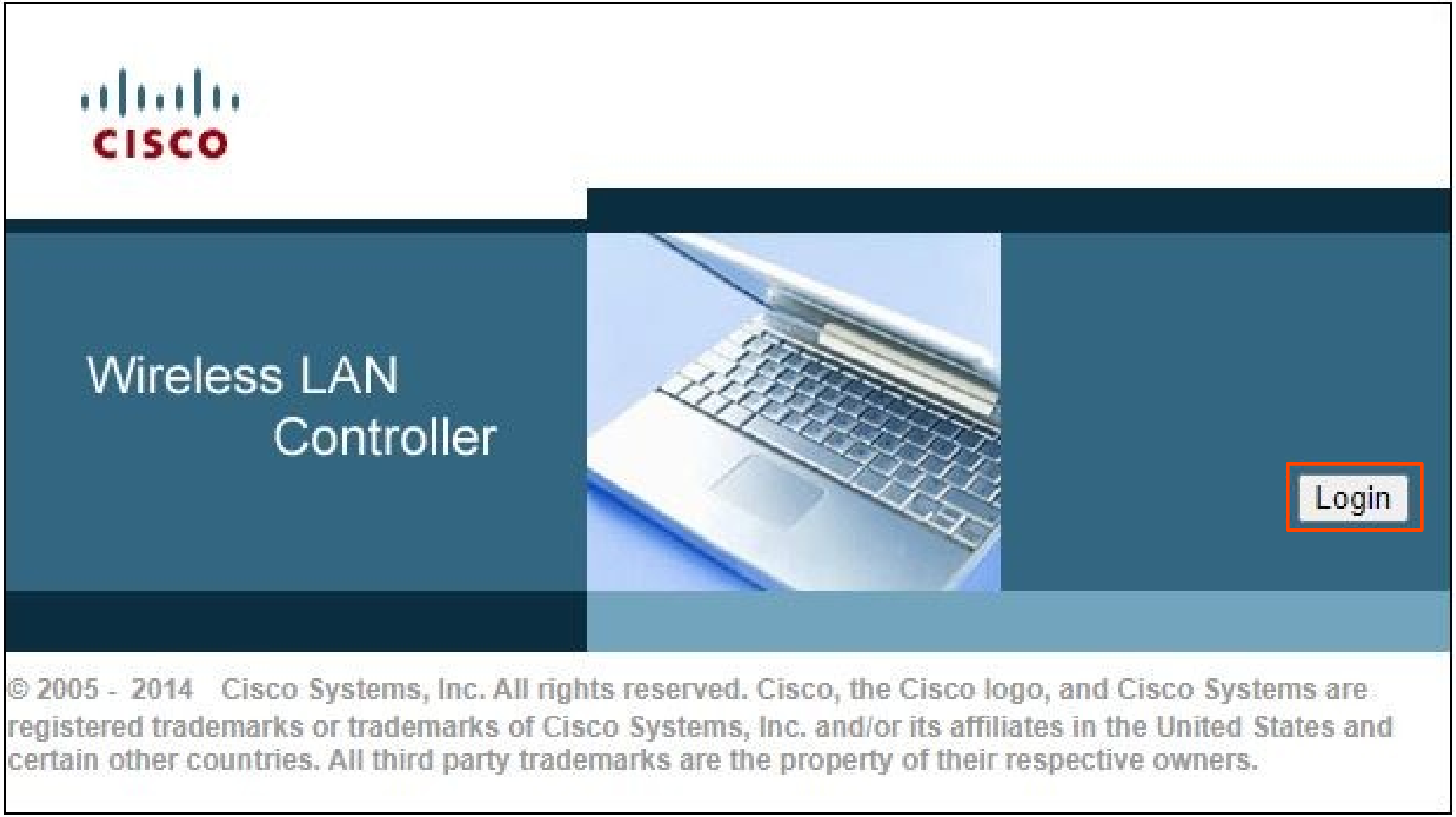
This server could not prove that it is **192.168.1.100**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.1.100 (unsafe)

Accessing the GUI

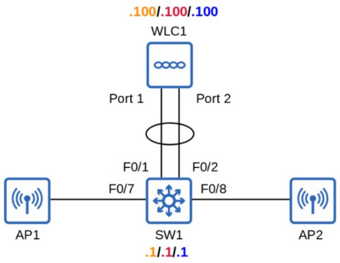


WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24

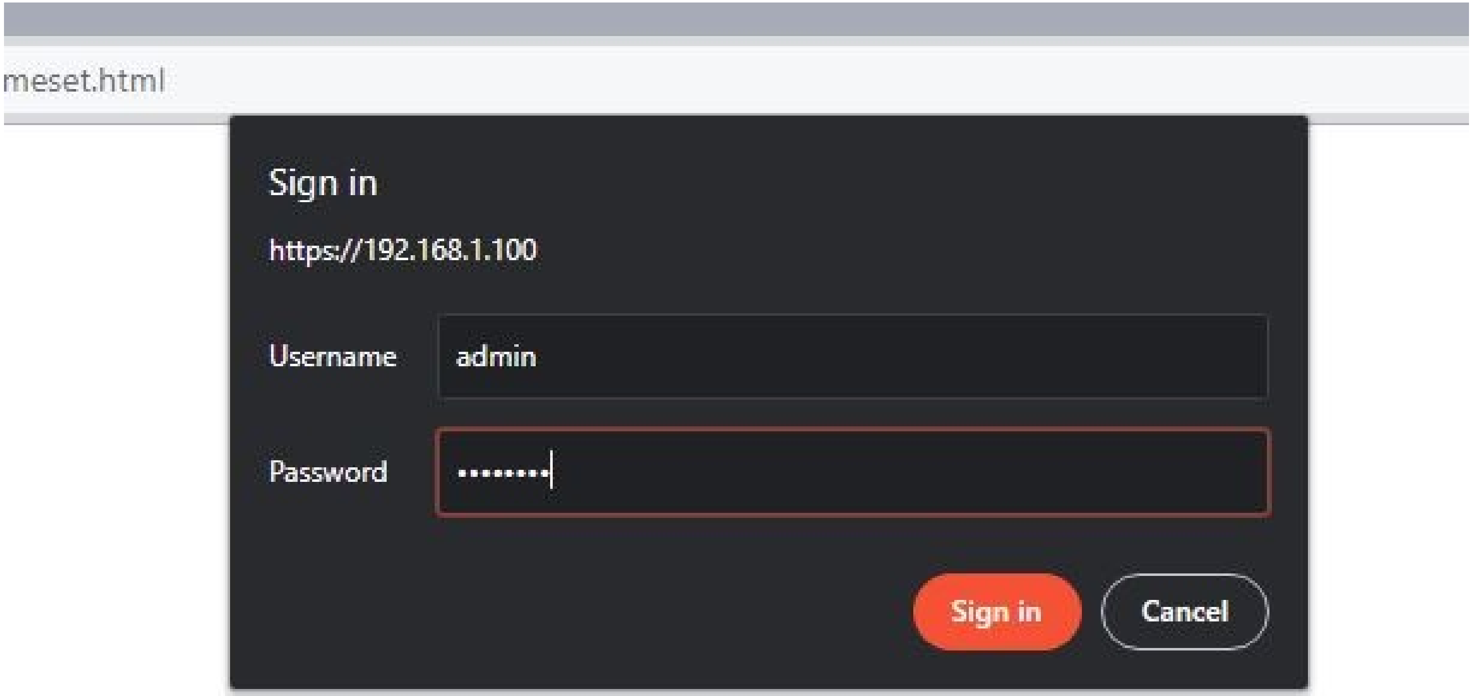


© 2005 - 2014 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All third party trademarks are the property of their respective owners.

Accessing the GUI



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



meset.html

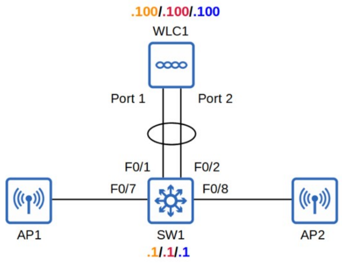
Sign in

https://192.168.1.100

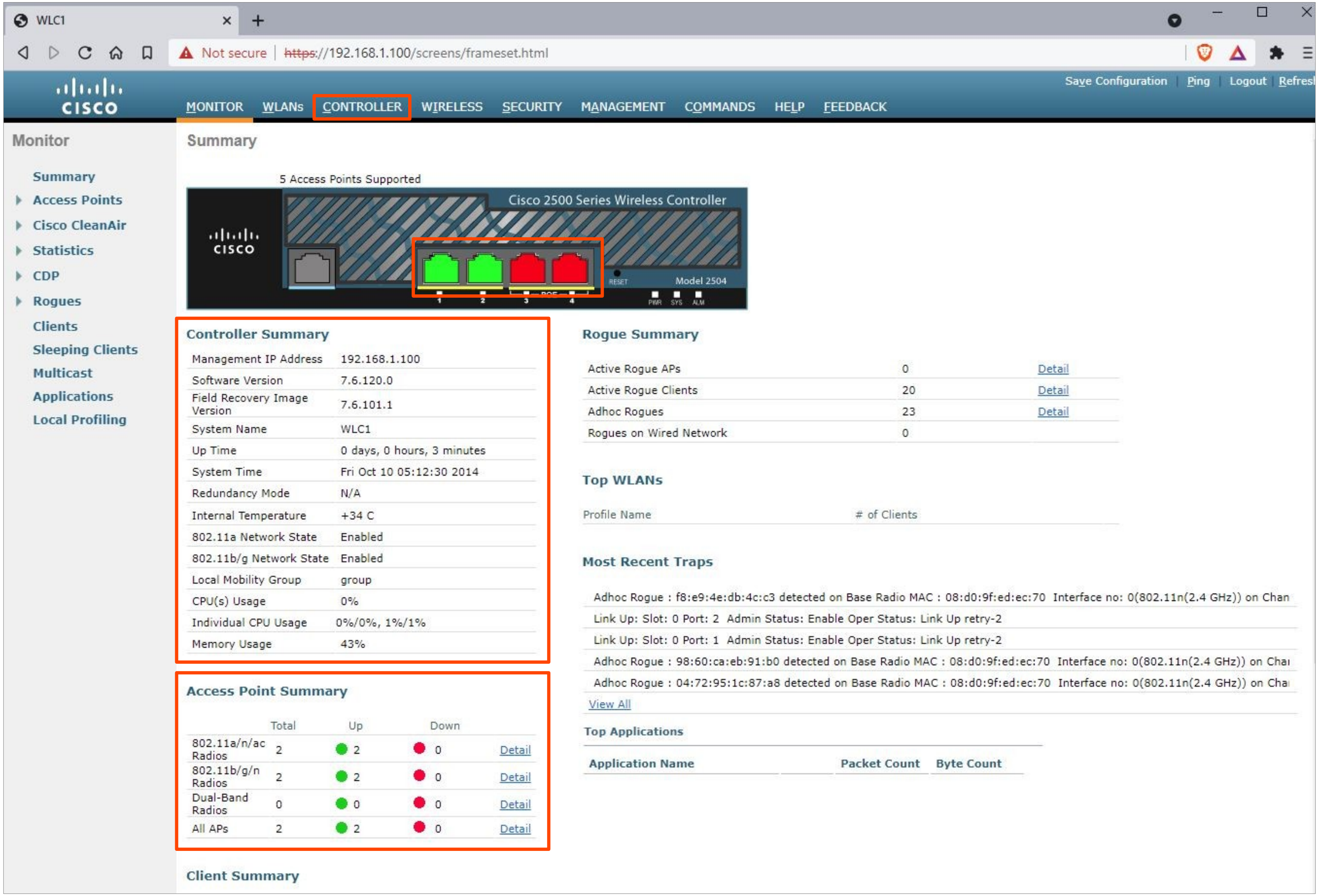
Username admin

Password ••••••••

Accessing the GUI



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



Summary

Controller Summary

Management IP Address	192.168.1.100
Software Version	7.6.120.0
Field Recovery Image Version	7.6.101.1
System Name	WLC1
Up Time	0 days, 0 hours, 3 minutes
System Time	Fri Oct 10 05:12:30 2014
Redundancy Mode	N/A
Internal Temperature	+34 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	group
CPU(s) Usage	0%
Individual CPU Usage	0%/0%, 1%/1%
Memory Usage	43%

Access Point Summary

	Total	Up	Down	
802.11a/n/ac Radios	2	● 2	● 0	Detail
802.11b/g/n Radios	2	● 2	● 0	Detail
Dual-Band Radios	0	● 0	● 0	Detail
All APs	2	● 2	● 0	Detail

Client Summary

Rogue Summary

Active Rogue APs	0	Detail
Active Rogue Clients	20	Detail
Adhoc Rogues	23	Detail
Rogues on Wired Network	0	

Top WLANs

Profile Name	# of Clients

Most Recent Traps

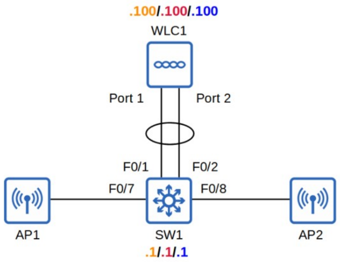
```
Adhoc Rogue : f8:e9:4e:db:4c:c3 detected on Base Radio MAC : 08:d0:9f:ed:ec:70  Interface no: 0(802.11n(2.4 GHz)) on Chan
Link Up: Slot: 0 Port: 2  Admin Status: Enable Oper Status: Link Up retry-2
Link Up: Slot: 0 Port: 1  Admin Status: Enable Oper Status: Link Up retry-2
Adhoc Rogue : 98:60:ca:eb:91:b0 detected on Base Radio MAC : 08:d0:9f:ed:ec:70  Interface no: 0(802.11n(2.4 GHz)) on Cha
Adhoc Rogue : 04:72:95:1c:87:a8 detected on Base Radio MAC : 08:d0:9f:ed:ec:70  Interface no: 0(802.11n(2.4 GHz)) on Cha
```

View All

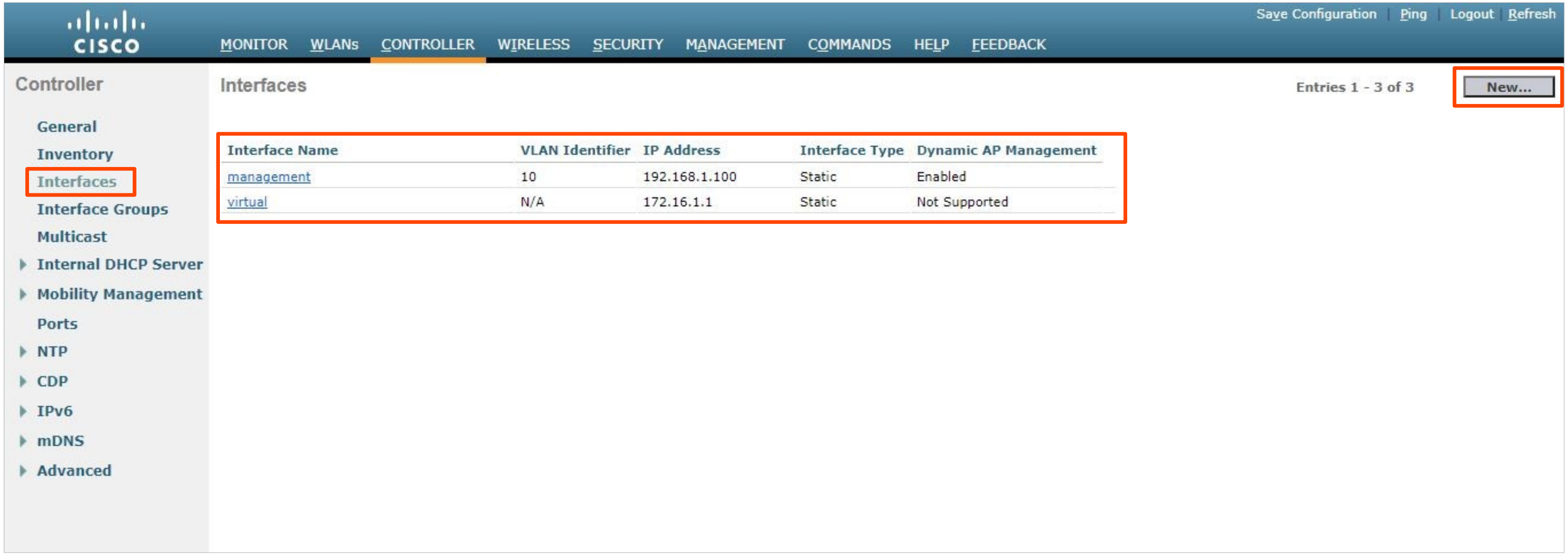
Top Applications

Application Name	Packet Count	Byte Count

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



Interfaces

Entries 1 - 3 of 3

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
management	10	192.168.1.100	Static	Enabled
virtual	N/A	172.16.1.1	Static	Not Supported

WLC Ports/Interfaces

- WLC **ports** are the physical ports that cables connect to.

- WLC **interfaces** are the logical interfaces within the WLC (ie. SVIs on a switch).

- WLCs have a few different kinds of **ports**:

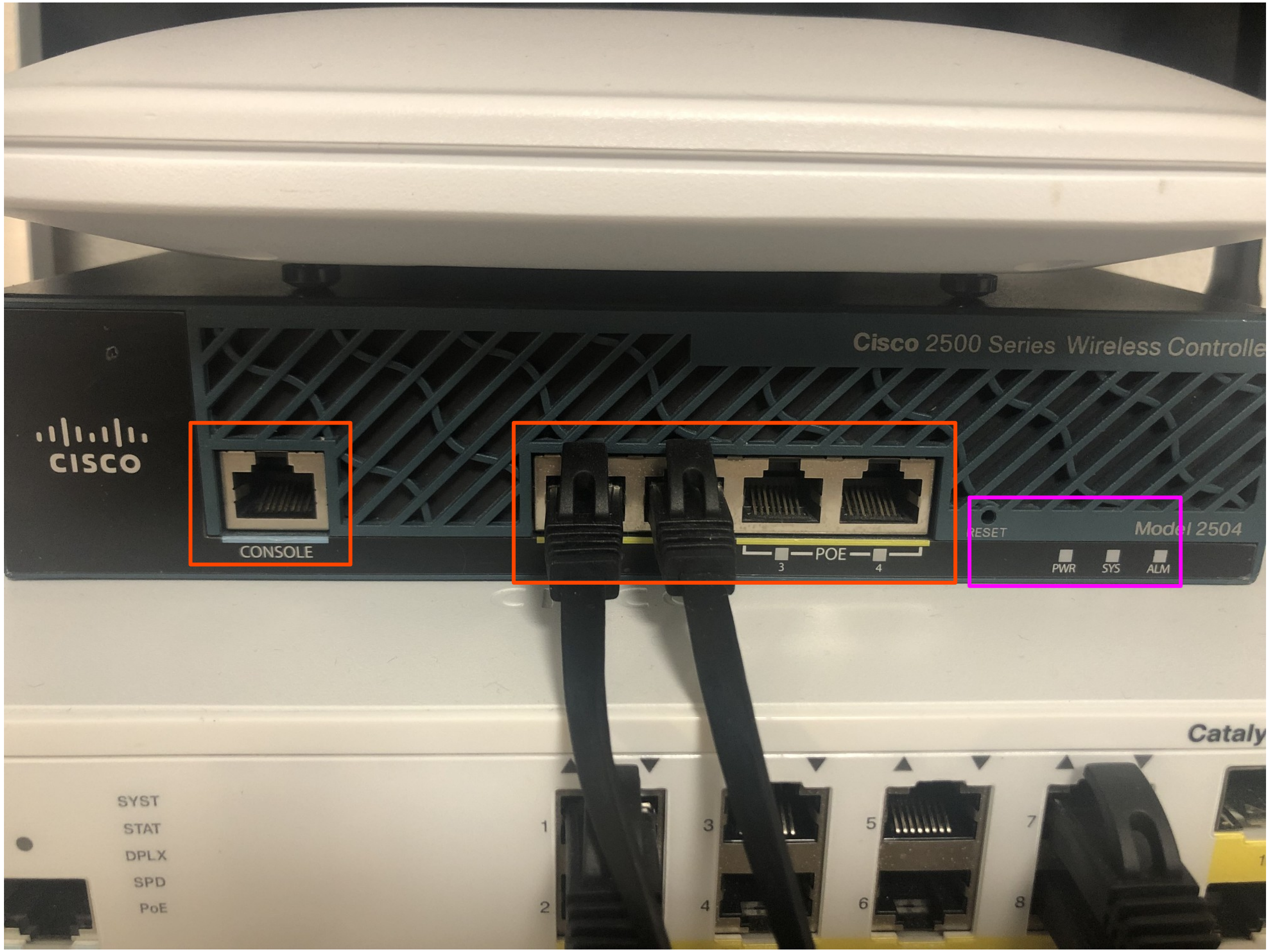
→**Service port**: A dedicated management port. Used for out-of-band management. Must connect to a switch access port because it only supports one VLAN. This port can be used to connect to the device while it is booting, perform system recovery, etc.

→**Distribution system port**: These are the standard network ports that connect to the 'distribution system' (wired network) and are used for data traffic. These ports usually connect to switch trunk ports, and if multiple distribution ports are used they can form a LAG.

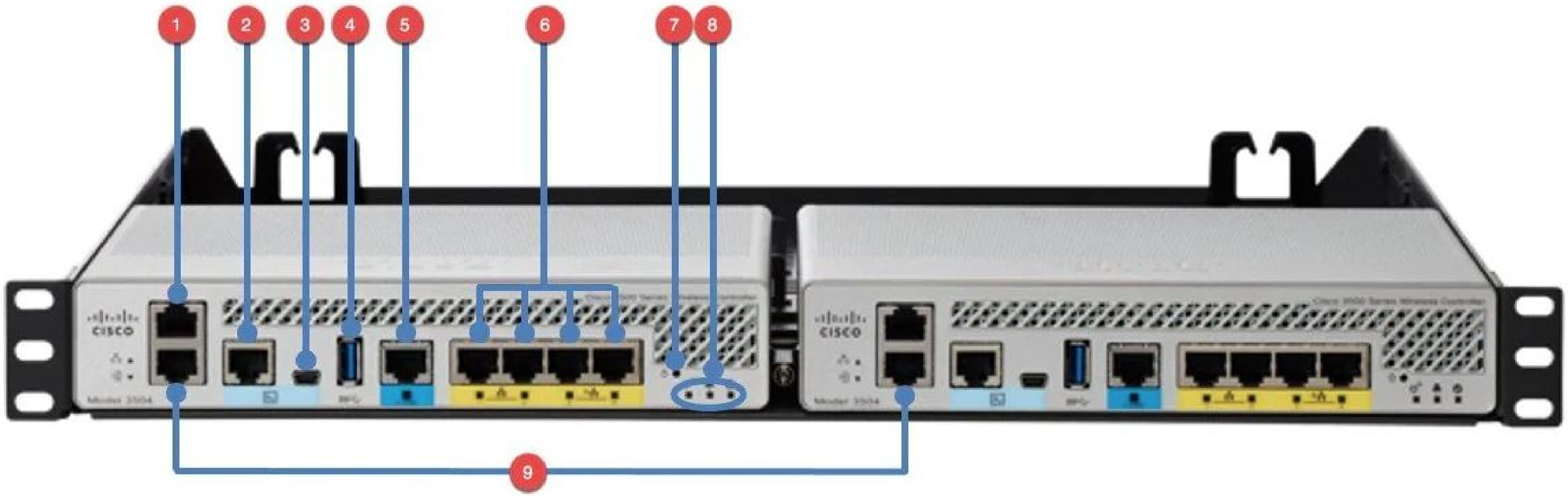
→**Console port**: This is a standard console port, either RJ45 or USB.

→**Redundancy port**: This port is used to connect to another WLC to form a high availability (HA) pair.

WLC Ports/Interfaces



WLC Ports/Interfaces



1) Service port
2) Console port (RJ45)
3) Console port (USB)
4) USB (for software updates)
5) Distribution system port (multi-gigabit)
6) Distribution system ports (1-gig)
7) Reset button
8) Status LEDs
9) Redundancy port

WLC Ports/Interfaces

- WLCs have a few different kinds of **interfaces**:

→**Management interface**: Used for management traffic such as Telnet, SSH, HTTP, HTTPS, RADIUS authentication, NTP, Syslog, etc. CAPWAP tunnels are also formed to/from the WLC's management interface.

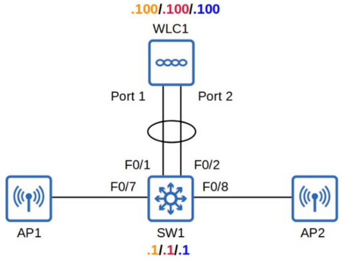
→**Redundancy management interface**: When two WLCs are connected by their redundancy ports, one WLC is 'active' and the other is 'standby'. This interface can be used to connect to and manage the 'standby' WLC.

→**Virtual interface**: This interface is used when communicating with wireless clients to relay DHCP requests, perform client web authentication, etc.

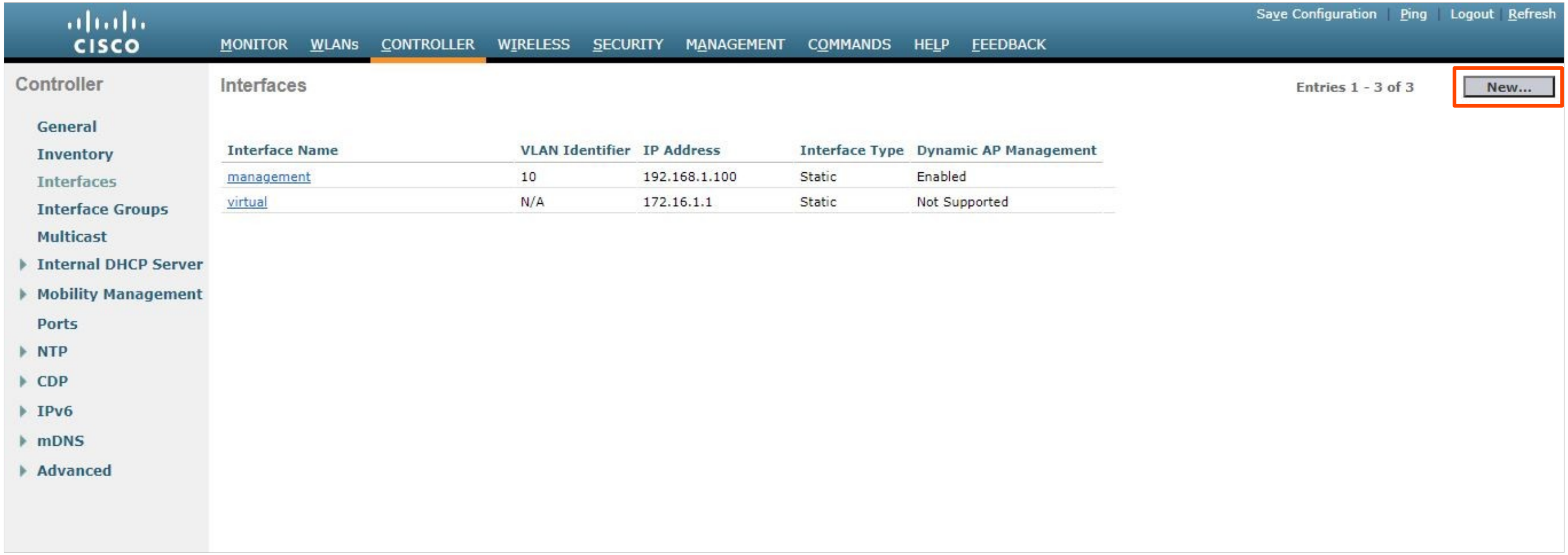
→**Service port interface**: If the service port is used, this interface is bound to it and used for out-of-band management.

→**Dynamic interface**: These are the interfaces used to map a WLAN to a VLAN. For example, traffic from the 'Internal' WLAN will be sent to the wired network from the WLC's 'Internal' dynamic interface.

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24

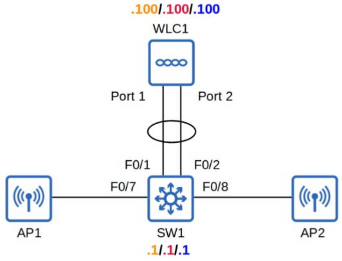


Interfaces

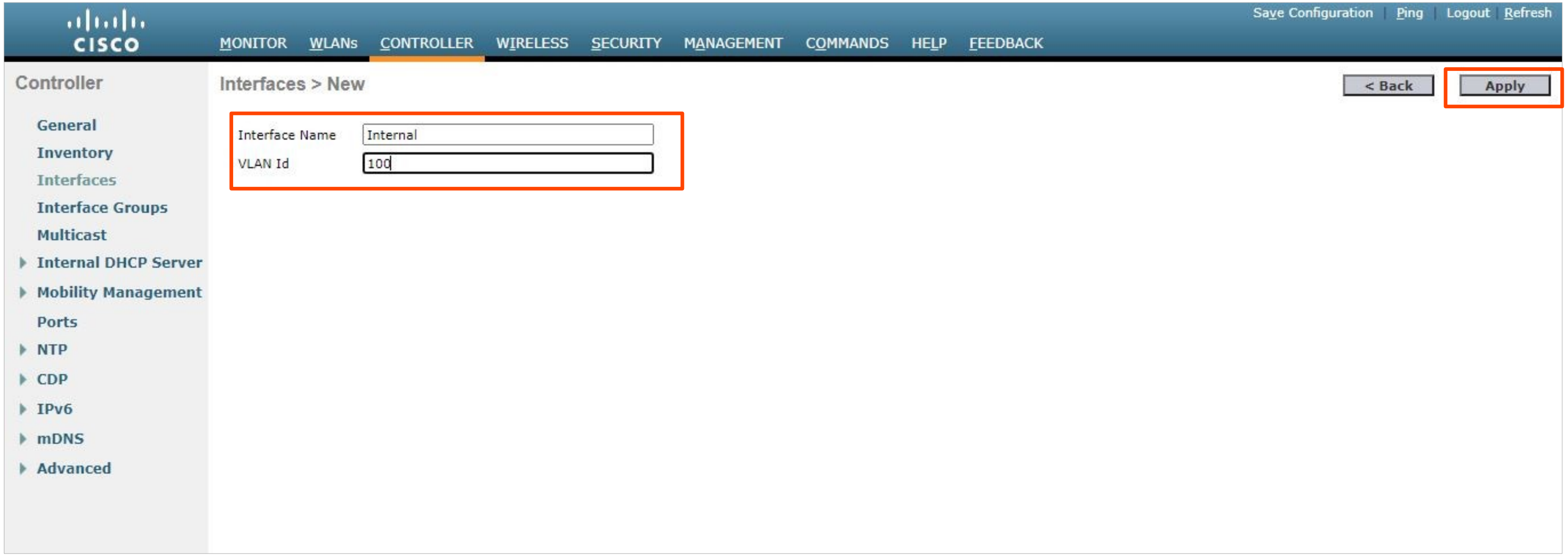
Entries 1 - 3 of 3

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
management	10	192.168.1.100	Static	Enabled
virtual	N/A	172.16.1.1	Static	Not Supported

WLC Configuration



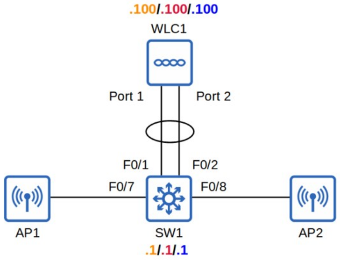
WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



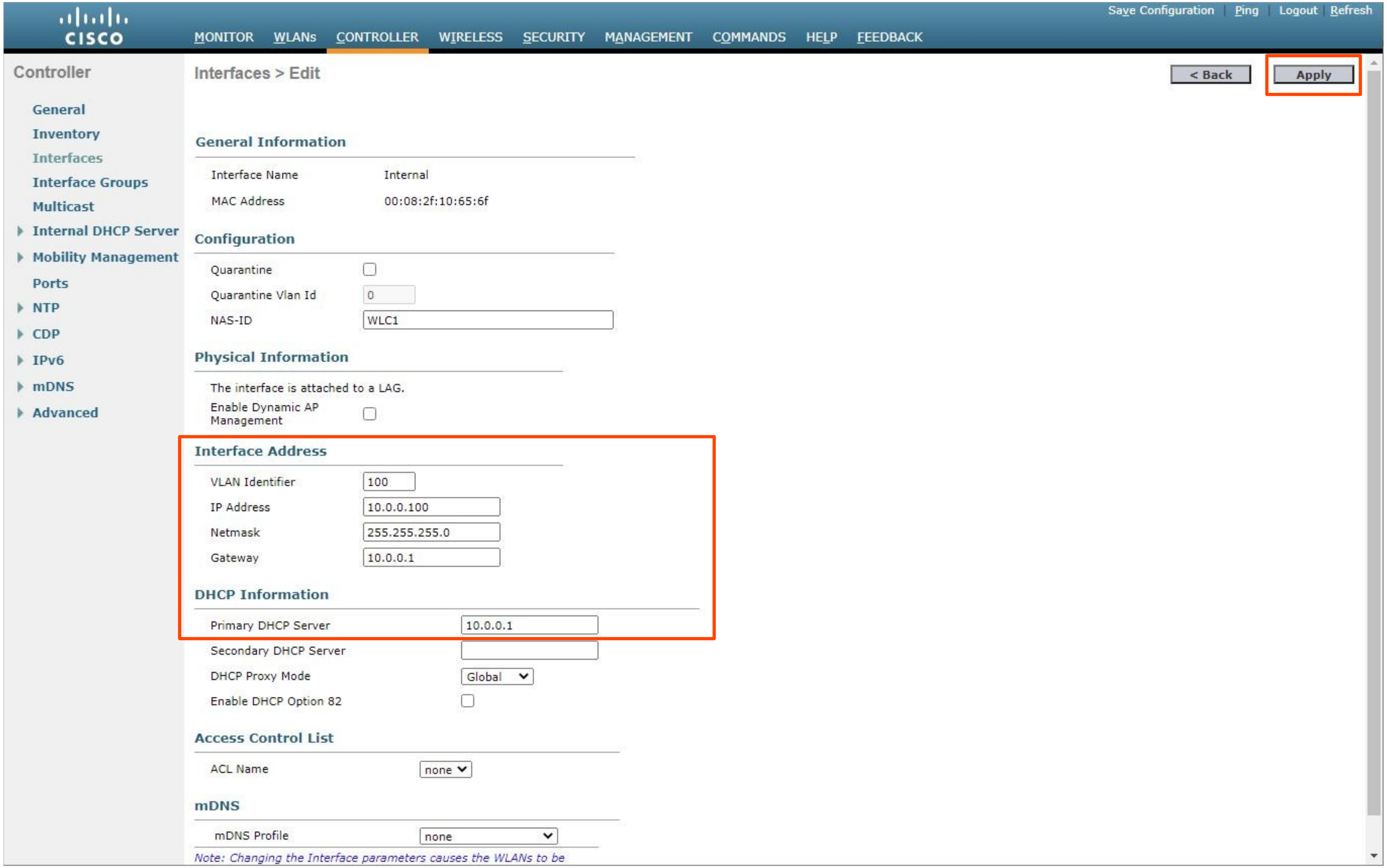
Interfaces > New

Interface Name: Internal
VLAN Id: 100

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



Interfaces > Edit

General Information

Interface Name	Internal
MAC Address	00:08:2f:10:65:6f

Configuration

Quarantine	□
Quarantine Vlan Id	0
NAS-ID	WLC1

Physical Information

The interface is attached to a LAG.

Enable Dynamic AP Management	□

Interface Address

VLAN Identifier	100
IP Address	10.0.0.100
Netmask	255.255.255.0
Gateway	10.0.0.1

DHCP Information

Primary DHCP Server	10.0.0.1
Secondary DHCP Server	
DHCP Proxy Mode	Global
Enable DHCP Option 82	□

Access Control List

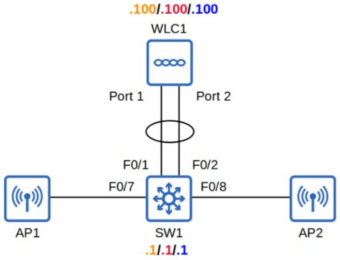
ACL Name	none

mDNS

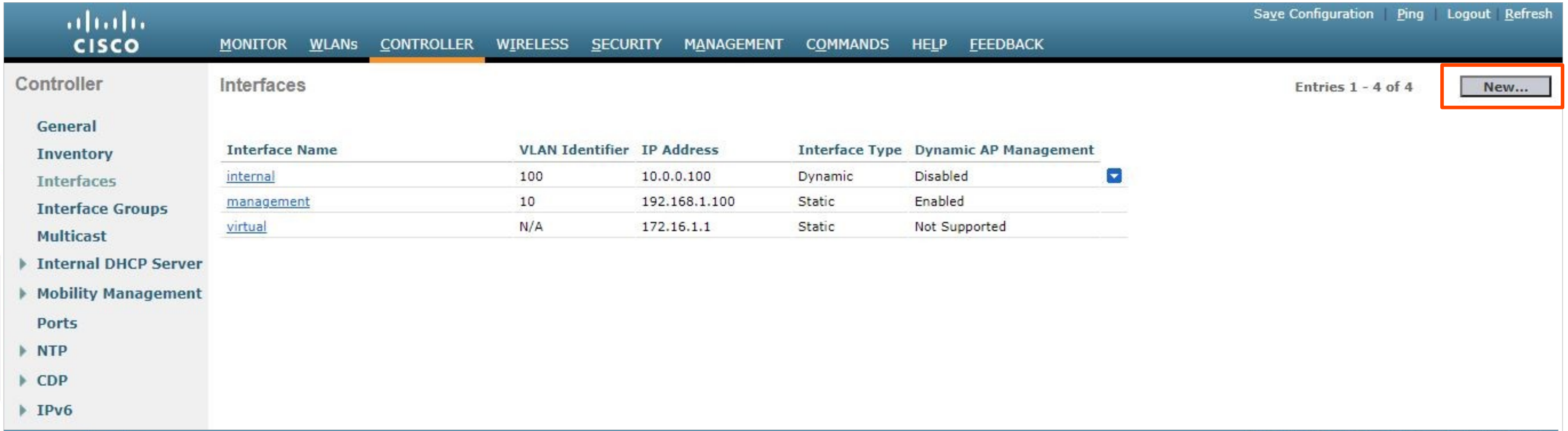
mDNS Profile	none

Note: Changing the Interface parameters causes the WLANs to be

WLC Configuration



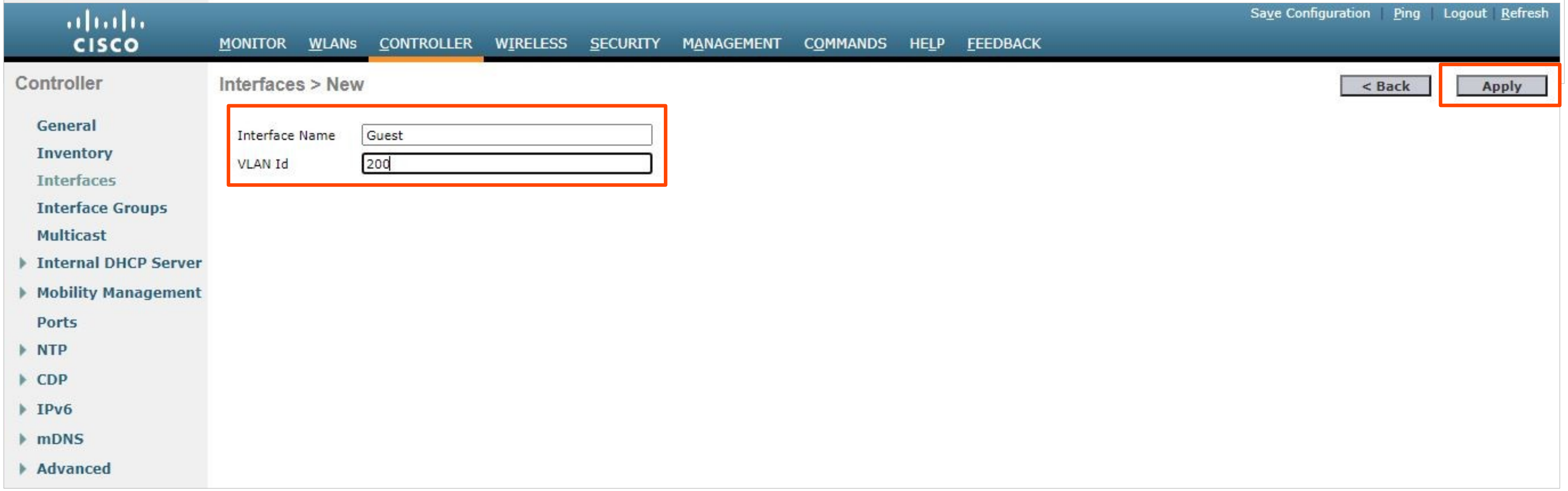
WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



Interfaces

Entries 1 - 4 of 4

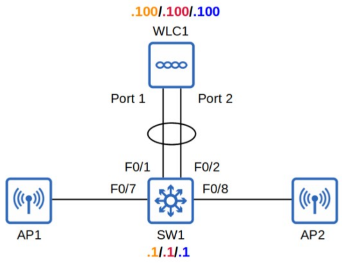
Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
internal	100	10.0.0.100	Dynamic	Disabled
management	10	192.168.1.100	Static	Enabled
virtual	N/A	172.16.1.1	Static	Not Supported



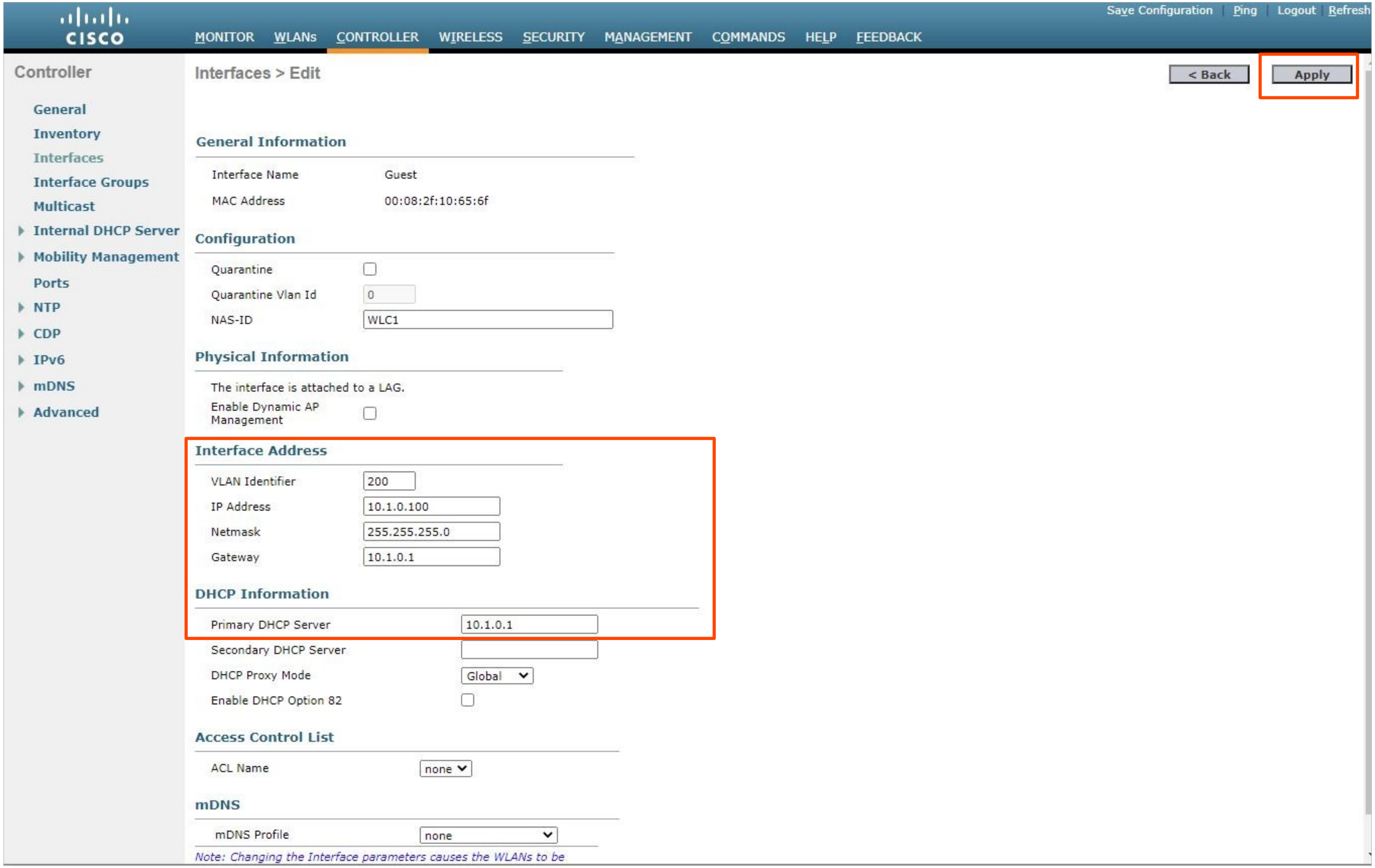
Interfaces > New

Interface Name	Guest
VLAN Id	200

WLC Configuration



WLANs/VLANs
VLAN 10: Management,
192.168.1.0/24
VLAN 100: Internal, SSID: Internal,
10.0.0.0/24
VLAN 200: Guest, SSID: Guest,
10.1.0.0/24



Interfaces > Edit

General Information

Interface Name	Guest
MAC Address	00:08:2f:10:65:6f

Configuration

Quarantine	□
Quarantine Vlan Id	0
NAS-ID	WLC1

Physical Information

The interface is attached to a LAG.

Enable Dynamic AP Management	□

Interface Address

VLAN Identifier	200
IP Address	10.1.0.100
Netmask	255.255.255.0
Gateway	10.1.0.1

DHCP Information

Primary DHCP Server	10.1.0.1
Secondary DHCP Server	
DHCP Proxy Mode	Global
Enable DHCP Option 82	□

Access Control List

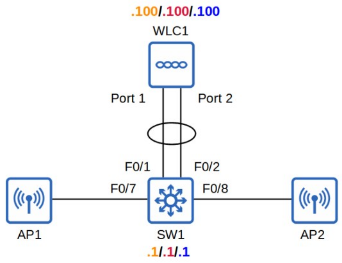
ACL Name	none

mDNS

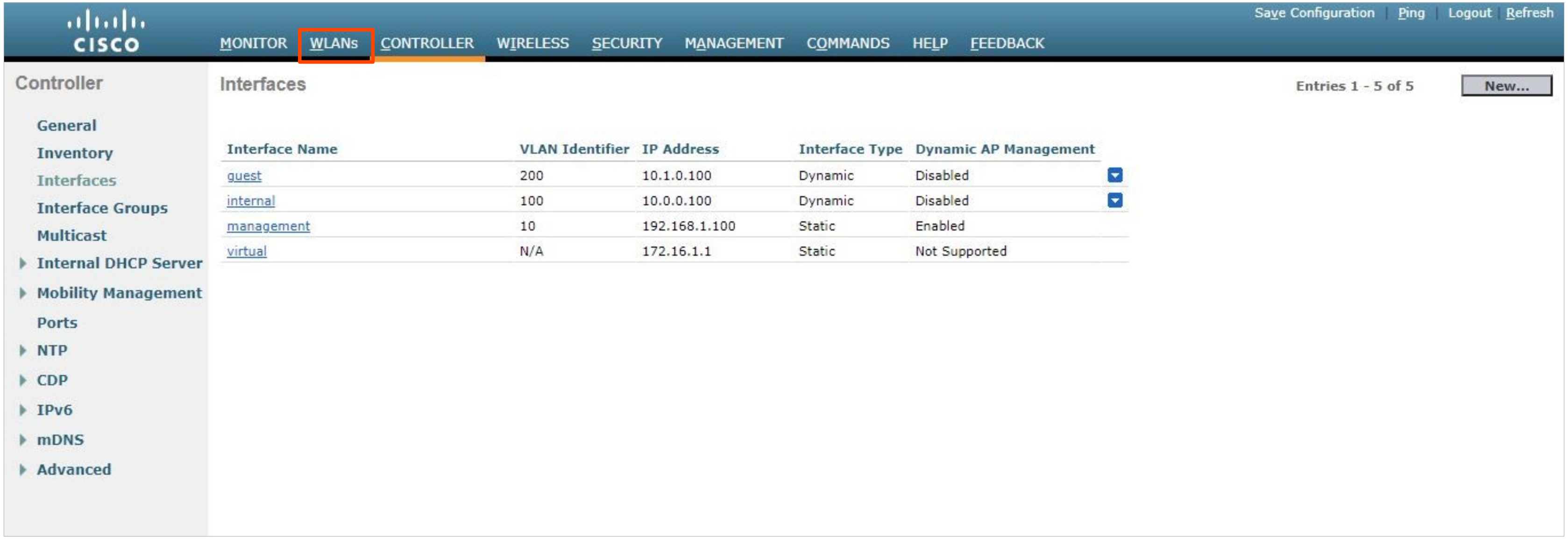
mDNS Profile	none

Note: Changing the Interface parameters causes the WLANs to be

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24

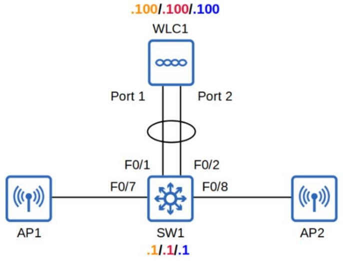


Interfaces

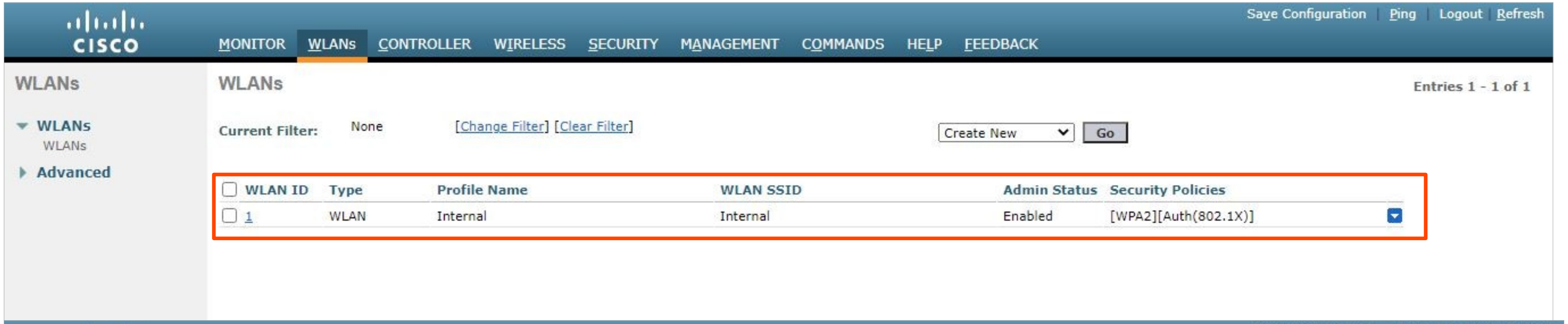
Entries 1 - 5 of 5

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
guest	200	10.1.0.100	Dynamic	Disabled
internal	100	10.0.0.100	Dynamic	Disabled
management	10	192.168.1.100	Static	Enabled
virtual	N/A	172.16.1.1	Static	Not Supported

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24

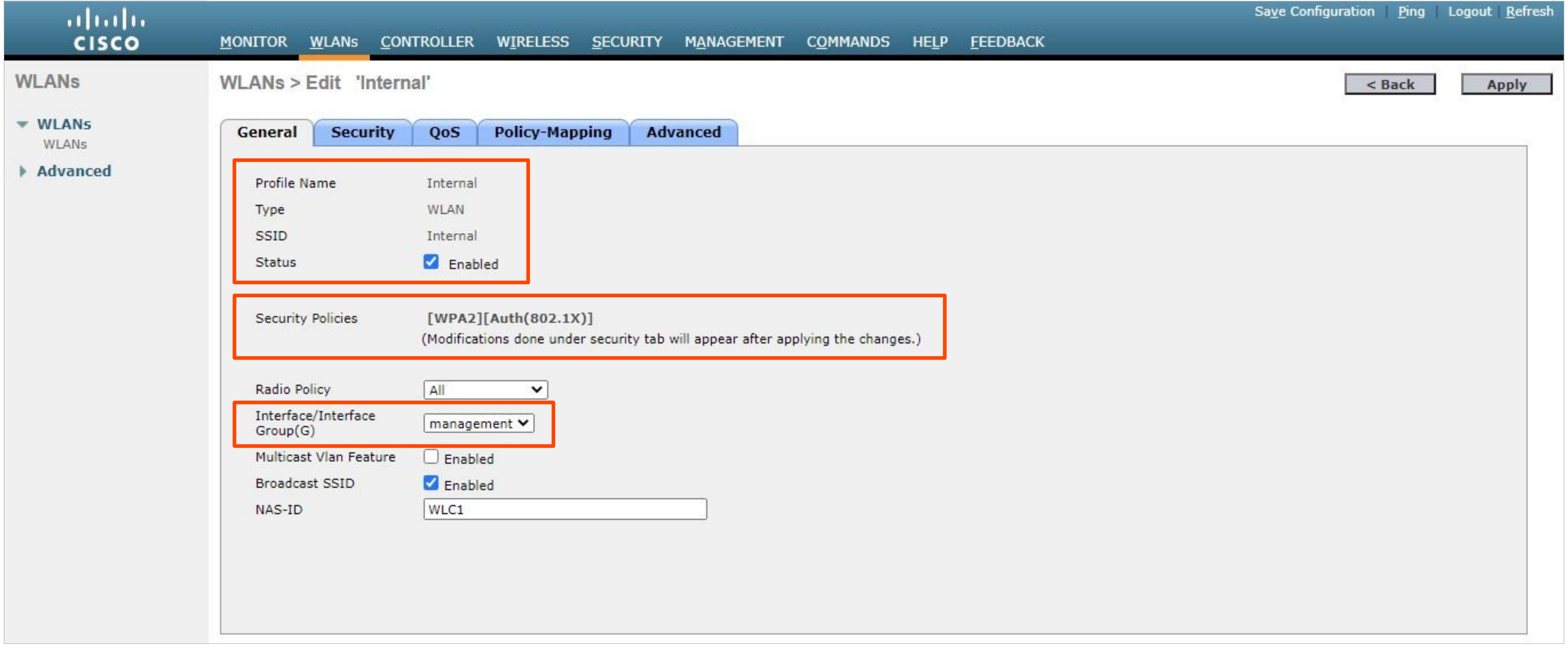

cisco
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
Create New
Go

WLANs

Entries 1 - 1 of 1

Current Filter: None [Change Filter] [Clear Filter]

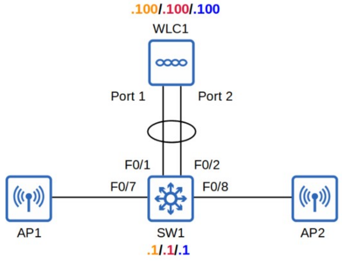
□ WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
□ 1	WLAN	Internal	Internal	Enabled	[WPA2][Auth(802.1X)]


cisco
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Policy-Mapping
Advanced

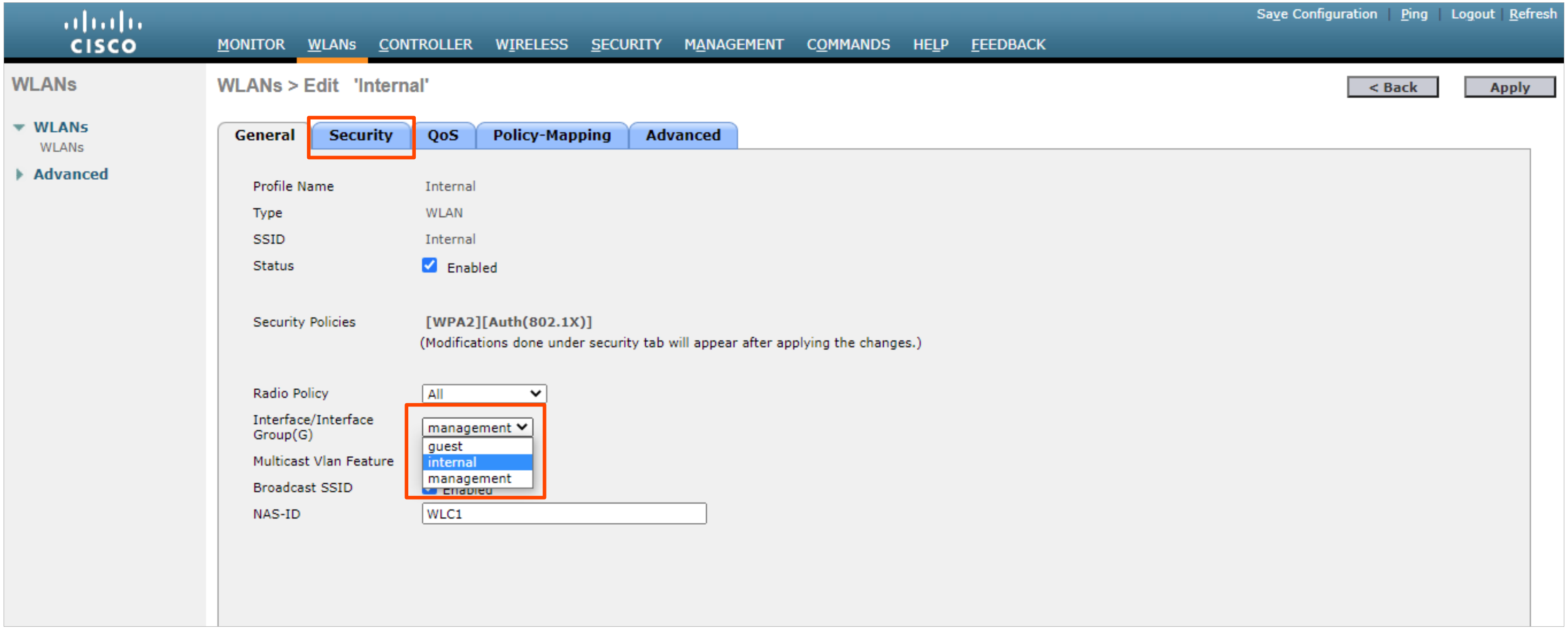
WLANs > Edit 'Internal'

Profile Name	Internal
Type	WLAN
SSID	Internal
Status	☑ Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	□ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	WLC1

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



WLANs > Edit 'Internal'

Profile Name Internal

Type WLAN

SSID Internal

Status ☑ Enabled

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

Radio Policy All

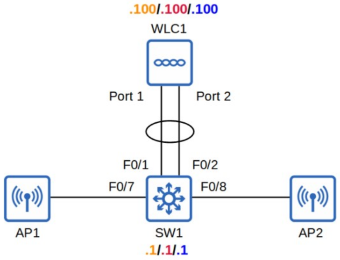
Interface/Interface Group(G) management
- guest
- internal
- management

Multicast Vlan Feature

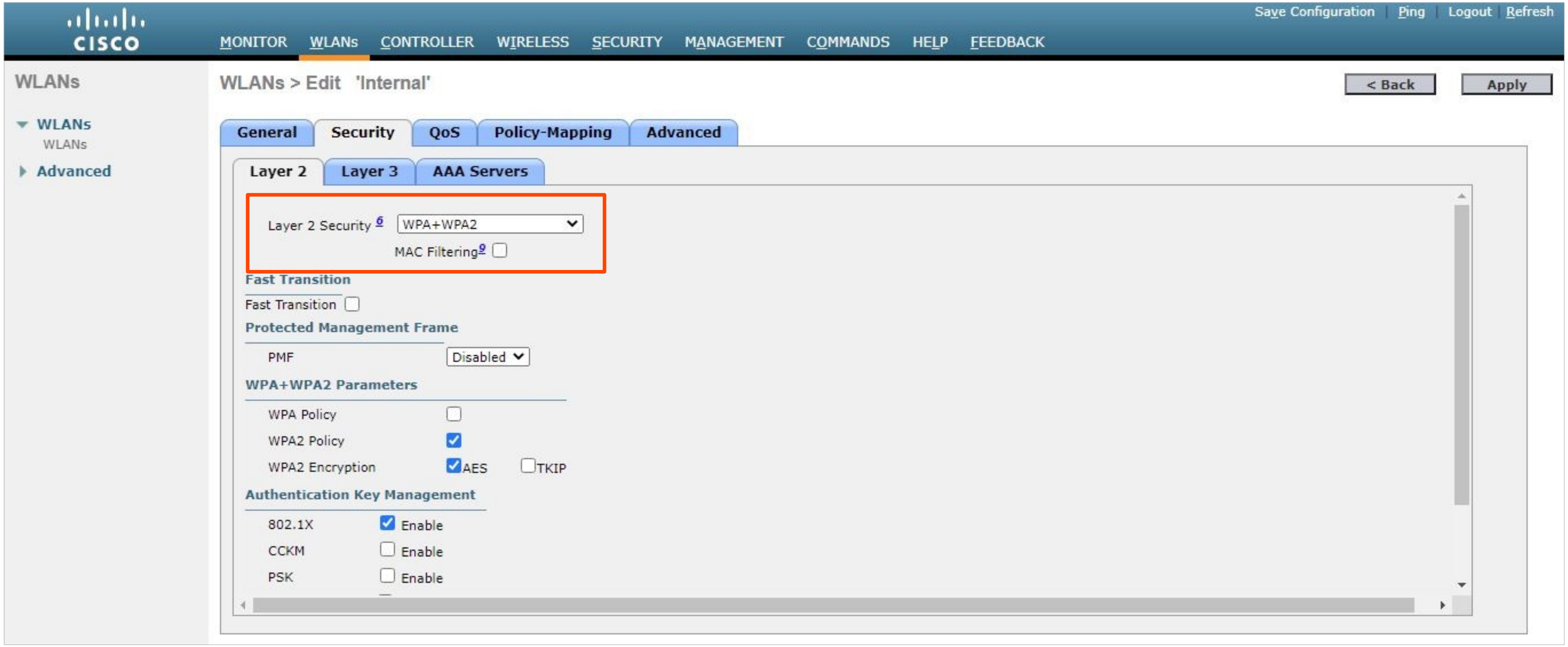
Broadcast SSID ☑ Enabled

NAS-ID WLC1

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



WLANs > Edit 'Internal'

Layer 2 Security 6 WPA+WPA2

MAC Filtering9 □

Fast Transition

Fast Transition □

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy □

WPA2 Policy ☑

WPA2 Encryption ☑AES □TKIP

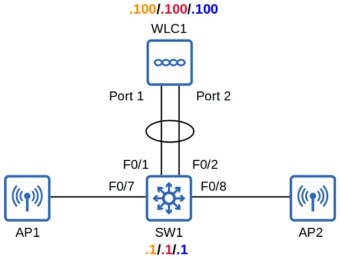
Authentication Key Management

802.1X ☑ Enable

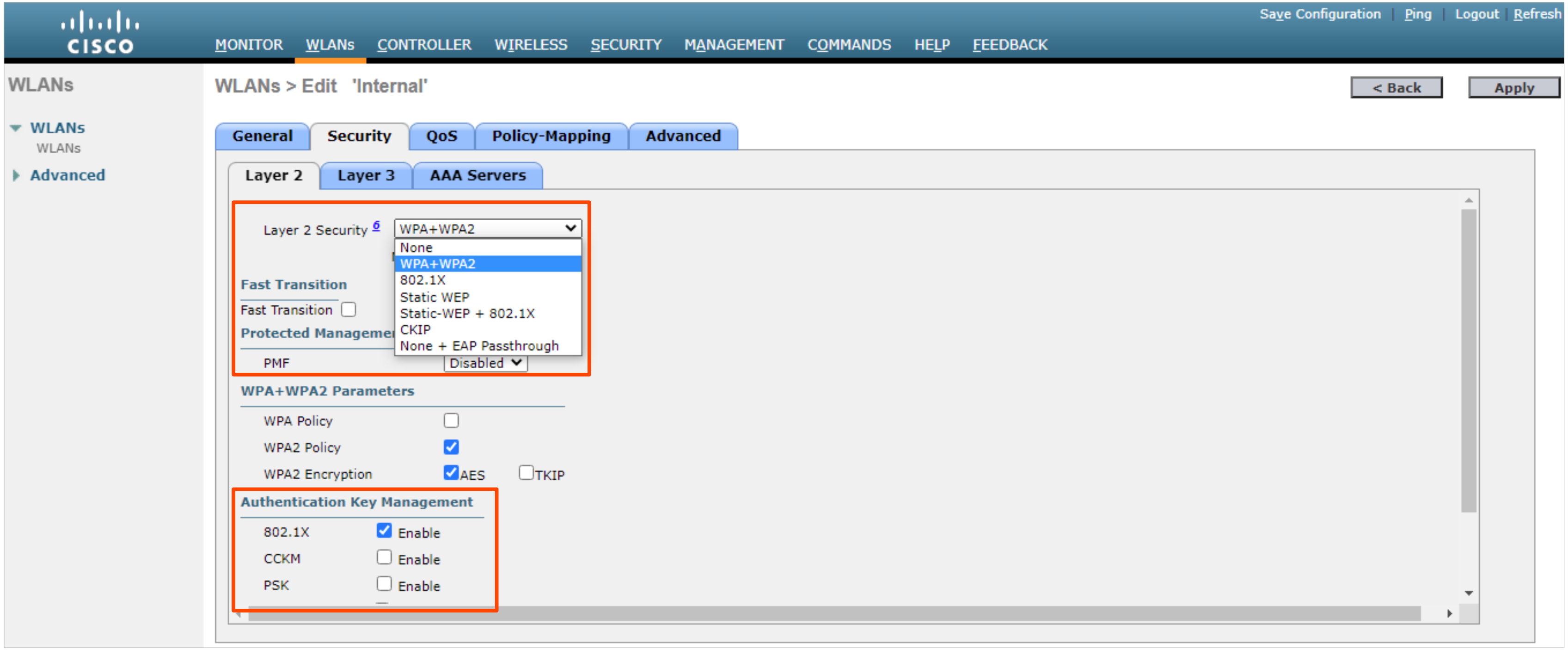
CCKM □ Enable

PSK □ Enable

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



WLANs > Edit 'Internal'

Layer 2 Security 6 WPA+WPA2

- None
- WPA+WPA2
- 802.1X
- Static WEP
- Static-WEP + 802.1X
- CKIP
- None + EAP Passthrough

Fast Transition

Fast Transition □

Protected Manageme

PMF Disabled

WPA+WPA2 Parameters

WPA Policy □

WPA2 Policy ☑

WPA2 Encryption ☑AES □TKIP

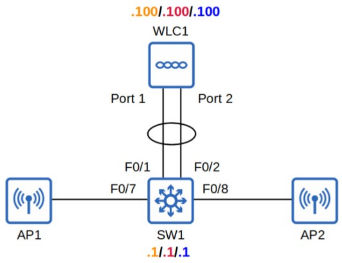
Authentication Key Management

802.1X ☑ Enable

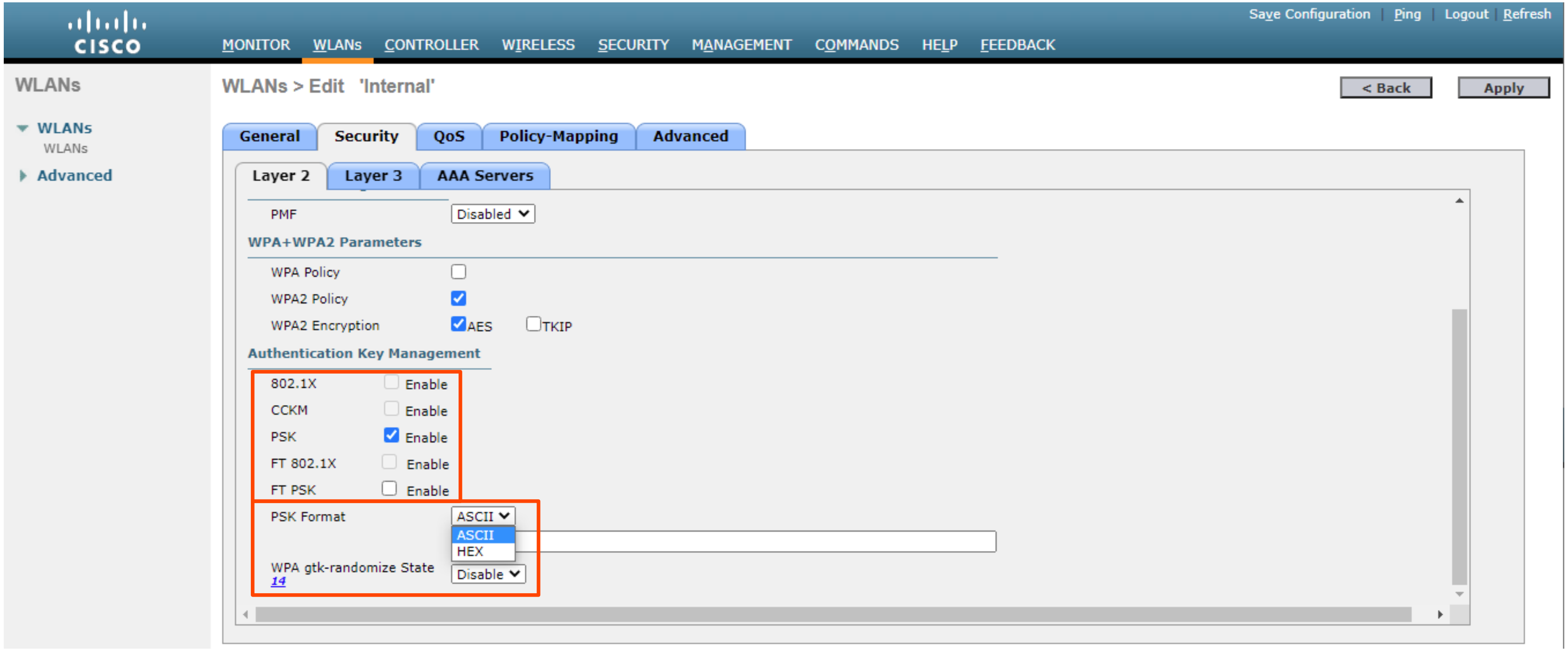
CCKM □ Enable

PSK □ Enable

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



CISCO
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General Security QoS Policy-Mapping Advanced
Layer 2 Layer 3 AAA Servers

WLANs > Edit 'Internal'

PMF: Disabled

WPA+WPA2 Parameters

WPA Policy ☐
WPA2 Policy ☑
WPA2 Encryption ☑AES ☐TKIP

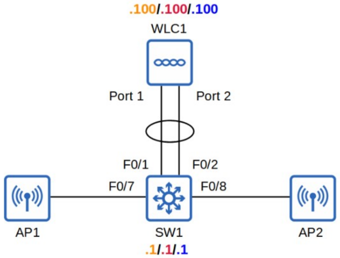
Authentication Key Management

802.1X ☐ Enable
CCKM ☐ Enable
PSK ☑ Enable
FT 802.1X ☐ Enable
FT PSK ☐ Enable

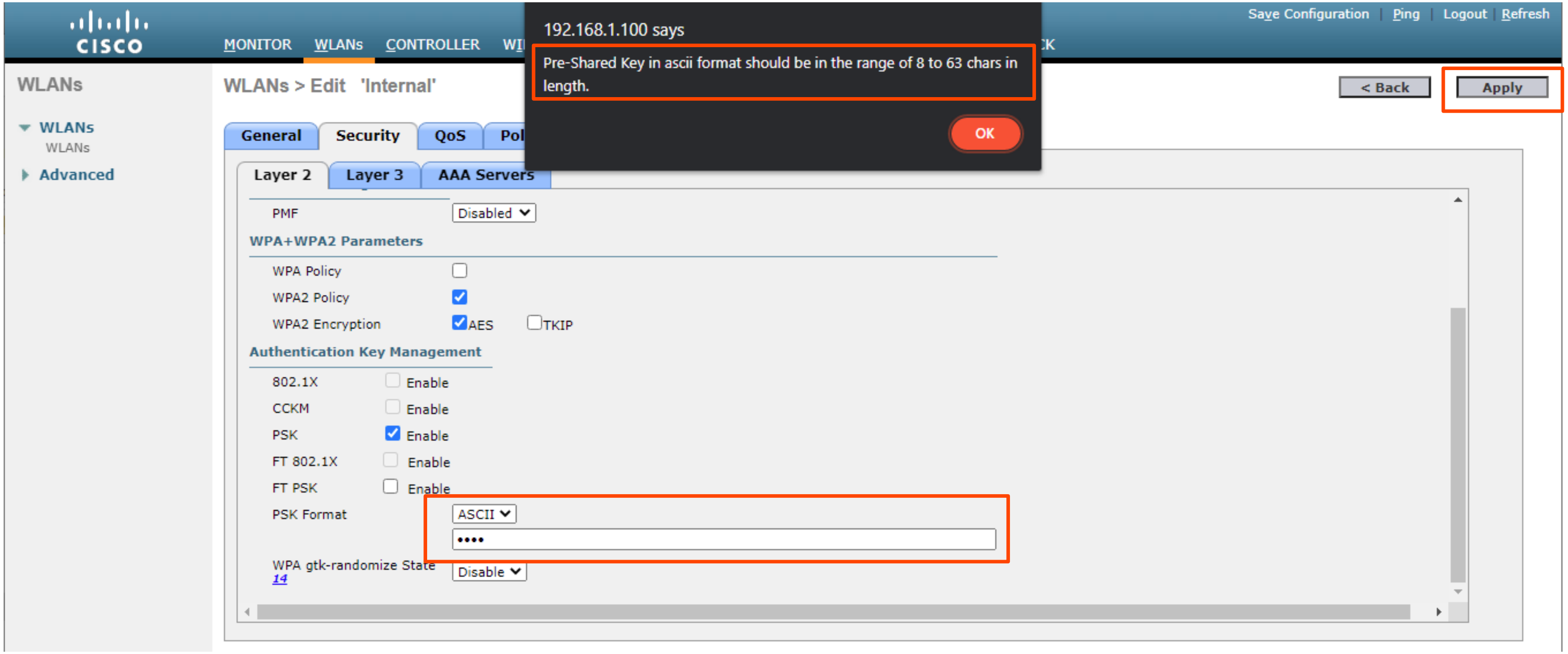
PSK Format: ASCII (ASCII / HEX)

WPA gtk-randomize State 14: Disable

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



192.168.1.100 says

Pre-Shared Key in ascii format should be in the range of 8 to 63 chars in length.

WLANs > Edit 'Internal'

PMF: Disabled

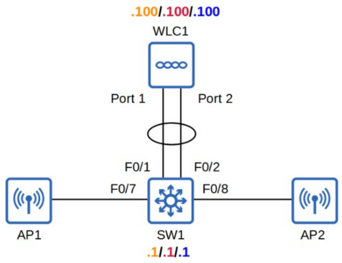
WPA+WPA2 Parameters

WPA Policy ☐
WPA2 Policy ☑
WPA2 Encryption ☑AES ☐TKIP

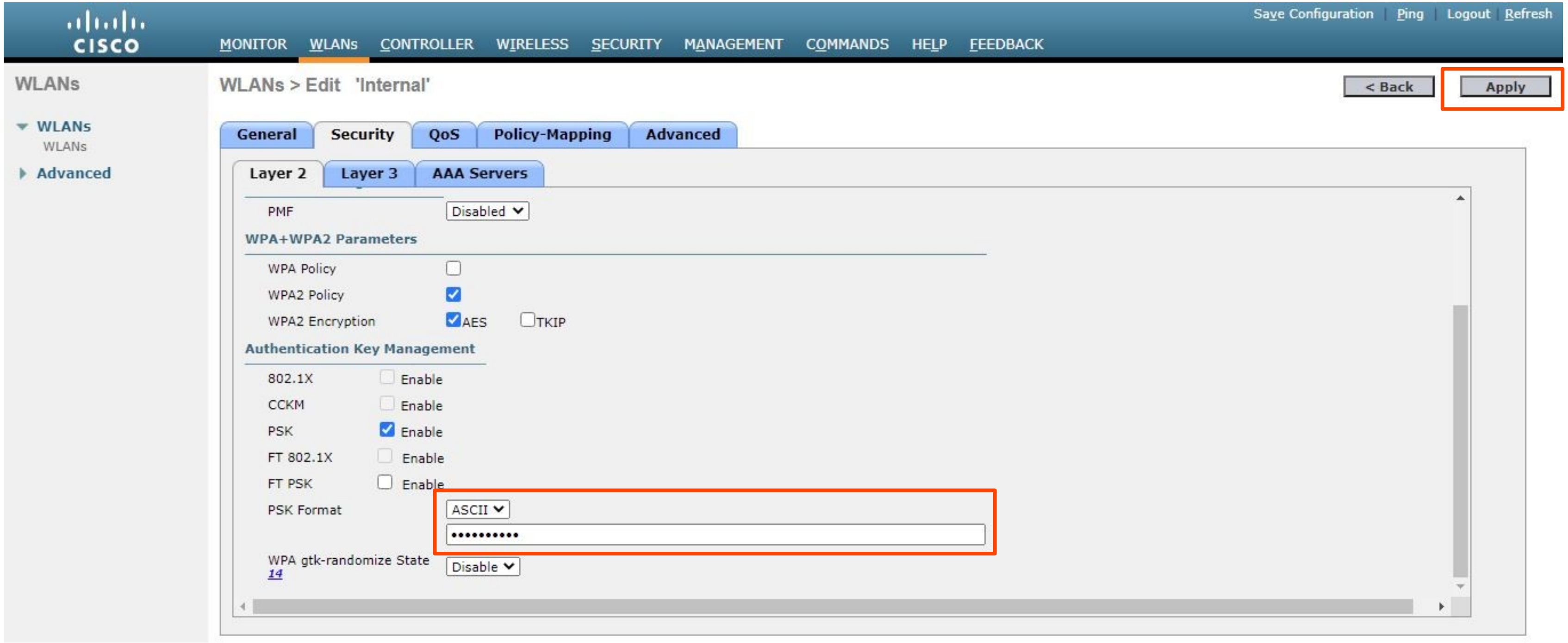
Authentication Key Management

802.1X ☐ Enable
CCKM ☐ Enable
PSK ☑ Enable
FT 802.1X ☐ Enable
FT PSK ☐ Enable
PSK Format: ASCII
••••
WPA gtk-randomize State 14: Disable

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



WLANs > Edit 'Internal'

PMF: Disabled

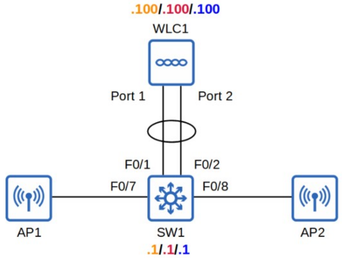
WPA+WPA2 Parameters

WPA Policy ☐
WPA2 Policy ☑
WPA2 Encryption ☑AES ☐TKIP

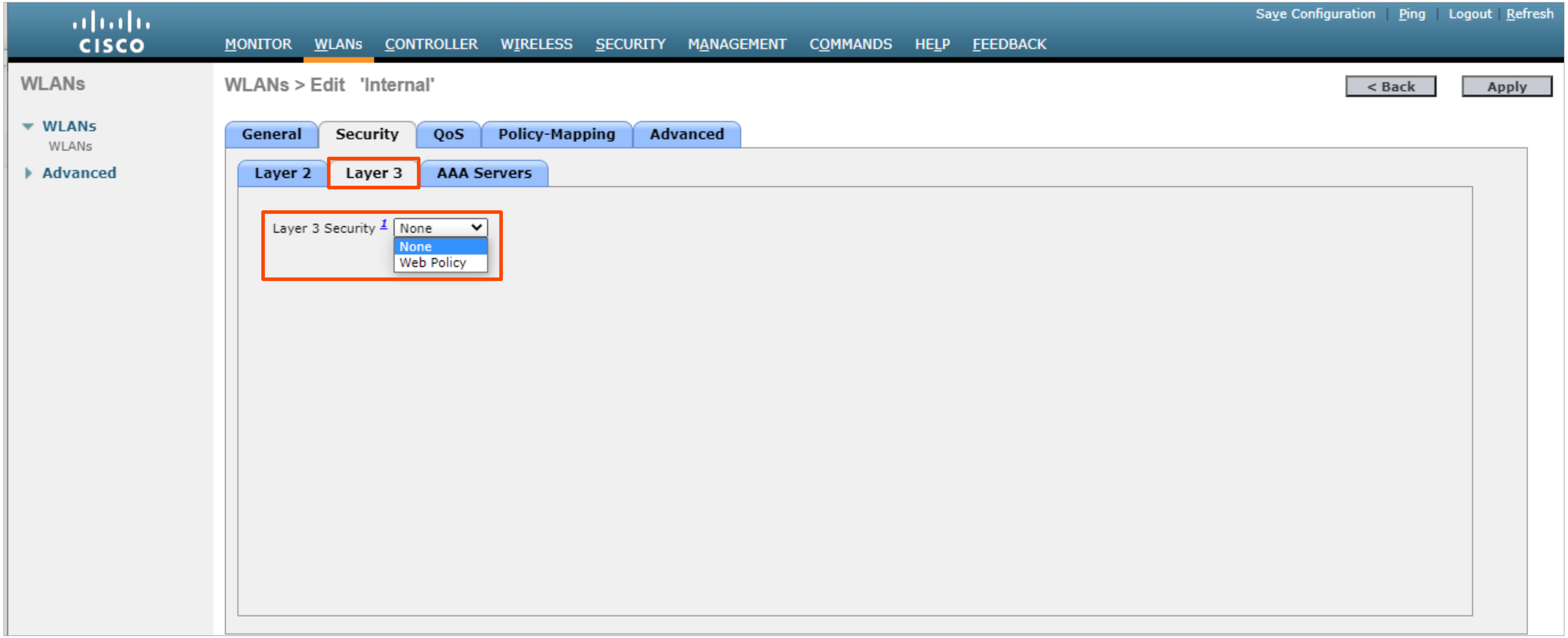
Authentication Key Management

802.1X ☐ Enable
CCKM ☐ Enable
PSK ☑ Enable
FT 802.1X ☐ Enable
FT PSK ☐ Enable
PSK Format: ASCII
••••••••••
WPA gtk-randomize State 14: Disable

WLC Configuration



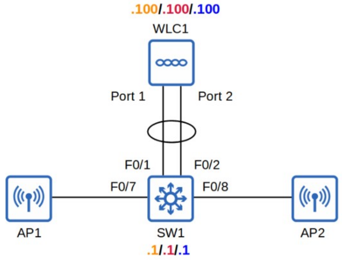
WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



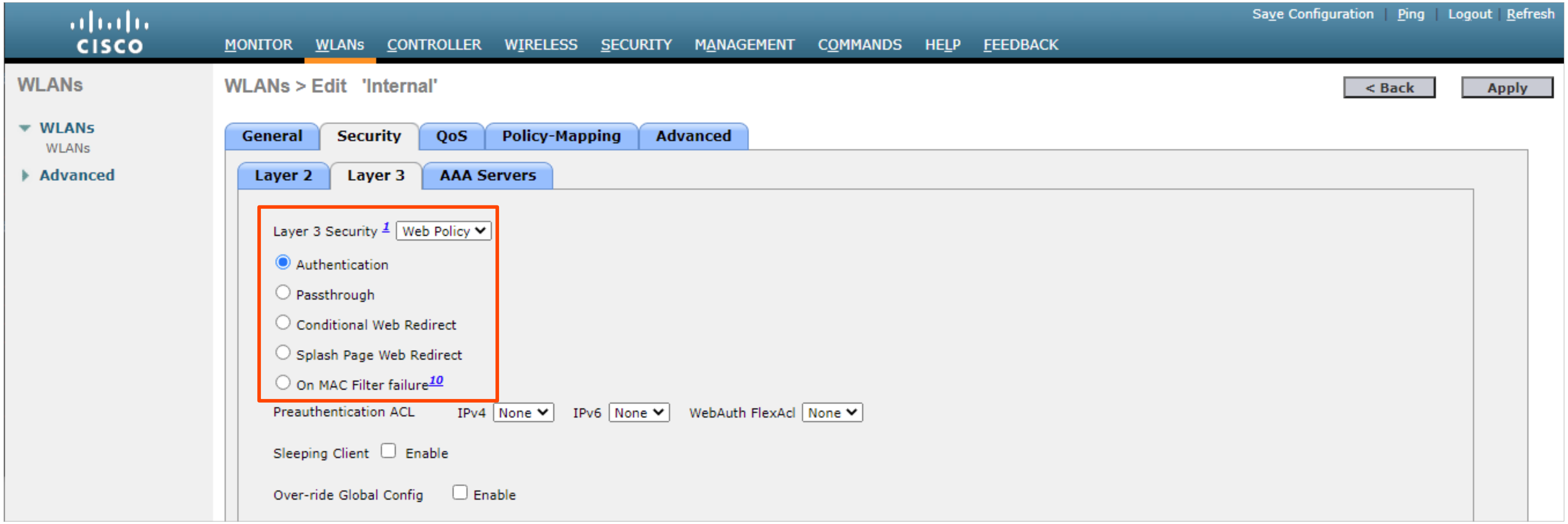
WLANs > Edit 'Internal'

Layer 3 Security [1] None

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



WLANs > Edit 'Internal'

Layer 3 Security [1] Web Policy

● Authentication

○ Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

○ On MAC Filter failure[10]

Preauthentication ACL IPv4 None IPv6 None WebAuth FlexAcl None

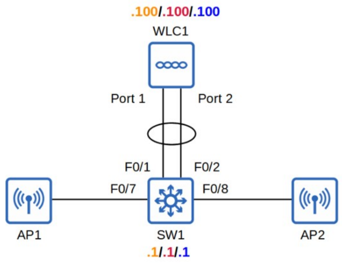
Sleeping Client □ Enable

Over-ride Global Config □ Enable

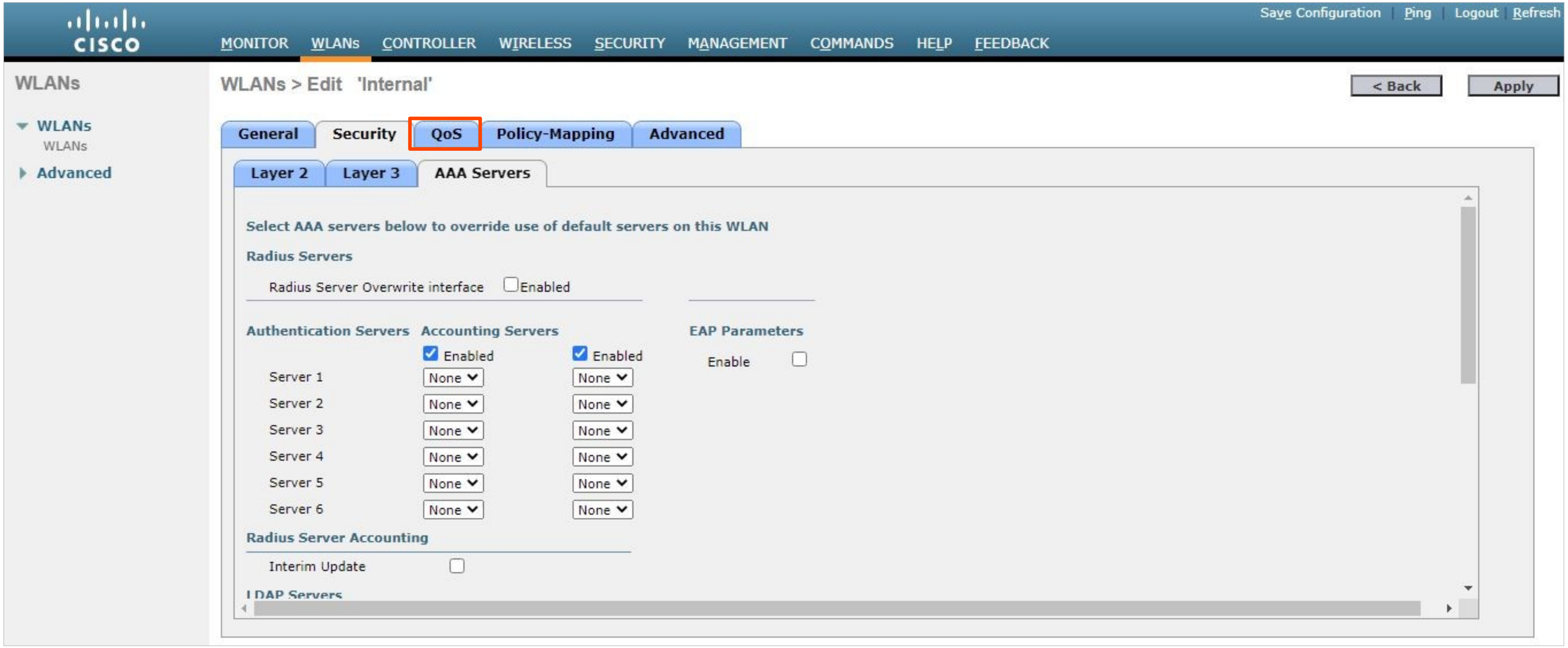
- **Web Authentication**: After the wireless clients gets an IP address and tries to access a web page, they will have to enter a username and password to authenticate.
- **Web Passthrough**: Similar to the above, but no username or password are required. A warning or statement is displayed and the client simply has to agree to gain access to the Internet.

- The **Conditional** and **Splash Page** web redirect options are similar, but additionally require 802.1X layer 2 authentication.

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



WLANs > Edit 'Internal'

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

Radius Servers

Radius Server Overwrite interface ☐ Enabled

EAP Parameters

Enable ☐

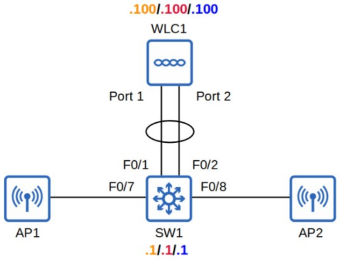
	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	None	None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

Radius Server Accounting

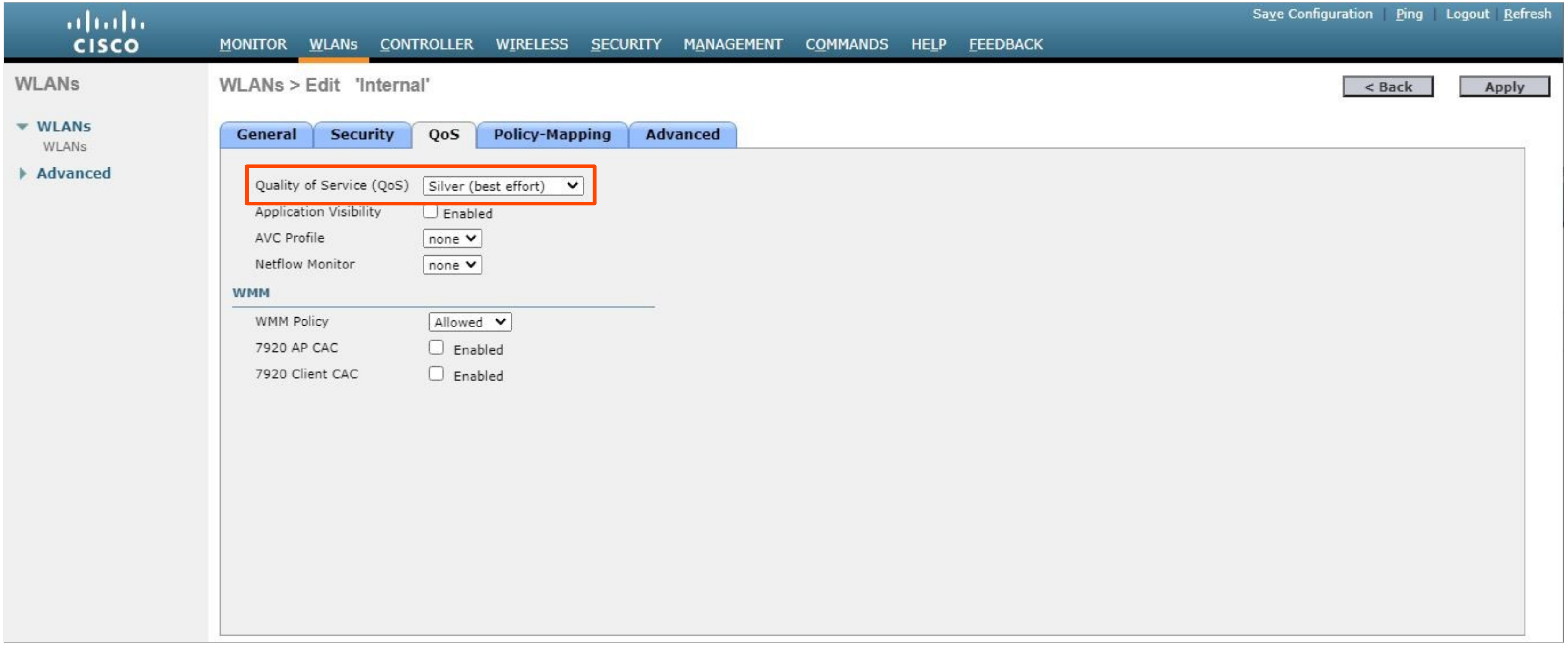
Interim Update ☐

LDAP Servers

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



WLANs > Edit 'Internal'

Quality of Service (QoS): Silver (best effort)

Application Visibility: □ Enabled

AVC Profile: none

Netflow Monitor: none

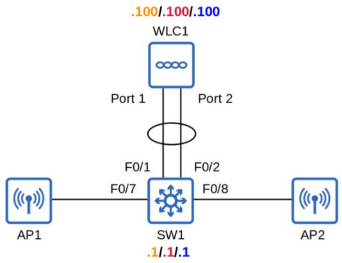
WMM

WMM Policy: Allowed

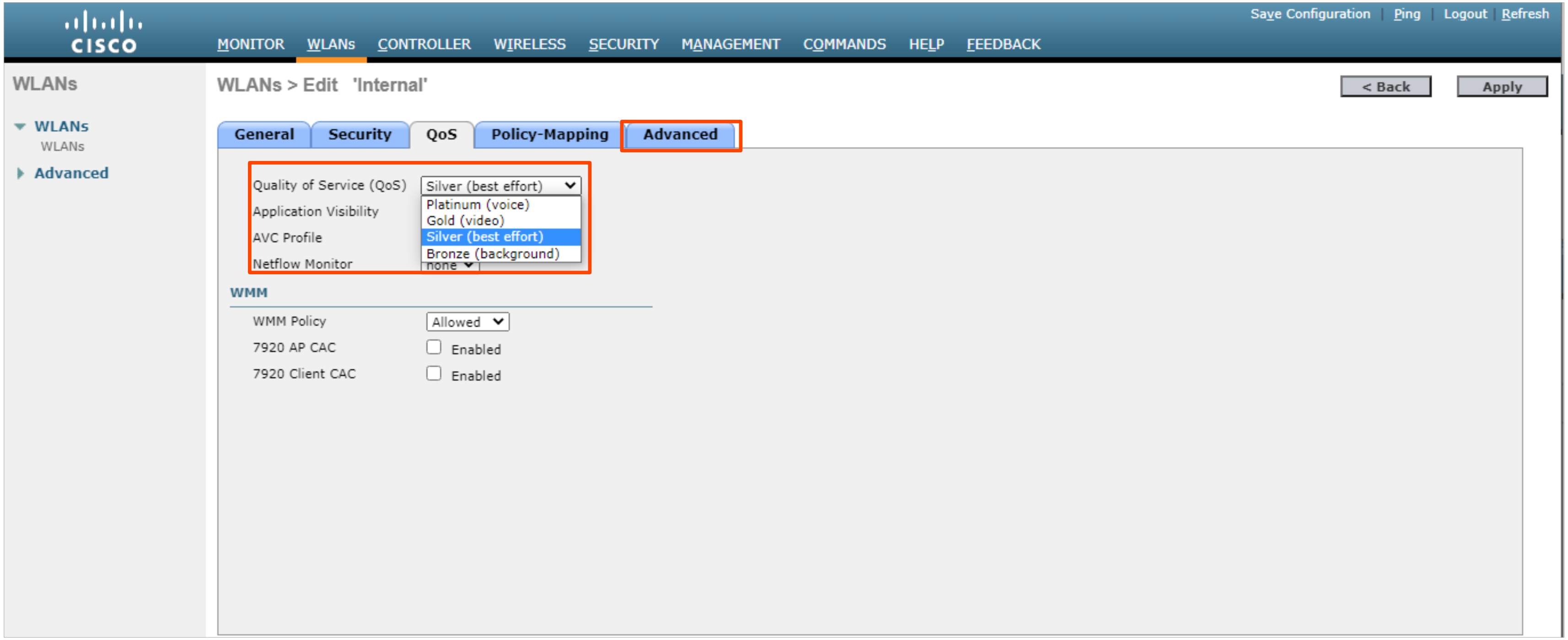
7920 AP CAC: □ Enabled

7920 Client CAC: □ Enabled

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



WLANs > Edit 'Internal'

Quality of Service (QoS): Silver (best effort)
- Platinum (voice)
- Gold (video)
- Silver (best effort)
- Bronze (background)

Application Visibility

AVC Profile

Netflow Monitor: none

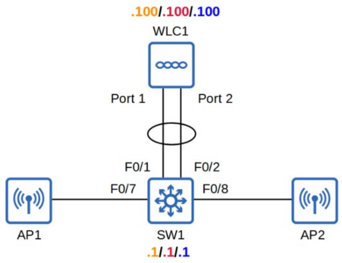
WMM

WMM Policy: Allowed

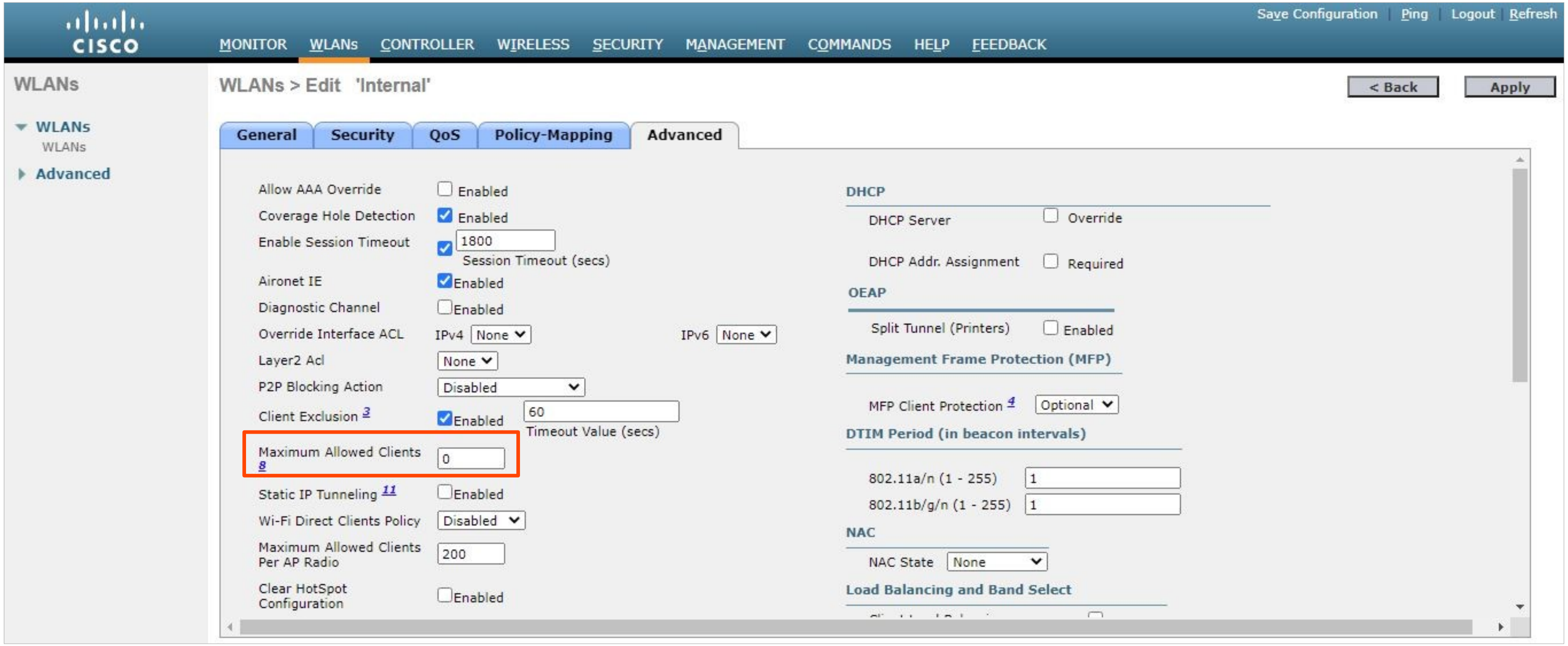
7920 AP CAC: □ Enabled

7920 Client CAC: □ Enabled

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



WLANs > Edit 'Internal'

Allow AAA Override ☐ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel ☐ Enabled
Override Interface ACL IPv4 None IPv6 None
Layer2 Acl None
P2P Blocking Action Disabled
Client Exclusion [3] ☑ Enabled 60 Timeout Value (secs)
Maximum Allowed Clients [8] 0
Static IP Tunneling [11] ☐ Enabled
Wi-Fi Direct Clients Policy Disabled
Maximum Allowed Clients Per AP Radio 200
Clear HotSpot Configuration ☐ Enabled

DHCP
DHCP Server ☐ Override
DHCP Addr. Assignment ☐ Required

OEAP
Split Tunnel (Printers) ☐ Enabled

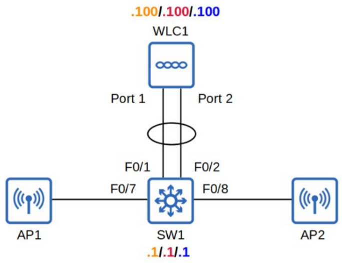
Management Frame Protection (MFP)
MFP Client Protection [4] Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

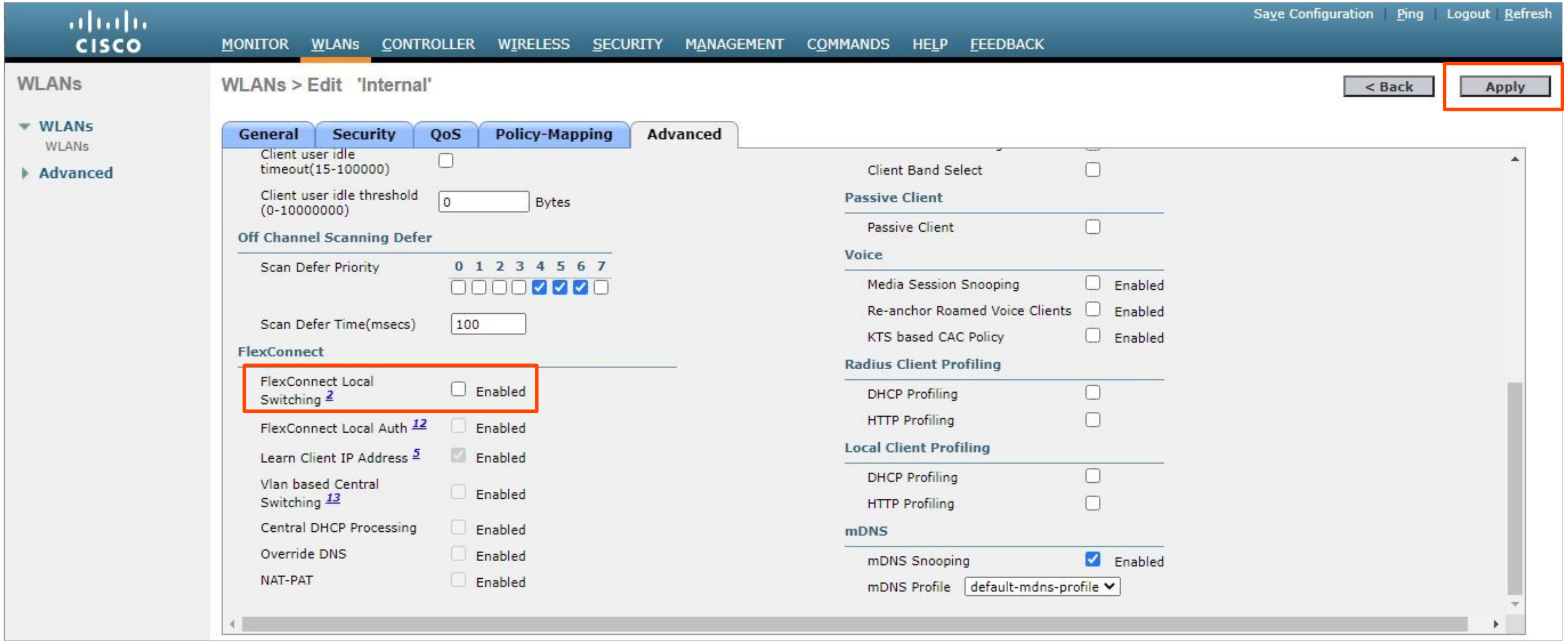
NAC
NAC State None

Load Balancing and Band Select

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



WLANs > Edit 'Internal'

Client user idle timeout(15-100000) □

Client user idle threshold (0-10000000) 0 Bytes

Off Channel Scanning Defer

Scan Defer Priority 0 □ 1 □ 2 □ 3 □ 4 ☑ 5 ☑ 6 ☑ 7 □

Scan Defer Time(msecs) 100

FlexConnect

FlexConnect Local Switching 2 □ Enabled

FlexConnect Local Auth 12 □ Enabled

Learn Client IP Address 5 ☑ Enabled

Vlan based Central Switching 13 □ Enabled

Central DHCP Processing □ Enabled

Override DNS □ Enabled

NAT-PAT □ Enabled

Client Band Select □

Passive Client

Passive Client □

Voice

Media Session Snooping □ Enabled

Re-anchor Roamed Voice Clients □ Enabled

KTS based CAC Policy □ Enabled

Radius Client Profiling

DHCP Profiling □

HTTP Profiling □

Local Client Profiling

DHCP Profiling □

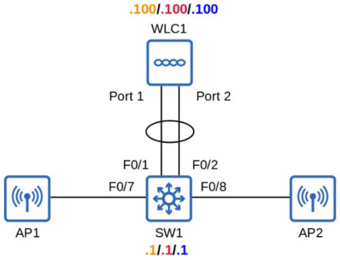
HTTP Profiling □

mDNS

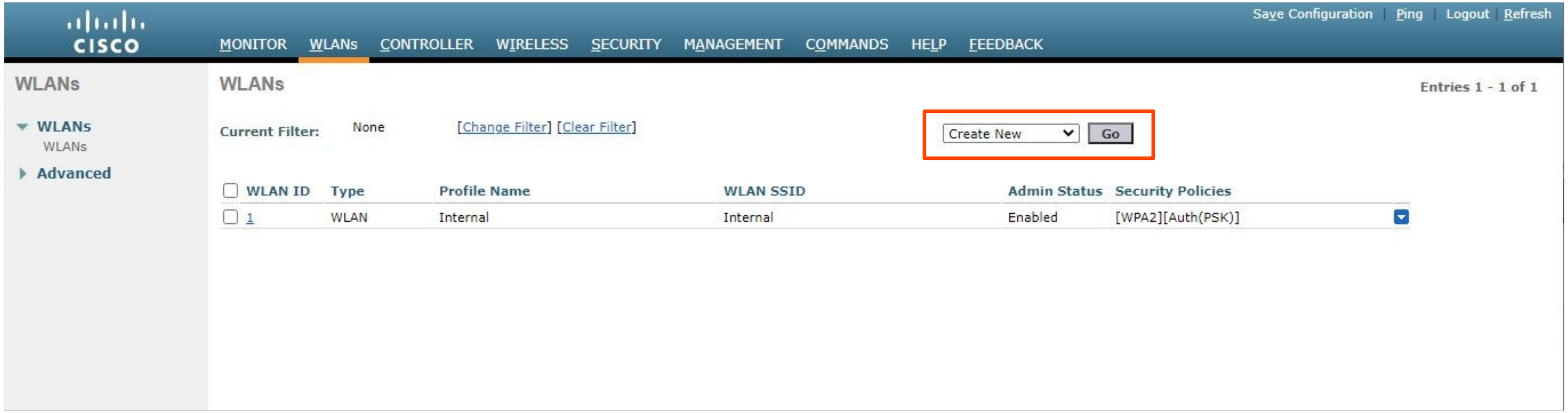
mDNS Snooping ☑ Enabled

mDNS Profile default-mdns-profile

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



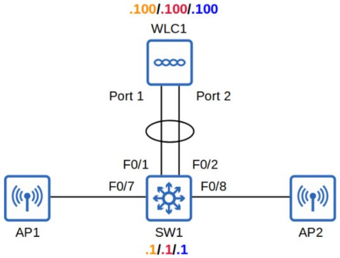
WLANs

Entries 1 - 1 of 1

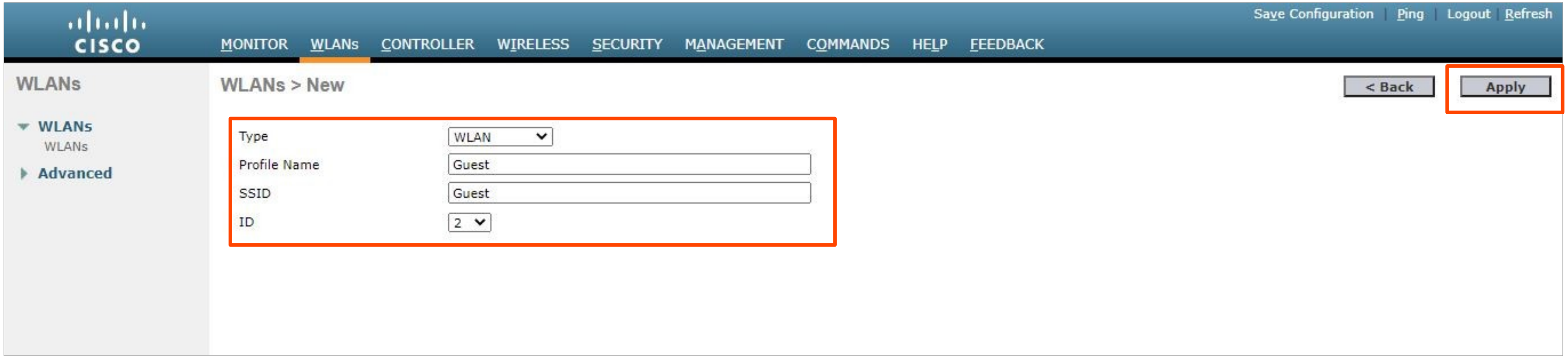
Current Filter: None [Change Filter] [Clear Filter]

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

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24

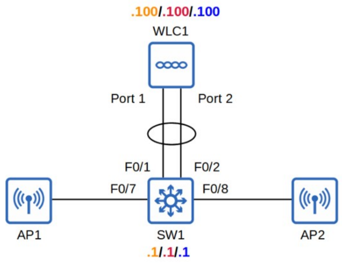


cisco
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
▾ WLANs
WLANs
▸ Advanced
< Back
Apply

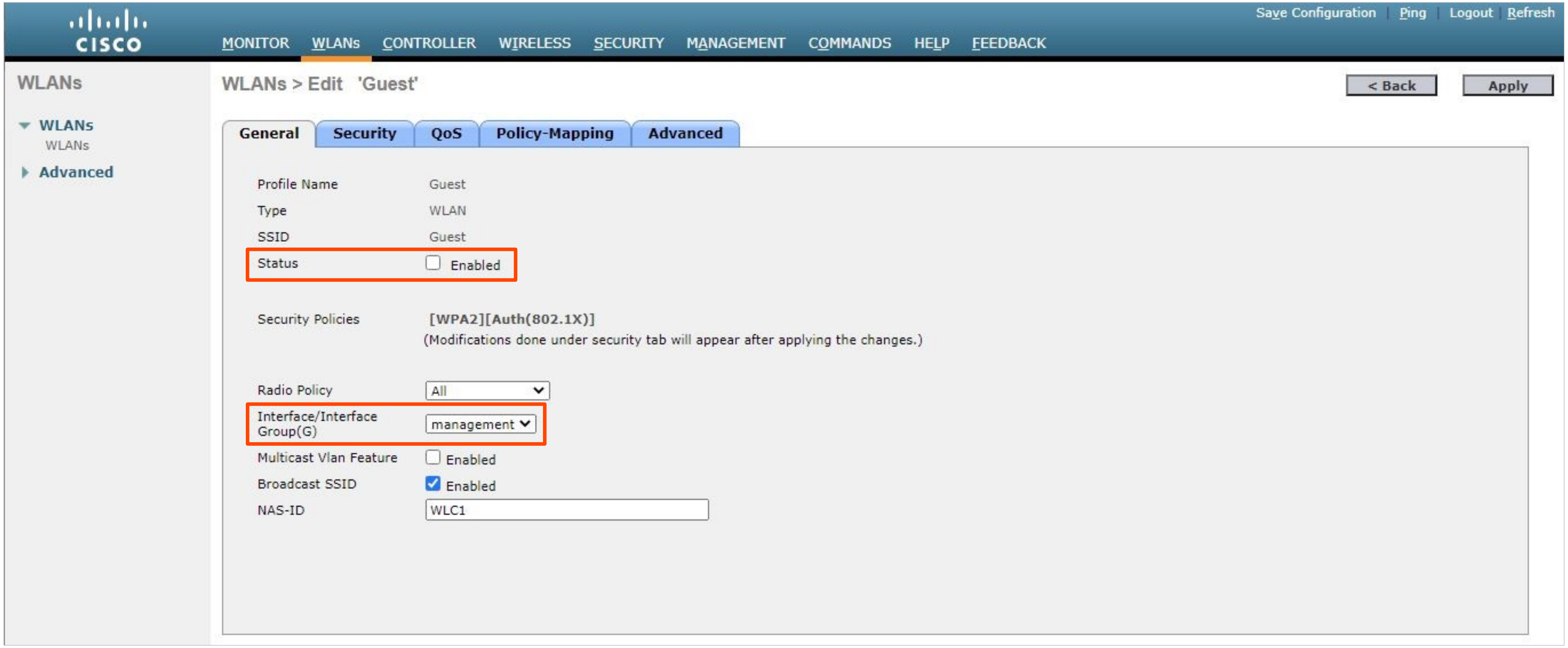
WLANs > New

Type	WLAN
Profile Name	Guest
SSID	Guest
ID	2

WLC Configuration



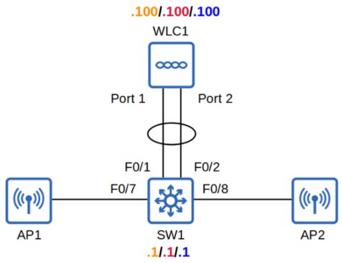
WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



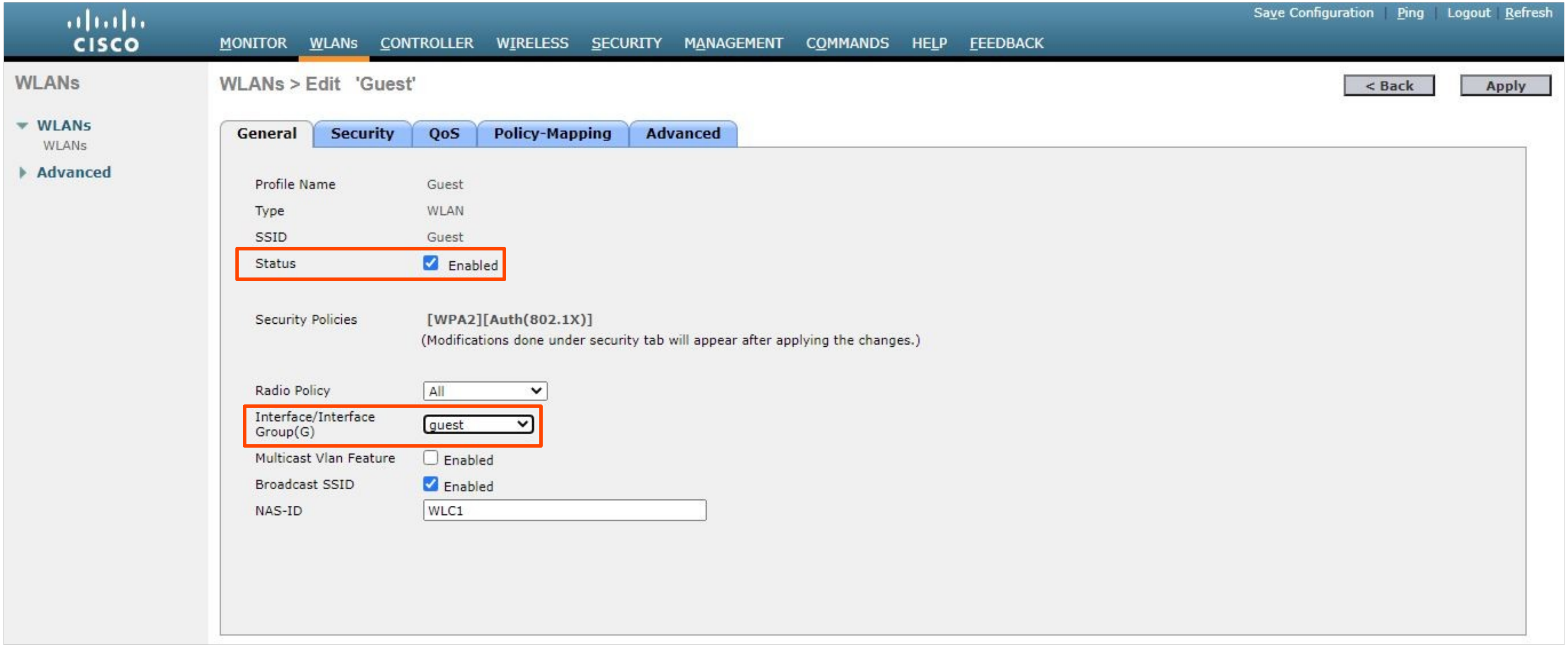
WLANs > Edit 'Guest'

Profile Name	Guest
Type	WLAN
SSID	Guest
Status	□ Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	□ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	WLC1

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



WLANs > Edit 'Guest'

Profile Name Guest

Type WLAN

SSID Guest

Status ☑ Enabled

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

Radio Policy All

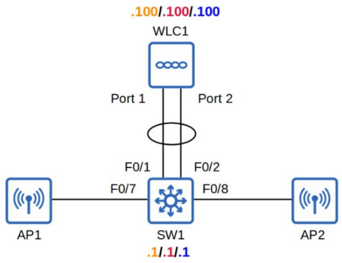
Interface/Interface Group(G) guest

Multicast Vlan Feature □ Enabled

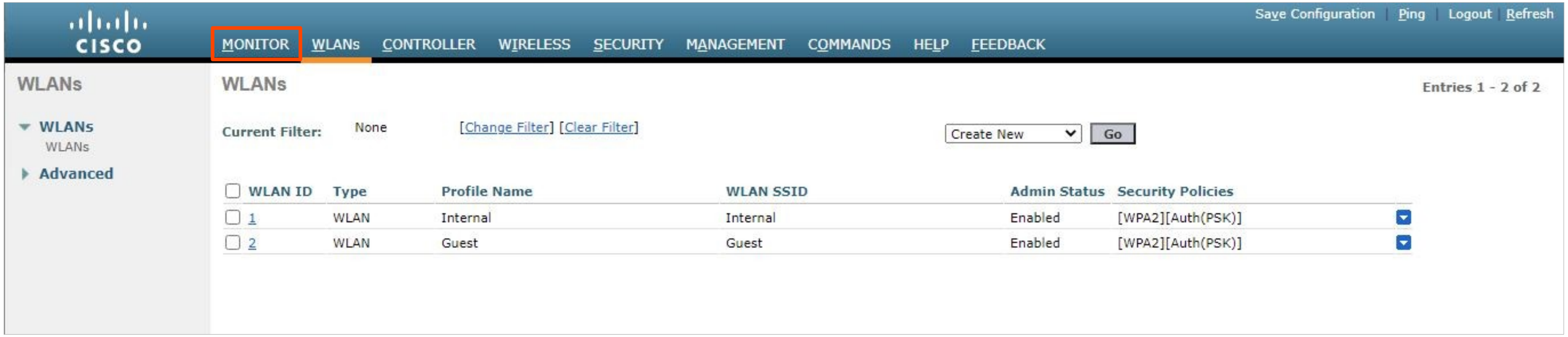
Broadcast SSID ☑ Enabled

NAS-ID WLC1

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



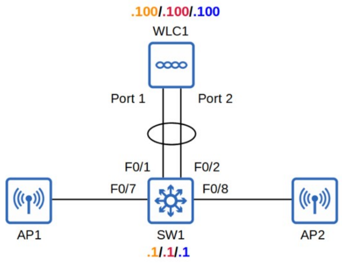
WLANs

Entries 1 - 2 of 2

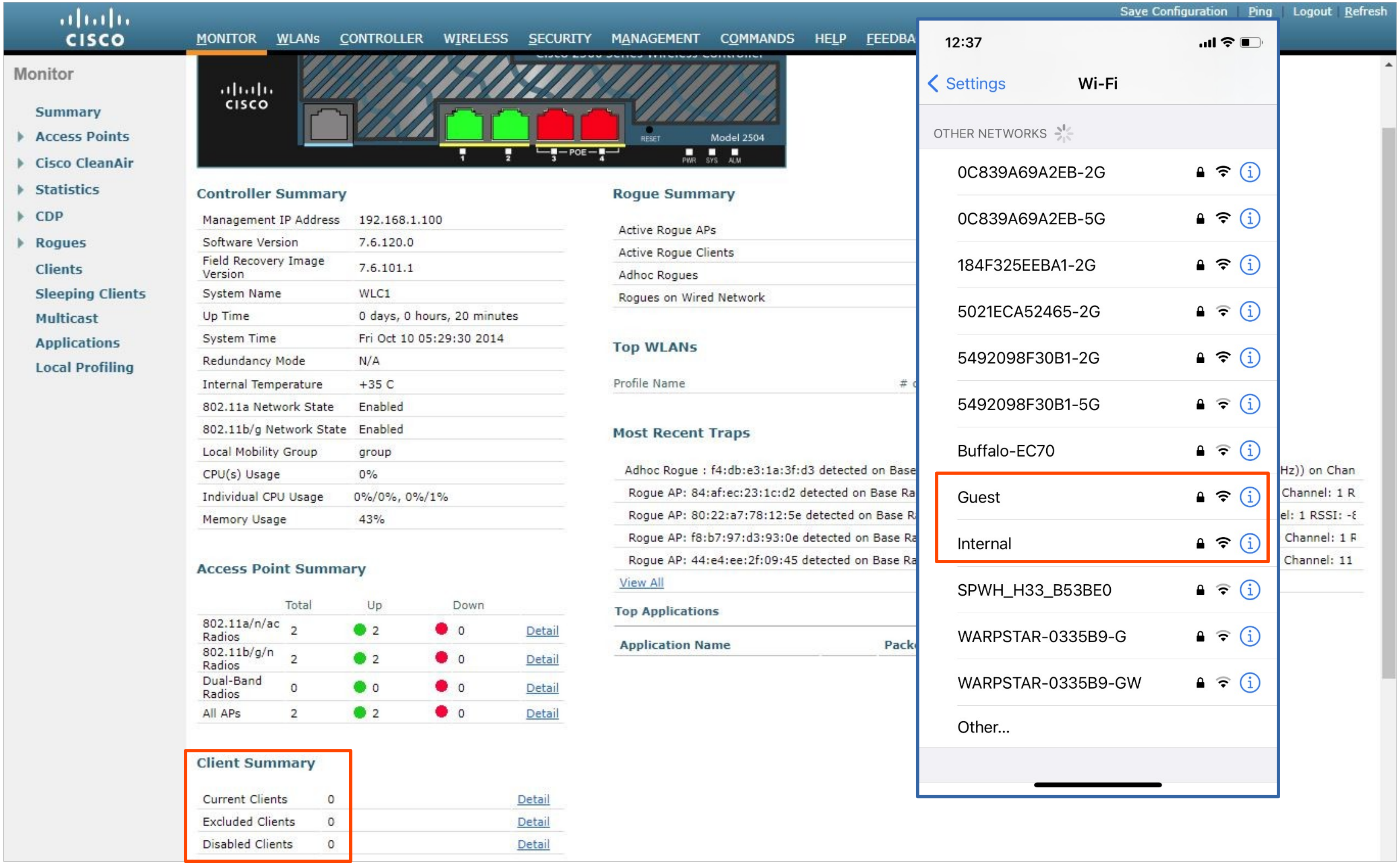
Current Filter: None [Change Filter] [Clear Filter]

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

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



Controller Summary

Management IP Address	192.168.1.100
Software Version	7.6.120.0
Field Recovery Image Version	7.6.101.1
System Name	WLC1
Up Time	0 days, 0 hours, 20 minutes
System Time	Fri Oct 10 05:29:30 2014
Redundancy Mode	N/A
Internal Temperature	+35 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	group
CPU(s) Usage	0%
Individual CPU Usage	0%/0%, 0%/1%
Memory Usage	43%

Access Point Summary

	Total	Up	Down	
802.11a/n/ac Radios	2	● 2	● 0	Detail
802.11b/g/n Radios	2	● 2	● 0	Detail
Dual-Band Radios	0	● 0	● 0	Detail
All APs	2	● 2	● 0	Detail

Client Summary

Current Clients	0	Detail
Excluded Clients	0	Detail
Disabled Clients	0	Detail

Rogue Summary

Active Rogue APs
Active Rogue Clients
Adhoc Rogues
Rogues on Wired Network

Top WLANs

Profile Name #

Most Recent Traps

```
Adhoc Rogue : f4:db:e3:1a:3f:d3 detected on Base
 Rogue AP: 84:af:ec:23:1c:d2 detected on Base Ra
 Rogue AP: 80:22:a7:78:12:5e detected on Base R
 Rogue AP: f8:b7:97:d3:93:0e detected on Base Ra
 Rogue AP: 44:e4:ee:2f:09:45 detected on Base Ra
```

```
Hz)) on Chan
Channel: 1 R
el: 1 RSSI: -8
Channel: 1 R
Channel: 11
```

View All

Top Applications

Application Name Pack

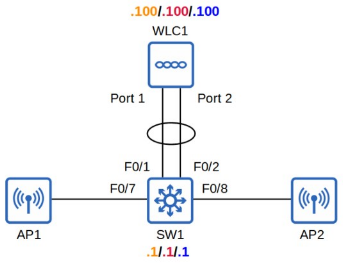
12:37

< Settings **Wi-Fi**

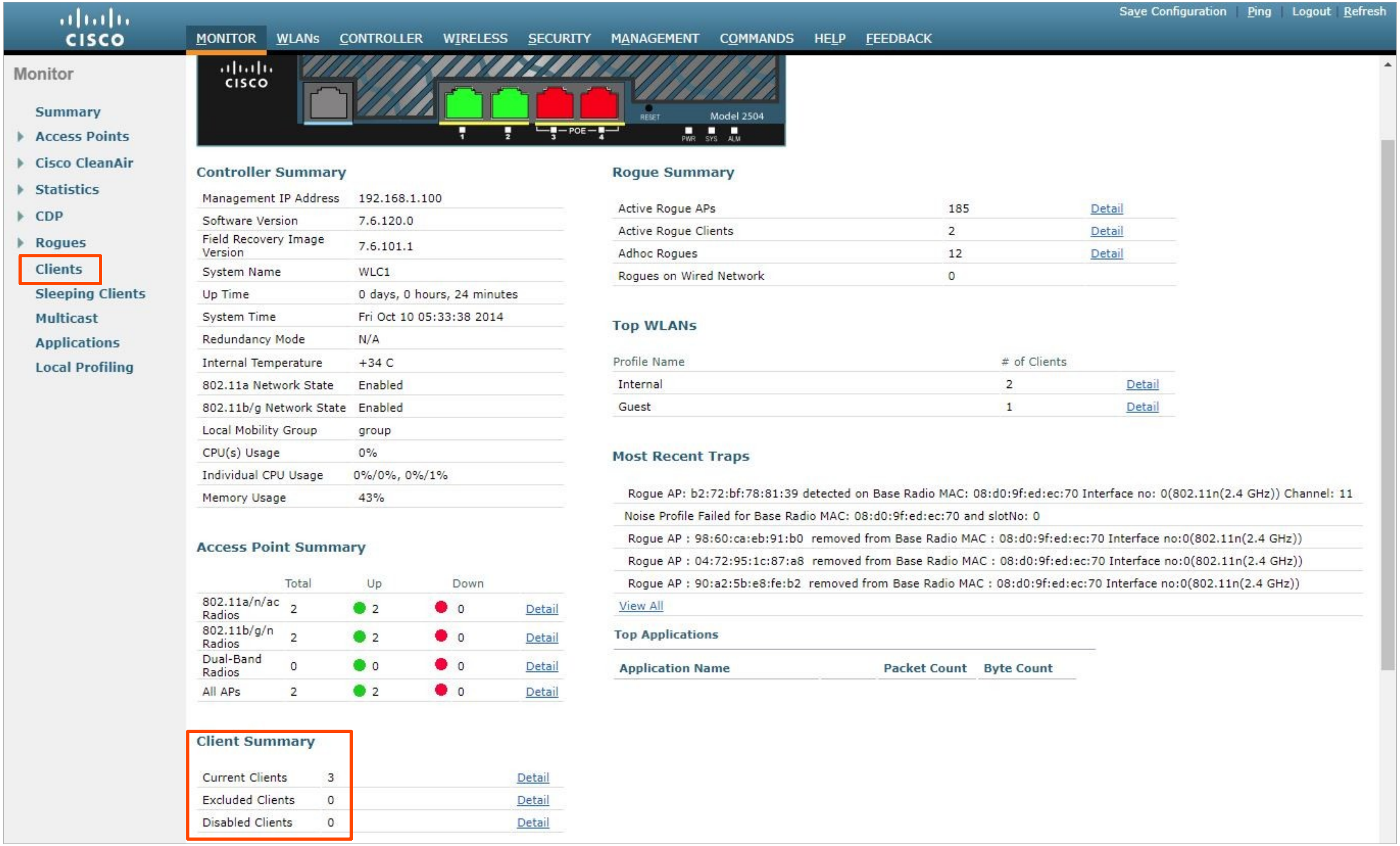
OTHER NETWORKS

- 0C839A69A2EB-2G
- 0C839A69A2EB-5G
- 184F325EEBA1-2G
- 5021ECA52465-2G
- 5492098F30B1-2G
- 5492098F30B1-5G
- Buffalo-EC70
- Guest
- Internal
- SPWH_H33_B53BE0
- WARPSTAR-0335B9-G
- WARPSTAR-0335B9-GW
- Other...

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



Controller Summary

Management IP Address	192.168.1.100
Software Version	7.6.120.0
Field Recovery Image Version	7.6.101.1
System Name	WLC1
Up Time	0 days, 0 hours, 24 minutes
System Time	Fri Oct 10 05:33:38 2014
Redundancy Mode	N/A
Internal Temperature	+34 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	group
CPU(s) Usage	0%
Individual CPU Usage	0%/0%, 0%/1%
Memory Usage	43%

Access Point Summary

	Total	Up	Down	
802.11a/n/ac Radios	2	● 2	● 0	Detail
802.11b/g/n Radios	2	● 2	● 0	Detail
Dual-Band Radios	0	● 0	● 0	Detail
All APs	2	● 2	● 0	Detail

Client Summary

Current Clients	3	Detail
Excluded Clients	0	Detail
Disabled Clients	0	Detail

Rogue Summary

Active Rogue APs	185	Detail
Active Rogue Clients	2	Detail
Adhoc Rogues	12	Detail
Rogues on Wired Network	0	

Top WLANs

Profile Name	# of Clients	
Internal	2	Detail
Guest	1	Detail

Most Recent Traps

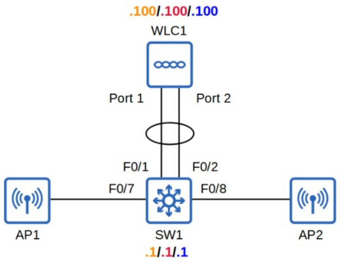
```
Rogue AP: b2:72:bf:78:81:39 detected on Base Radio MAC: 08:d0:9f:ed:ec:70 Interface no: 0(802.11n(2.4 GHz)) Channel: 11
Noise Profile Failed for Base Radio MAC: 08:d0:9f:ed:ec:70 and slotNo: 0
Rogue AP : 98:60:ca:eb:91:b0  removed from Base Radio MAC : 08:d0:9f:ed:ec:70 Interface no:0(802.11n(2.4 GHz))
Rogue AP : 04:72:95:1c:87:a8  removed from Base Radio MAC : 08:d0:9f:ed:ec:70 Interface no:0(802.11n(2.4 GHz))
Rogue AP : 90:a2:5b:e8:fe:b2  removed from Base Radio MAC : 08:d0:9f:ed:ec:70 Interface no:0(802.11n(2.4 GHz))
```

View All

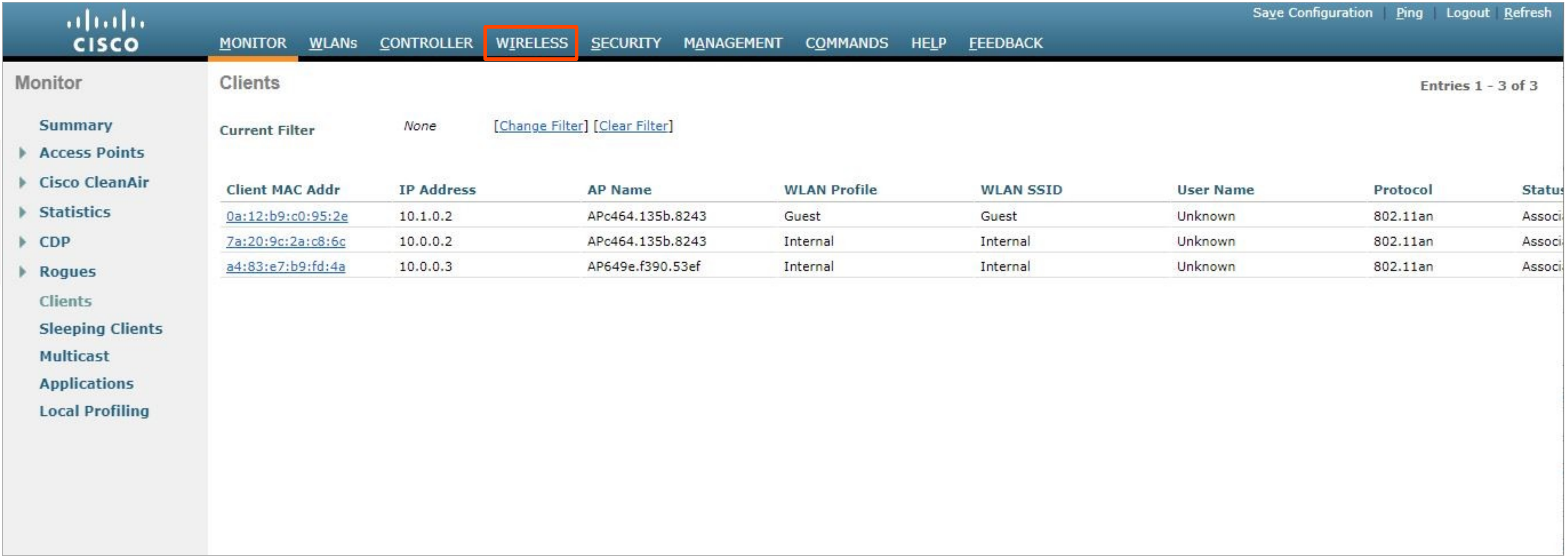
Top Applications

Application Name	Packet Count	Byte Count

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



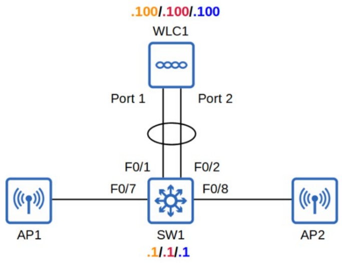
Clients

Entries 1 - 3 of 3

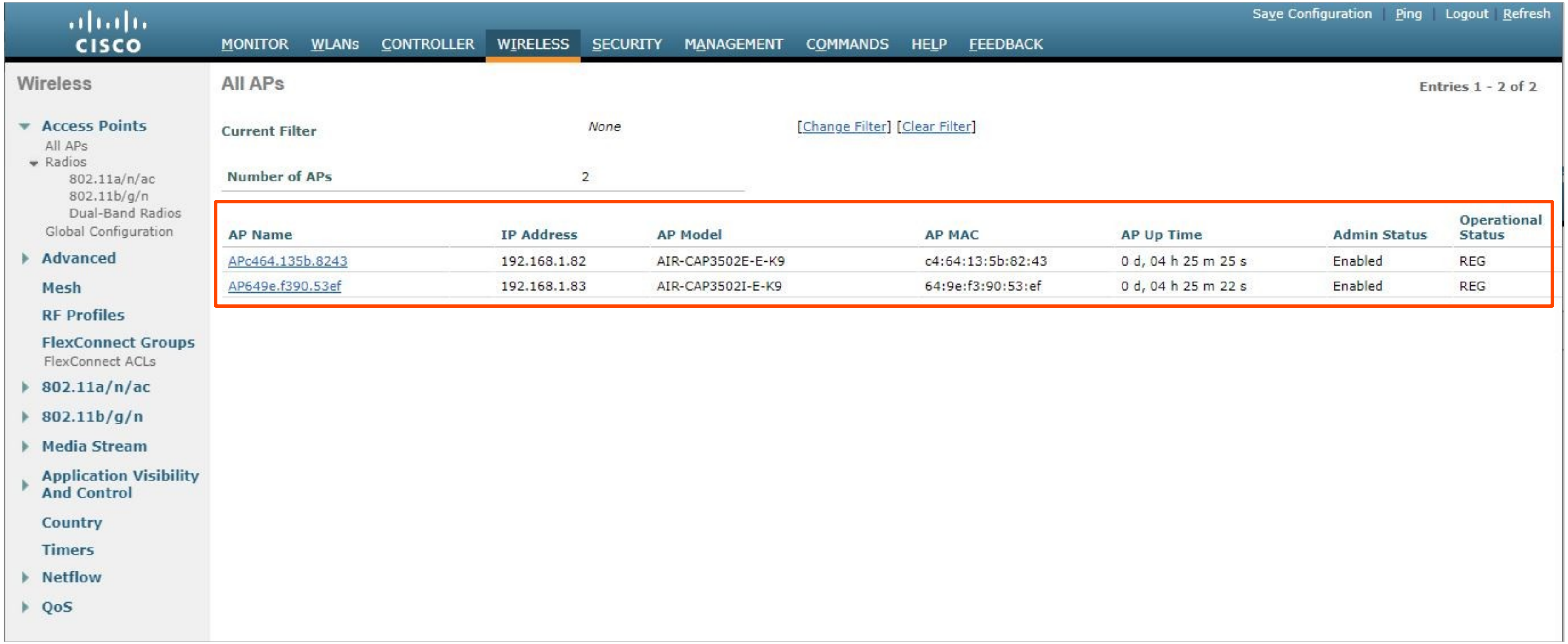
Current Filter None [Change Filter] [Clear Filter]

Client MAC Addr	IP Address	AP Name	WLAN Profile	WLAN SSID	User Name	Protocol	Statu
0a:12:b9:c0:95:2e	10.1.0.2	APc464.135b.8243	Guest	Guest	Unknown	802.11an	Associ
7a:20:9c:2a:c8:6c	10.0.0.2	APc464.135b.8243	Internal	Internal	Unknown	802.11an	Associ
a4:83:e7:b9:fd:4a	10.0.0.3	AP649e.f390.53ef	Internal	Internal	Unknown	802.11an	Associ

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



All APs

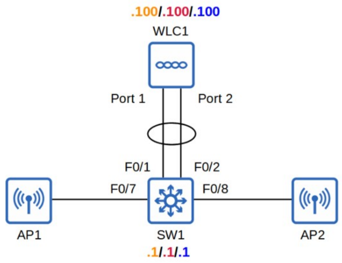
Entries 1 - 2 of 2

Current Filter: None [Change Filter] [Clear Filter]

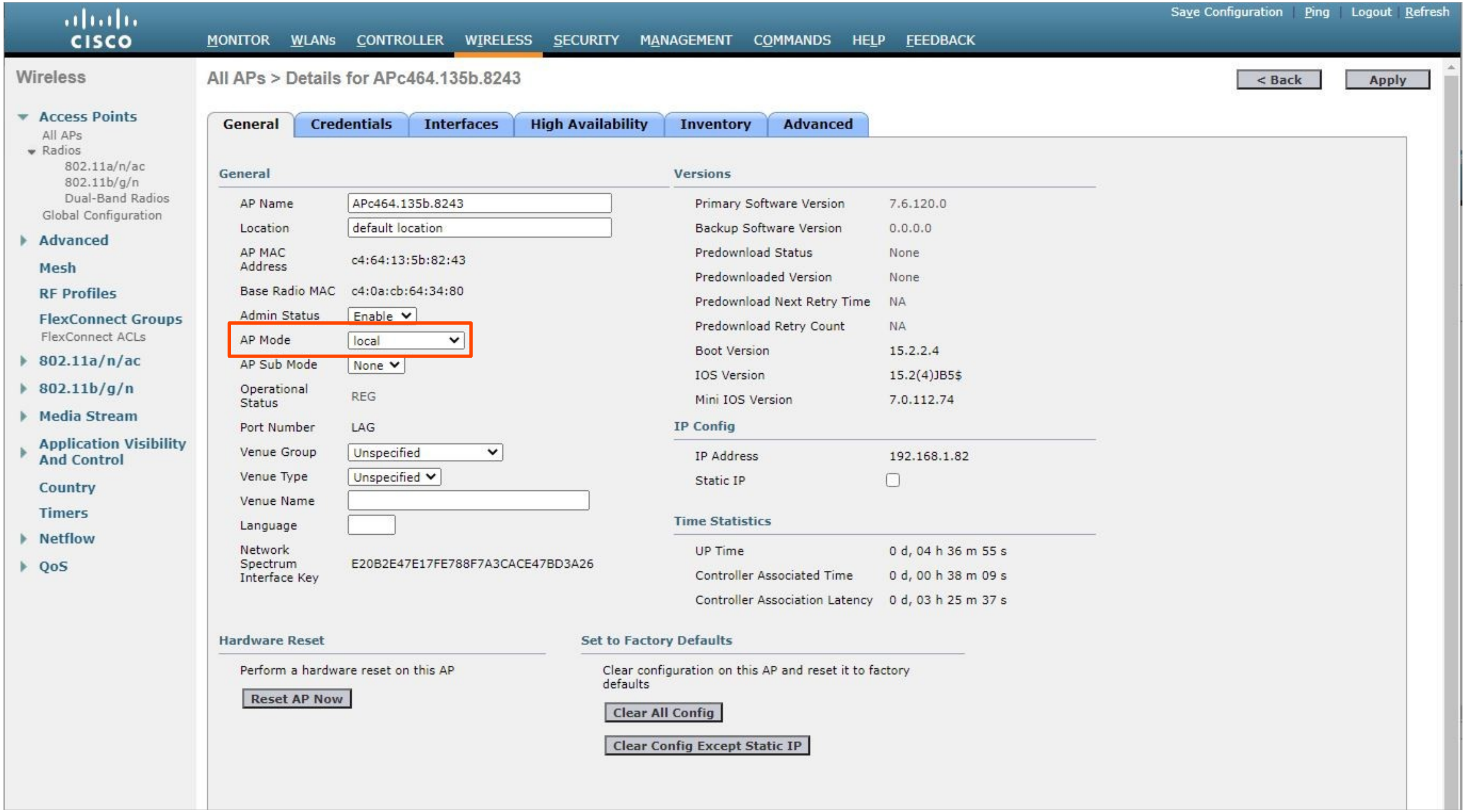
Number of APs: 2

AP Name	IP Address	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status
APc464.135b.8243	192.168.1.82	AIR-CAP3502E-E-K9	c4:64:13:5b:82:43	0 d, 04 h 25 m 25 s	Enabled	REG
AP649e.f390.53ef	192.168.1.83	AIR-CAP3502I-E-K9	64:9e:f3:90:53:ef	0 d, 04 h 25 m 22 s	Enabled	REG

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



All APs > Details for APc464.135b.8243

General

AP Name	APc464.135b.8243
Location	default location
AP MAC Address	c4:64:13:5b:82:43
Base Radio MAC	c4:0a:cb:64:34:80
Admin Status	Enable
AP Mode	local
AP Sub Mode	None
Operational Status	REG
Port Number	LAG
Venue Group	Unspecified
Venue Type	Unspecified
Venue Name	
Language	
Network Spectrum Interface Key	E20B2E47E17FE788F7A3CACE47BD3A26

Versions

Primary Software Version	7.6.120.0
Backup Software Version	0.0.0.0
Predownload Status	None
Predownloaded Version	None
Predownload Next Retry Time	NA
Predownload Retry Count	NA
Boot Version	15.2.2.4
IOS Version	15.2(4)JB5$
Mini IOS Version	7.0.112.74

IP Config

IP Address	192.168.1.82
Static IP	□

Time Statistics

UP Time	0 d, 04 h 36 m 55 s
Controller Associated Time	0 d, 00 h 38 m 09 s
Controller Association Latency	0 d, 03 h 25 m 37 s

Hardware Reset

Perform a hardware reset on this AP

Reset AP Now

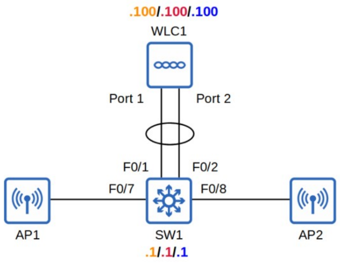
Set to Factory Defaults

Clear configuration on this AP and reset it to factory defaults

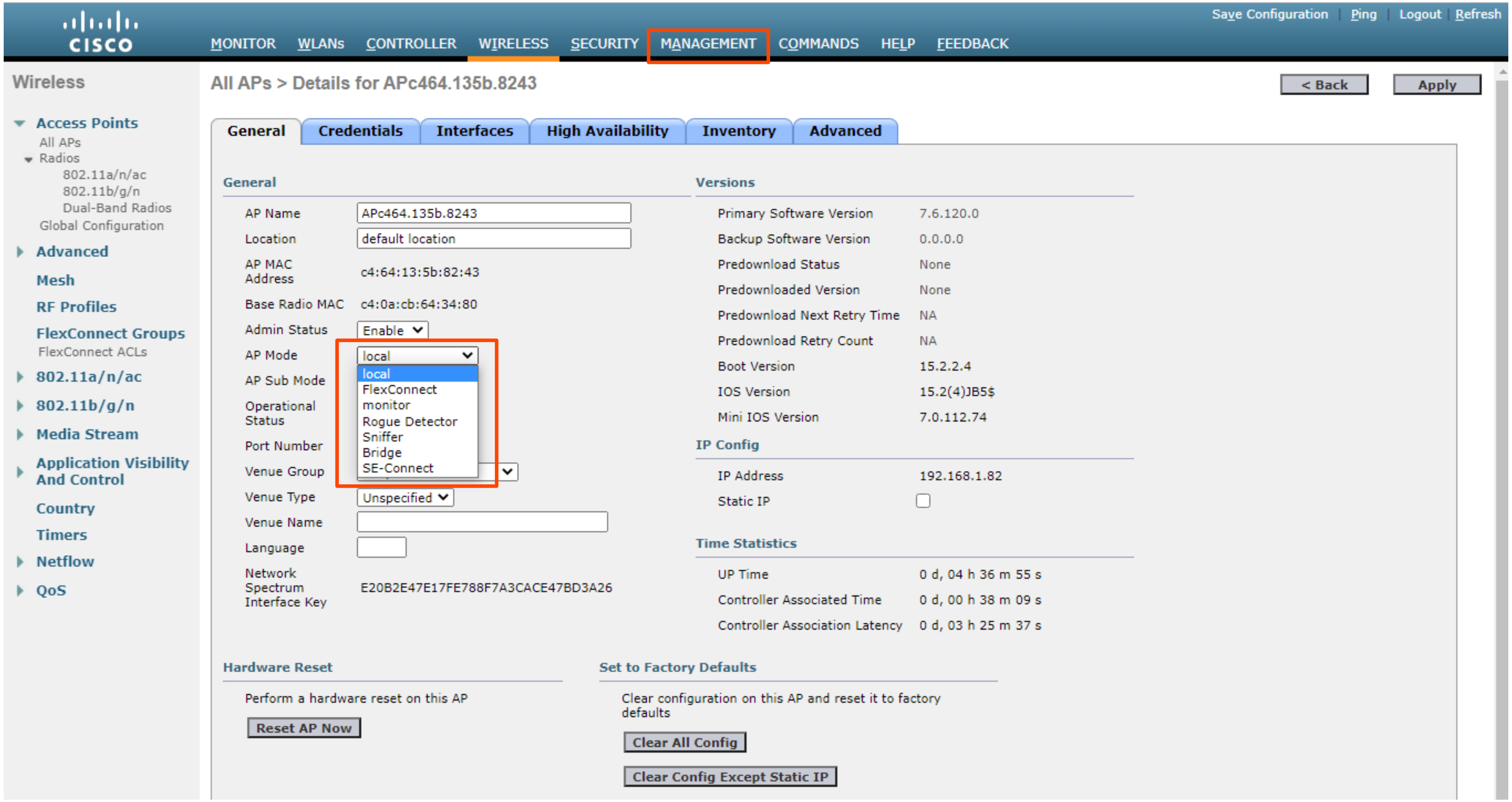
Clear All Config

Clear Config Except Static IP

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



All APs > Details for APc464.135b.8243

General

AP Name	APc464.135b.8243
Location	default location
AP MAC Address	c4:64:13:5b:82:43
Base Radio MAC	c4:0a:cb:64:34:80
Admin Status	Enable
AP Mode	local
AP Sub Mode	
Operational Status	
Port Number	
Venue Group	
Venue Type	Unspecified
Venue Name	
Language	
Network Spectrum Interface Key	E20B2E47E17FE788F7A3CACE47BD3A26

AP Mode options: local, FlexConnect, monitor, Rogue Detector, Sniffer, Bridge, SE-Connect

Versions

Primary Software Version	7.6.120.0
Backup Software Version	0.0.0.0
Predownload Status	None
Predownloaded Version	None
Predownload Next Retry Time	NA
Predownload Retry Count	NA
Boot Version	15.2.2.4
IOS Version	15.2(4)JB5$
Mini IOS Version	7.0.112.74

IP Config

IP Address	192.168.1.82
Static IP	□

Time Statistics

UP Time	0 d, 04 h 36 m 55 s
Controller Associated Time	0 d, 00 h 38 m 09 s
Controller Association Latency	0 d, 03 h 25 m 37 s

Hardware Reset

Perform a hardware reset on this AP

Reset AP Now

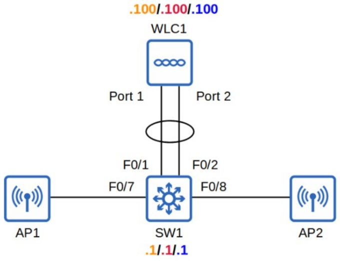
Set to Factory Defaults

Clear configuration on this AP and reset it to factory defaults

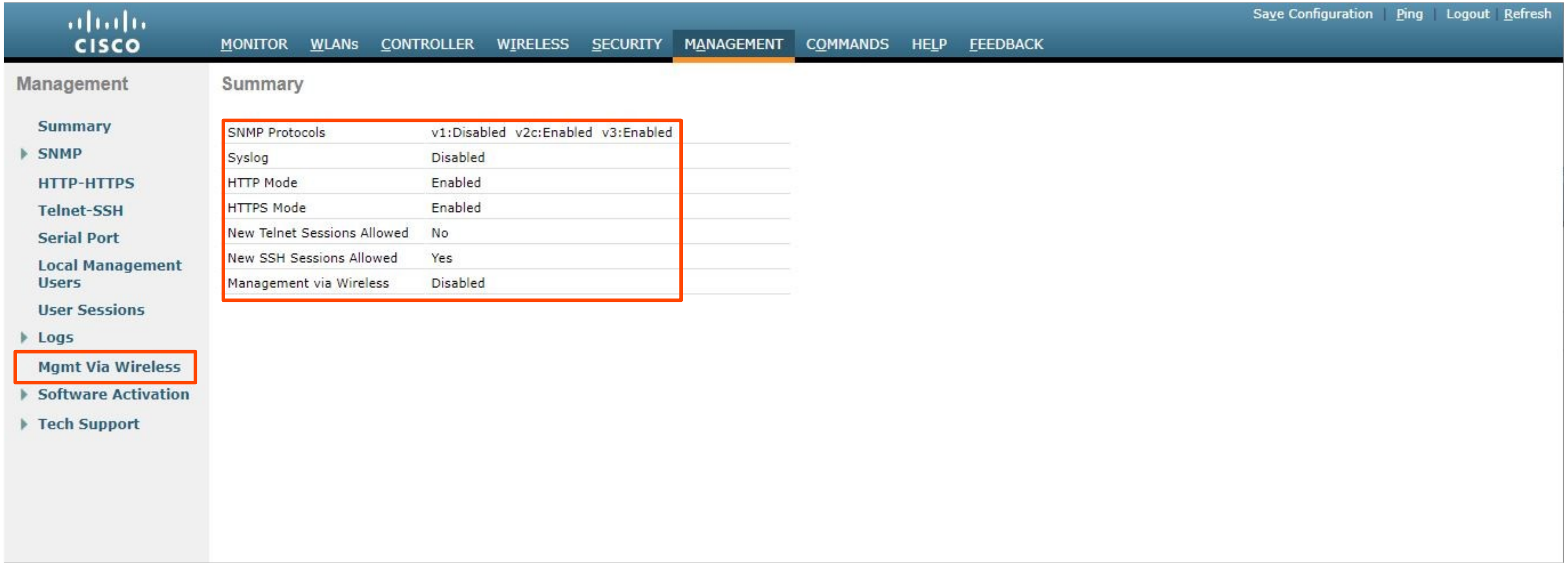
Clear All Config

Clear Config Except Static IP

WLC Configuration

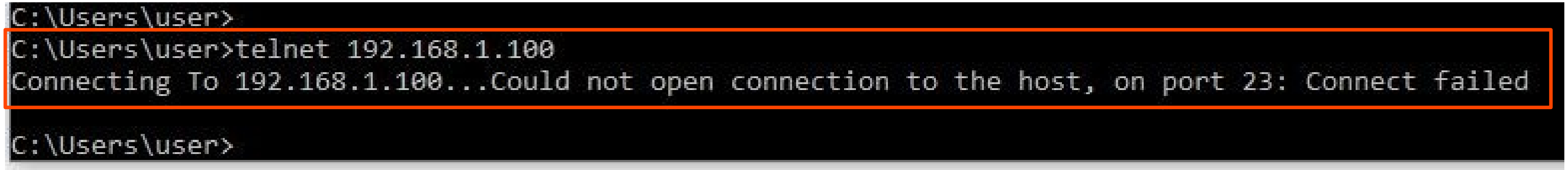


WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



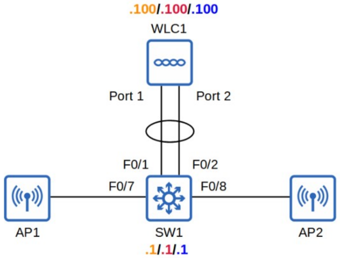
Summary

SNMP Protocols	v1:Disabled v2c:Enabled v3:Enabled
Syslog	Disabled
HTTP Mode	Enabled
HTTPS Mode	Enabled
New Telnet Sessions Allowed	No
New SSH Sessions Allowed	Yes
Management via Wireless	Disabled

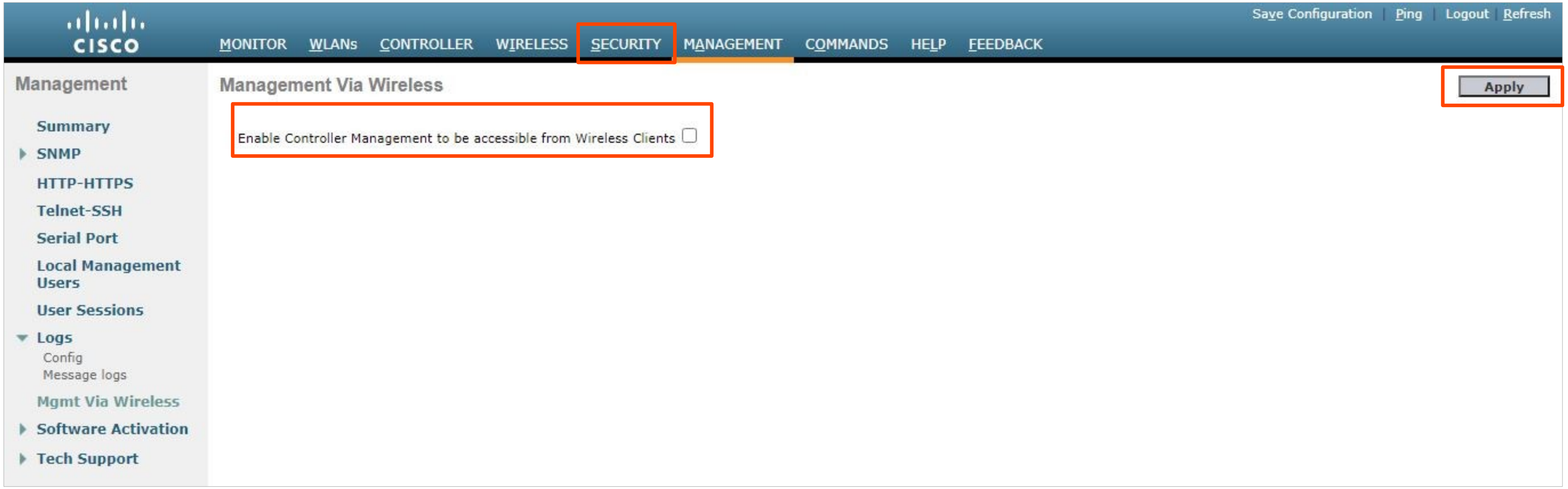


```
C:\Users\user>
C:\Users\user>telnet 192.168.1.100
Connecting To 192.168.1.100...Could not open connection to the host, on port 23: Connect failed

C:\Users\user>
```

WLC Configuration



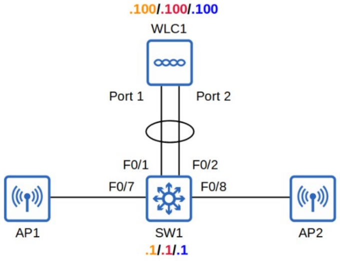
WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



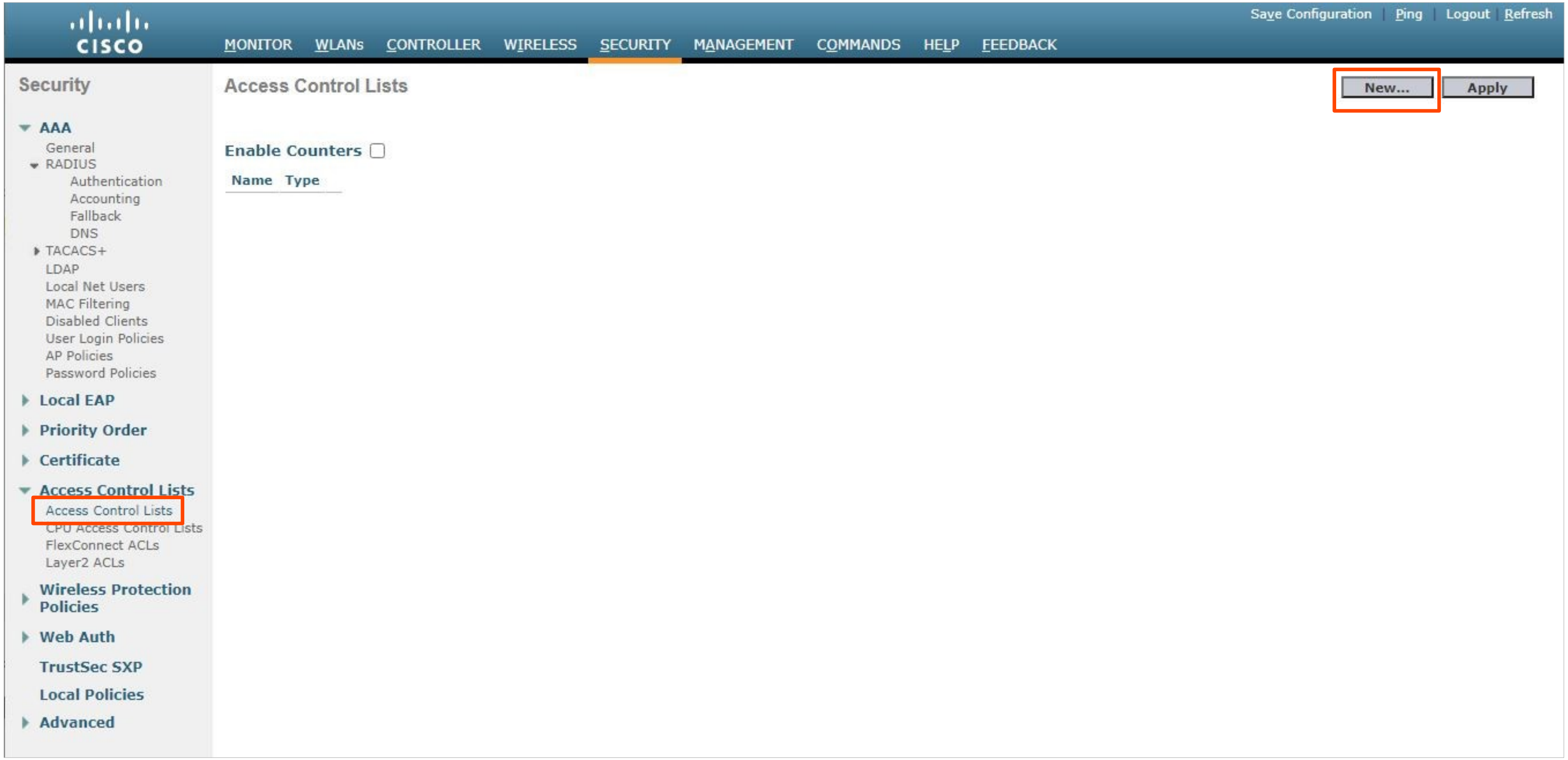
Management Via Wireless

Enable Controller Management to be accessible from Wireless Clients □

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24

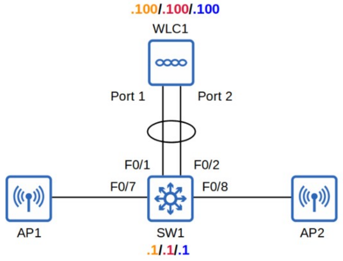


Access Control Lists

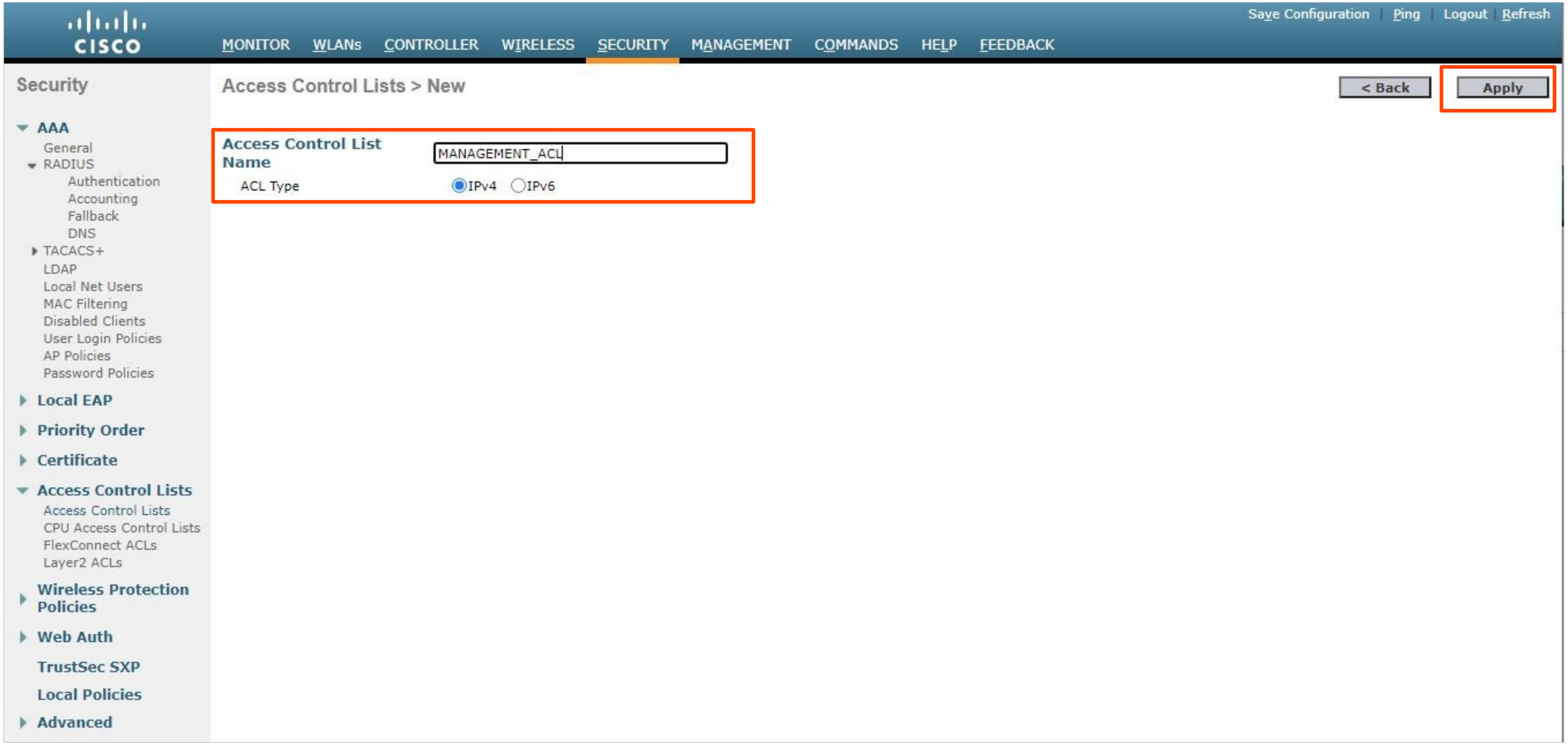
Enable Counters □

Name	Type

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24

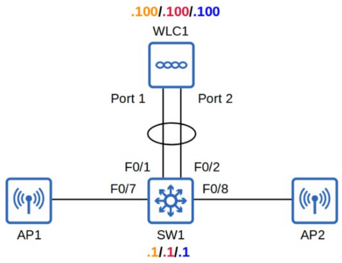


Access Control Lists > New

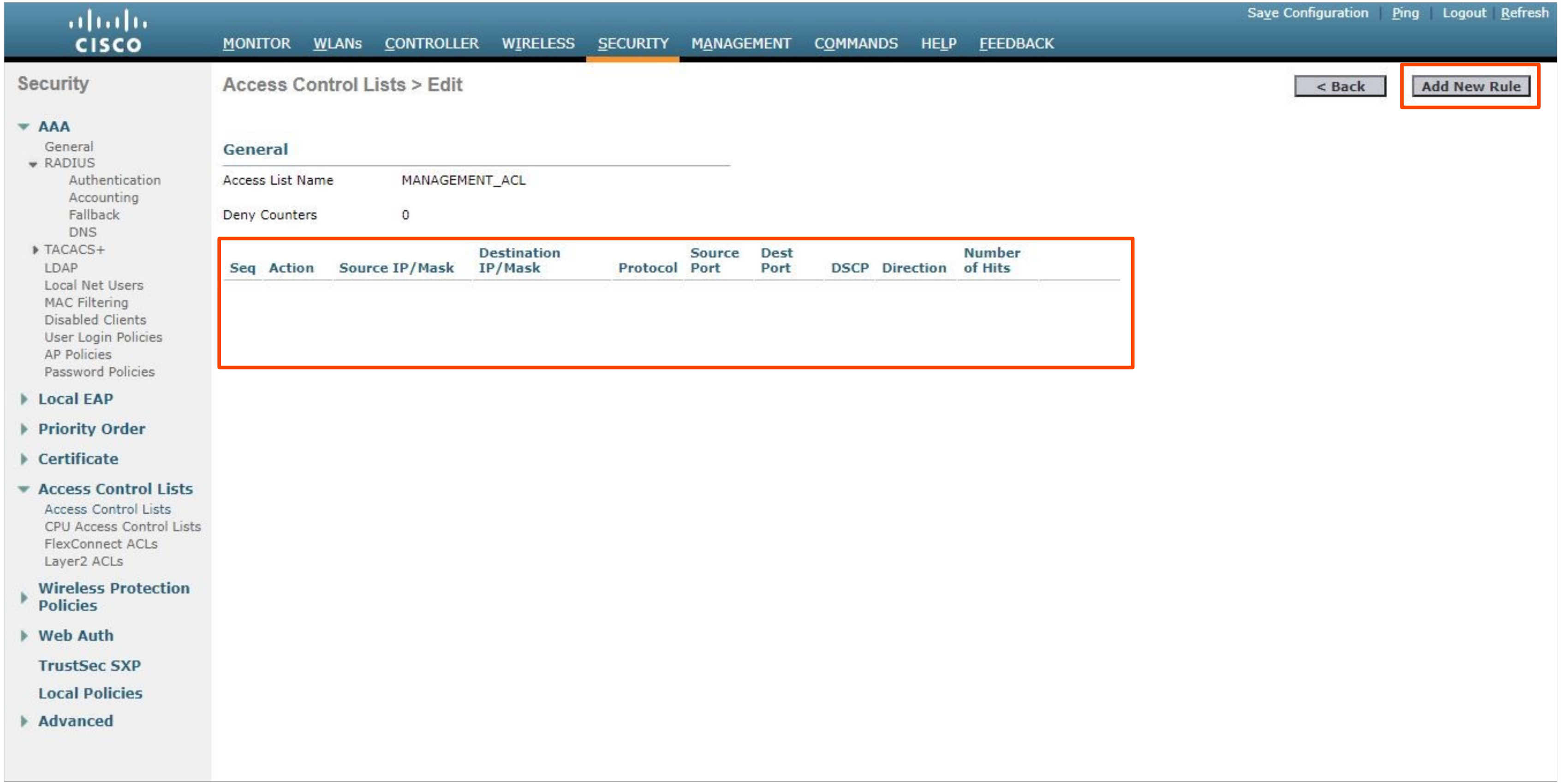
Access Control List Name: MANAGEMENT_ACL

ACL Type ● IPv4 ○ IPv6

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



Access Control Lists > Edit

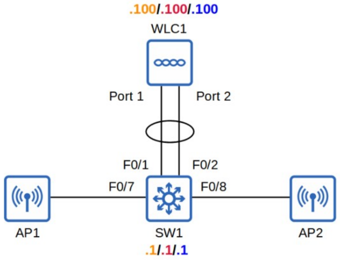
General

Access List Name MANAGEMENT_ACL

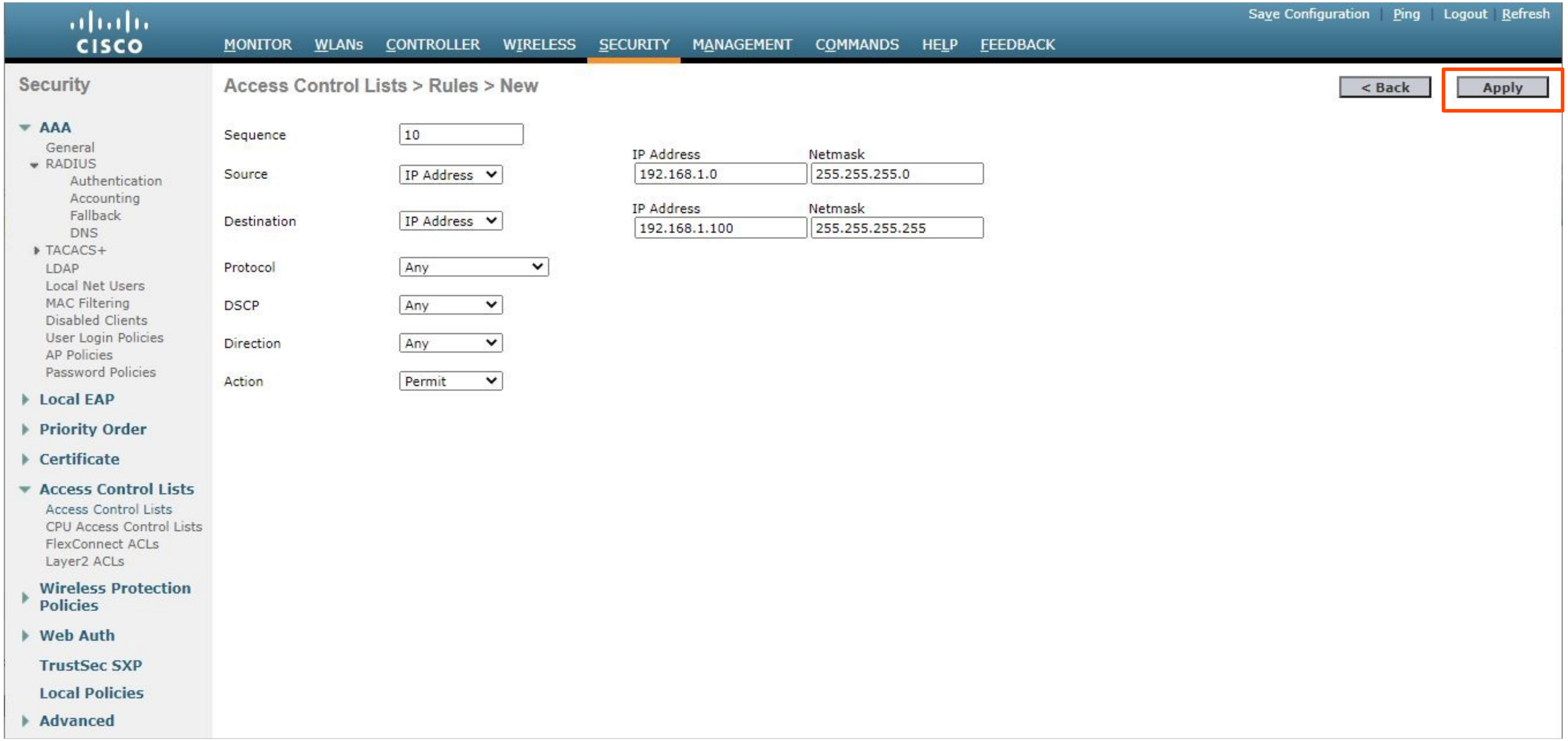
Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits

WLC Configuration



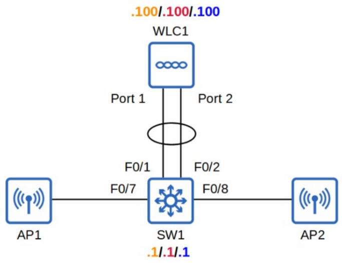
WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



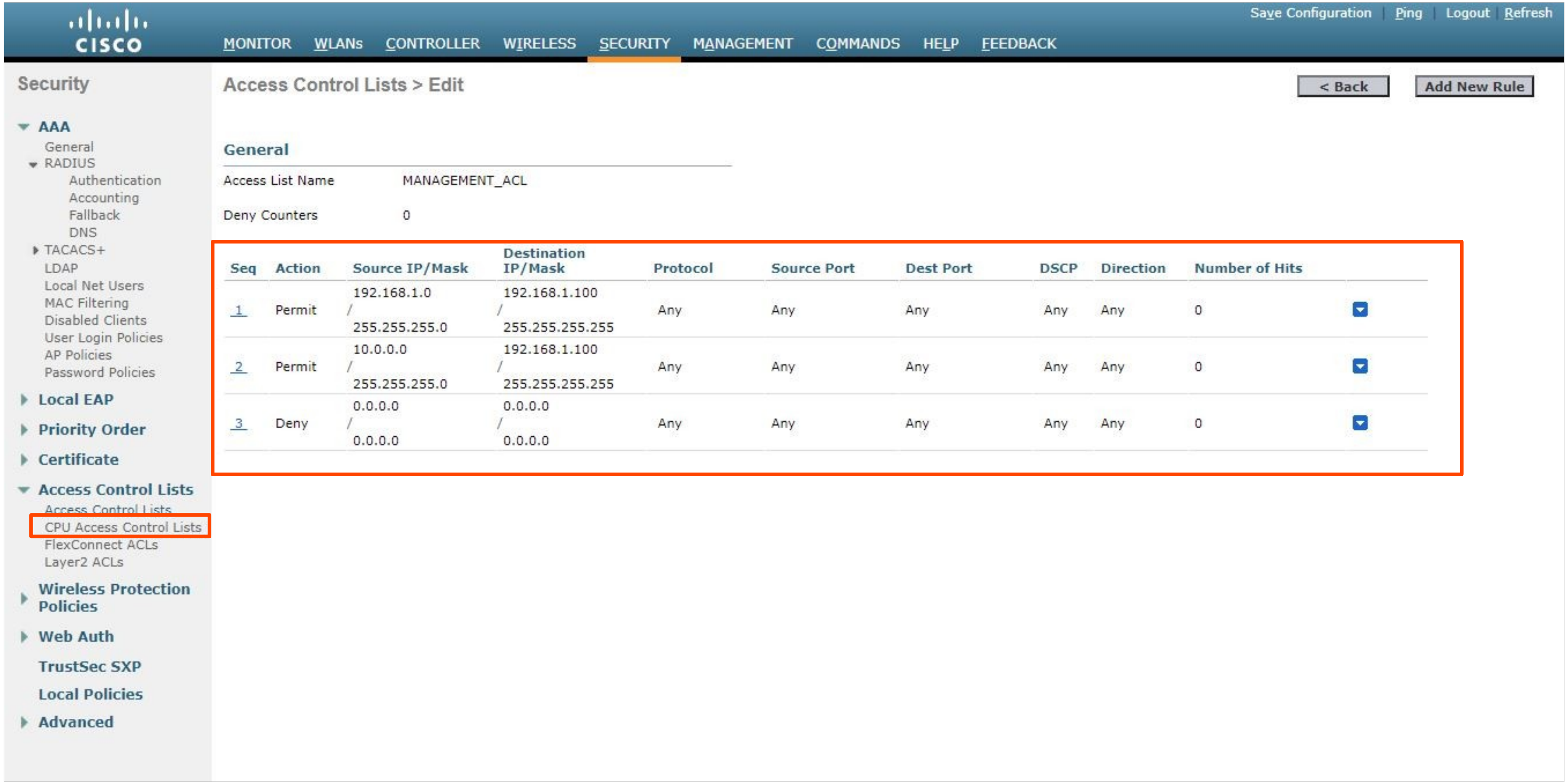
Access Control Lists > Rules > New

Sequence	10		
		IP Address	Netmask
Source	IP Address	192.168.1.0	255.255.255.0
		IP Address	Netmask
Destination	IP Address	192.168.1.100	255.255.255.255
Protocol	Any		
DSCP	Any		
Direction	Any		
Action	Permit		

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



Access Control Lists > Edit

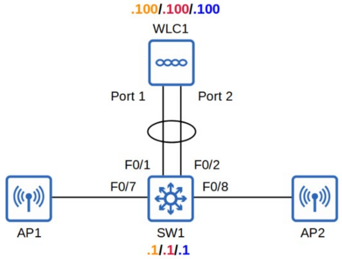
General

Access List Name MANAGEMENT_ACL

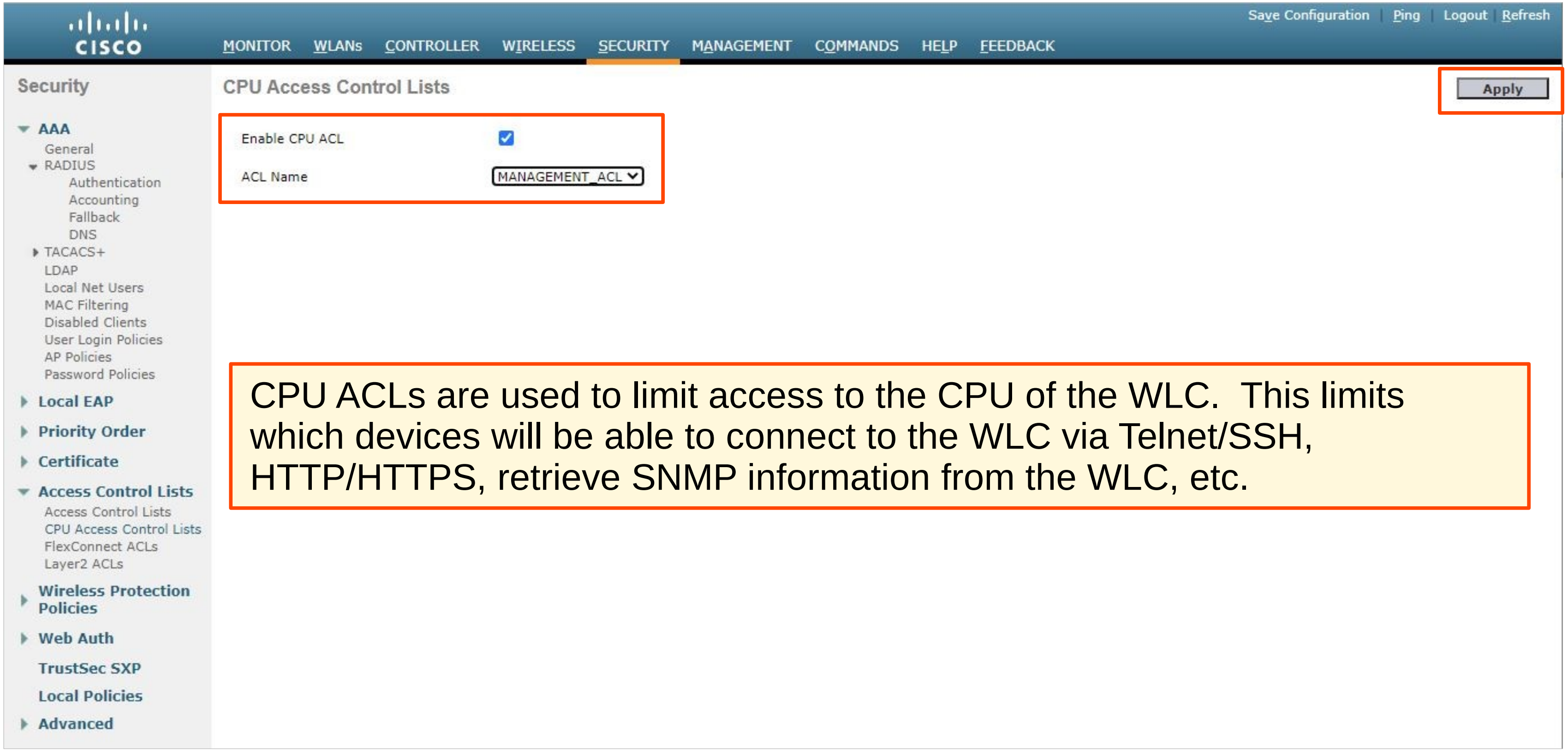
Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	192.168.1.0 / 255.255.255.0	192.168.1.100 / 255.255.255.255	Any	Any	Any	Any	Any	0
2	Permit	10.0.0.0 / 255.255.255.0	192.168.1.100 / 255.255.255.255	Any	Any	Any	Any	Any	0
3	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



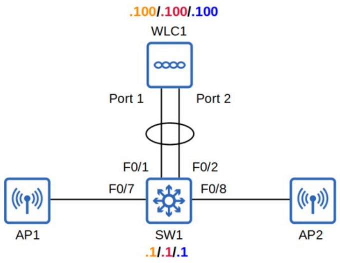
CPU Access Control Lists

Enable CPU ACL ☑

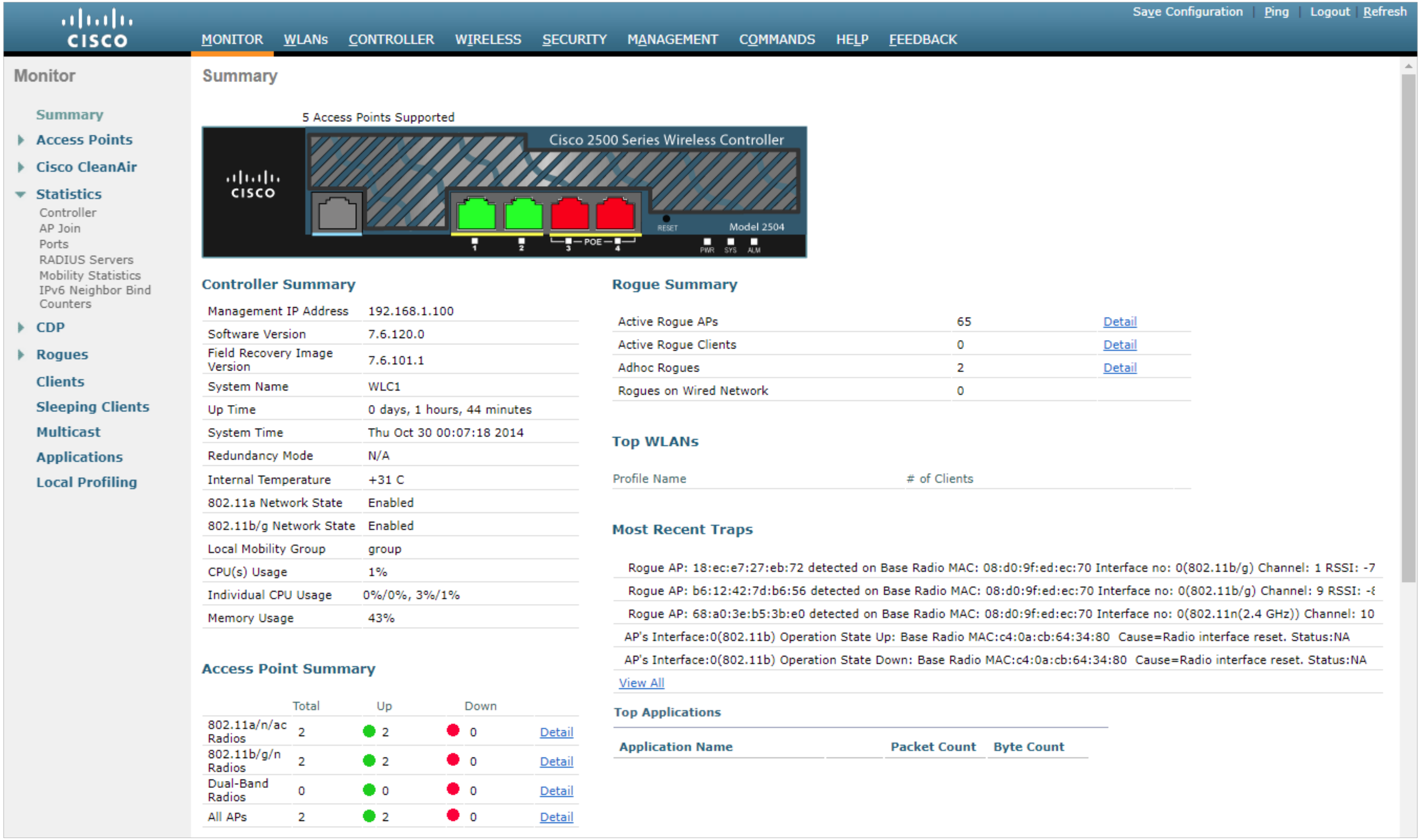
ACL Name MANAGEMENT_ACL

CPU ACLs are used to limit access to the CPU of the WLC. This limits which devices will be able to connect to the WLC via Telnet/SSH, HTTP/HTTPS, retrieve SNMP information from the WLC, etc.

WLC Configuration



WLANs/VLANs
VLAN 10: Management, 192.168.1.0/24
VLAN 100: Internal, SSID: Internal, 10.0.0.0/24
VLAN 200: Guest, SSID: Guest, 10.1.0.0/24



Summary

5 Access Points Supported

Controller Summary

Management IP Address	192.168.1.100
Software Version	7.6.120.0
Field Recovery Image Version	7.6.101.1
System Name	WLC1
Up Time	0 days, 1 hours, 44 minutes
System Time	Thu Oct 30 00:07:18 2014
Redundancy Mode	N/A
Internal Temperature	+31 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	group
CPU(s) Usage	1%
Individual CPU Usage	0%/0%, 3%/1%
Memory Usage	43%

Access Point Summary

	Total	Up	Down	
802.11a/n/ac Radios	2	● 2	● 0	Detail
802.11b/g/n Radios	2	● 2	● 0	Detail
Dual-Band Radios	0	● 0	● 0	Detail
All APs	2	● 2	● 0	Detail

Rogue Summary

Active Rogue APs	65	Detail
Active Rogue Clients	0	Detail
Adhoc Rogues	2	Detail
Rogues on Wired Network	0	

Top WLANs

Profile Name	# of Clients

Most Recent Traps

```
Rogue AP: 18:ec:e7:27:eb:72 detected on Base Radio MAC: 08:d0:9f:ed:ec:70 Interface no: 0(802.11b/g) Channel: 1 RSSI: -7
Rogue AP: b6:12:42:7d:b6:56 detected on Base Radio MAC: 08:d0:9f:ed:ec:70 Interface no: 0(802.11b/g) Channel: 9 RSSI: -8
Rogue AP: 68:a0:3e:b5:3b:e0 detected on Base Radio MAC: 08:d0:9f:ed:ec:70 Interface no: 0(802.11n(2.4 GHz)) Channel: 10
AP's Interface:0(802.11b) Operation State Up: Base Radio MAC:c4:0a:cb:64:34:80  Cause=Radio interface reset. Status:NA
AP's Interface:0(802.11b) Operation State Down: Base Radio MAC:c4:0a:cb:64:34:80  Cause=Radio interface reset. Status:NA
```

View All

Top Applications

Application Name	Packet Count	Byte Count

Things we covered

- Topology introduction
- Switch configuration
- WLC setup
- WLC interface configuration
- WLAN configuration
- Additional WLC features

Quiz 1

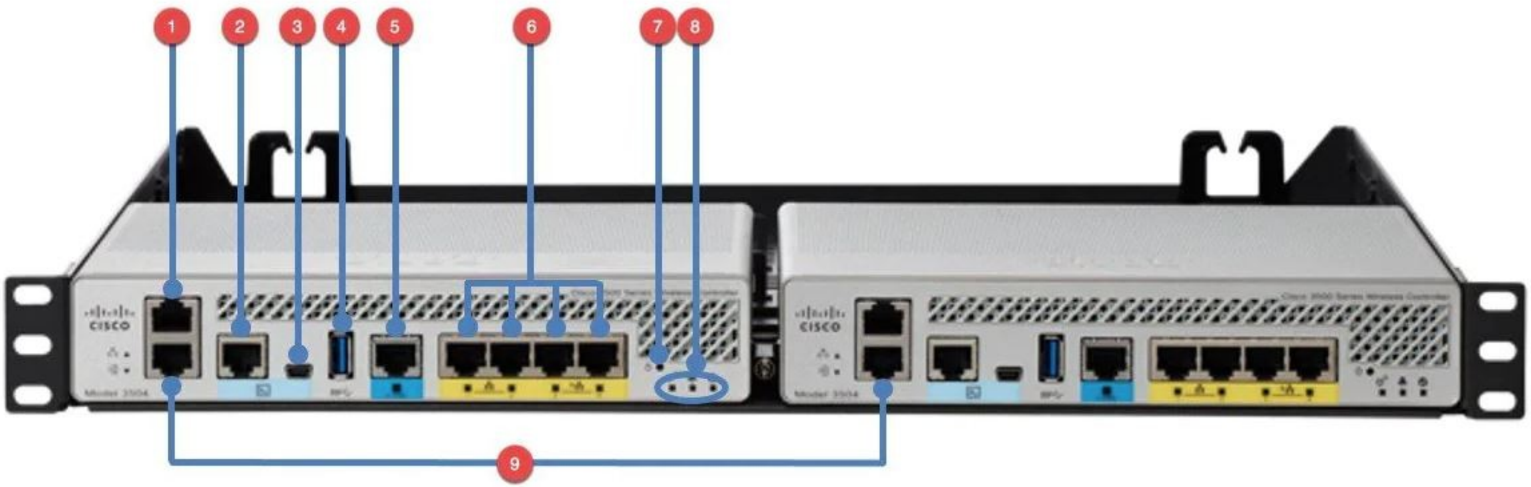
Which WLC port can be used to form an HA pair with another WLC?

a) Distribution system port

b) Redundancy port

c) High Availability port

d) Service port



Quiz 2

Which WLC interface type maps a WLAN to a VLAN?

a) Dynamic interface

b) Virtual interface

c) Distribution system interface

d) Service port interface

Quiz 3

Which of the following is a type of Layer 3 authentication?

a) 802.1X

b) WPA/WPA2

c) Static WEP

d) Web Authentication

Quiz 4

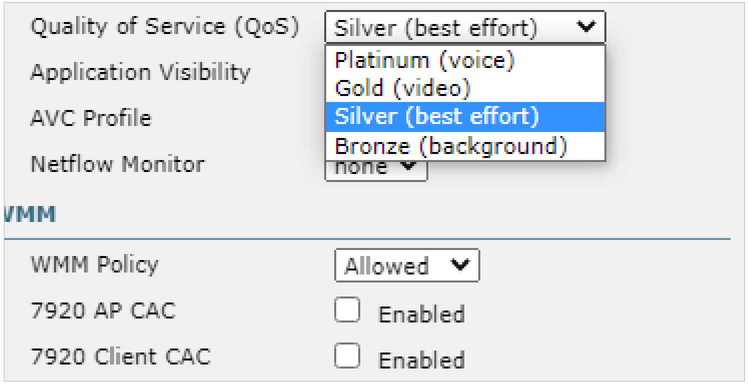
Which WLC QoS setting should be used for video traffic?

a) Platinum

b) Gold

c) Silver

d) Bronze



Quality of Service (QoS) Silver (best effort)

- Platinum (voice)
- Gold (video)
- Silver (best effort)
- Bronze (background)

Application Visibility

AVC Profile

Netflow Monitor none

WMM

WMM Policy Allowed

7920 AP CAC □ Enabled

7920 Client CAC □ Enabled

Quiz 5

Which WLC port type can form a LAG to pass standard data traffic?

a) LAG port

b) Distribution system port

c) Service port

d) Console port