



# 4K/UHD Five-Input Universal Matrix Switcher with Wireless Presentation Link

---

IT Deployment Guide

AT-UHD-SW-510W

Atlona Manuals  
Switchers

## Version Information

---

Version	Release Date	Notes
1	Dec 2017	Initial release
2	Jul 2018	Port numbers updated
3	Sep 2019	Added documentation for configuring AirPlay/Google Cast across multiple VLANs using a Cisco WLC. See Appendix.
4	Oct 2019	Added 1900 (UDP) and 8009 (TCP) Google Cast ports to Network Ports table.
5	Jan 2020	Added documentation on limiting mDNS announcements (“fencing”).

# Table of Contents

---

<b>IT Deployment Guide</b>	<b>4</b>
Introduction	4
Networking Terminology	4
Content Capture	5
Product Security	5
System Access Control and Management	5
Wired and Wireless Network Security	6
Network Ports	6
Obtaining the IP Address of the AT-UHD-SW-510W	7
Deployment Modes	8
Basic Switcher Mode	8
Standalone Wireless Access Point / Hotspot Mode	9
Enterprise Network Mode	10
Dedicated Network Mode	14
WiFi Modes	15
Access Point	15
Connect	15
Disabled	15
Firewall Modes	15
Block Private Network	16
Block Internet	16
Block All	17
None	17
Bandwidth Utilization	18
Chromecast™	18
AirPlay®	19
Miracast™ over Infrastructure	20
<b>Appendix</b>	<b>21</b>
Configuring AirPlay/Google Cast across multiple VLANs using a Cisco WLC	21
Limiting mDNS Announcements	26
mDNS Fencing Overview	26
NOTICE: Wireless Coverage and Configuration Warning	27
Configuring Access Point Groups	27
Configuring mDNS Policies	30
Verifying Functionality	34

# IT Deployment Guide

---

## Introduction

The Atlona **AT-UHD-SW-510W** is a 5x2, multi-format matrix switcher with wireless presentation capability. It provides universal BYOD (bring your own device) compatibility with HDMI, DisplayPort, and USB-C inputs, plus wireless connectivity for mobile devices. The SW-510W is HDCP 2.2 compliant, and features matrixed or mirrored HDMI and HDBaseT outputs. The HDBaseT output is ideal for use with the Atlona AT-UHD-EX-100CE-RX-PSE HDBaseT receiver, or the AT-HDVS-SC-RX scaling HDBaseT receiver. It also includes automatic input switching and automatic display control capability, both applicable to wired and wireless source connections. This unique multi-format matrix switcher and wireless gateway provides a universal connectivity solution for presentation devices in a wide range of professional AV applications.

The USB-C port on the SW-510W is ideal for newer Mac, Chromebook, and Windows PCs. All inputs and the local HDMI output are compatible with video signals up to 4K/UHD @ 60 Hz with 4:4:4 chroma sampling, as well as data rates up to 18 Gbps. For integration convenience and flexibility, simultaneous 18 Gbps HDMI and 10 Gbps HDBaseT outputs make the SW-510W ideal for various presentation scenarios such as primary and confidence displays in a corporate auditorium or lecture hall. The HDBaseT output extends video, audio, control, and Ethernet up to 100 meters. (For AV signals exceeding 10 Gbps, 4K/UHD video will be subsampled to 4:2:0, or HDR metadata removed for HDBaseT transmission.)

## Networking Terminology

### Enterprise/Corporate Network

A network which the corporate/company employees connect to and has access to all the resources of the company.

### Guest Network

A network that is dedicated only for the guests visiting the company. Typically, guests would be connecting their endpoints (laptops/tablets/mobile) to the Guest Network to get Internet access. Users connected to the Guest Network will not have visibility or access to the Enterprise Network.

### Dedicated Network

In many IT environments, while designing the network, a network administrator may dedicate a separate physical or logical network for AV units. This Dedicated Network may or may not have access to Internet depending on the network design.

### Firewall

A firewall is a device that monitors the incoming and outgoing network traffic and takes a decision whether to allow or block the traffic, based on a defined set of security rules; it acts as a barrier between trusted and untrusted networks. The AT-UHD-SW-510W has an built-in software firewall.

### Wireless Access Point

Wireless Access Point (WAP) is a networking device that creates a Wireless Local Area Network (WLAN) in an office or home. WAPs broadcast a Service Set Identifier (SSID) which is used by the wireless endpoints to connect to the wireless network. In general, a WAP shares an Ethernet connection with the wired network (by connecting to a router/switch), providing access to the entire network. Autonomous Wireless Access Points (AWAP) were the first type of access points to be introduced in the wireless market. They were ideal for small scale wireless networks and were capable of supporting up to 10 to 20 clients. Each autonomous WAP acted as a separate entity and hence had to be managed individually. In an Enterprise Network, which spans across multiple floors, managing autonomous access points is a big challenge for a network administrator. To overcome this challenge, Wireless LAN Controllers were introduced.

### Lightweight Access Points and Wireless LAN Controller

The Wireless LAN Controller (WLC) is the device that helps a network administrator in managing each Lightweight Access Points (LAP). Lightweight Access Points are new-generation Access Points which register themselves with a WLC and depend on WLC for configuration. The LAP sends all management and data packets to the WLC, which handle the switching of packets between wireless endpoints and wired portion of the network. WLC also handles authentication and association of the wireless clients. Entire WLAN configuration is done on the WLC. The LAP downloads the entire configuration from each WLC and act as a wireless interface to the wireless clients.

## Content Capture

The AT-UHD-SW-510W is capable of receiving AV content using only the supported casting protocols. Information is rendered on the local display and played using the analog or digital audio interface. Content is not stored, unless moderator mode is enabled. If moderator mode is enabled, then the AT-UHD-SW-510W will receive AV streams and store the first intraframe (I-frame) and following P-frames for each stream until the new I-frame arrives. Once this occurs, all previous frames will be removed. The AT-UHD-SW-510W will also generate an image of the I-frame and will have it available to be called through the API. The concept is to incorporate a method of control which allows the moderator to decide on which content is to be displayed.

## Product Security

The AT-UHD-SW-510W delivers content using either wired or wireless protocols. Depending upon how the AT-UHD-SW-510W is integrated on the network, security will vary.

Encryption	AES-128	WPA2-PSK	None
AirPlay	●	---	---
Googlecast	●	---	---
Miracast P2P	---	●	---
Miracast over Infrastructure	---	---	●

The AT-UHD-SW-510W provides different methods of network deployment, and if it is deployed with Access Point mode enabled, the WPA2-PSK encryption will be applied to all casting protocols as part of Wi-Fi secure layer. The AT-UHD-SW-510W also has Connect Mode and Ethernet mode available whereby security protocol depends on protocol itself, as illustrated in the table above.

## System Access Control and Management

The AT-UHD-SW-510SW can to be configured using the Web GUI or AMS (Atlona Management System). In order to configure the unit, the user is required to enter a password. If the default password is not changed, then the AT-UHD-SW-510W will prompt the user that the default password is being used during the login session.

The AT-UHD-SW-510W allows the user to login to the Web GUI using either the HTTP or HTTPS protocol. In addition, the unit can be configured to restrict the login process to the HTTPS protocol.

The AT-UHD-SW-510W allows user to export and import configuration files and logs. However, all passwords and security certifications will be encrypted.

Physical access to the system via USB keyboard and mouse: It is possible to connect a keyboard and mouse, directly to the AT-UHD-SW-510W, permitting a user to access the system with minimal security permissions. However, no major changes can be performed without a security password. The security password is not provided to any customer. USB ports can be disabled on the AT-UHD-SW-510W (as of firmware 1.1.2 or above), preventing direct connection of a keyboard or mouse.

API communication to the unit is allowed mainly for switch and display control. Username, password, or network changes cannot be performed using the API.

API commands can be sent using Telnet, RS-232, or REST, allowing any or all communication methods to be disabled.

## Wired and Wireless Network Security

The AT-UHD-SW-510SW supports secure authentication to corporate networks through the use of 802.1x standards for both Wifi and Ethernet. The following 802.1x modes are supported:

- EAP-TLS
- TTLS
- PEAP

For information about using the AT-UHD-SW-510W built-in firewall option, refer to [Firewall Modes \(page 15\)](#).

## Network Ports

The following table provides a lists of ports that are required to be open in order to communicate with computer and mobile devices on the same network.

Port	TCP	UDP	Comments
22	Yes	Assigned	Secure Shell (SSH)
23	Yes	Assigned	Telnet
53	Yes	Yes	Domain Name System (DNS)
68	Assigned	Yes	Bootstrap Protocol (BOOTP) client / DHCP
80	Yes	Assigned	Hypertext Transfer Protocol (HTTP)
137	Yes	Yes	NetBIOS Name Service
138	Assigned	Yes	NetBIOS Datagram Service
139	Yes	Assigned	NetBIOS Session Service
443	Yes	Assigned	Hypertext Transfer Protocol over TLS/SSL (HTTPS)
445	Yes	Yes	Microsoft-DS (Directory Services)
520	No	Yes	Routing Information Protocol (RIP)
1900	No	Yes	Google Cast™
5353	Assigned	Yes	Multicast DNS (mDNS)
6000 - 6200	No	Yes	BYOD Protocol Servers*
7000	Yes	No	BYOD Protocol Servers*
7100	Yes	No	BYOD Protocol Servers*
7250	Yes	No	BYOD Protocol Servers*
8009	Yes	No	Google Cast™
47000	Yes	No	BYOD Protocol Servers*

\*These service ports are required in order for Miracast, AirPlay®, and Chromecast™ to function properly.

## Obtaining the IP Address of the AT-UHD-SW-510W

1. Make sure the AT-UHD-SW-510W is powered.
2. Insert a USB drive into the **AUX** port of the AT-UHD-SW-510W.
3. Wait approximately 10 seconds.
4. Remove the USB drive from the **AUX** port insert the drive into an available USB port on a computer.
5. Two files will be present on the USB drive. One file is formatted for Windows and the other is formatted for Linux.

Windows:            AtlonaReport-Win-GWB-20170821200241.txt  
Linux:                AtlonaReport-Unix-GWB-20170821200241.txt

6. Double-click the desired file to open it. Information, similar to the following, will be displayed:

Ethernet #1  
  IP : 192.168.41.68  
  MAC : B8:98:B0:05:7E:73

Ethernet #2  
  IP : 169.254.7.58  
  MAC : B8:98:B0:05:7E:72

7. The IP address of the AT-UHD-SW-510W is listed under Ethernet #1.

## Deployment Modes

The AT-UHD-SW-510W can be deployed in the following modes:

1. **Basic Switcher Mode** (page 8)
2. **Standalone Wireless Access Point / Hotspot Mode** (page 9)
3. **Enterprise Network Mode** (page 10)  
Enterprise mode can be configured in the following variations:
  - a. Wired Mode
  - b. Wireless Mode
  - c. Wired plus Guest Wireless Mode
  - d. Wired plus Wireless with different subnets
4. **Dedicated Network Mode** (page 14)
  - a. Dedicated mode - wired + enterprise mode - wireless

### Basic Switcher Mode

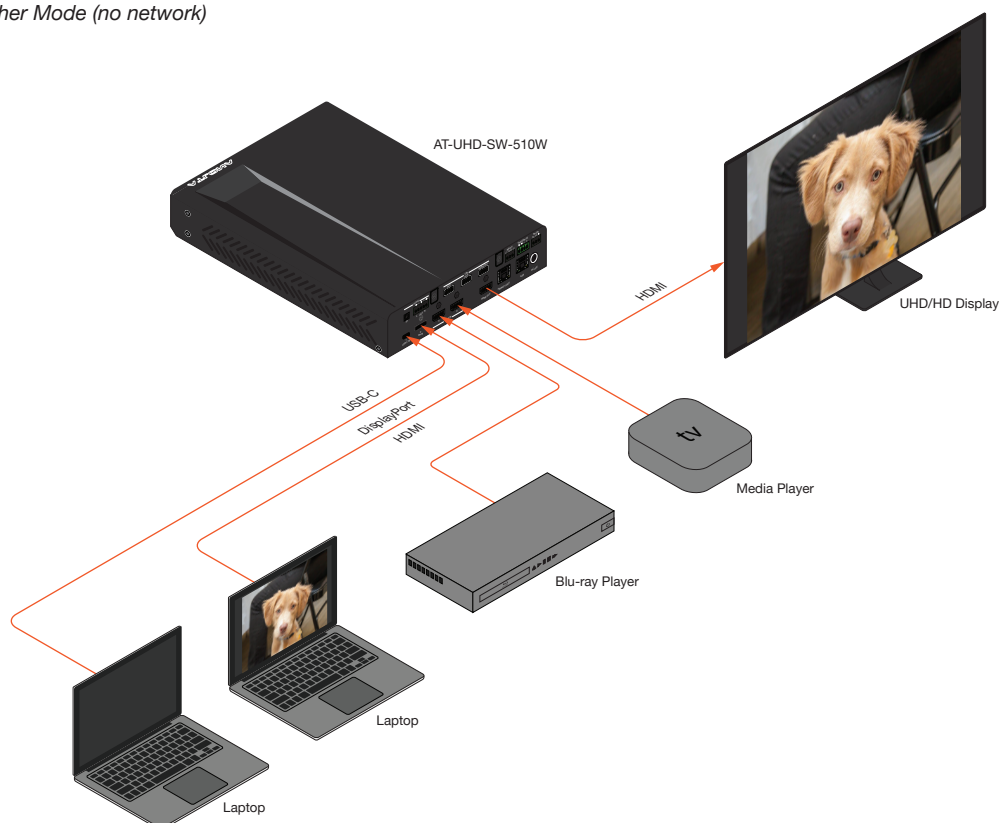
The AT-UHD-SW-510W can be deployed in “standalone” scenario, where the organization doesn’t want to use either network or the wireless BYOD mirroring capabilities of the AT-UHD-SW-510W. In this configuration, the AT-UHD-SW-510W is used as a basic switcher. Refer to *Figure 1*, below.

To boot the AT-UHD-SW-510W in this mode, disconnect the Ethernet cable and wireless USB antennas from the unit and connect the power supply. The unit will boot normally and will continue to act as a 4-input, 1-output switcher.



**NOTE:** In this mode, if the configuration must be changed then it should only be done through RS-232.

Figure 1 - Basic Switcher Mode (no network)





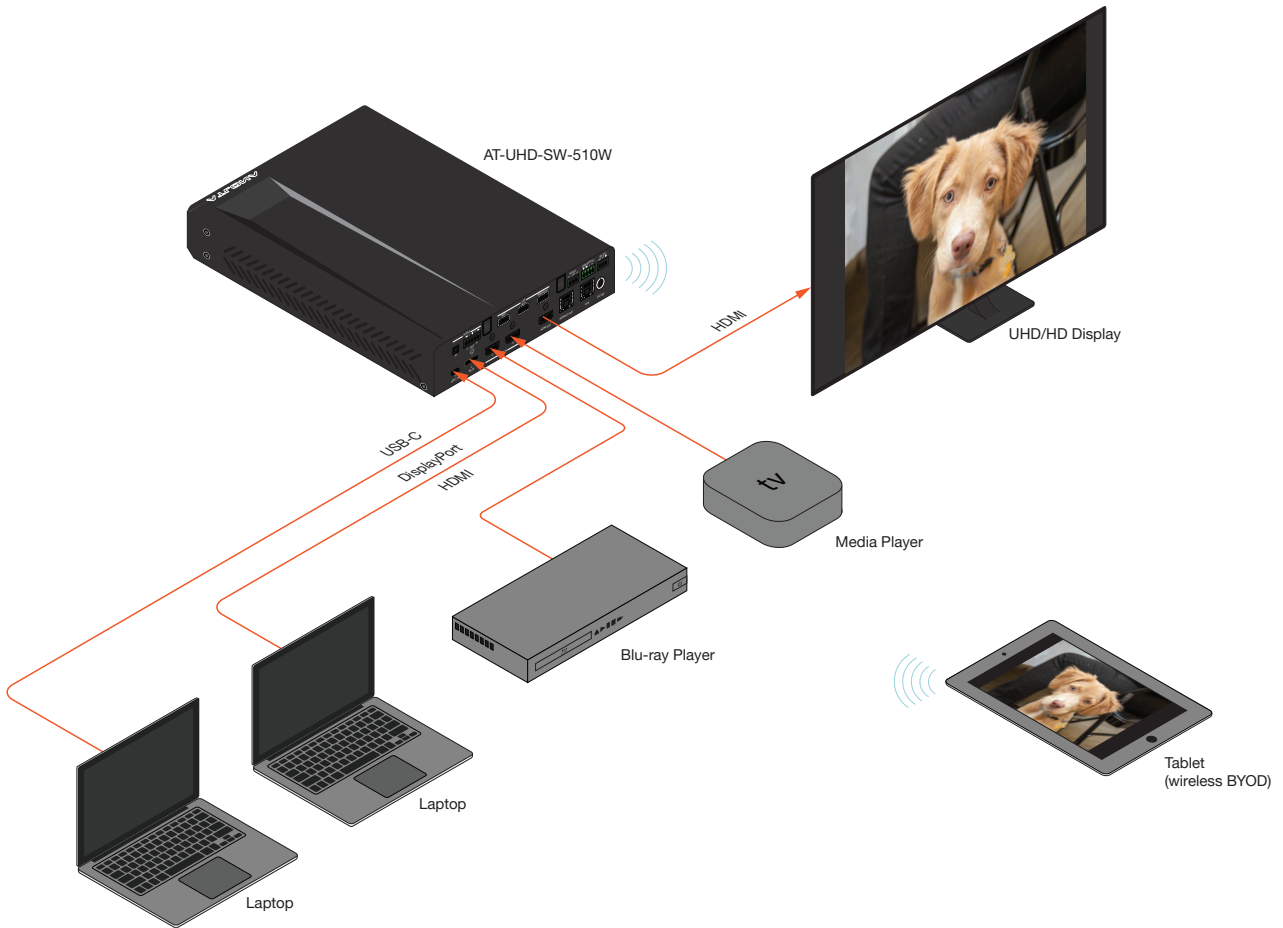
**Standalone Wireless Access Point / Hotspot Mode**

In this mode, the AT-UHD-SW-510W will act as a Standalone Wireless Access Point (WAP) and doesn't have to be physically connected to either the Enterprise or Guest Network. Wireless clients (laptop/tablet/smartphone) can connect to the SSID of the unit and cast their screen, wirelessly.

Users connected to the WAP will not have access to the Internet. Both the wireless SSID and password can be changed through the web GUI of the AT-UHD-SW-510W.

To change the configuration of the AT-UHD-SW-510W in WAP/Hotspot mode, a wireless client connected to the WAP can access the unit using the WAP IP address of the AT-UHD-SW-510W.

Figure 2 - Standalone Wireless Access Point / Hotspot Mode



## Enterprise Network Mode

The AT-UHD-SW-510W can be integrated into the existing Enterprise Network / Guest Network by connecting the AT-UHD-SW-510W through Ethernet or Wireless (in some cases using both) on the unit. In this mode, users that are connected to the Enterprise Network / Guest Network will be able to share their screen content.

The following are variations of Enterprise mode.

### Wired Mode

In this mode, the AT-UHD-SW-510W will be connected to the Enterprise Network through the Ethernet interface present on the unit. The AT-UHD-SW-510W will be assigned an IP address by the DHCP server (if available).

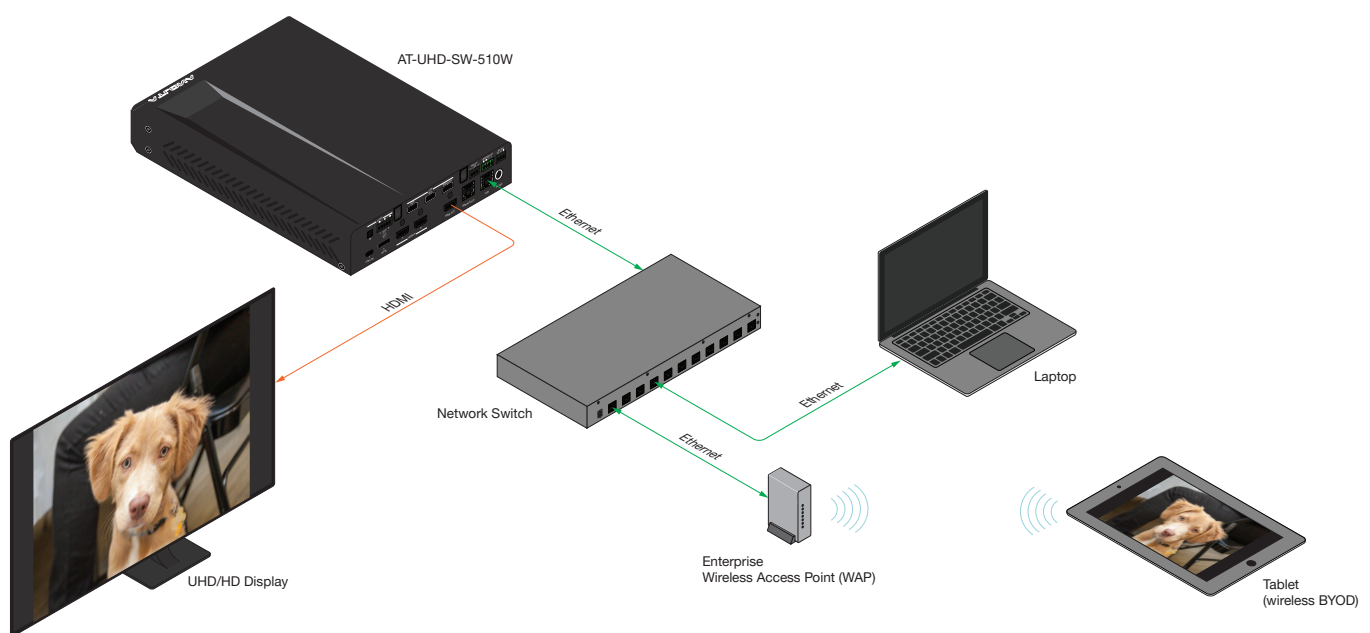
Since the unit is connected to the Enterprise Network, all the users connected to the same network will be able to discover the unit during the screen casting process.

To change the IP configuration of the AT-UHD-SW-510W, open the desired web browser and enter the IP address of the AT-UHD-SW-510W. Refer to [Obtaining the IP Address of the AT-UHD-SW-510W \(page 7\)](#) for information.



**NOTE:** In this mode, the AT-UHD-SW-510W no longer functions as a Access Point. Instead, clients connect to the Enterprise Wireless Access Point. Although not specifically used in this scenario, both antenna modules should remain connected to the AT-UHD-SW-510W and will not interfere with the Enterprise Wireless Access Point. The antenna modules are necessary when using Connect Mode, Access Point Mode, and Miracast, should the unit need to be configured to any of these modes.

Figure 3 - Wired mode



### Wireless Mode

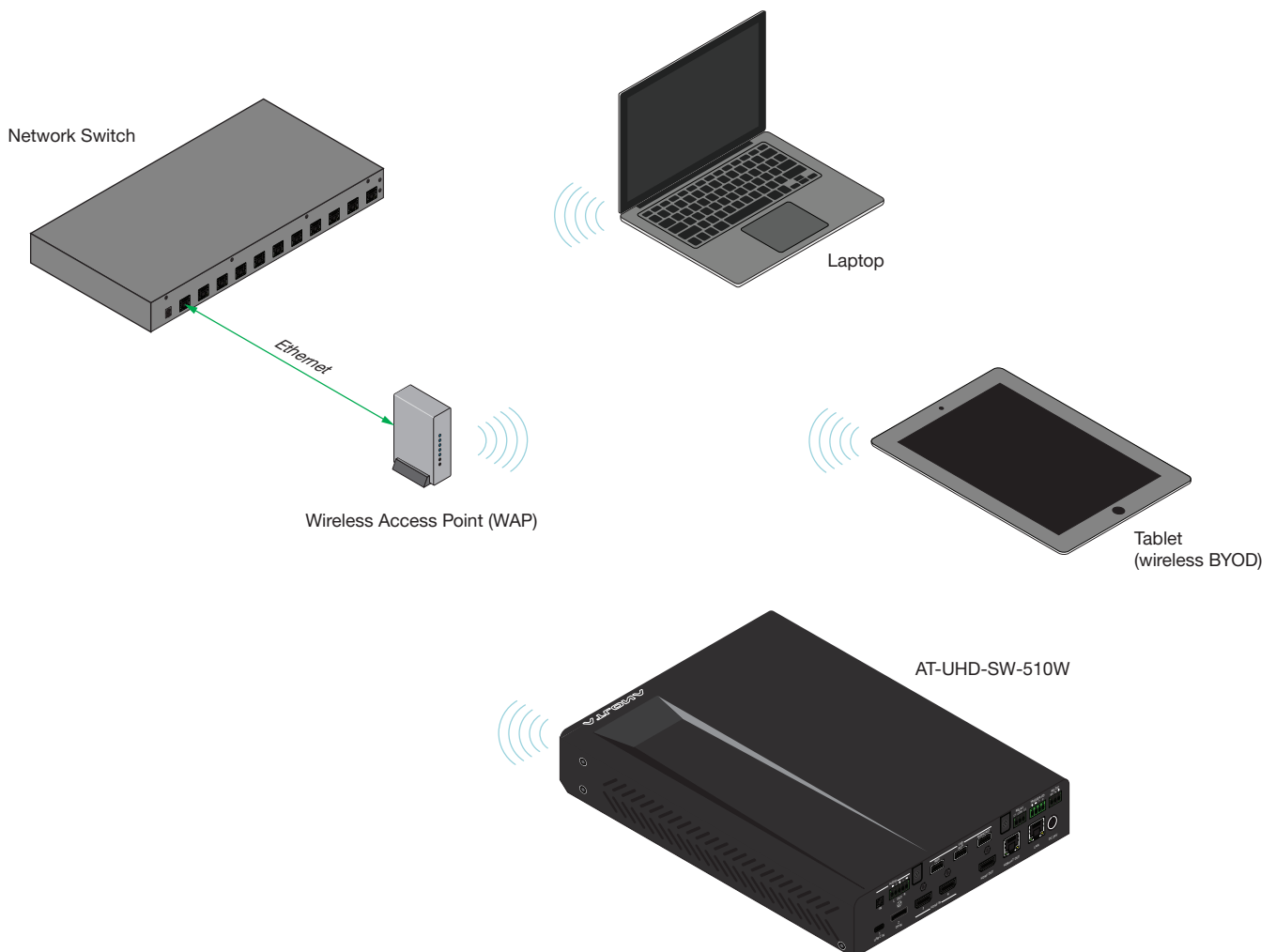
In this mode, the AT-UHD-SW-510W will be connected to the Enterprise Network through the Wireless interface, present on the unit. The Ethernet interface on the unit will not be connected to the network.

To enable this mode, the AT-UHD-SW-510W must already be connected to a network using the Ethernet interface.

1. Login into the web GUI of the AT-UHD-SW-510W. Refer to the User Manual for more information on the login procedure.
2. In the web GUI, click **Administration** > **Networking** from the menu bar on the left.
3. Under the **Wifi** tab, select Connect from the **Mode** drop-down list.
5. Click the **Pick** button.
6. Select the SSID from the list of nearby SSIDs and enter the password.

In this mode, the unit is acting as a Wireless Client and will connect to the nearby Enterprise Wireless Access Point. All the users connected to the Enterprise Wireless Network will be able to discover the unit and cast their screen.

Figure 4 - Wireless Mode

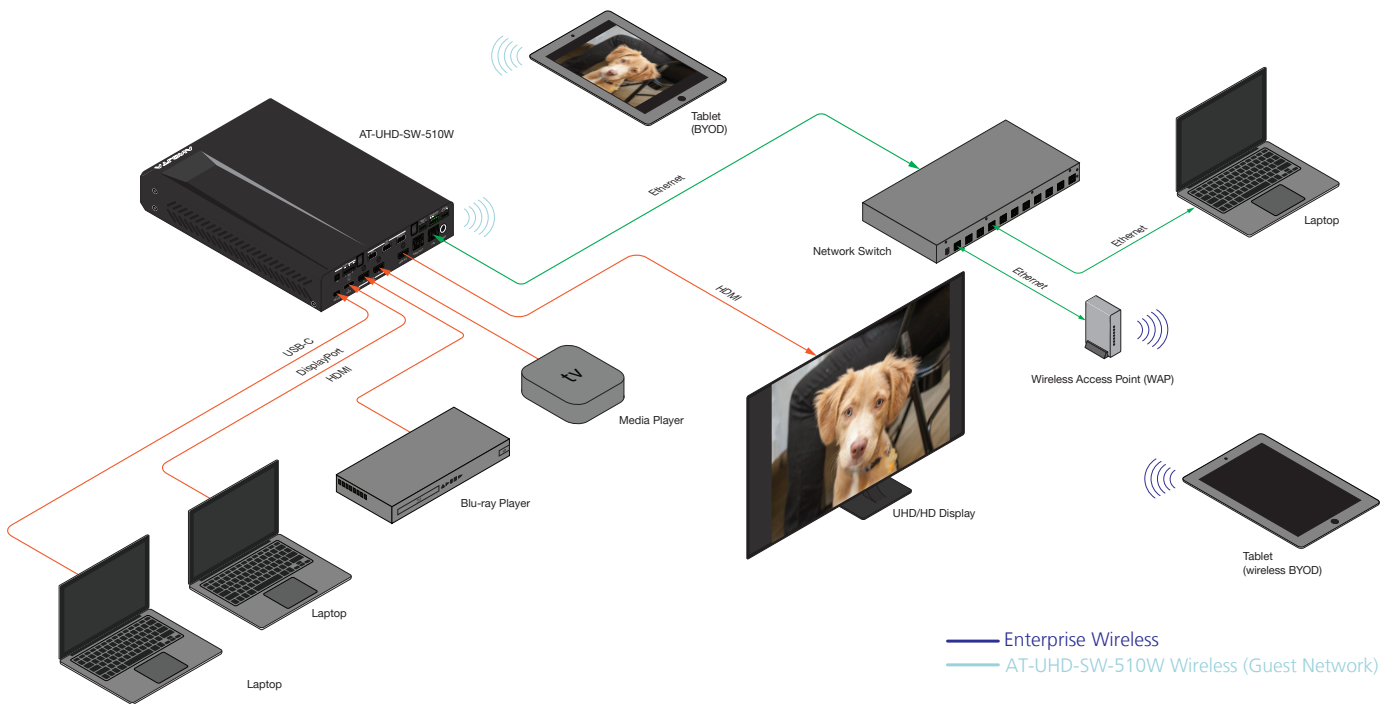


## Wired plus Guest Wireless Mode

To configure environments where both company employees and guests require access, use the Ethernet interface for employees and the wireless network for guests or employees who want to use Miracast™ to mirror their screen. In order to configure the AT-UHD-SW-510W to operate in this mode, connect the Ethernet interface of the AT-UHD-SW-510W to the Enterprise Network and enable WAP.

Enabling both WAP with the Ethernet interface, provides a bridge between these two networks. If the network, connected to the Ethernet of the unit, has Internet access, then this will also allow Internet access to guests. The AT-UHD-SW-510W firewall can be used to block Internet access to guest users. Refer to the [Firewall Modes \(page 15\)](#) section of this guide for more information.

Figure 5 - Wired plus Guest Wireless Mode



## Wired plus Wireless with different subnets

All the above-mentioned scenarios work well, if both wired network and wireless network are in the same network/subnet. But there could be cases where the wired network might be using a different IP addressing scheme when compared to the wireless network.

The biggest challenge in this type of environment is the discovery of the unit from a different wireless network. Wireless casting, like AirPlay®, uses a two-step procedure to communicate with the clients:

1. To discover the unit using DNS-SD (DNS - Service Discovery) / Bonjour and after successful discovery, it will use normal UDP unicast for communication purpose.
2. Since Bonjour / DNS-SD uses a local multicast IP address of 224.0.0.251, it can only work within a single VLAN and cannot propagate between multiple VLANs.

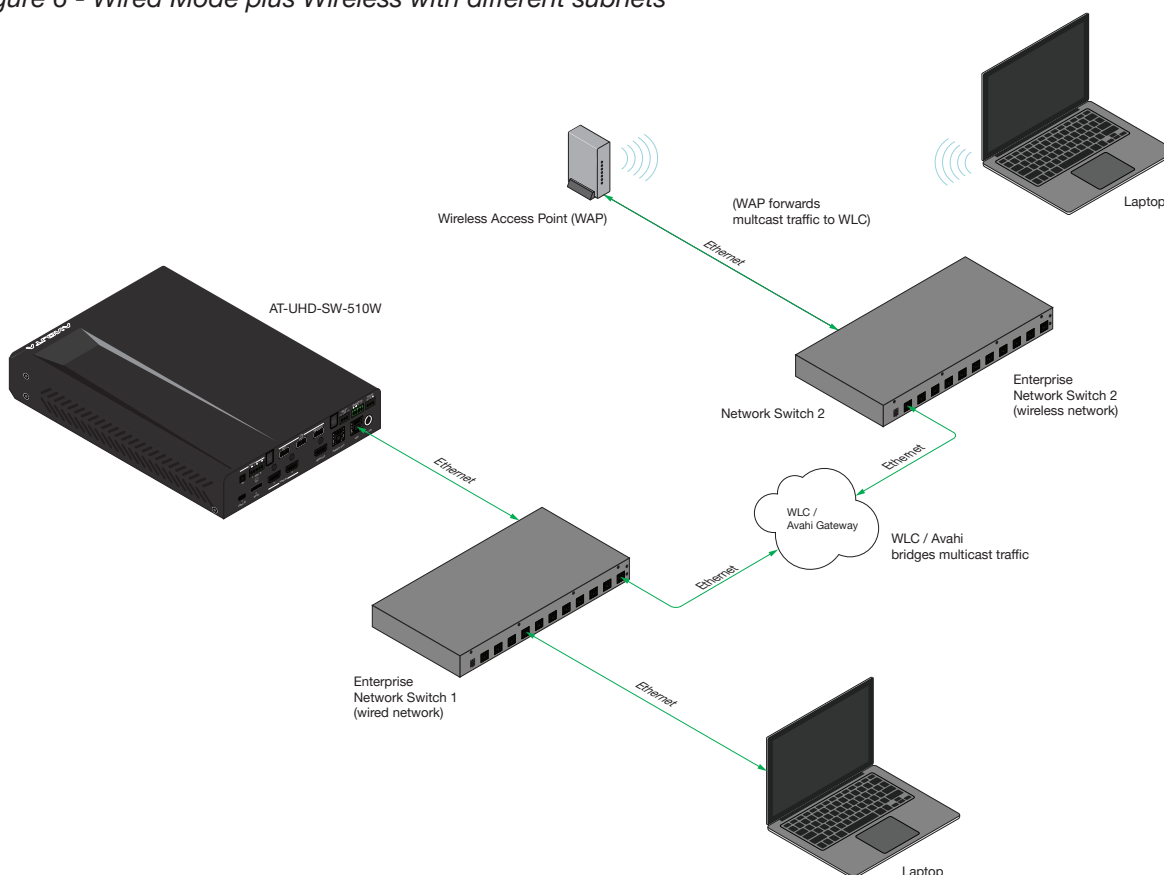
To make the Bonjour/DNS-SD to flow between multiple VLANs, we need to either have multicast routing enabled on the network or have a Wireless LAN Controller (for wireless) that can handle the multicast routing.

For more information on how to configure your Wireless LAN Controller (WLC) to support multicast routing, refer to [Configuring AirPlay/Google Cast across multiple VLANs using a Cisco WLC \(page 21\)](#).

Another method is to create an Avahi Reflector. The Avahi Reflector can be used in the environments where there is no WLC. The Avahi Reflector functions like a bridge between 2 VLANs and helps the unit discover the end points present on a different network. For more information, refer to the following link:

### [Avahi Gateway Setup](#)

Figure 6 - Wired Mode plus Wireless with different subnets



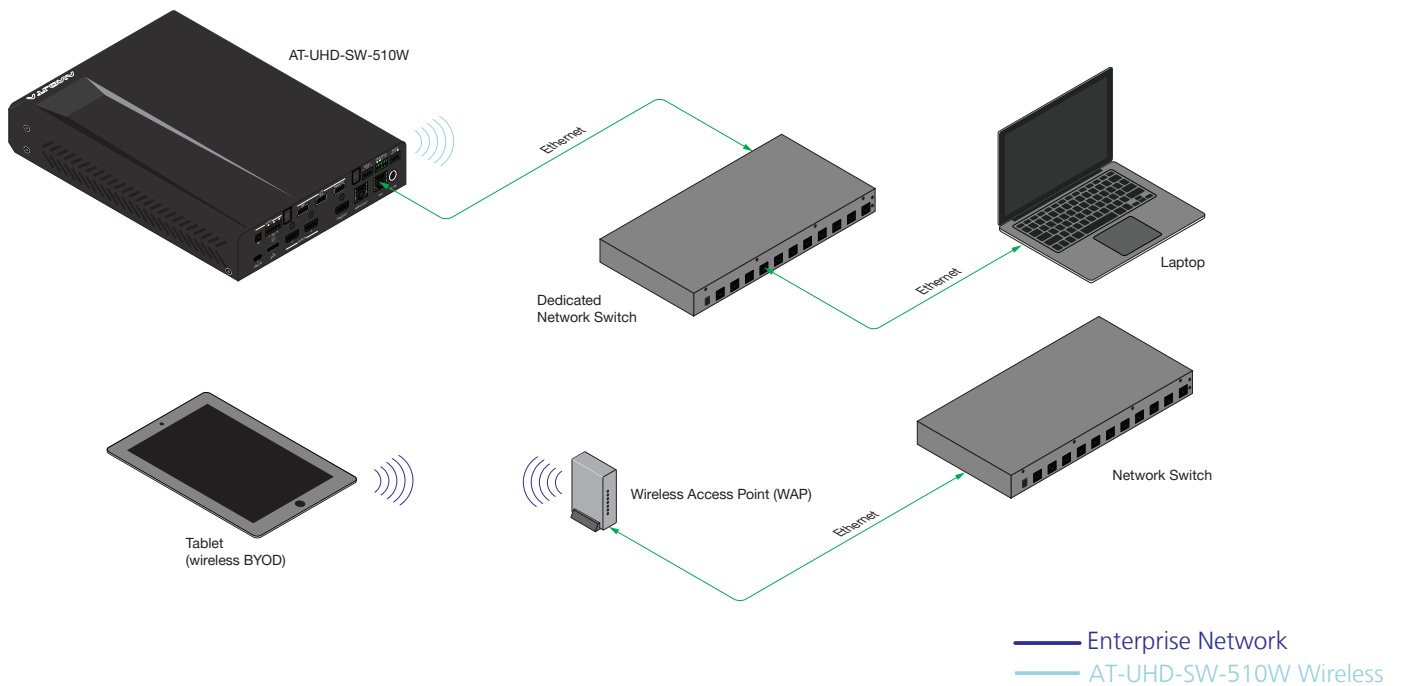
### Dedicated Network Mode

In some environments, an IT administrator may want to dedicate a separate physical switch or logical Virtual LAN configurations for all their AV units. The AT-UHD-SW-510 can be integrated with this Dedicated Network either through Ethernet or a wireless connection (similar to Enterprise modes).

### Wired Mode plus Wireless

If the Dedicated Network is only being used for managing the unit, then in order for company users to cast their screen, connect the AT-UHD-SW-510W to the Wireless SSID of the company. All the users connected to the company Wireless SSID will be able to discover the unit and cast their screen.

Figure 7 - Wired Mode plus Wireless



## WiFi Modes

The AT-UHD-SW-510W has three WiFi modes: Access Point, Connect, and Disabled. To set the WiFi mode, access the web GUI, then go to **Administration > Networking > Wifi**. Refer to the User Manual for more information.

### Access Point

Select this option to configure the AT-UHD-SW-510W as a Wireless Access Point, allowing other wireless devices to connect to the same wired network as the AT-UHD-SW-510W.

### Connect

Select this option to allow the AT-UHD-SW-510W to connect to an available wireless network.

### Disabled

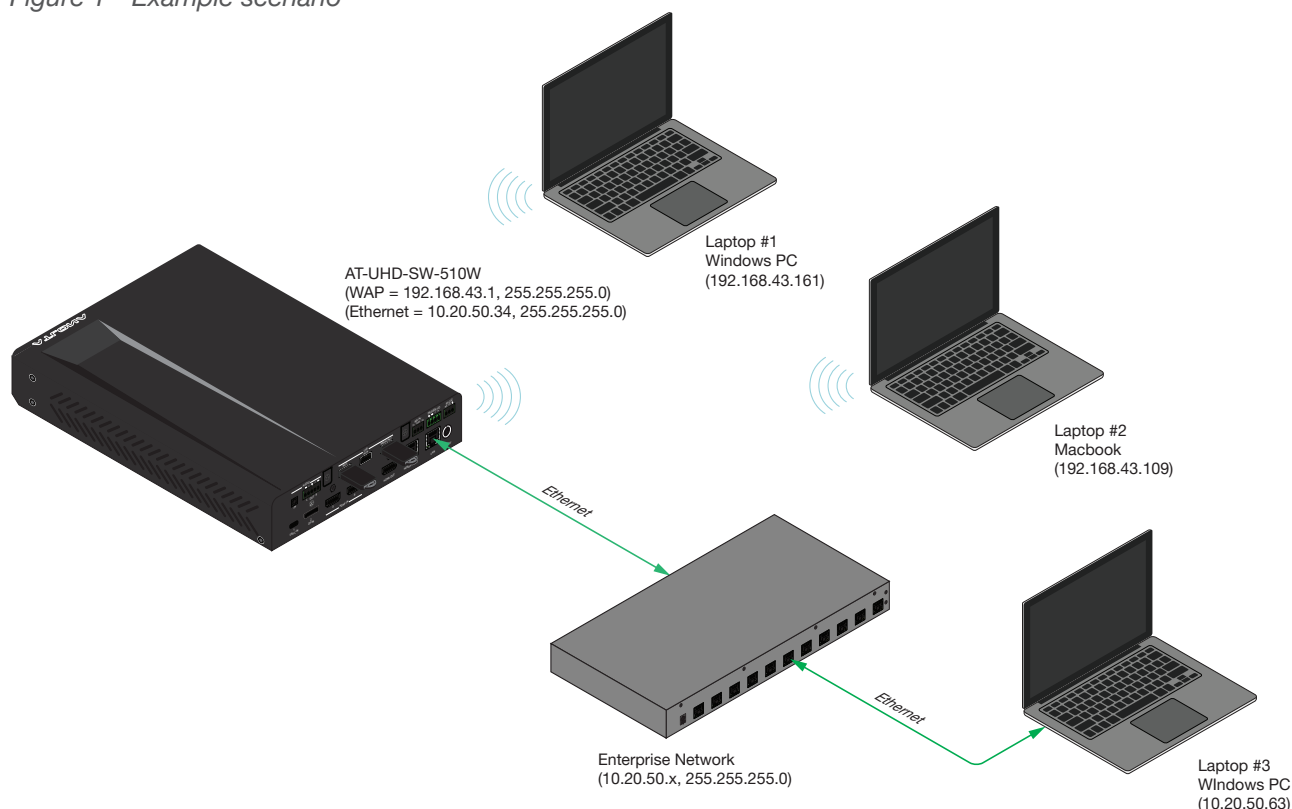
Select this option to disable WiFi on the AT-UHD-SW-510W.

## Firewall Modes

When Access Point is selected from the Wifi **Mode** drop-down list, a **Firewall** drop-down list becomes available. This allows control of incoming and outgoing network traffic. The AT-UHD-SW-510W provides the following firewall modes: Block Private Network, Block Internet, Block All, and None.

The following illustration is an example scenario and can be referenced for each firewall mode, beginning on the next page.

Figure 1 - Example scenario



### Block Private Network

Select this option to block the connected devices from accessing different private networks. It should be noted that this mode does not restrict access within the AT-UHD-SW-510W private network.

- Clients connected to the AT-UHD-SW-510W WAP, will have access to the clients present on the same private network.
- Clients connected to the AT-UHD-SW-510W WAP do not have access to the clients present on the different private network (same network as the Ethernet interface).
- Clients connected to the AT-UHD-SW-510W WAP have access to the Internet.

#### Applied to Figure 1 (page 12):

- Laptop #1 and Laptop #2 can reach one another (same private network).
- Laptop #1 and Laptop #2 cannot reach Laptop #3 (different private network access is blocked).
- Laptop #1 and Laptop #2 have Internet access.

### Block Internet

Select this option to block Internet access (Google, YouTube, etc).

- Clients connected to the AT-UHD-SW-510W WAP do not have access to the Internet.
- Clients connected to the AT-UHD-SW-510W WAP, have access to the clients present on the same private network.
- Clients connected to the AT-UHD-SW-510W WAP, have access to the clients that are present on the different private network (same network as Ethernet interface).

#### Applied to Figure 1 (page 12):

- Laptop #1 and Laptop #2 do not have Internet access.
- Laptop #1 and Laptop #2 can reach one another (same private network).
- Laptop #1 and Laptop #2 can reach Laptop #3 (different private network access is allowed).



## Block All

Select this option to block access to all networks.



**NOTE:** Selecting this option does not prevent access to the AT-UHD-SW-510W and can be accessed using 192.168.43.1 and 10.20.50.34, as shown in the example illustration (Figure 1), on page 9. 192.168.43.1 is the gateway WAP IP Address and 10.20.50.34 is the IP address that the unit received from the DHCP server, on the Enterprise Network.

- Clients connected to the AT-UHD-SW-510W WAP have access to the clients present on the same private network.
- Clients connected to the AT-UHD-SW-510W WAP do not have access to the clients present on different private networks (same network as Ethernet interface).
- Clients connected to the AT-UHD-SW-510W WAP do not have access to the Internet.

### Applied to Figure 1 (page 12):

- Laptop #1 and Laptop #2 can reach one another (same private network).
- Laptop #1 and Laptop #2 cannot reach Laptop #3 (different private network access is blocked).
- Laptop #1 and Laptop #2 do not have Internet access.

## None

Select this option to disable the firewall on the AT-UHD-SW-510W. All incoming and outgoing traffic is permitted.

- All available networks are reachable.
- Clients connected to the AT-UHD-SW-510W WAP, have access to clients that are connected to the same private network.
- Clients connected to the AT-UHD-SW-510W WAP, have access to clients that are connected to the a different private network (same network as Ethernet interface).
- Clients connected to the AT-UHD-SW-510W WAP have Internet access.

### Applied to Figure 1 (page 12):

- Laptop #1 and Laptop #2 can reach one another (same private network).
- Laptop #1 and Laptop #2 can reach Laptop #3 (different bridged private network).
- Laptop #1 and Laptop #2 have access to the Internet (private to public network).

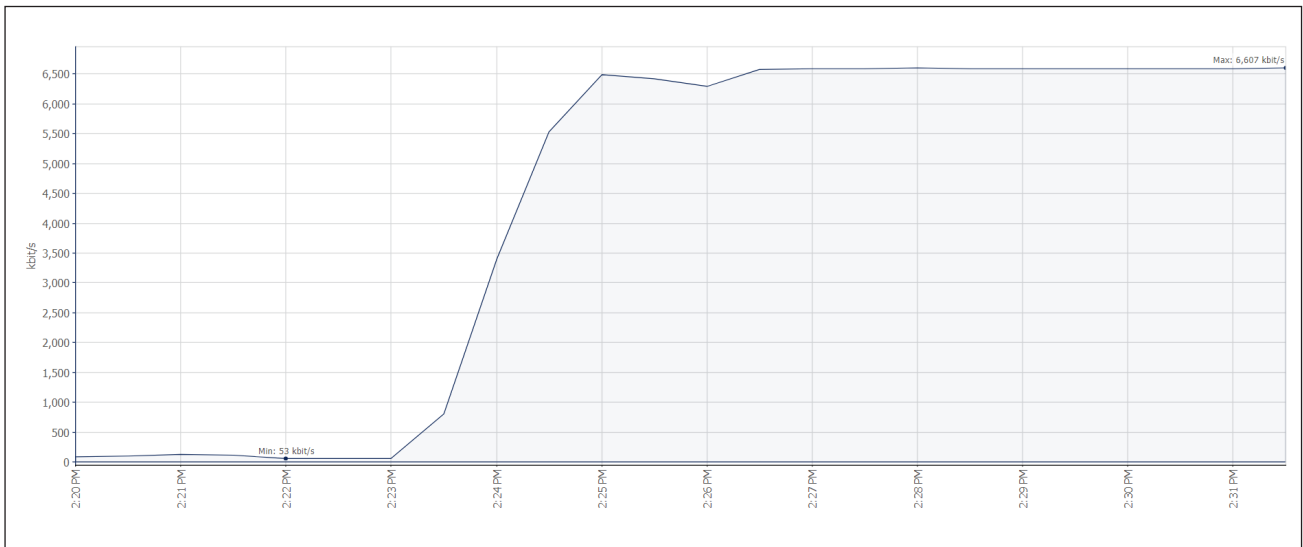
## Bandwidth Utilization

The data below, provides information on bandwidth utilization, based on the casting protocol being used. Both video and document content was used as metrics. Note that these values may vary, depending upon the network environment.

### Chromecast™

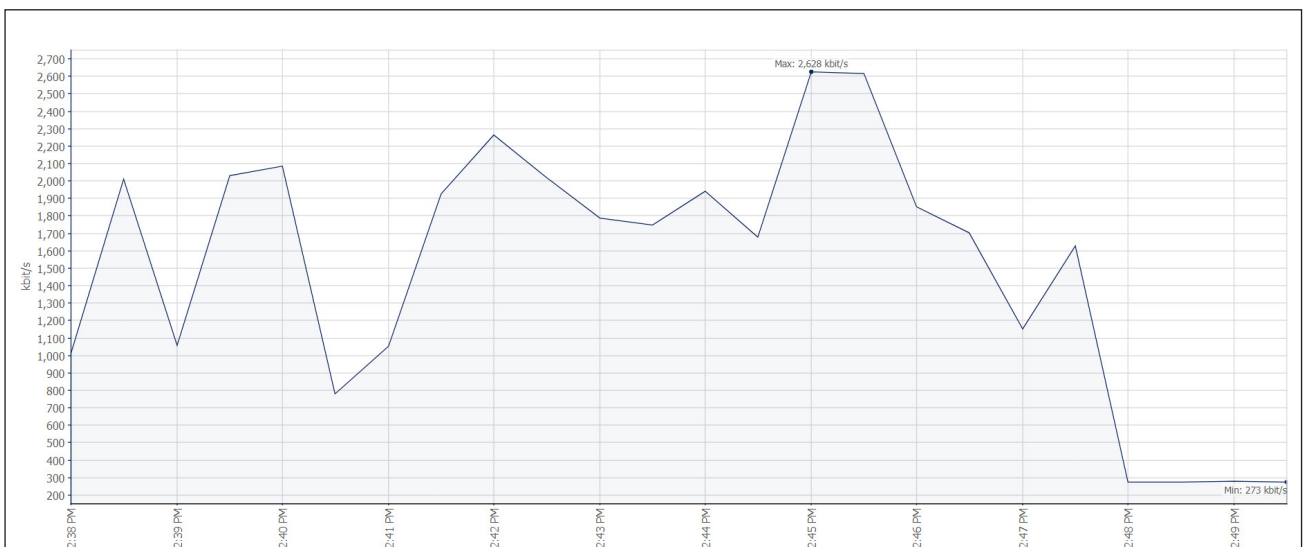
#### Video Content (1920 x 1080p @ 59.94 Hz / 60 Hz)

- Maximum bandwidth consumption: ~ 6.607 Mbps



#### Document (with random scrolling)

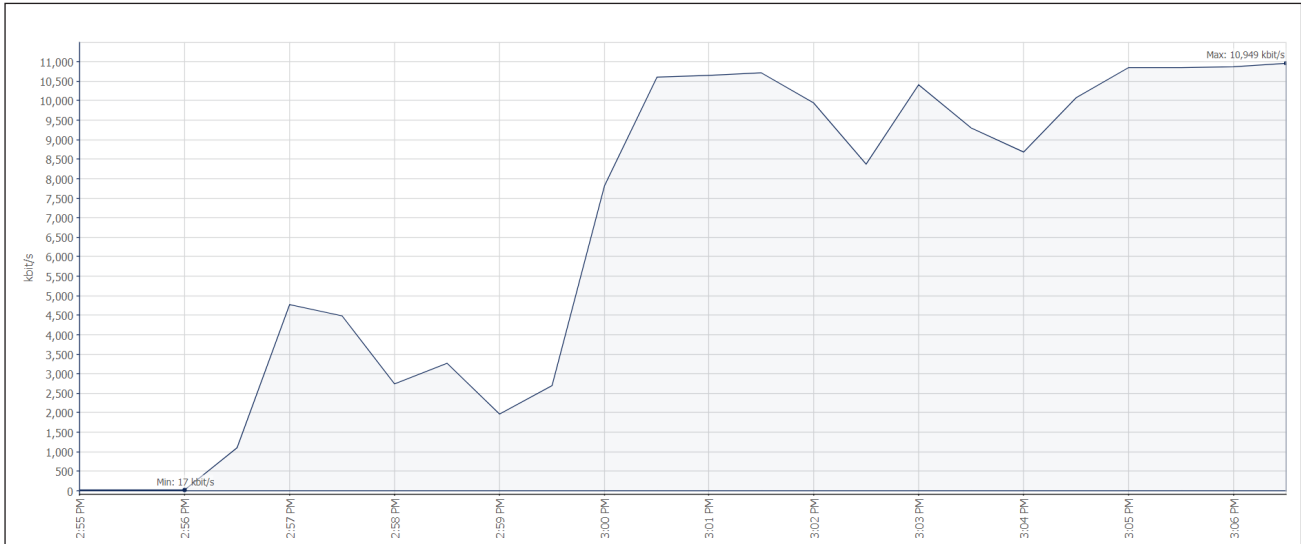
- Maximum bandwidth consumption: ~ 2.628 Mbps



## AirPlay®

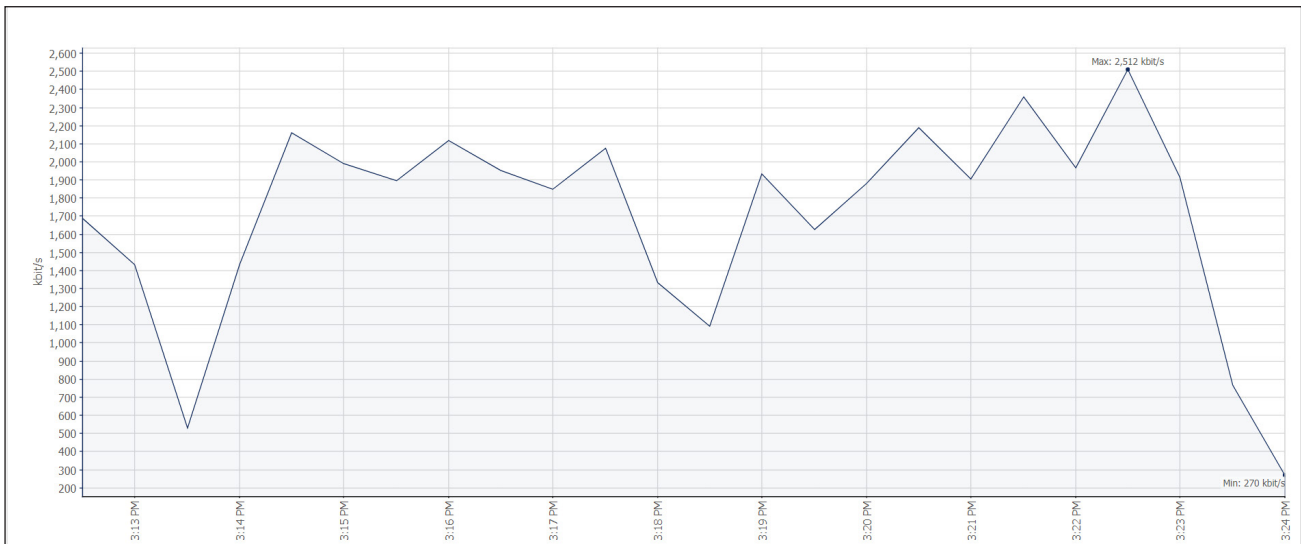
### Video Content (1920 x 1080p @ 59.94 Hz / 60 Hz)

- Maximum bandwidth consumption: ~ 10.949 Mbps



### Document (with random scrolling)

- Maximum bandwidth consumption: ~ 2.512 Mbps



## Miracast™ over Infrastructure

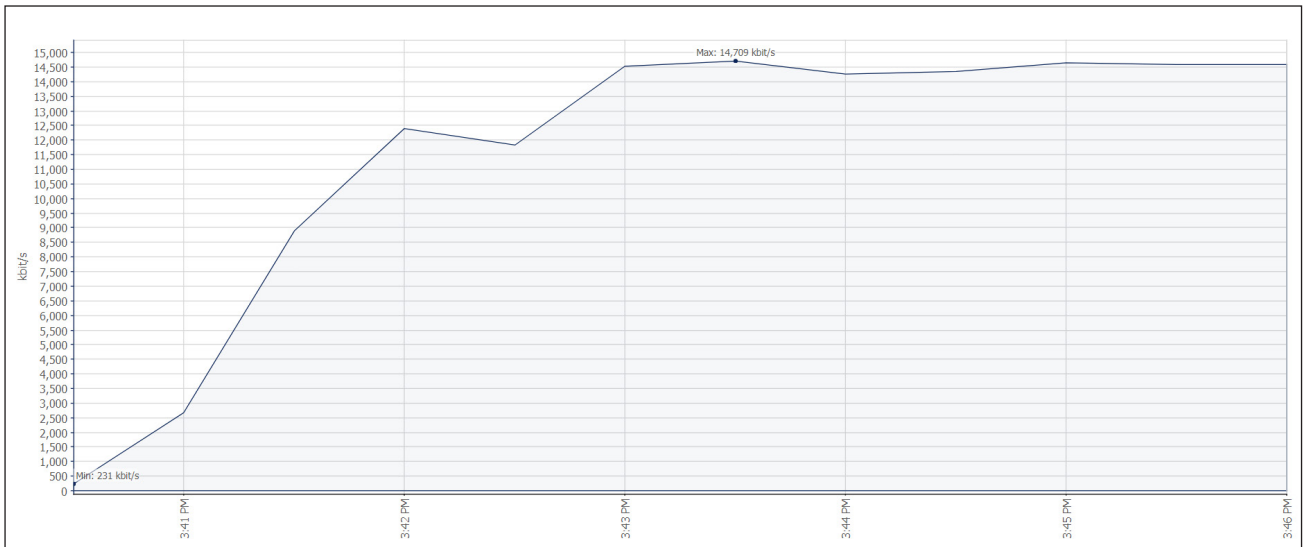
For more information on Miracast, refer to the following link: [Miracast over Infrastructure](#)



**NOTE:** Miracast P2P uses WiFi Direct and does not use the existing network resources.

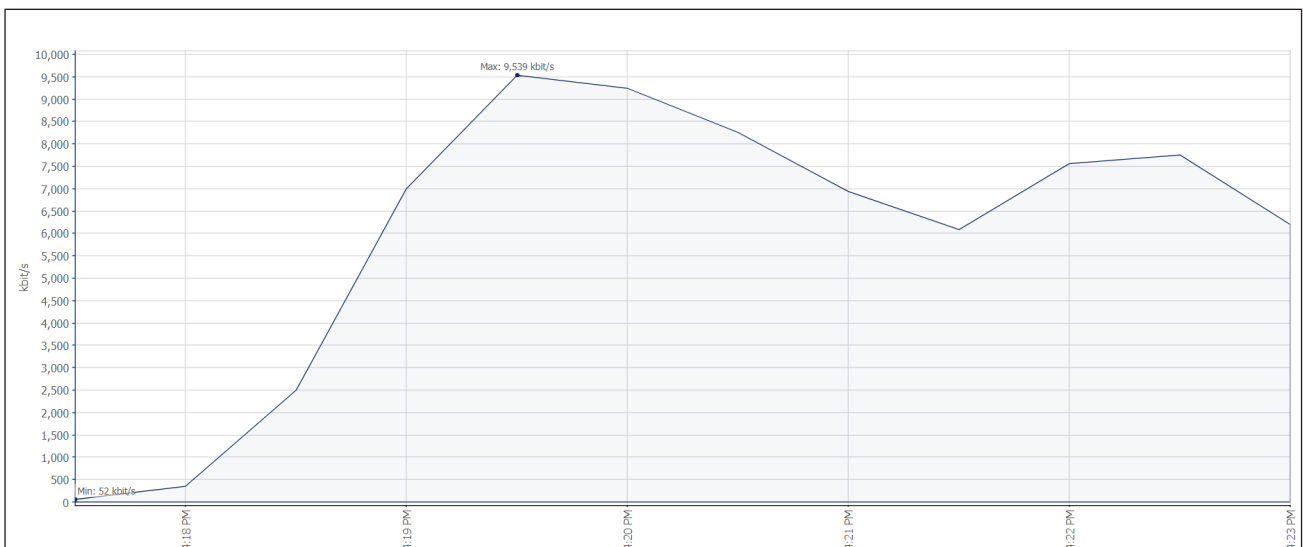
### Video Content (1920 x 1080p @ 59.94 Hz / 60 Hz)

- Maximum bandwidth consumption: ~ 14.709 Mbps



### Document (with random scrolling)

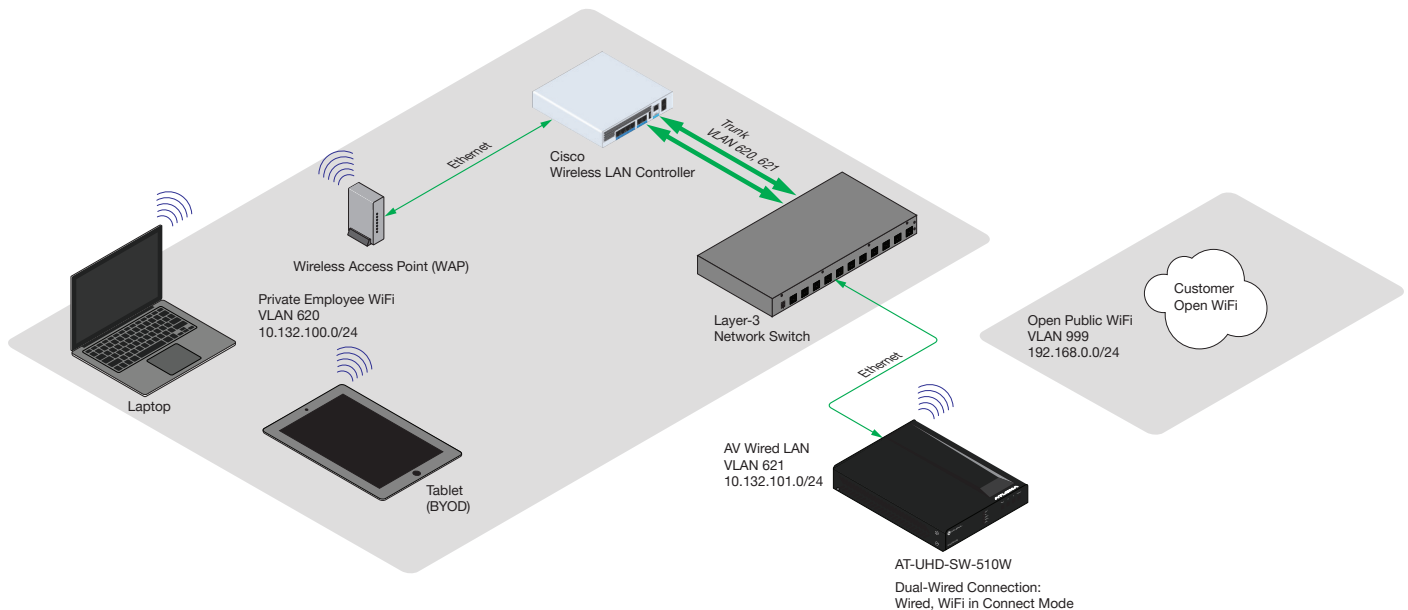
- Maximum bandwidth consumption: ~ 9.539 Mbps



## Appendix

### Configuring AirPlay/Google Cast across multiple VLANs using a Cisco WLC

AT-UHD-SW-510W BYOD devices allows casting of video and audio content from various sources and configurations. The purpose of this section is to provide guidance on forwarding mDNS (multicast DNS) service announcements in complex enterprise networks. Specifically, an environment with multiple VLANs, a Cisco Wireless LAN Controller, and Lightweight access points. The illustration below shows a simplified network environment.



In this example, the customer wants to dual home the AT-UHD-SW-510W connecting to an open public access network for customers and guests, but also wants to allow casting for employees connected to the private network. The challenge, here, is to restrict employees to the private network, without providing direct access to the AT-UHD-SW-510W WiFi in Access Point mode, which will allow employees to connect to the companies' existing private employee WiFi network to share content and cast to displays in the conference rooms.

#### Benefits of this configuration:

1. Guests can connect to the wireless guest network and perform casting.
2. Employees who are connected to the internal (private) WiFi network can cast directly to the AT-UHD-SW-510W without switching to any other network.
3. Environments are separated with nothing forwarded between zones.



**NOTE:** Open Public WiFi can use the same Wireless LAN Controller (WLC) and access points. However, the Open WiFi VLAN should not be configured for mDNS forwarding.

For this configuration to work, mDNS forwarding must be configured between VLANs. mDNS forwarding allows the AT-UHD-SW-510W BYOD device to show up as a "castable" device on endpoints. Only one mDNS forwarder should be configured per network to avoid forwarding loops. In this example, we will configure the Cisco WLC to be the mDNS forwarder.

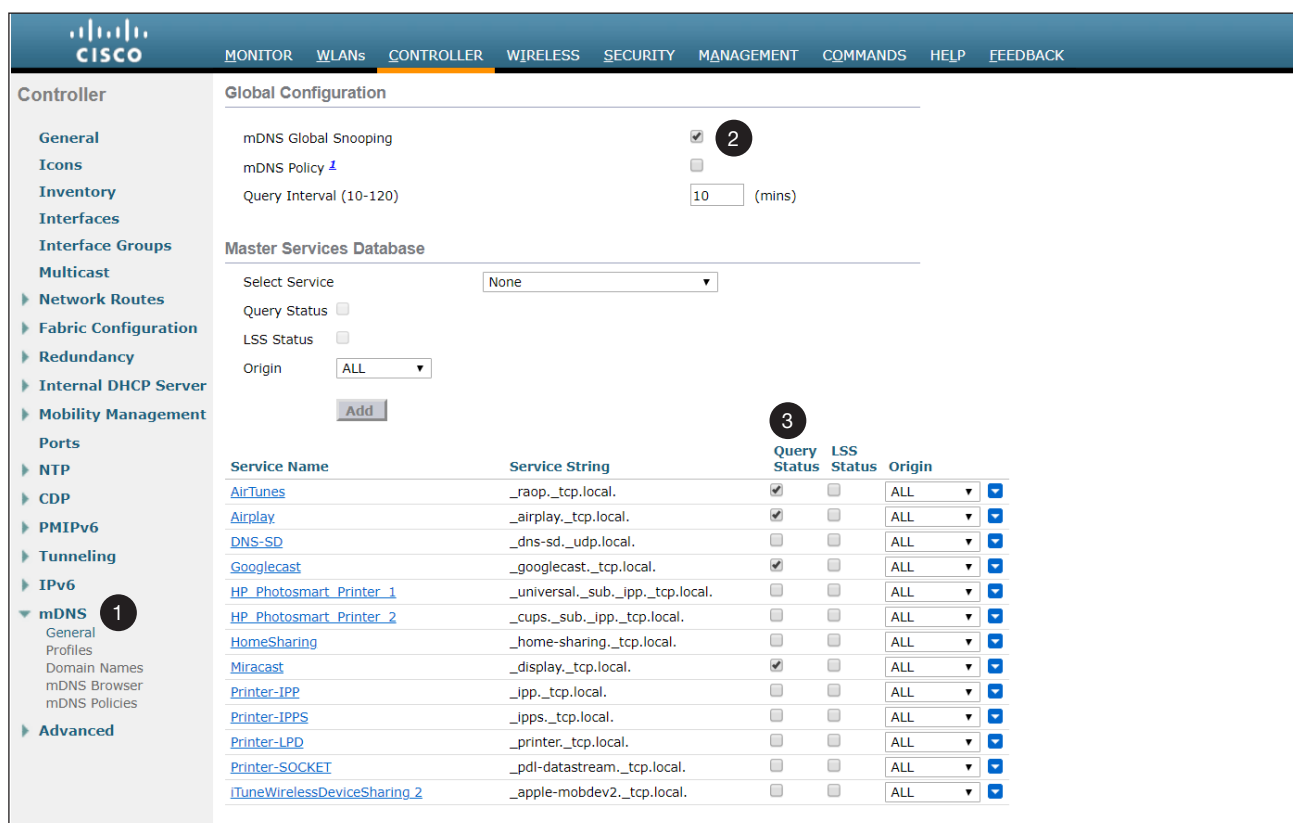
For this example, the following is given:

1. The wireless clients are on VLAN 620 and the AT-UHD-SW-510W BYOD device is on VLAN 621.
2. The WLC will need to be configured to forward mDNS service announcements between both VLANs.
3. The WLC is connected over a trunk line, encapsulating the VLANs.
4. The Layer 3 switch is configured with VLAN 620 and VLAN 621 and is the default gateway routing between the VLANs.

This solution has no multicast routing configured on the Layer-3 switch, only IGMP snooping and querying. All WLC configuration is done in the Advanced configuration section, located in the upper-right corner of the Main Dashboard of the WLC interface. In this example, the Cisco 3504 interface is shown, running version 8.5.131.0.

### Configuring the WLC for mDNS forwarding

1. Activate global mDNS Global Snooping on the WLC. In order to do this, an mDNS profile will be setup to determine which mDNS service announcements will be forwarded. In left-hand menu bar, click **mDNS > General**.
2. Click the **mDNS Global Snooping** check box to enable this feature.
3. Under the **Query Status** column, make sure the following boxes are checked (enabled):
  - `_raop._tcp.local`
  - `_airplay._tcp.local`
  - `_googlecast._tcp.local`
  - `_display._tcp.local`



**Global Configuration**

mDNS Global Snooping  **2**

mDNS Policy [1](#)

Query Interval (10-120)  (mins)

**Master Services Database**

Select Service:

Query Status

LSS Status

Origin:

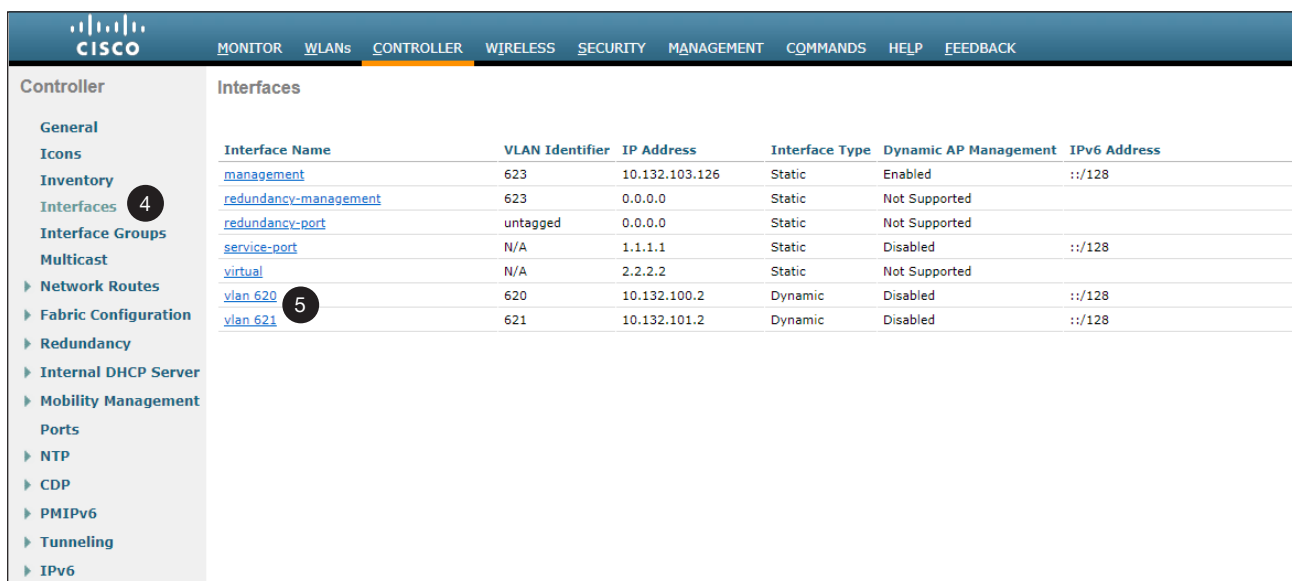
**Add** **3**

Service Name	Service String	Query Status	LSS Status	Origin
<a href="#">AirTunes</a>	<code>_raop._tcp.local</code>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ALL
<a href="#">Airplay</a>	<code>_airplay._tcp.local</code>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ALL
<a href="#">DNS-SD</a>	<code>_dns-sd._udp.local</code>	<input type="checkbox"/>	<input type="checkbox"/>	ALL
<a href="#">Googlecast</a>	<code>_googlecast._tcp.local</code>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ALL
<a href="#">HP_Photosmart_Printer_1</a>	<code>_universal._sub._ipp._tcp.local</code>	<input type="checkbox"/>	<input type="checkbox"/>	ALL
<a href="#">HP_Photosmart_Printer_2</a>	<code>_cups._sub._ipp._tcp.local</code>	<input type="checkbox"/>	<input type="checkbox"/>	ALL
<a href="#">HomeSharing</a>	<code>_home-sharing._tcp.local</code>	<input type="checkbox"/>	<input type="checkbox"/>	ALL
<a href="#">Miracast</a>	<code>_display._tcp.local</code>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ALL
<a href="#">Printer-IPP</a>	<code>_ipp._tcp.local</code>	<input type="checkbox"/>	<input type="checkbox"/>	ALL
<a href="#">Printer-IPPS</a>	<code>_jpps._tcp.local</code>	<input type="checkbox"/>	<input type="checkbox"/>	ALL
<a href="#">Printer-LPD</a>	<code>_printer._tcp.local</code>	<input type="checkbox"/>	<input type="checkbox"/>	ALL
<a href="#">Printer-SOCKET</a>	<code>_pdl-datastream._tcp.local</code>	<input type="checkbox"/>	<input type="checkbox"/>	ALL
<a href="#">iTuneWirelessDeviceSharing_2</a>	<code>_apple-mobdev2._tcp.local</code>	<input type="checkbox"/>	<input type="checkbox"/>	ALL

**IMPORTANT:** Some of the mDNS services might already be present in the Master Services Database. Verify that the specified services are added before proceeding to Step 4.

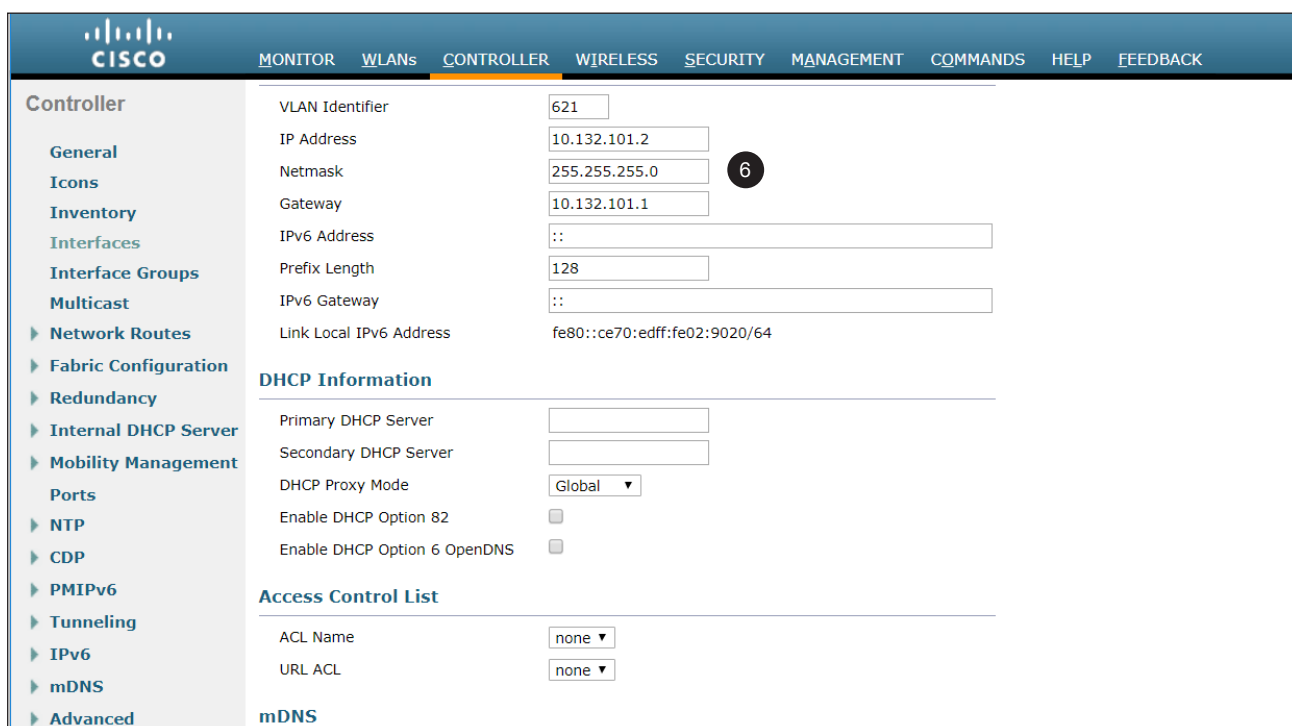
The WLC will need to have an interface created for VLAN 620 and VLAN 621. The WLC already had an interface on the working Wi-Fi network (VLAN 620), but it is necessary to create an interface on VLAN 621. In the example we did not assign an SSID to this VLAN as it is only used to forward mDNS announcements.

4. In the left-hand menu, click **Interfaces**. Create interfaces for both VLANs if they do not exist.
5. Click on the VLAN name to edit it.



Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
<a href="#">management</a>	623	10.132.103.126	Static	Enabled	::/128
<a href="#">redundancy-management</a>	623	0.0.0.0	Static	Not Supported	
<a href="#">redundancy-port</a>	untagged	0.0.0.0	Static	Not Supported	
<a href="#">service-port</a>	N/A	1.1.1.1	Static	Disabled	::/128
<a href="#">virtual</a>	N/A	2.2.2.2	Static	Not Supported	
<a href="#">vlan_620</a>	620	10.132.100.2	Dynamic	Disabled	::/128
<a href="#">vlan_621</a>	621	10.132.101.2	Dynamic	Disabled	::/128

6. Configure the IP settings for the VLAN interface. In the example below, the interface is configured with an IP address of 10.132.101.2. The Layer-3 switch has a default gateway of 10.132.101.1.



VLAN Identifier: 621  
 IP Address: 10.132.101.2  
 Netmask: 255.255.255.0  
 Gateway: 10.132.101.1  
 IPv6 Address: ::  
 Prefix Length: 128  
 IPv6 Gateway: ::  
 Link Local IPv6 Address: fe80::ce70:edff:fe02:9020/64

**DHCP Information**

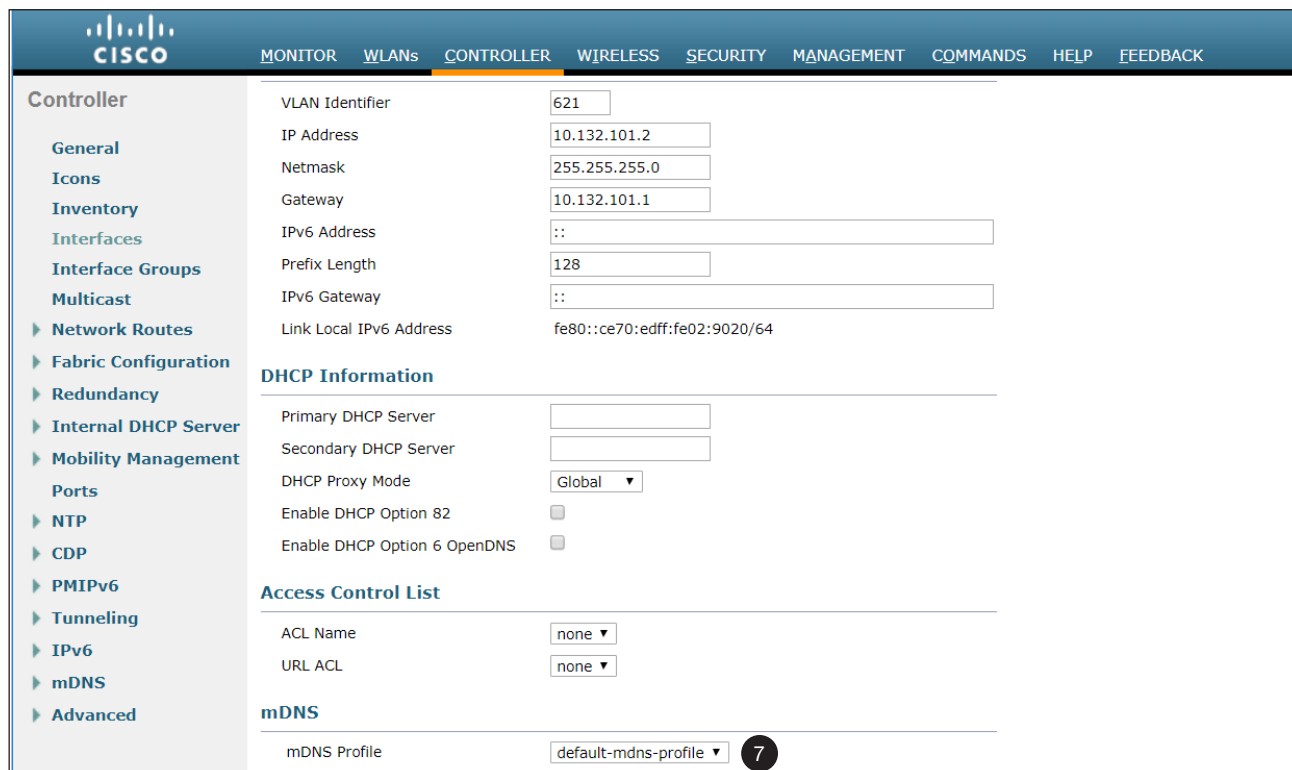
Primary DHCP Server:   
 Secondary DHCP Server:   
 DHCP Proxy Mode: Global  
 Enable DHCP Option 82:   
 Enable DHCP Option 6 OpenDNS:

**Access Control List**

ACL Name: none  
 URL ACL: none

**mDNS**

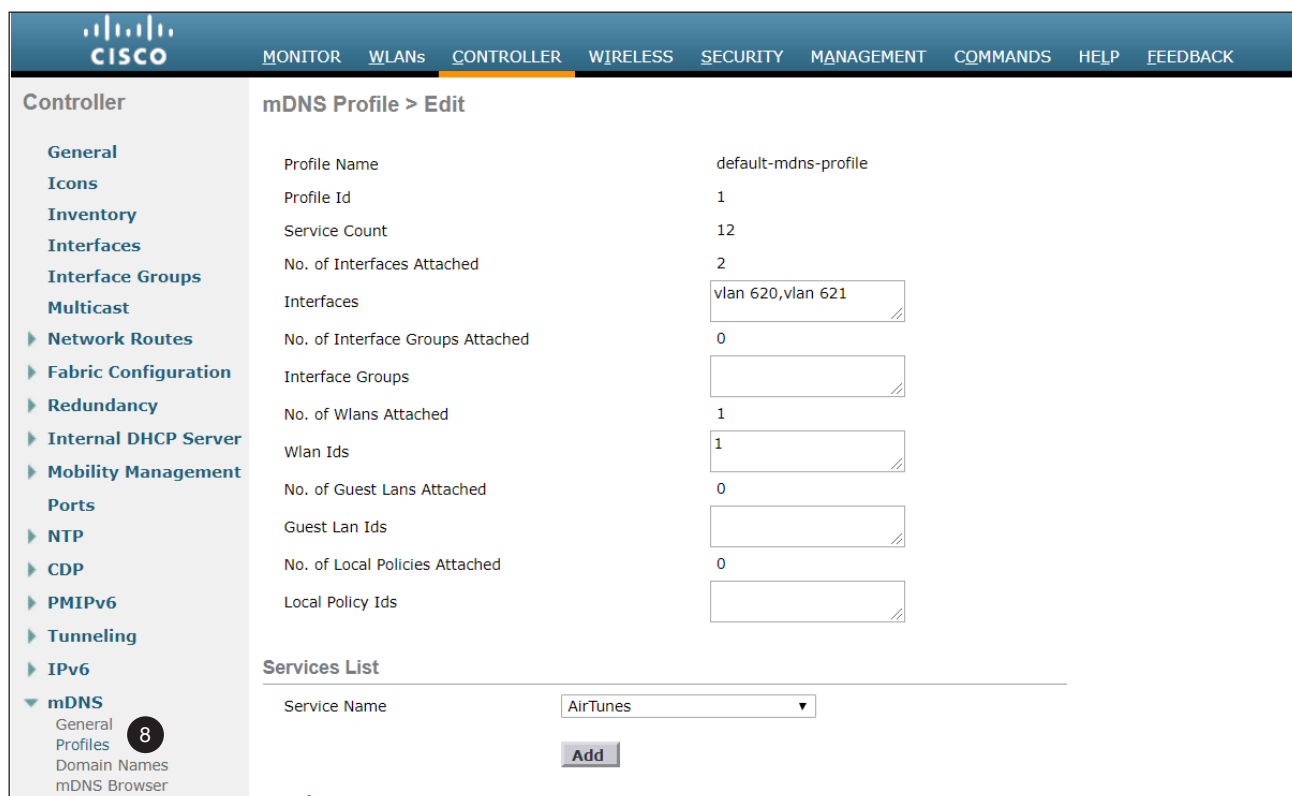
7. Enable mDNS on the interfaces. For each interface assign a mDNS profile to apply. Click the **mDNS Profile** drop-down list and select **default-mdns-profile** for interface VLAN 620 and VLAN 621.



The screenshot shows the Cisco Controller configuration page for a VLAN. The left-hand menu is expanded to show various configuration options. The main configuration area is divided into several sections:

- General:** VLAN Identifier (621), IP Address (10.132.101.2), Netmask (255.255.255.0), Gateway (10.132.101.1), IPv6 Address (::), Prefix Length (128), IPv6 Gateway (::), and Link Local IPv6 Address (fe80::ce70:edff:fe02:9020/64).
- DHCP Information:** Primary DHCP Server, Secondary DHCP Server, DHCP Proxy Mode (Global), Enable DHCP Option 82, and Enable DHCP Option 6 OpenDNS.
- Access Control List:** ACL Name (none) and URL ACL (none).
- mDNS:** mDNS Profile (default-mdns-profile) with a circled '7' next to the dropdown menu.

8. Validate that the default mDNS profile is applied to the interfaces. In the left-hand menu, click **mDNS > Profiles > default-mdns-profile**.



The screenshot shows the Cisco Controller configuration page for the mDNS Profile. The left-hand menu is expanded to show various configuration options. The main configuration area is divided into several sections:

- mDNS Profile > Edit:** Profile Name (default-mdns-profile), Profile Id (1), Service Count (12), No. of Interfaces Attached (2), Interfaces (vlan 620,vlan 621), No. of Interface Groups Attached (0), Interface Groups, No. of Wlans Attached (1), Wlan Ids (1), No. of Guest Lans Attached (0), Guest Lan Ids, No. of Local Policies Attached (0), and Local Policy Ids.
- Services List:** Service Name (AirTunes) with an Add button.

The left-hand menu is expanded to show various configuration options, with **mDNS** selected and **Profiles** highlighted with a circled '8'.



The profile was attached to VLAN 620 and VLAN 621, as shown on the previous page. WLC configuration is complete. The WLC is now caching mDNS announcements and responding to mDNS requests from end devices.

9. Validate incoming mDNS service announcements. SSH into the WLC for advanced mDNS debugging and troubleshooting. A useful command for checking service announcements is `show mdns service detailed <service name>`. Use this command to verify you are seeing the mDNS announcements from the AT-UHD-SW-510W BYOD device connected to the wired subnet (VLAN 621).

```
(Cisco Controller) >show mdns service detailed Googlecast
Service Name..... Googlecast
Service String..... _googlecast._tcp.local.
Service Id..... 4
Service query status..... Enabled
Service LSS status..... Disabled
Service learn origin..... Wireless and Wired
Number of Profiles..... 1
Profile..... default-mdns-profile

Number of Service Providers ..... 1
Number of priority MAC addresses ..... 0

ServiceProvider          MAC Address          AP Radio MAC          Vlan Id  Type      TTL      Time left
-----
sw510-earl._googlecast._tcp.local.  00:1E:06:36:70:57  -----          621     Wired     4500     4024
```

Here, the AT-UHD-SW-510W BYOD device (hostname “sw510-earl”) announcing Google Cast services on VLAN 621 by using the command `show mdns service detailed Googlecast`. AirPlay can Miracast can also be shown by specifying those service names, as shown below.

`show mdns service detailed Airplay`

```
(Cisco Controller) >show mdns service detailed Airplay
Service Name..... Airplay
Service String..... _airplay._tcp.local.
Service Id..... 2
Service query status..... Enabled
Service LSS status..... Disabled
Service learn origin..... Wireless and Wired
Number of Profiles..... 1
Profile..... default-mdns-profile

Number of Service Providers ..... 2
Number of priority MAC addresses ..... 0

ServiceProvider          MAC Address          AP Radio MAC          Vlan Id  Type      TTL      Time left
-----
EARL - Samsung Q70 Series 55"._airplay._tcp.local.  24:FC:E5:15:B8:3A  -----          621     Wired     4500     4032
sw510-earl._airplay._tcp.local.  00:1E:06:36:70:57  -----          621     Wired     4500     4032
```

`show mdns service detailed Miracast`

```
(Cisco Controller) >show mdns service detailed Miracast
Service Name..... Miracast
Service String..... _display._tcp.local.
Service Id..... 8
Service query status..... Enabled
Service LSS status..... Disabled
Service learn origin..... Wireless and Wired
Number of Profiles..... 1
Profile..... default-mdns-profile

Number of Service Providers ..... 1
Number of priority MAC addresses ..... 0

ServiceProvider          MAC Address          AP Radio MAC          Vlan Id  Type      TTL      Time left
-----
sw510-earl._display._tcp.local.  00:1E:06:36:70:57  -----          621     Wired     4500     3915
```

## Limiting mDNS Announcements

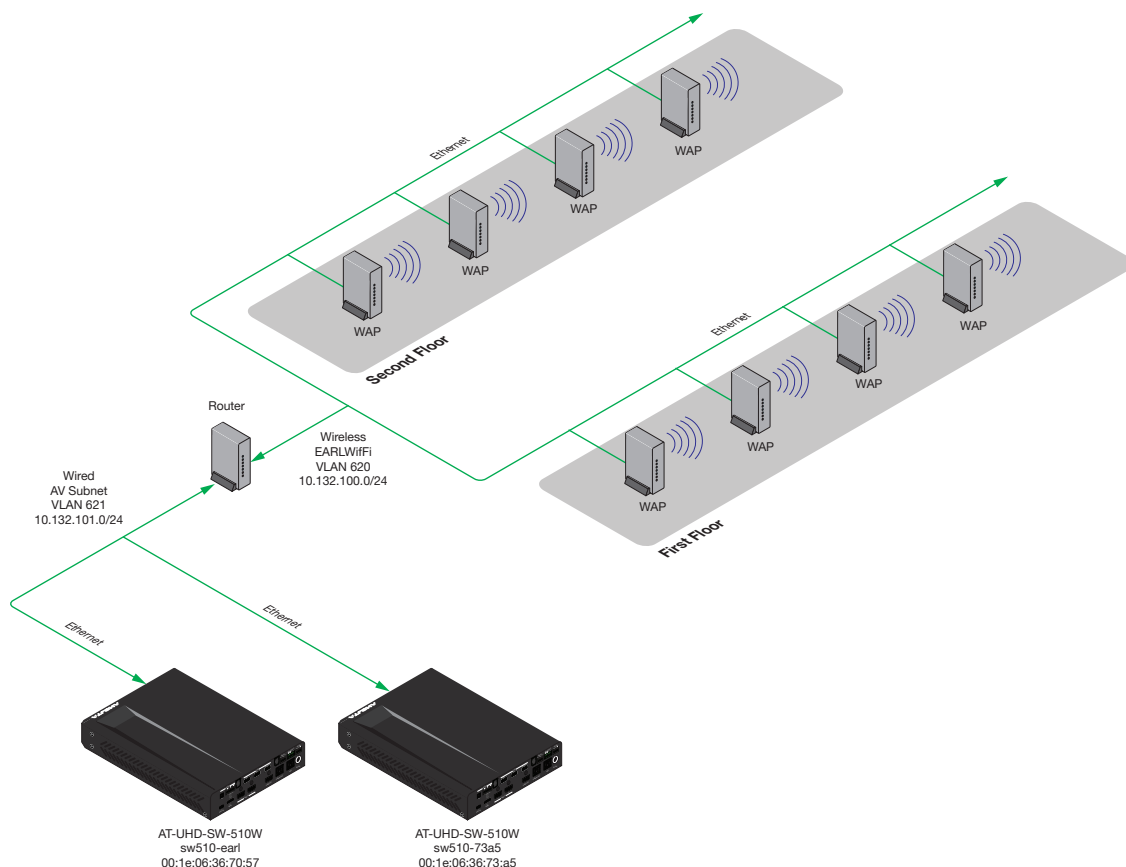
The AT-UHD-SW-510W allows video and audio casting to several types of sources. Wireless networks using Cisco Wireless LAN Controllers(WLC) must be configured to forward mDNS announcements for both AirPlay and Google Cast service announcements, in order to be accessible on wireless client devices. In large enterprise networks environments with multiple AT-UHD-SW-510W units, it may be desirable to limit (“fencing”) the number of units that can be available when attempting to cast.

The section assumes the following:

- A Cisco WLC is being used with lightweight access points (AP) to provide wireless network access.
- A WLC is configured to properly forward mDNS announcements and both AirPlay and Google Cast can be used to cast to wired AT-UHD-SW-510W units through wireless clients.
- To restrict the AT-UHD-SW-510W access, based on the client’s location.

### mDNS Fencing Overview

In the example below, the facility has two floors with access points. Each floor has a conference room with an AT-UHD-SW-510W used for casting. The challenge is to have clients, which are connected to access points on the first floor, to be able to only access the AT-UHD-SW-510W in the first-floor conference room. Clients on the second floor should only be able to access the second floor conference room. To do this, the WLC will be configured to use AP Groups and mDNS profiles, in order to limit which clients can access each AT-UHD-SW-510W.



### NOTICE: Wireless Coverage and Configuration Warning

This solution relies on properly designed client roaming to function correctly. It is possible that a wireless client could physically move (walk) from the first floor to the second floor without the wireless client roaming from the first floor access point to the second floor access point. A wireless client's job is to stay connected to an access point until the signal is no longer reachable. This condition is most likely due to an excessively large of overlap of wireless cells. Access points can't be forced to roam to a different access point, but there are some ways to get it to roam faster.

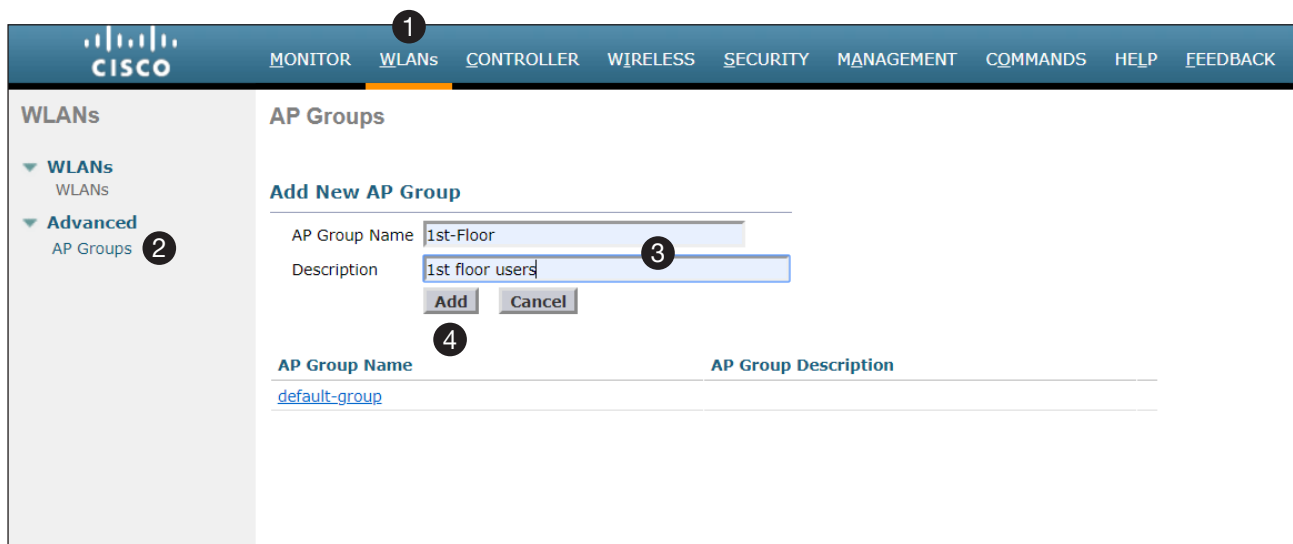
- Decrease power on the access points.
- Decrease the power on client devices.
- Disable lower data rates, globally, on the WLC.

If all any of these fail, a re-survey of the area for smaller wireless cells should solve the problem. To create smaller wireless cells, use more access points and configure the access point to use less power.

### Configuring Access Point Groups

In the example below, the Cisco WLC is running version 8.5.131.

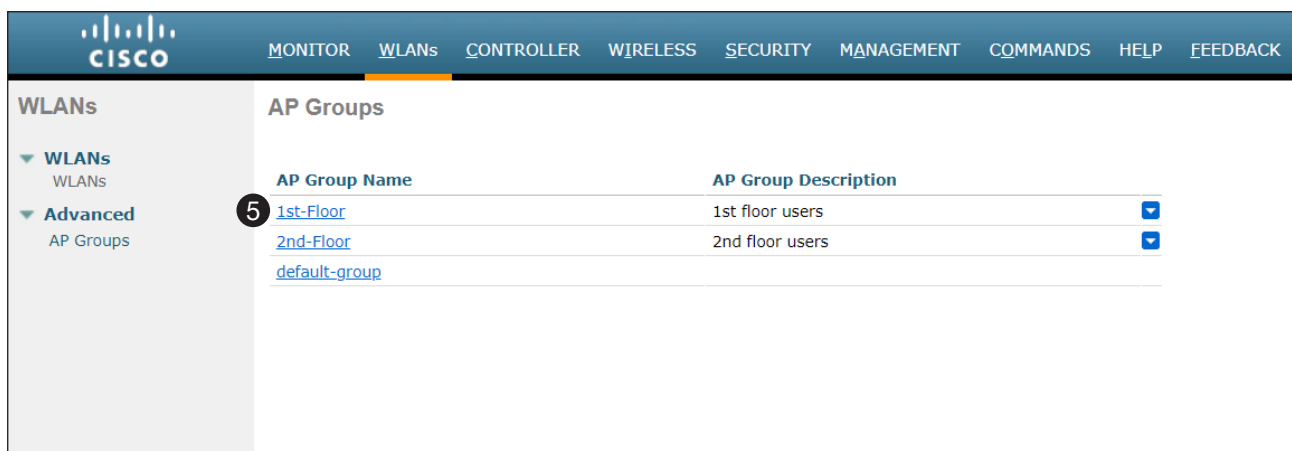
1. Connect to the controller through HTTPS, then click **WLANS** in the top menu system.
2. Click **Advanced > AP Groups > Add Group**.
3. Enter the name of the group in the **AP Group Name** and a description in the **Description** field.
4. Click the **Add** button to commit changes. Repeat steps 2 through 4 to create a second group named `2nd-Floor` with the description `2nd floor users`.



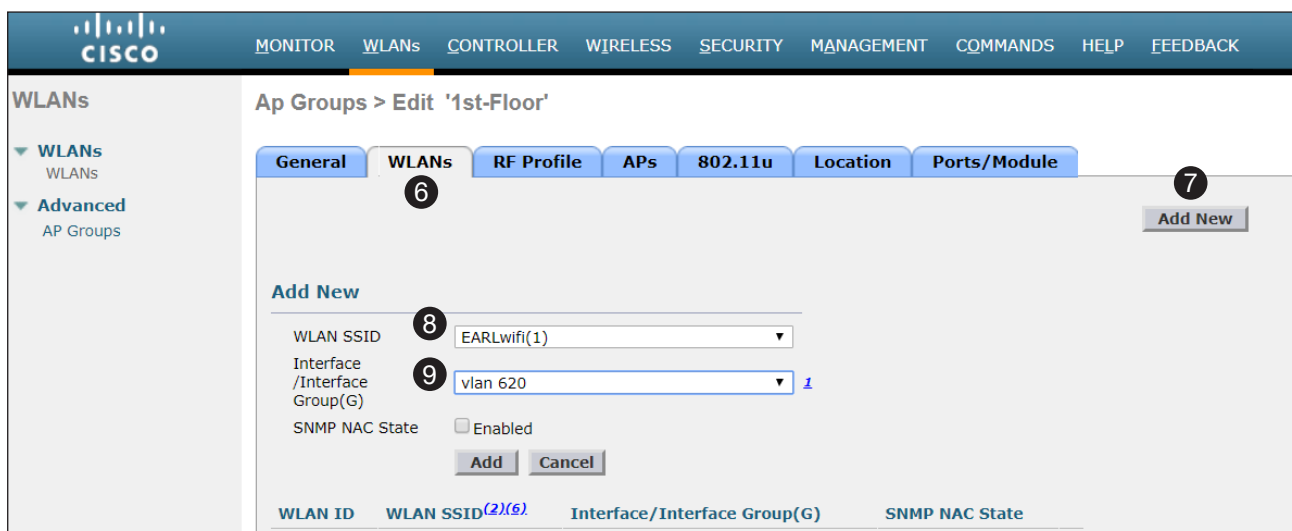
The newly-created groups should now appear under the **AP Group Name** section, as shown on the next page.

The next step will assign the WLAN that will be recognized from access points within the AP Group. In the following example, both first and second floors will use the `sw510-earlwifi` SSID and interface `VLAN 620`.

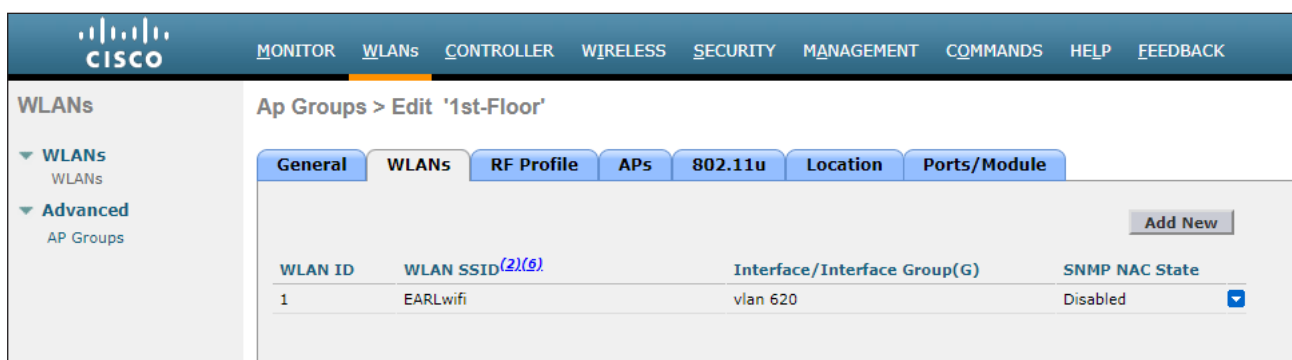
- Click on **1st-Floor** to edit the AP Group Name.



- Click **WLANs** in the top menu bar.
- Click the **Add New** button.
- Click the **WLAN SSID** drop-down list and select the desired SSID.
- Click the **Interface / Interface Group (G)** drop-down list and select the desired interface. Repeat steps 5 through 7 for the 2nd-floor group.

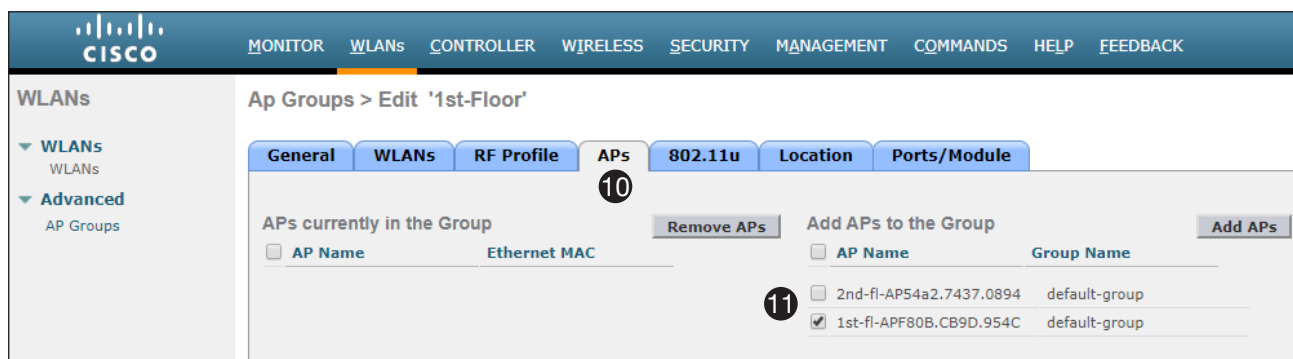


Once completed, the SSID and interface should be assigned to the AP group, as shown in the example below.




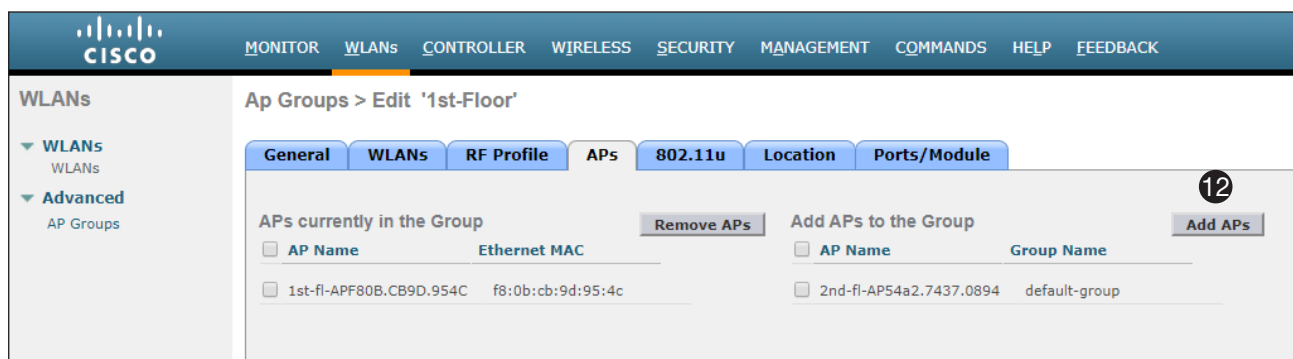
10. Click the **APs** tab.

11. Select the AP names to assign to the group, by clicking the check box next to the desired access points.



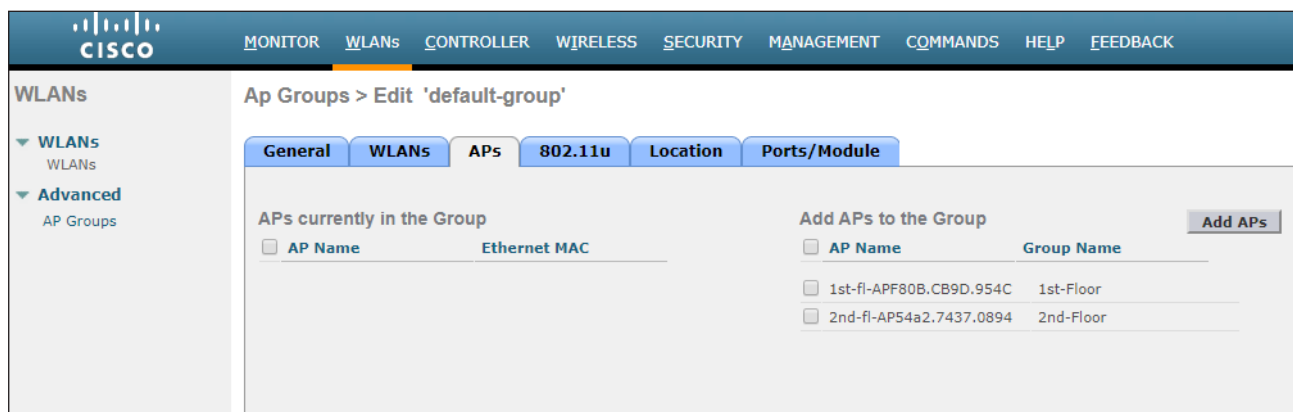
12. Click the **Add APs** button to add the selected access points to the group.

 **IMPORTANT:** Adding APs to an AP Group will cause the AP to reboot.



An AP is now assigned to the 1st Floor AP Group. Continue adding the desired access points to the AP Group. Next, switch to the 2nd Floor AP Group and assign an AP to that AP Group. Once the WLC finishes rebooting, the APs should be assigned to their respective groups. Note that the access points are no longer assigned to the default-group.

At this point the AP Access Groups group configuration is complete. Wireless clients should be able to access the SSIDs from both AT-UHD-SW-510W units and should be able to cast to all devices. The next step is to “limit” the access, which is the purpose of fencing. Although two separate AP Groups exist, they are configured the same and will behave the same.



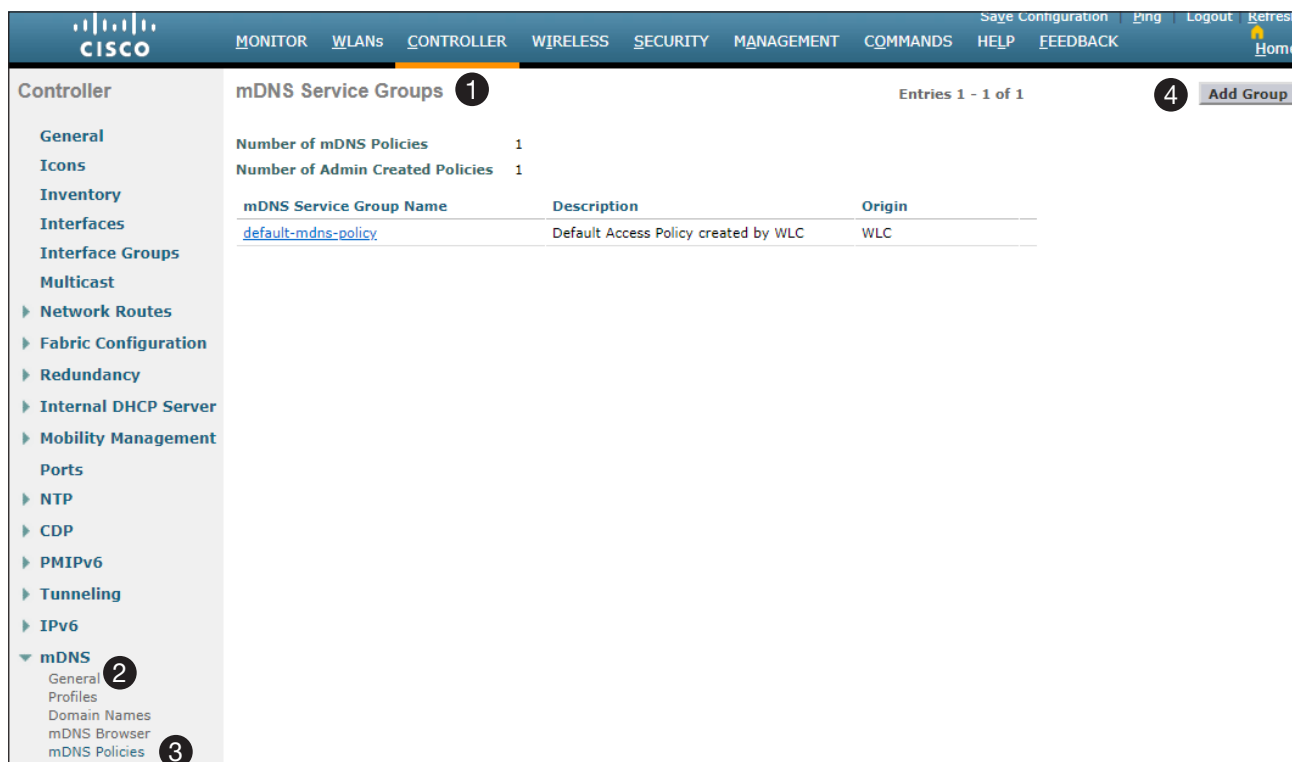
### Configuring mDNS Policies

The mDNS policy is where limiting (fencing) which AP Groups can see which AT-UHD-SW-510W units. In the procedure below, an mDNS policy will be created to restrict certain users to specific devices. The mDNS policy can use 802.1X authentication to pass a user-id or role, or can use location information through association with an access point or an AP Group. The AP Groups that were configured in the previous section will be used.



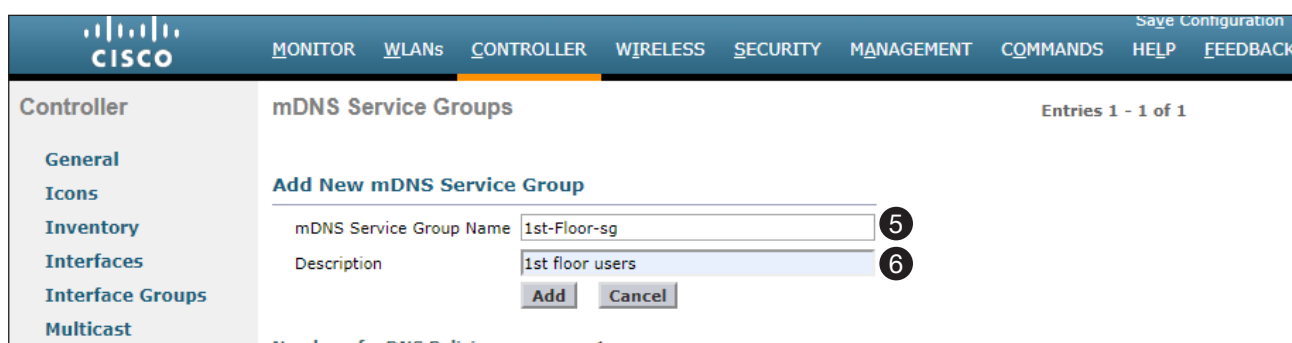
**NOTE:** It is important to note that the following procedure does not alter the mDNS profile. For example, the AP Group configuration was started using the `default-mdns-profile` to the wired and wireless interfaces. This profile is never changed.

1. Click **CONTROLLER** in the top menu bar.
2. Click the **mDNS** menu in the left-hand menu bar to expand it.
3. Click **mDNS Policies**.
4. Click the **Add Group** button.



The screenshot shows the Cisco Controller interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left-hand menu is expanded to 'mDNS', with sub-items: 'General', 'Profiles', 'Domain Names', 'mDNS Browser', and 'mDNS Policies'. The main content area is titled 'mDNS Service Groups' and shows a table with one entry: 'default-mdns-policy' with description 'Default Access Policy created by WLC' and origin 'WLC'. A table header shows columns for 'mDNS Service Group Name', 'Description', and 'Origin'. A circled '1' is next to the title, a circled '2' is next to 'mDNS Policies' in the menu, a circled '3' is next to 'mDNS Policies' in the sub-menu, and a circled '4' is next to the 'Add Group' button.

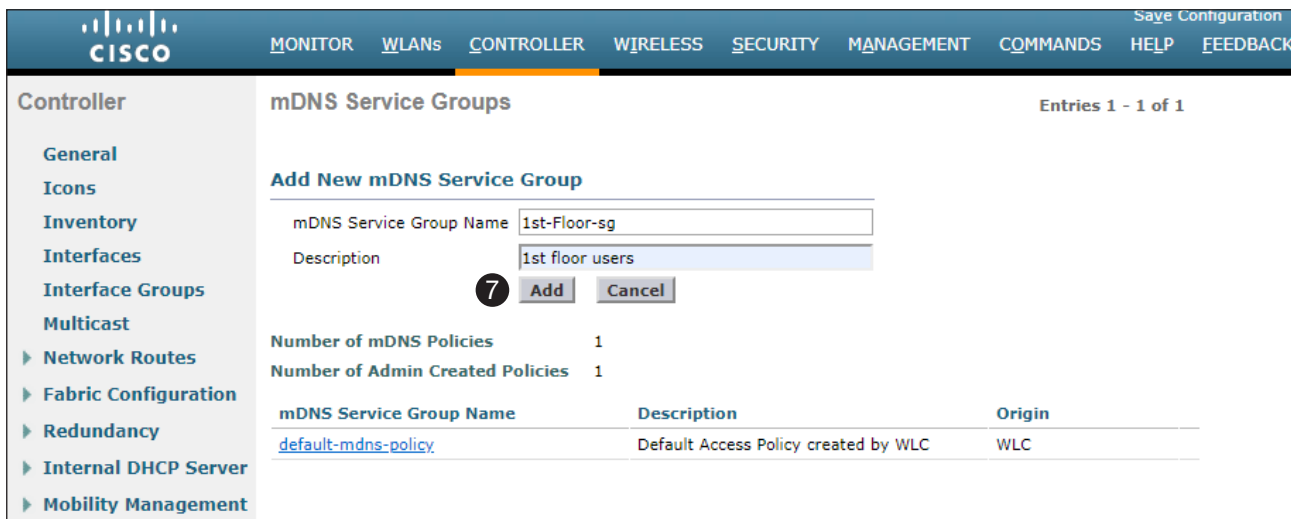
5. Enter new mDNS service group name in the **mDNS Service Group Name** field.
6. Enter the mDNS service group description in the **Description** field.



The screenshot shows the 'Add New mDNS Service Group' form. The 'mDNS Service Group Name' field contains '1st-Floor-sg' and the 'Description' field contains '1st floor users'. There are 'Add' and 'Cancel' buttons below the fields. A circled '5' is next to the name field and a circled '6' is next to the description field.

- Click the **Add** button to commit changes.

In this example, the name `1st-Floor-sg` is used for the Service Group Name and `1st Floor Users` is used for the description. Repeat steps 4 through 7 for the second group on the second floor.



The screenshot shows the Cisco Controller interface for mDNS Service Groups. The 'Add New mDNS Service Group' form is displayed with the following fields:

- mDNS Service Group Name: `1st-Floor-sg`
- Description: `1st floor users`

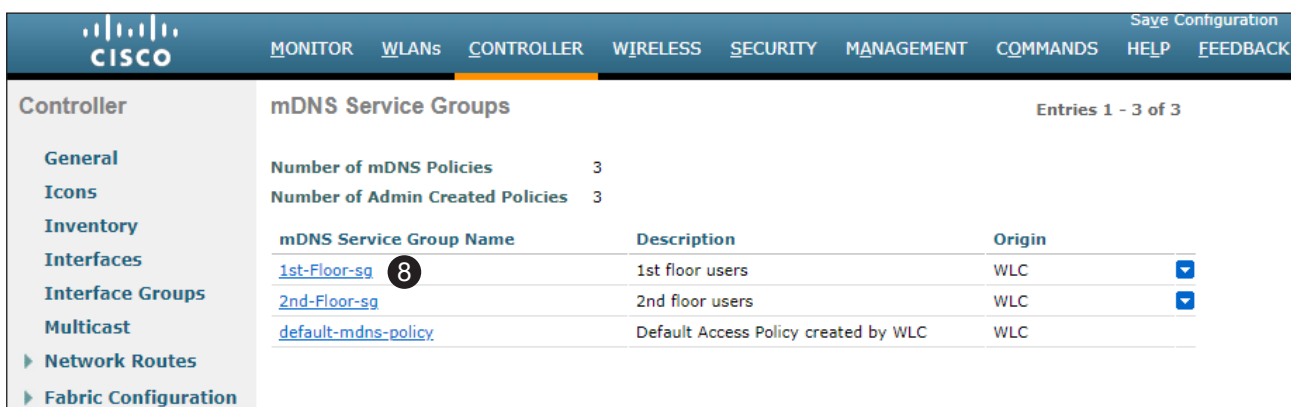
A circled '7' highlights the **Add** button. Below the form, the following statistics are shown:

- Number of mDNS Policies: 1
- Number of Admin Created Policies: 1

mDNS Service Group Name	Description	Origin
<a href="#">default-mdns-policy</a>	Default Access Policy created by WLC	WLC

The next step is to build a policy of rules that decide which units can be accessed. Each policy can have multiple rules. However, for this policy, the MAC address of the AT-UHD-SW-510W will be assigned to the first floor AP group. This will restrict any wireless client, that is connected to any access point AP on the 1st Floor AP Group, to be available to the AT-UHD-SW-510W on the first floor.

- Click `1st-Floor-sg`, under the **mDNS Service Group Name** column, to edit the service group.



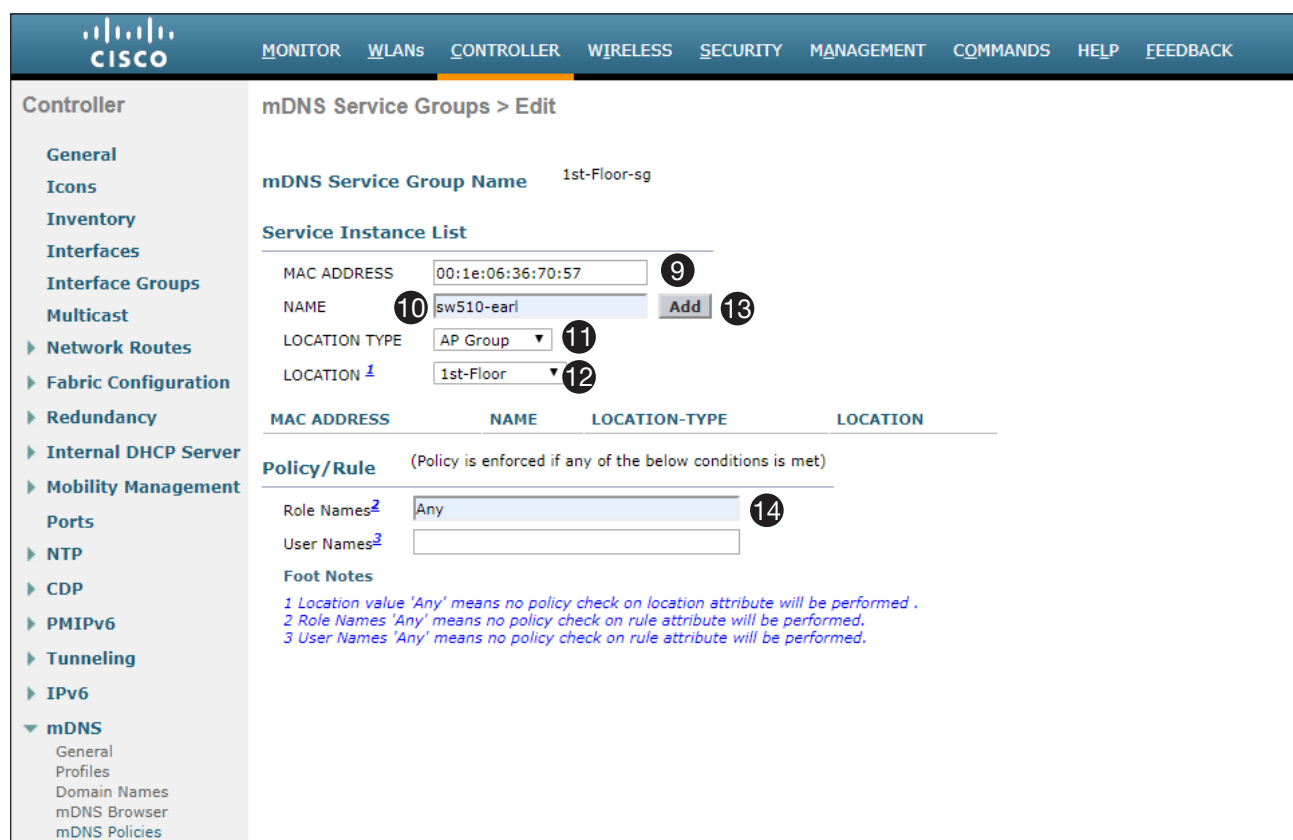
The screenshot shows the Cisco Controller interface for mDNS Service Groups. The list of service groups is displayed with the following statistics:

- Number of mDNS Policies: 3
- Number of Admin Created Policies: 3

mDNS Service Group Name	Description	Origin
<a href="#">1st-Floor-sg</a> <span style="border: 1px solid black; border-radius: 50%; padding: 2px;">8</span>	1st floor users	WLC
<a href="#">2nd-Floor-sg</a>	2nd floor users	WLC
<a href="#">default-mdns-policy</a>	Default Access Policy created by WLC	WLC

9. Enter the MAC address of the AT-UHD-SW-510W in the **MAC ADDRESS** field. In this example, this refers to the AT-UHD-SW-510W with the SSID `sw510-earl`.
10. Enter the SSID, associated with the above MAC address in the **NAME** field.
11. Click the **LOCATION TYPE** drop-down list and select `AP Group`.
12. Click the **LOCATION** drop-down list and select `1st-Floor`.
13. Click the **Add** button to commit changes and create the rule
14. In the **Role Names** field, enter `Any`. This will apply the roles to any user, then click **Apply** at the bottom of the page to add the role name to the policy.

Repeat steps 8 through 12 for the `2nd-Floor-sg`.



The screenshot shows the Cisco mDNS Service Groups configuration page. The page title is "mDNS Service Groups > Edit". The "mDNS Service Group Name" is "1st-Floor-sg". The "Service Instance List" section contains a table with the following data:

MAC ADDRESS	NAME	LOCATION-TYPE	LOCATION
00:1e:06:36:70:57	sw510-earl	AP Group	1st-Floor

The "Policy/Rule" section is titled "(Policy is enforced if any of the below conditions is met)". It includes the following fields:

- Role Names<sup>2</sup>: Any
- User Names<sup>3</sup>: (empty)

Foot Notes:

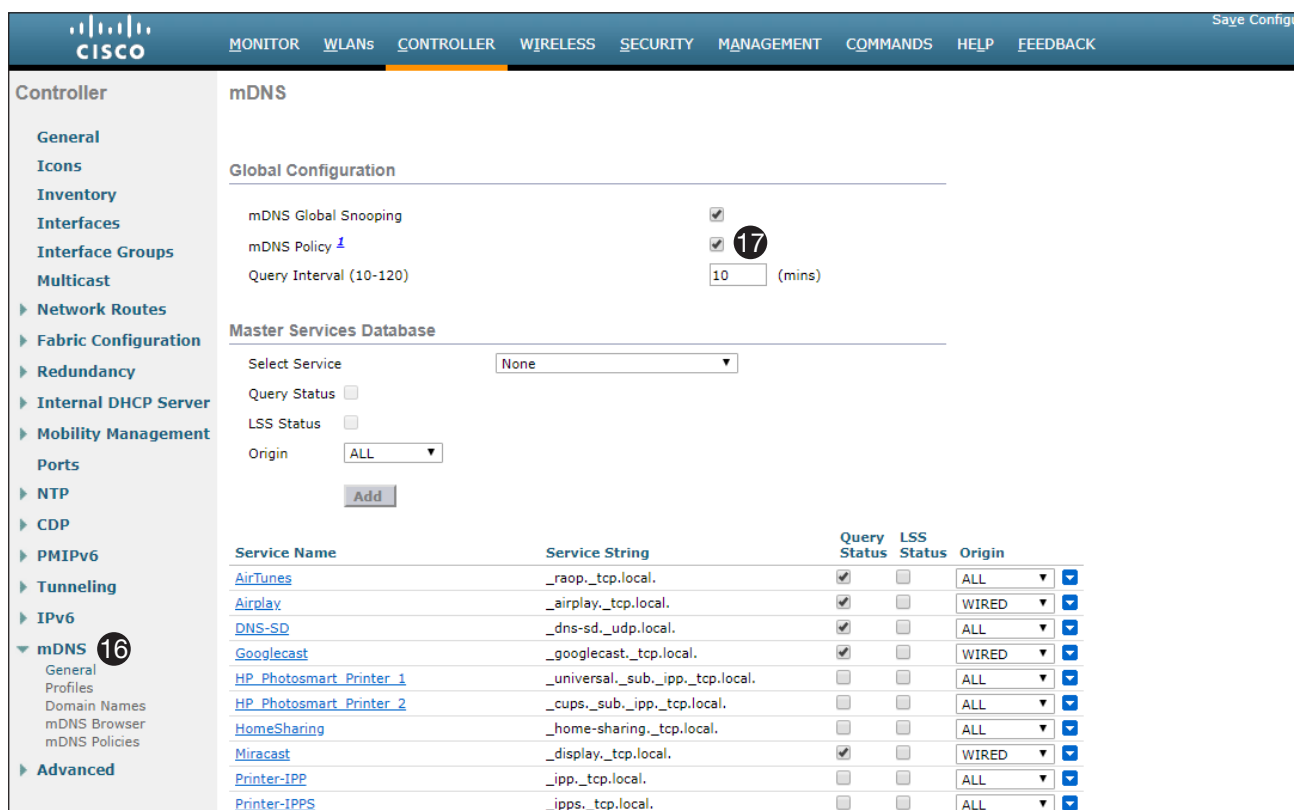
- 1 Location value 'Any' means no policy check on location attribute will be performed.
- 2 Role Names 'Any' means no policy check on rule attribute will be performed.
- 3 User Names 'Any' means no policy check on rule attribute will be performed.

The final step to apply the policies is to check the policy box on the **mDNS > General** page.



15. Click **CONTROLLER** in the top menu bar.
16. Click the **mDNS** menu in the left-hand menu bar to expand it, then click **General**.
17. Check the **mDNS Policy** box to apply mDNS policies.

Configuration is complete.



The screenshot displays the Cisco Controller's mDNS configuration interface. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar shows the 'Controller' menu with 'mDNS' selected and highlighted with a '16' callout. The main content area is titled 'mDNS' and contains the following sections:

- Global Configuration:**
  - mDNS Global Snooping:
  - mDNS Policy:  (17)
  - Query Interval (10-120): 10 (mins)
- Master Services Database:**
  - Select Service: None
  - Query Status:
  - LSS Status:
  - Origin: ALL
  - Add button
- Service List Table:**

Service Name	Service String	Query Status	LSS Status	Origin
<a href="#">AirTunes</a>	_raop._tcp.local.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ALL
<a href="#">Airplay</a>	_airplay._tcp.local.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	WIRED
<a href="#">DNS-SD</a>	_dns-sd._udp.local.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ALL
<a href="#">Googlecast</a>	_googlecast._tcp.local.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	WIRED
<a href="#">HP Photosmart Printer 1</a>	_universal._sub._ipp._tcp.local.	<input type="checkbox"/>	<input type="checkbox"/>	ALL
<a href="#">HP Photosmart Printer 2</a>	_cups._sub._ipp._tcp.local.	<input type="checkbox"/>	<input type="checkbox"/>	ALL
<a href="#">HomeSharing</a>	_home-sharing._tcp.local.	<input type="checkbox"/>	<input type="checkbox"/>	ALL
<a href="#">Miracast</a>	_display._tcp.local.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	WIRED
<a href="#">Printer-IPP</a>	_ipp._tcp.local.	<input type="checkbox"/>	<input type="checkbox"/>	ALL
<a href="#">Printer-IPPS</a>	_ipps._tcp.local.	<input type="checkbox"/>	<input type="checkbox"/>	ALL

mDNS announcement should now be limited. First-floor users should only access the AT-UHD-SW-510W in the first-floor conference room. Second-floor users should only access the AT-UHD-SW-510W in the second-floor conference room.

## Verifying Functionality



**WARNING:** mDNS announcements may be cached by wireless client.

Some wireless clients may cache mDNS announcements so that they appear to be available, even though the client is out of range. For example, if a presentation is shared on the first floor, then the individual moves to the second-floor, the mDNS announcements from the AT-UHD-SW-510W may be shown. However, attempting to cast to the first-floor device (from the second floor) no longer works. This is caused by the end-client device caching mDNS entries.

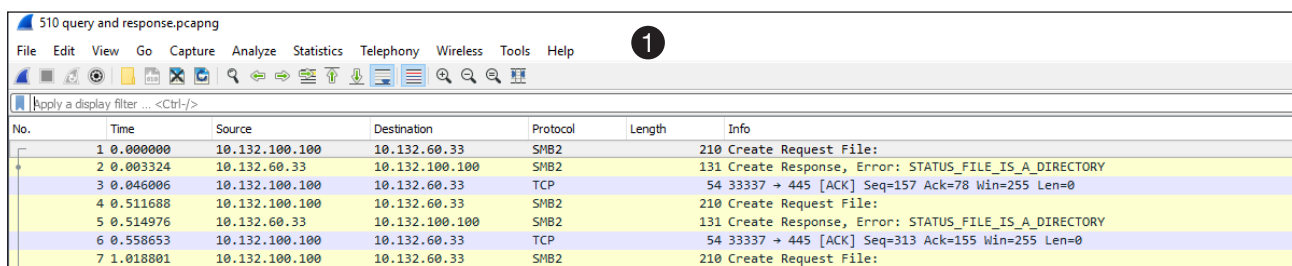
Solutions:

1. Clear the mDNS cache.
2. Use a sniffer to capture network traffic and search for announcements coming from the WLC. Refer to the instructions below for an example using Wireshark.

## Capturing Traffic and Searching for mDNS Announcements

The best way to verify mDNS announcements is to perform a packet capture. The following example uses Wireshark, which is a free packet capture tool.

1. Start the capture on the wireless interface, then beginning casting using Google Cast™. After a few moments, stop the capture.



2. In the filter box, enter the IP address.
3. Click the arrow, to the far right in the filter box, to apply the filter setting. The mDNS queries for the controller will be displayed.
4. Expand the Answers section. In this example, the AT-UHD-SW-510W with the SSID of sw510-ear1 is responding with the `_googlecast._tcp.local` service.

