



IT Deployment Guide for Wireless BYOD Products

AT-UHD-SW-510W AT-OME-MS52W AT-WAVE-101

Atlona Manuals
Switchers

Version Information

| Version | Release Date | Notes |
|---------|--------------|--|
| 4 | Dec 2022 | - updated color format - added port 7236 port to Network Ports (page 6) . |

Table of Contents

| | |
|---|-----------|
| IT Deployment Guide | 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 / AT-OME-MS52W | 7 |
| Deployment Modes | 8 |
| Basic Switcher Mode | 8 |
| Standalone Wireless Access Point / Hotspot Mode | 9 |
| Enterprise Network Mode | 11 |
| Dedicated Network Mode | 18 |
| WiFi Modes | 19 |
| Access Point | 19 |
| Connect to WiFi | 19 |
| Disabled | 19 |
| Firewall Modes | 19 |
| Block Private Network | 20 |
| Block Internet | 20 |
| Block All | 21 |
| None | 21 |
| Bandwidth Utilization | 22 |
| Chromecast™ | 22 |
| AirPlay® | 23 |
| Miracast™ over Infrastructure | 24 |
| Appendix | 25 |
| QoS and Screen Casting on the AT-UHD-SW-510W | 25 |
| Connectivity Methods | 25 |
| Reference Material | 26 |
| Microsoft Miracast over Infrastructure Connection Establishment (MS-MICE) | 27 |
| Projection Phase Detail | 28 |
| Does RTP use congestion feedback mechanisms? | 31 |
| RTCP Protocol | 32 |
| Unofficial AirPlay Protocol Specification | 33 |
| RTSP RFC | 33 |
| Configuring AirPlay/Google Cast across multiple VLANs using a Cisco WLC | 34 |
| Limiting mDNS Announcements | 39 |
| mDNS Fencing Overview | 39 |
| Important Wireless Coverage and Configuration Notice | 40 |
| Configuring Access Point Groups | 40 |
| Configuring mDNS Policies | 43 |
| Verifying Functionality | 47 |

IT Deployment Guide

Use of the term “Atlona device” within this document

Unless otherwise specified, the term “Atlona device” refers to any of the following BYOD products: AT-UHD-SW-510W, AT-OME-MS52W, or AT-WAVE-101.

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 Atlona device has a 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

This Atlona device 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 Atlona device will receive AV streams and store the first intra-coded picture frame (I-frame) and following predicted-picture (P-frame) for each stream until the new I-frame arrives. Once this occurs, all previous frames will be removed. The Atlona device 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 Atlona device delivers content using either wired or wireless protocols. Depending upon how the unit is integrated on the network, security will vary.

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

The Atlona device 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 the Wi-Fi secure layer. Each unit also has WiFi and Ethernet mode available, whereby security protocol depends on protocol itself, as illustrated in the table above.

System Access Control and Management

The Atlona device can be configured using the Web server or Velocity with Integrated 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 Atlona device will prompt the user that the default password is being used during the login session.

The Atlona device allows the user to login to the Web server using either the HTTP or HTTPS protocol. In addition, the unit can be configured to restrict the login process to the HTTPS protocol.

The Atlona device 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 Atlona device, 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 Atlona device (AT-UHD-SW-510W and AT-OME-MS52W 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

Both the AT-UHD-SW-510W and AT-OME-MS52W support 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 / AT-OME-MS52W built-in firewall option, refer to [Firewall Modes \(page 19\)](#).

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* |
| 7236 | Yes | No | Miracast RTSP Control Port |
| 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 / AT-OME-MS52W

1. Make sure the AT-UHD-SW-510W / AT-OME-MS52W is powered.
2. Insert a USB drive into the **AUX** port of the AT-UHD-SW-510W / AT-OME-MS52W.
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 / AT-OME-MS52W is listed under Ethernet #1.

Deployment Modes

The Atlona device 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 11)**
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 18)**
 - a. Dedicated mode - wired + enterprise mode - wireless

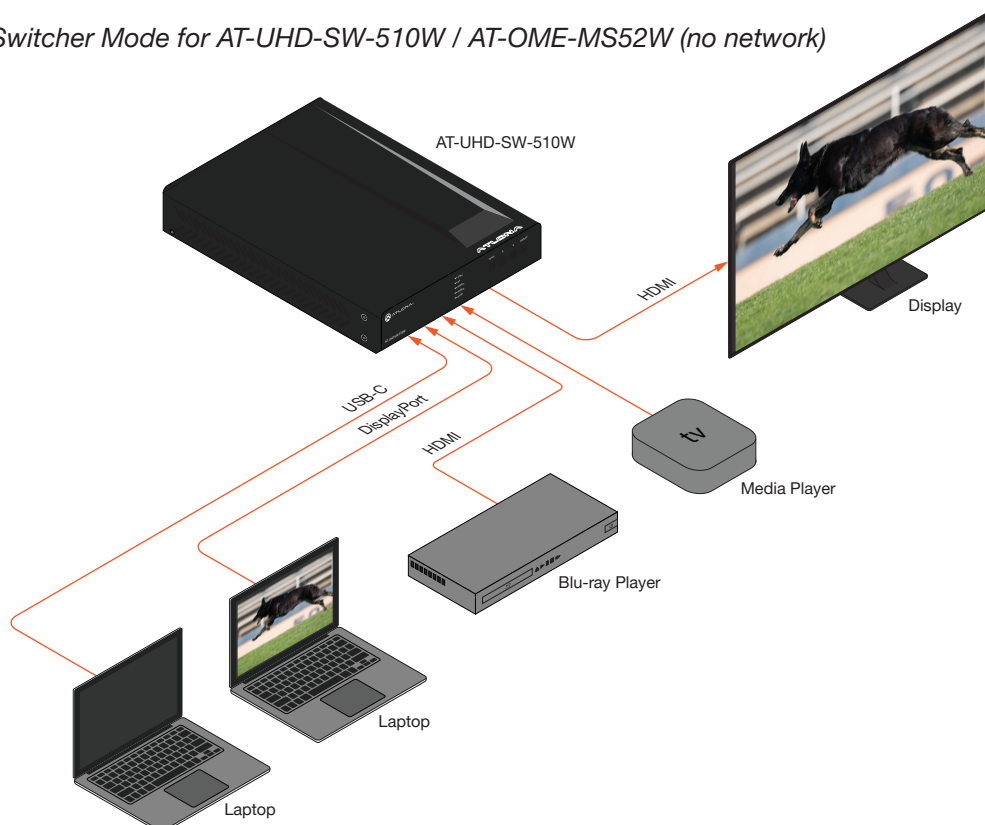
Basic Switcher Mode

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

To boot the AT-UHD-SW-510W / AT-OME-MS52W 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 for AT-UHD-SW-510W / AT-OME-MS52W (no network)



Standalone Wireless Access Point / Hotspot Mode

In this mode, the Atlona device 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 server of the Atlona device.

To change the configuration of the Atlona device in WAP/Hotspot mode, a wireless client connected to the WAP can access the unit using the WAP IP address of the Atlona device.

Figure 2 - Standalone Wireless Access Point / Hotspot Mode (AT-UHD-SW-510W / AT-OME-MS52W)

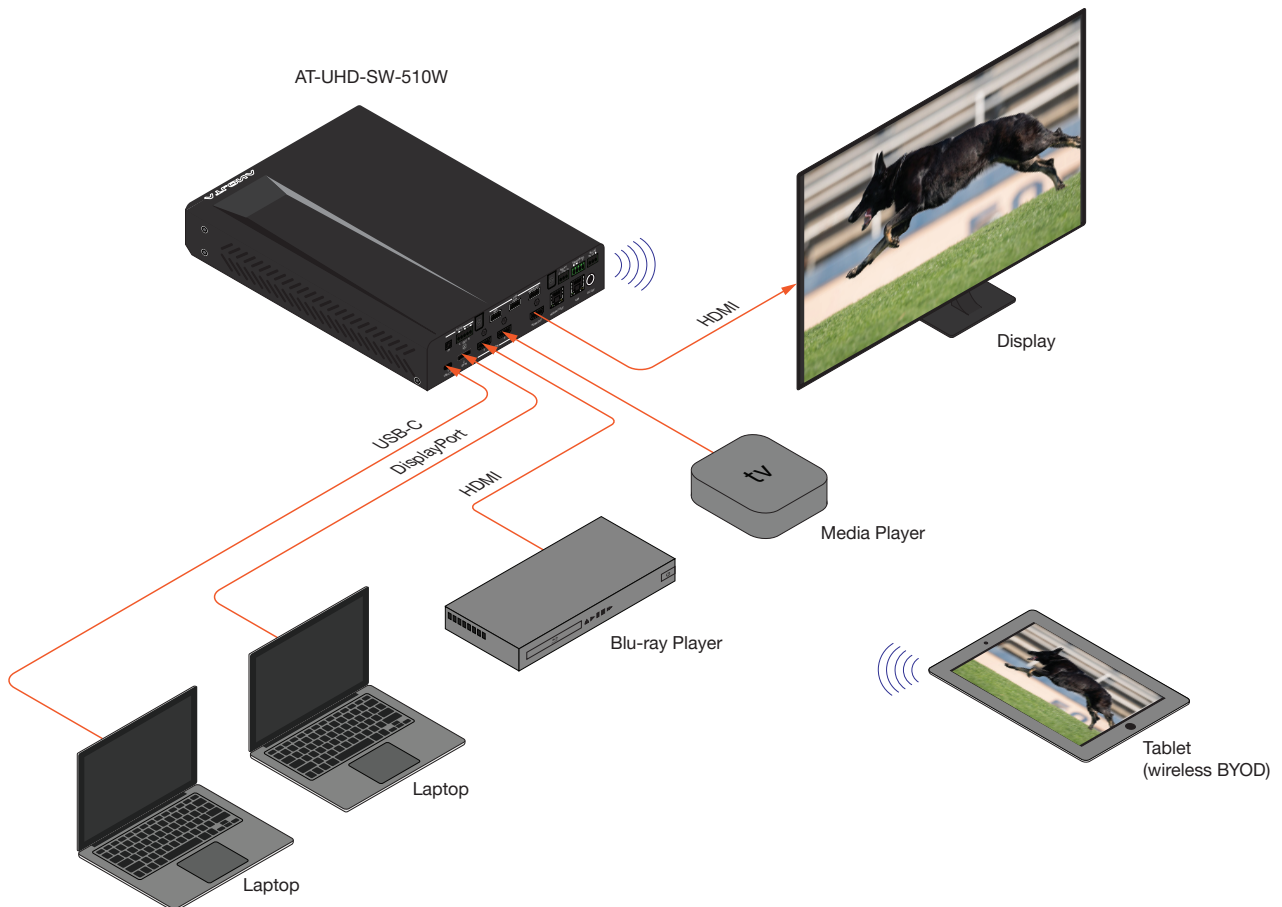
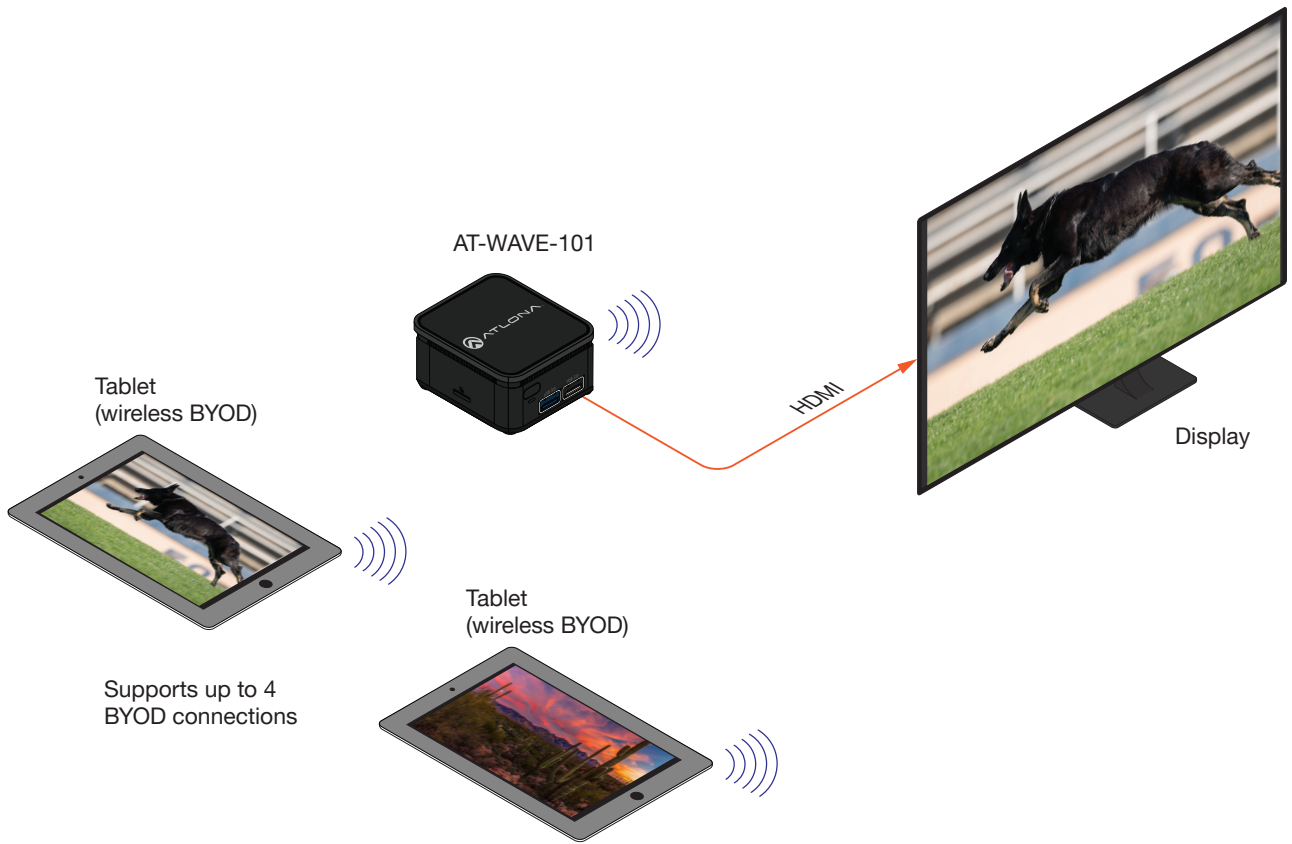


Figure 2a - Standalone Wireless Access Point / Hotspot Mode (AT-WAVE-101)



Enterprise Network Mode

The Atlona device can be integrated into the existing Enterprise Network / Guest Network by connecting the Atlona device 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 Atlona device will be connected to the Enterprise Network through the Ethernet interface present on the unit. The Atlona device 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 Atlona device, open the desired web browser and enter the IP address of the Atlona device. Refer to [Obtaining the IP Address of the AT-UHD-SW-510W / AT-OME-MS52W \(page 7\)](#) for information.



NOTE: In this mode, the AT-UHD-SW-510W / AT-OME-MS52W 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 / AT-OME-MS52W and will not interfere with the Enterprise Wireless Access Point. The antenna modules must be connected if using **Connect to WiFi** mode, **Access Point** mode, and the Miracast protocol.

Figure 3 - Wired mode (AT-UHD-SW-510W / AT-OME-MS52W)

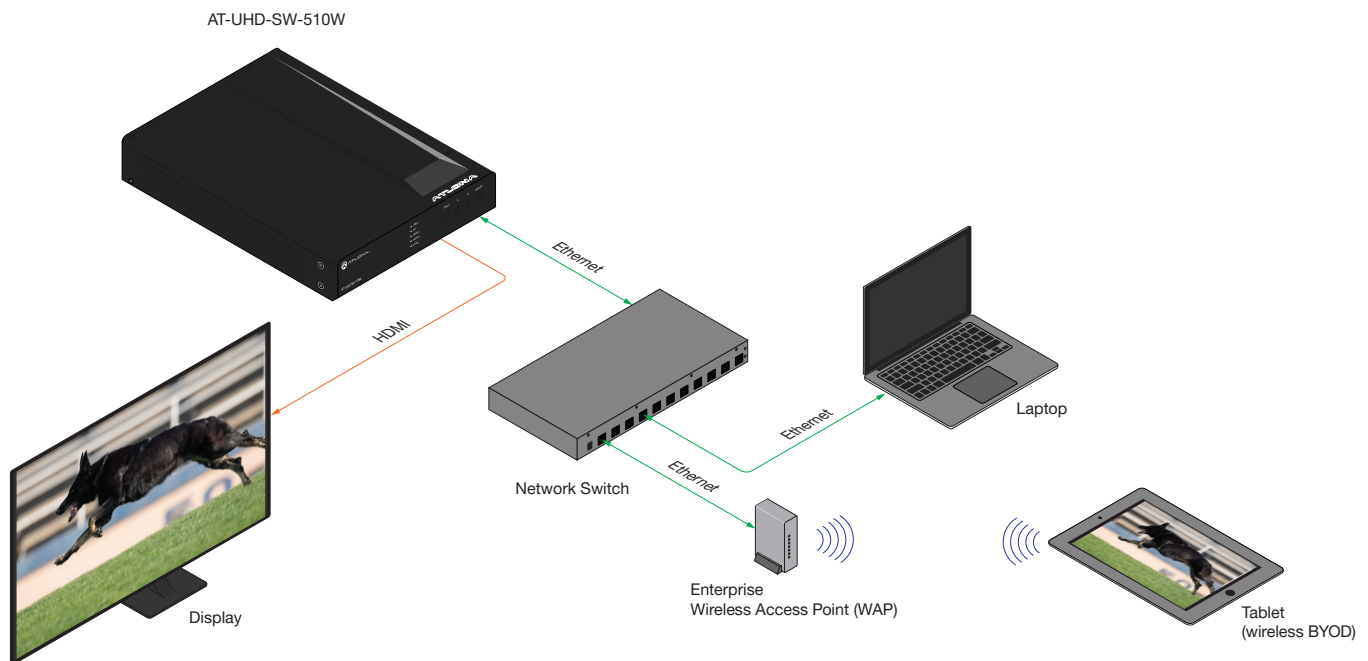
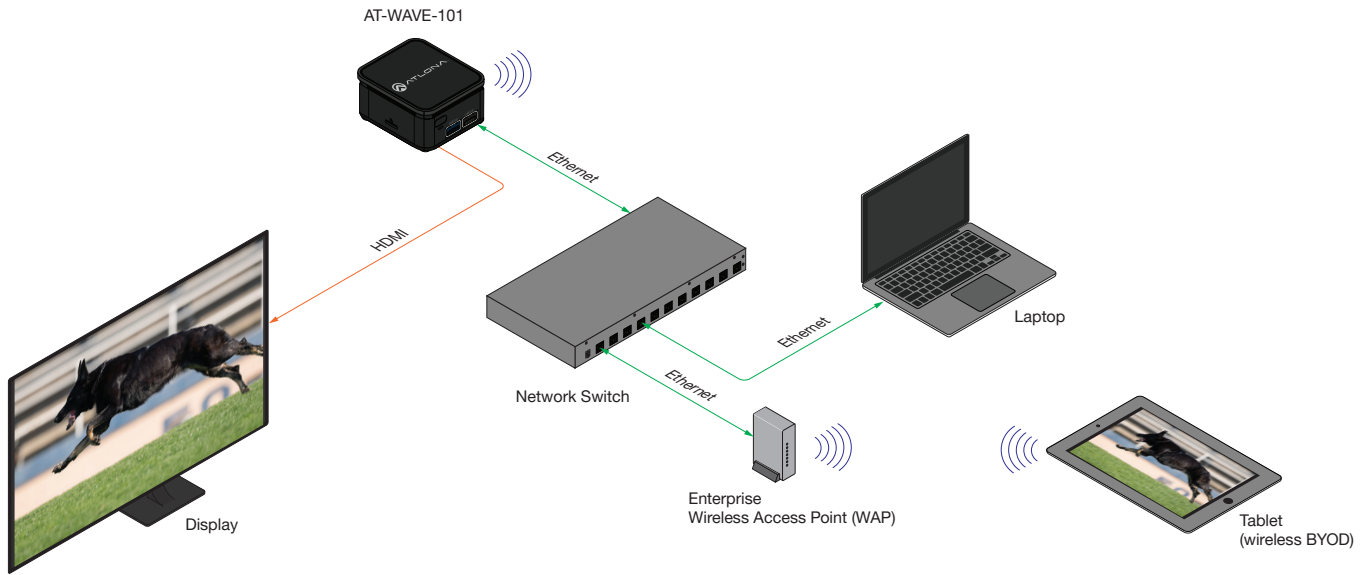


Figure 3a - Wired mode (AT-WAVE-101)



Connect Mode

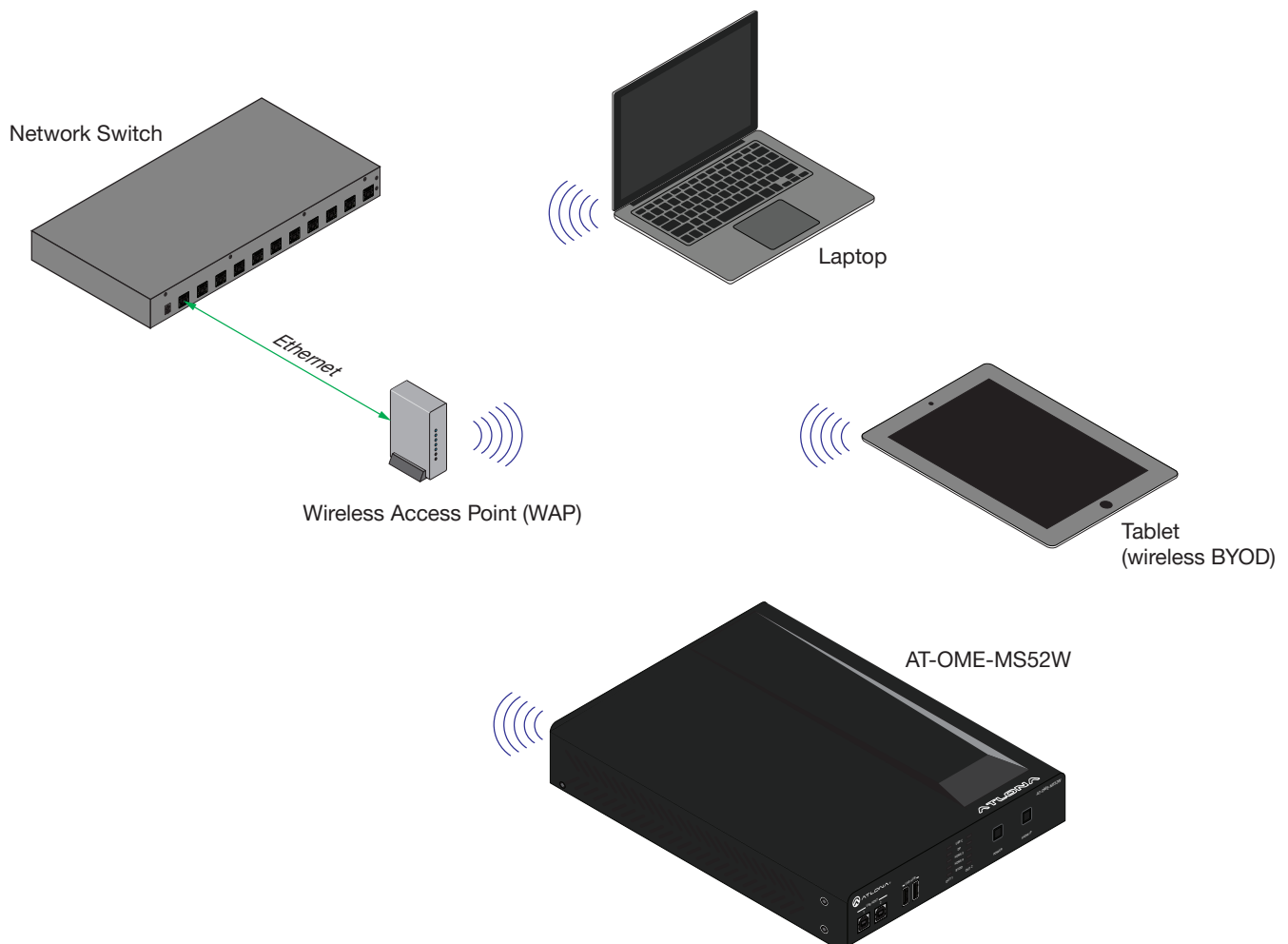
In this mode, the Atlona device will be connected to the Enterprise Network through the Wireless interface, present on the unit. The Ethernet interface on the unit will not be connected to the network.

To enable this mode, the Atlona device must already be connected to a network using the Ethernet interface.

1. Login into the web server of the Atlona device. Refer to the User Manual for more information on the login procedure.
2. In the web server, click **Administration > Networking** from the menu bar on the left.
3. Under the **WiFi** window group, select **Connect to WiFi** 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



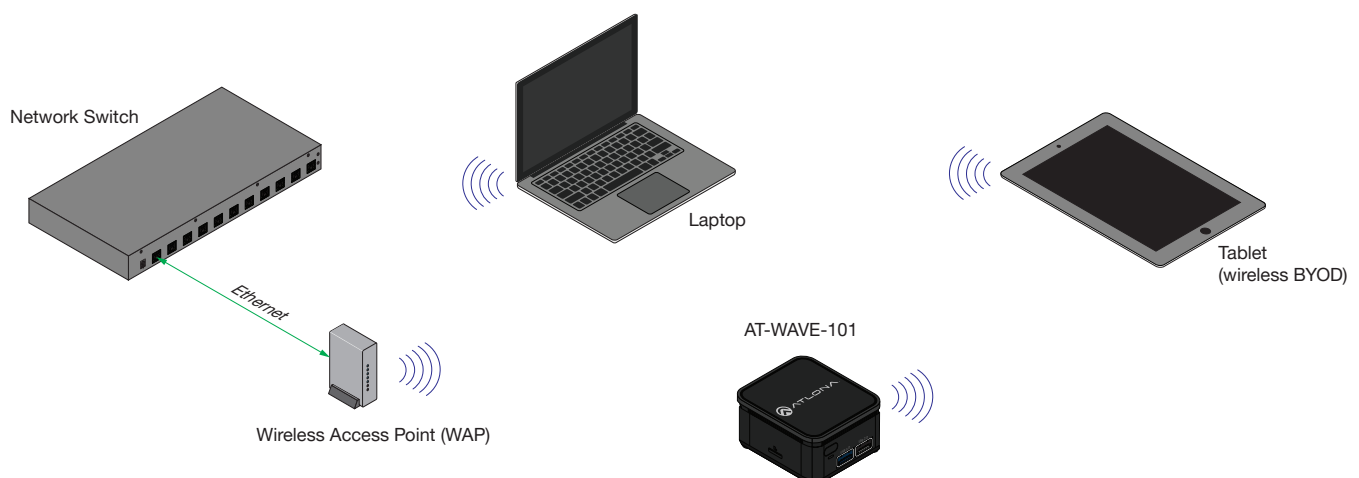
Connect Mode (WAVE-101 only)

In this mode, the Atlona device 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 Atlona device must already be connected to a network using the Ethernet interface. In order to enable the **Connect Mode**, an external Wi-Fi USB dongle must be connected to the AT-WAVE-101.

1. Go to the **Settings** page. The **Settings** page can be accessed from `http://<IP Address>/settings`.
2. Click on the **Network** tab.
3. On the right-hand side, locate the Mode drop-down list, under the **Wireless** section. The default Mode setting is **Disabled**.
4. Click the drop-down list and select **Connect Mode**.
5. Enter the SSID of the desired network in the **SSID** field. Alternatively, click the ellipsis button [...], to the right, to display a list of available networks, then click the desired network.
6. Enter the correct password in the **Password** field.
7. Click the **Type** drop-down list and select **DHCP**.
8. Click the **Gateway Priority** drop-down list and select **Ethernet**.
9. Click the **SAVE** button.
10. The **Detected possible IP address change** screen will be displayed and will auto-refresh after approximately 10 seconds.
11. Once the unit connects to the external Wi-Fi, the status indicator, under the **Wireless** section, will be green. Hovering the mouse pointer over the indicator should display **Connected**. The MAC address will also be displayed under the indicator.

Figure 4a - Connect Mode (AT-WAVE-101)



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 / AT-OME-MS52W to operate in this mode, connect the Ethernet interface of the AT-UHD-SW-510W / AT-OME-MS52W 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 / AT-OME-MS52W firewall can be used to block Internet access to guest users. Refer to the [Firewall Modes \(page 19\)](#) section of this guide for more information.

Figure 5 - Wired plus Guest Wireless Mode (AT-UHD-SW-510W / AT-OME-MS52W)

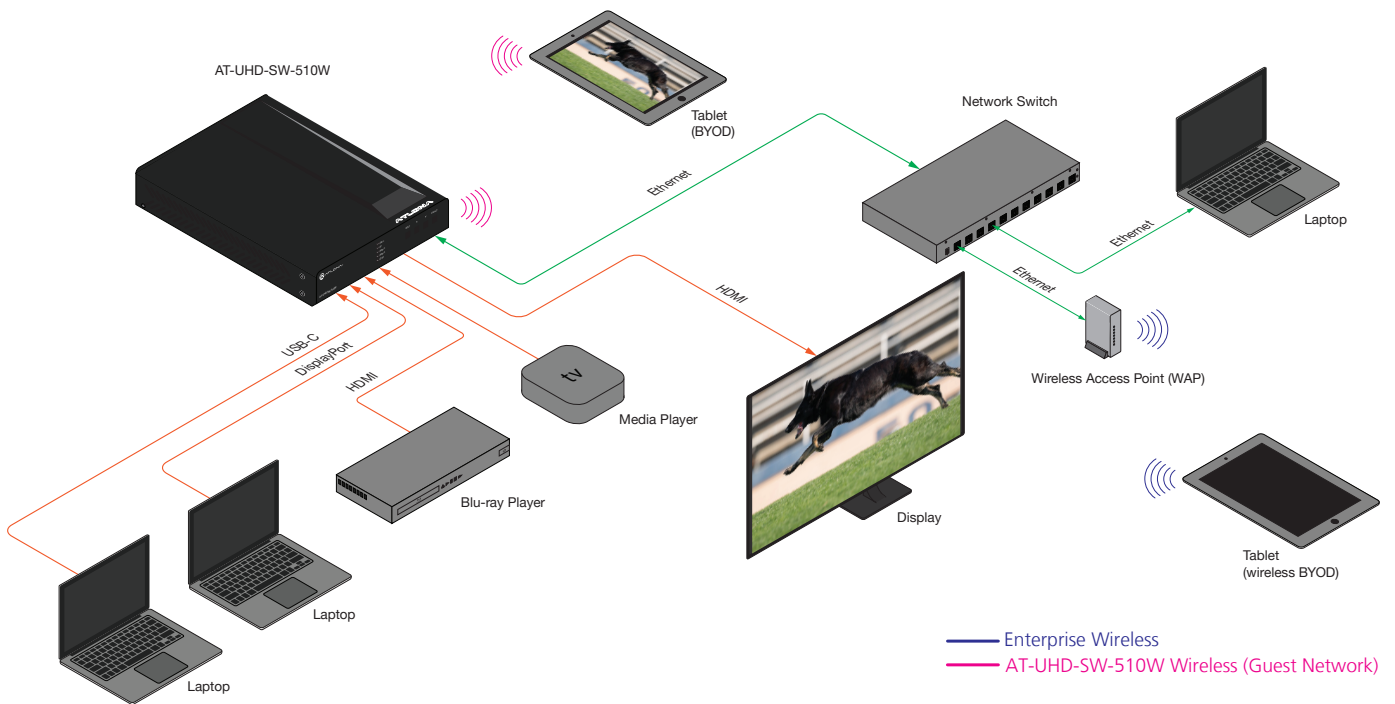
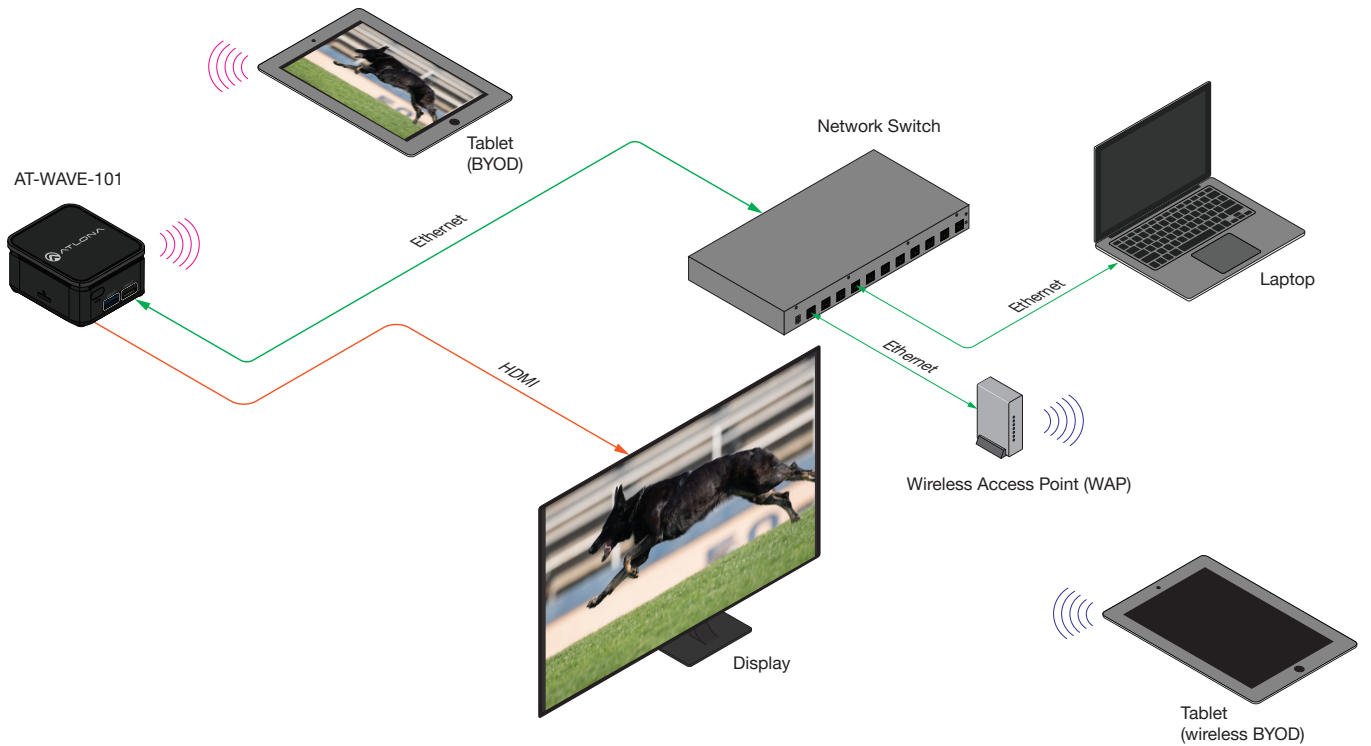


Figure 5a - Wired plus Guest Wireless Mode (AT-WAVE-101)



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.

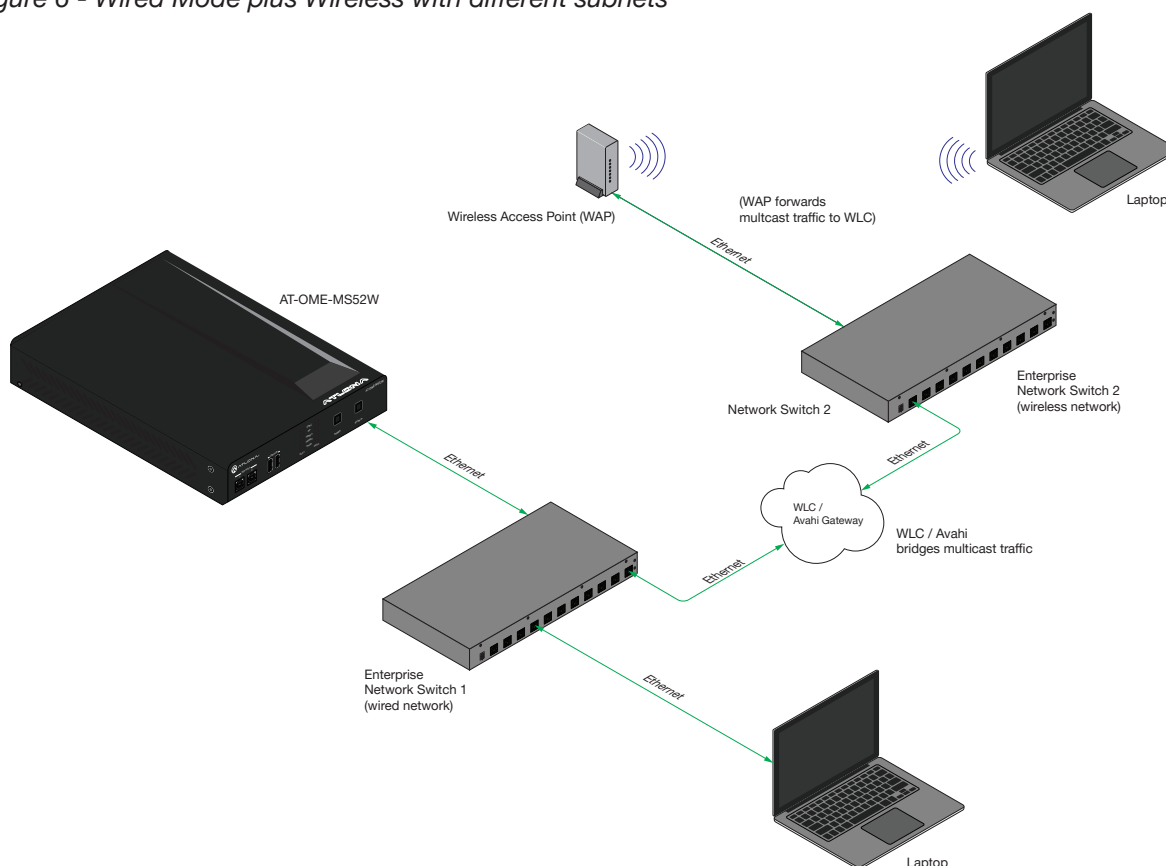
To make the Bonjour/DNS-SD to flow between multiple VLANs, we need to either have multicast routing enabled on the network or have a Wireless LAN Controller (for wireless) that can handle the multicast routing.

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 \(page 34\)](#).

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



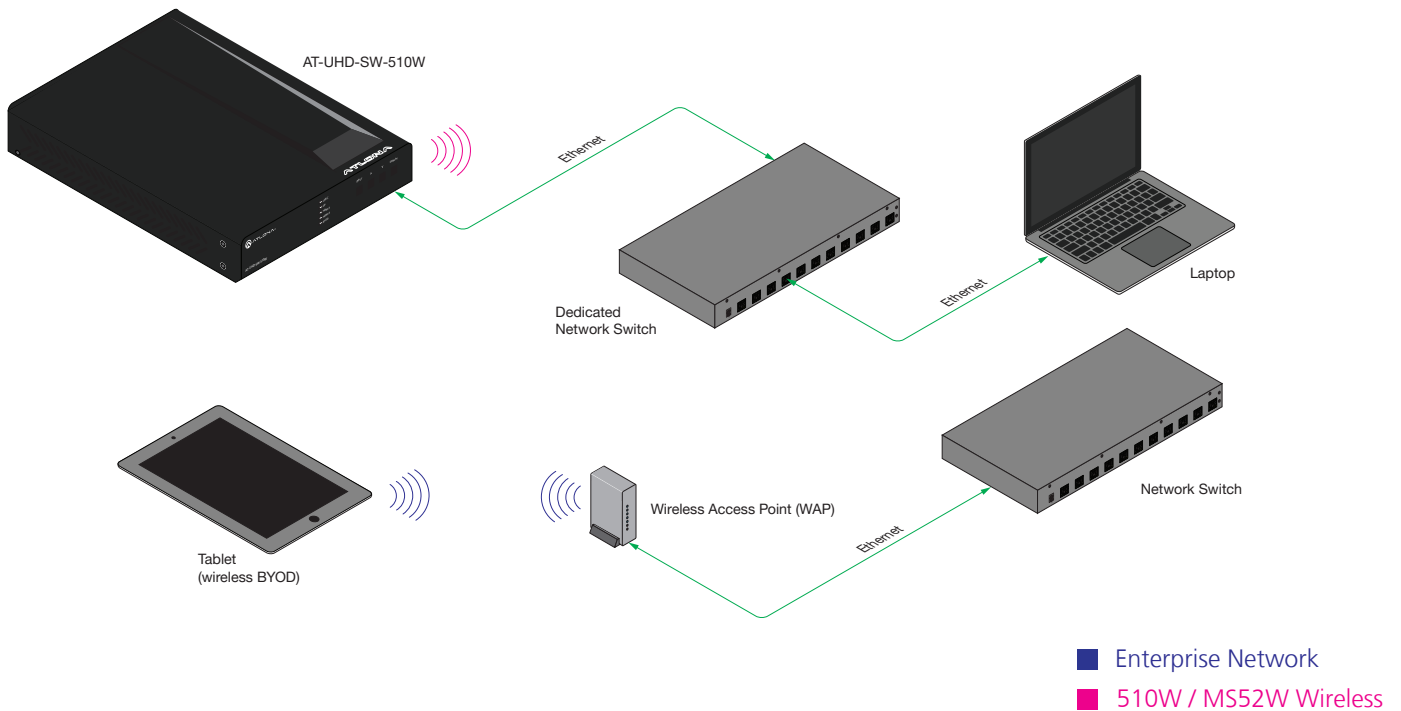
Dedicated Network Mode

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-510W / AT-OME-MS52W 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 / AT-OME-MS52W 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 / AT-OME-MS52W has three WiFi modes: **Access Point**, **Connect to WiFi**, and **Disabled**. To set the WiFi mode, access the web server, click **Administration** > **Networking** in the side menu bar, then click the **Mode** drop-down list, under the **WiFi** window group. Refer to the User Manual for more information.

Access Point

Select this option to configure the AT-UHD-SW-510W / AT-OME-MS52W as a Wireless Access Point, allowing other wireless devices to connect to the same wired network as the AT-UHD-SW-510W / AT-OME-MS52W.

Connect to WiFi

Select this option to allow the AT-UHD-SW-510W / AT-OME-MS52W to connect to an available wireless network.

Disabled

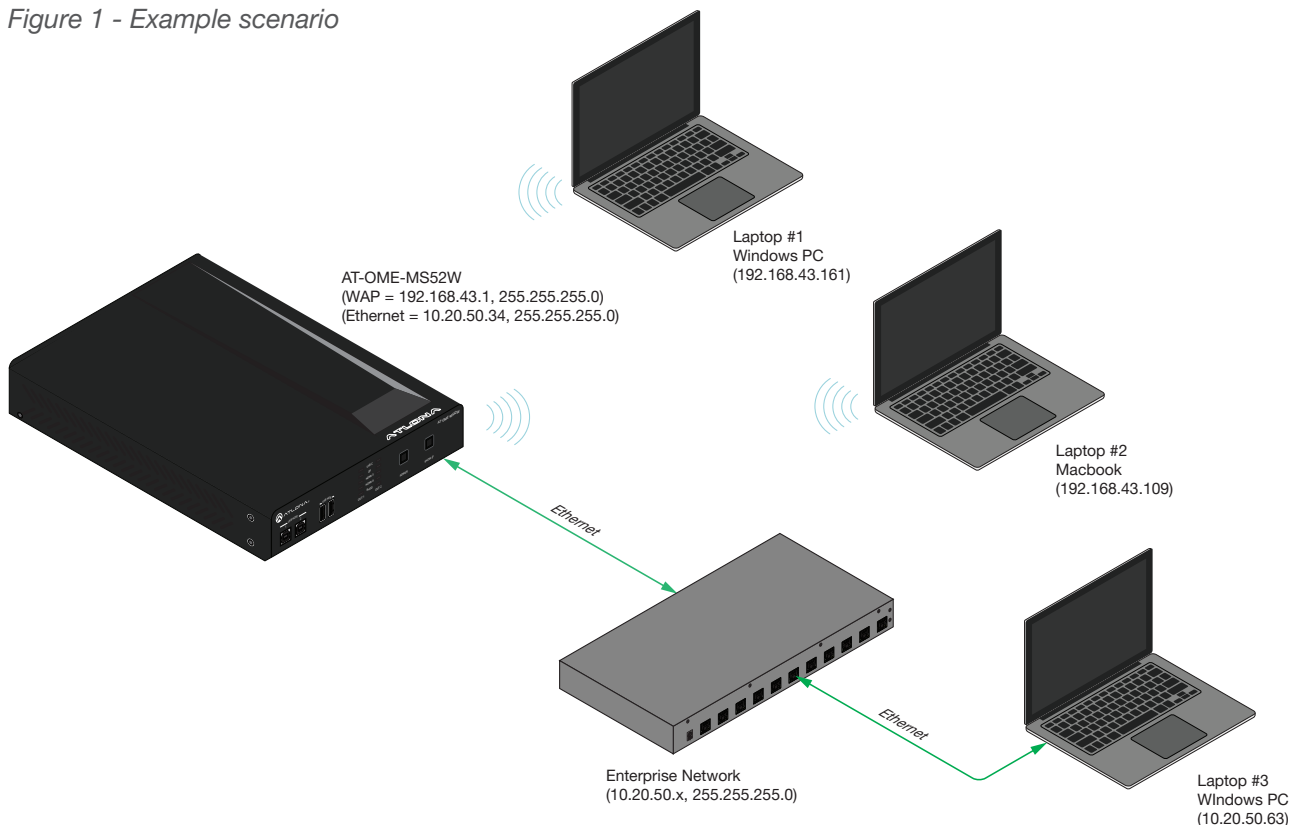
Select this option to disable WiFi on the AT-UHD-SW-510W / AT-OME-MS52W.

Firewall Modes

When **Access Point** is selected from the **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 / AT-OME-MS52W 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 / AT-OME-MS52W private network.

- Clients connected to the AT-UHD-SW-510W / AT-OME-MS52W WAP, will have access to the clients present on the same private network.
- Clients connected to the AT-UHD-SW-510W / AT-OME-MS52W 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 / AT-OME-MS52W 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 / AT-OME-MS52W WAP do not have access to the Internet.
- Clients connected to the AT-UHD-SW-510W / AT-OME-MS52W WAP, have access to the clients present on the same private network.
- Clients connected to the AT-UHD-SW-510W / AT-OME-MS52W 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 / AT-OME-MS52W and can be accessed using 192.168.43.1 and 10.20.50.34. 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 / AT-OME-MS52W WAP have access to the clients present on the same private network.
- Clients connected to the AT-UHD-SW-510W / AT-OME-MS52W 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 / AT-OME-MS52W 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 / AT-OME-MS52W. All incoming and outgoing traffic is permitted.

- All available networks are reachable.
- Clients connected to the AT-UHD-SW-510W / AT-OME-MS52W WAP, have access to clients that are connected to the same private network.
- Clients connected to the AT-UHD-SW-510W / AT-OME-MS52W 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 / AT-OME-MS52W 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).

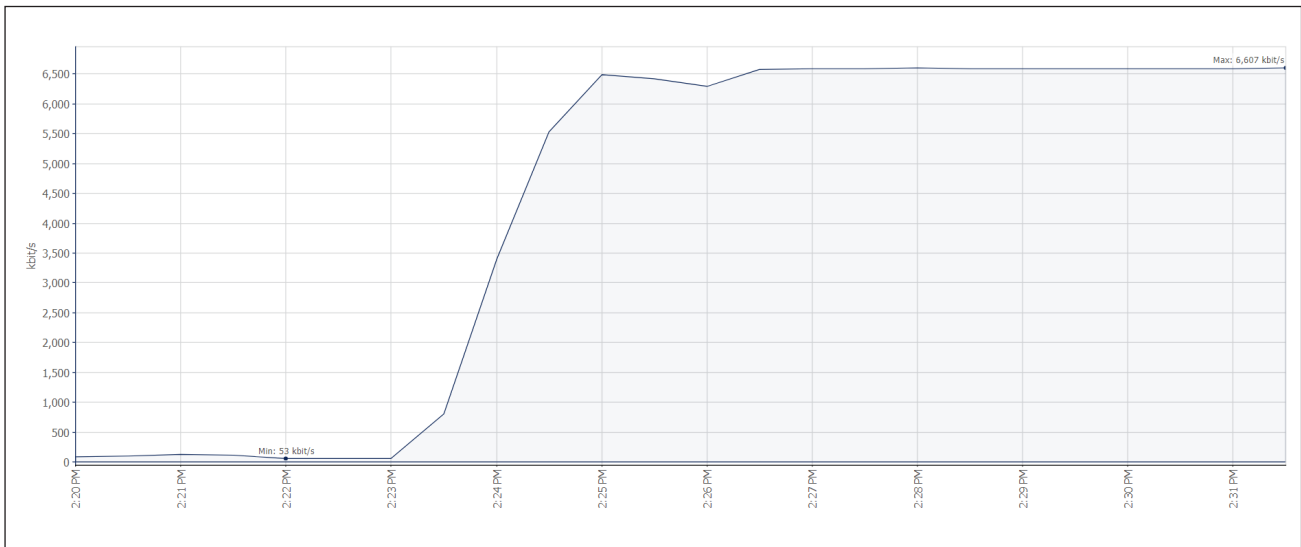
Bandwidth Utilization

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™

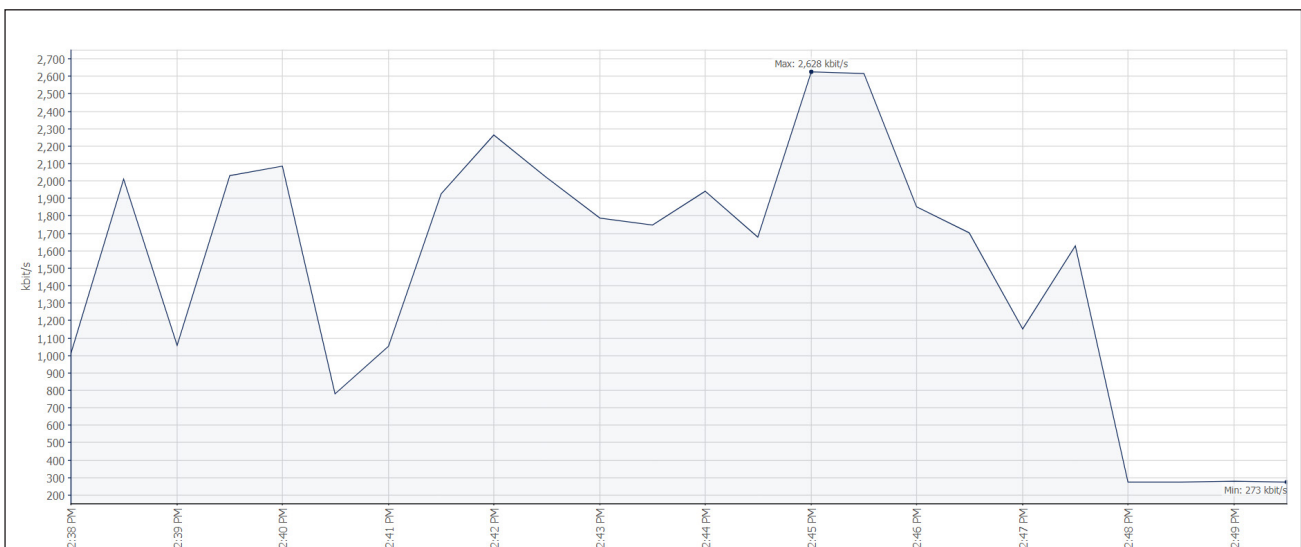
Video Content (1920 x 1080p @ 59.94 Hz / 60 Hz)

- Maximum bandwidth consumption: ~ 6.607 Mbps



Document (with random scrolling)

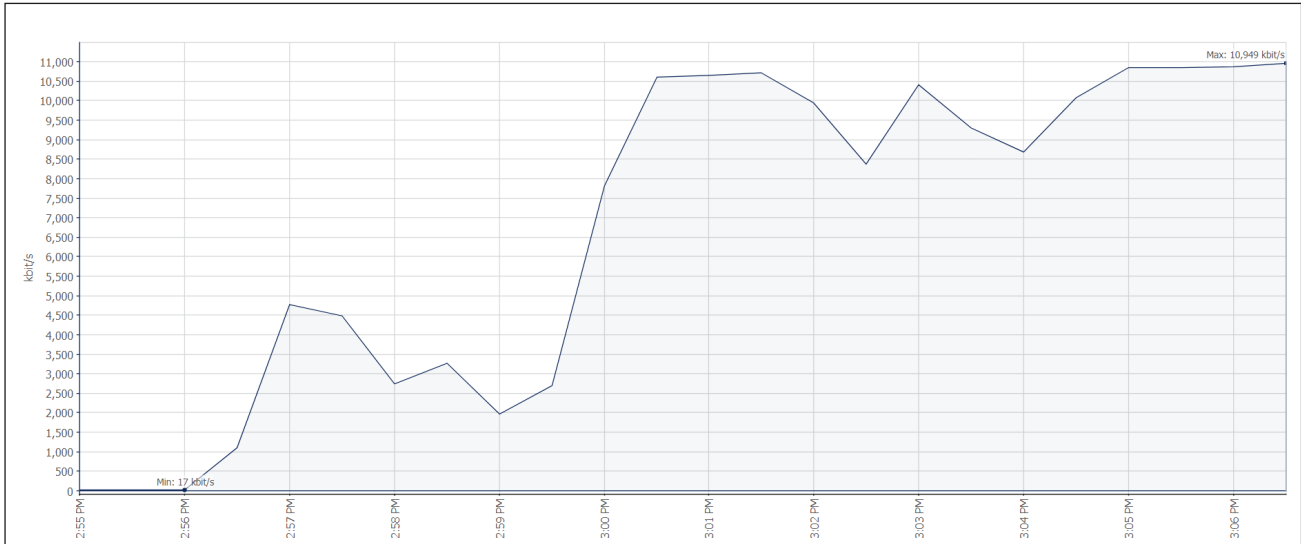
- Maximum bandwidth consumption: ~ 2.628 Mbps



AirPlay®

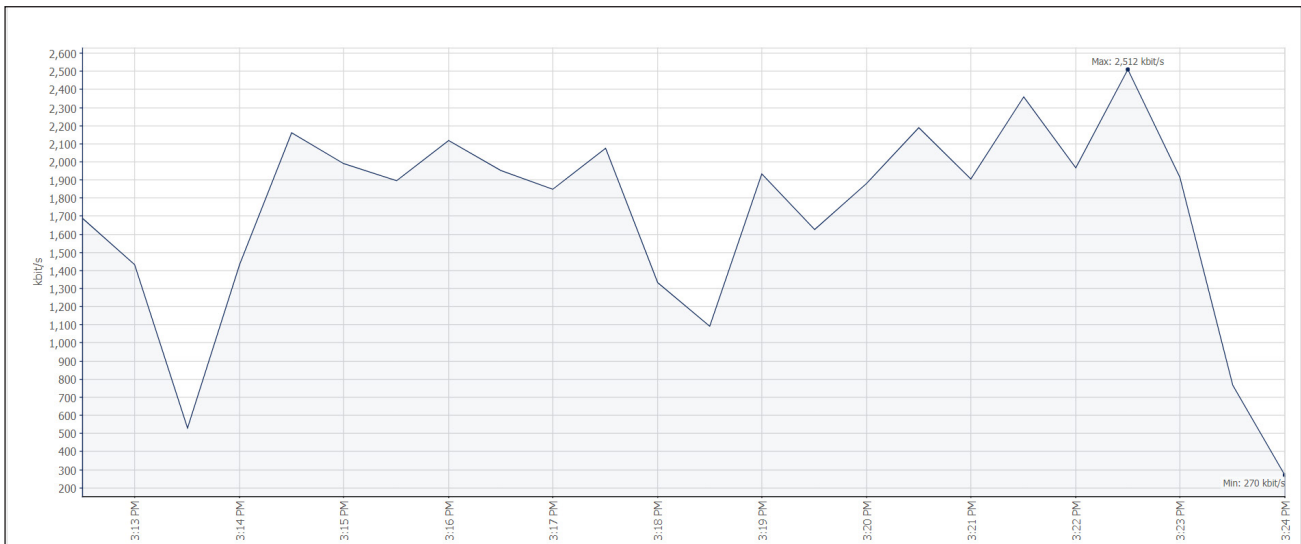
Video Content (1920 x 1080p @ 59.94 Hz / 60 Hz)

- Maximum bandwidth consumption: ~ 10.949 Mbps



Document (with random scrolling)

- Maximum bandwidth consumption: ~ 2.512 Mbps



Miracast™ over Infrastructure

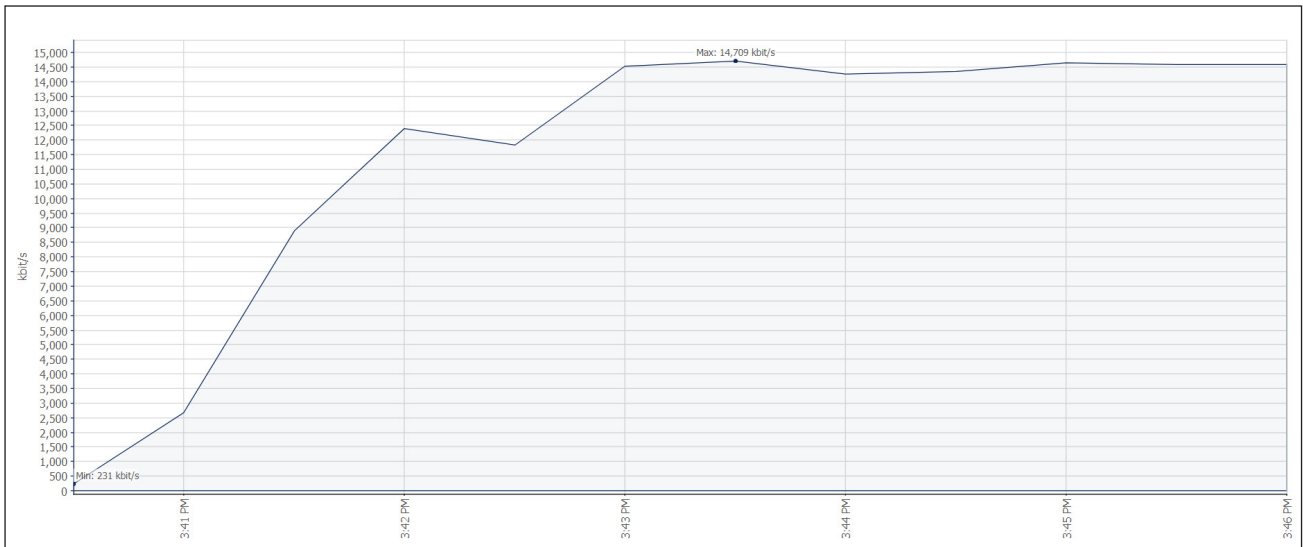
For more information on Miracast, refer to the following link: [Miracast over Infrastructure](#)



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

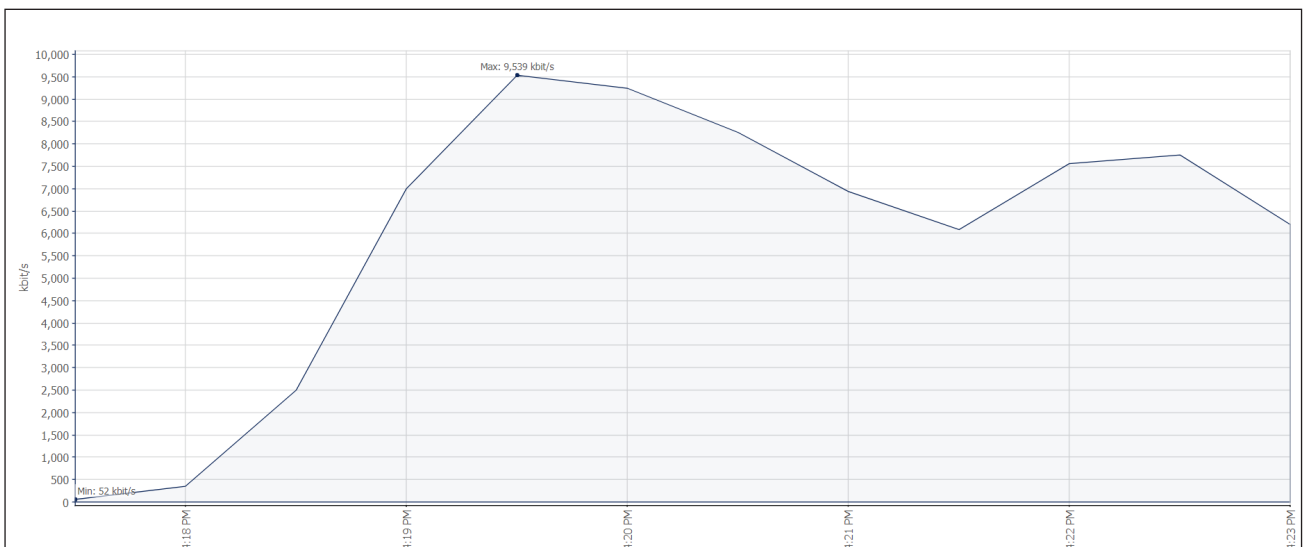
Video Content (1920 x 1080p @ 59.94 Hz / 60 Hz)

- Maximum bandwidth consumption: ~ 14.709 Mbps



Document (with random scrolling)

- Maximum bandwidth consumption: ~ 9.539 Mbps



Appendix

QoS and Screen Casting on the AT-UHD-SW-510W

Quality of Service (QoS) is a group of technologies that work to ensure reliable timely delivery of high-priority applications and traffic during times of limited network capacity and constrained resources. QoS accomplishes this by differentiated handling and capacity allocation for specific flows of traffic. This enables the network administrator to assign prioritization of traffic and the amount of bandwidth assigned per application or traffic flow.

Network design can alleviate many QOS problems. More bandwidth solves most issues. Building physically separate video networks and keeping traffic local to one network switch are other ways to avoid bottlenecks with design. Use QoS when these redesign options aren't feasible.

The AT-UHD-SW-510W supports many connectivity methods to cast video. The first step is to determine which method is being used.

Connectivity Methods

- **Microsoft Miracast P2P (MS-P2P)**
Client discovers the AT-UHD-SW-510W using SSID discovery. Miracast creates a wireless direct connection from the client to the AT-UHD-SW-510W, which is used for all following communication. This direct wireless connection (not to be confused with connecting to the AT-UHD-SW-510W wirelessly via the configured SSID, or traditional WiFi) is sometimes referred to as WiDi, Miracast, or Traditional Miracast.
- **Miracast over Infrastructure (MS-MICE)**
Client connects wired or wirelessly to a network the AT-UHD-SW-510W is connected to. This includes connecting to the configured AT-UHD-SW-510W SSID using WiFi. Miracast discovery and streaming take place over the network infrastructure.
- **Google Cast**
Client connects wired or wirelessly to a network the AT-UHD-SW-510W is connected to. This includes connecting to the configured AT-UHD-SW-510W SSID using WiFi. Google Cast discovery and streaming take place over the network infrastructure.
- **Airplay**
Client connects wired or wirelessly to a network the AT-UHD-SW-510W is connected to. Airplay discovery and streaming take place over the network infrastructure.

P2P Casting

Because Miracast P2P use direct wireless connections to the AT-UHD-SW-510W traditional QoS strategies are not effective. Performance issues when using direct wireless connections typically are related to the wireless connection itself and the surrounding wireless airspace. Miracast P2P casting also does not perform as well as infrastructure modes (MS-MICE, AirPlay and Google Cast). Infrastructure modes typically support larger bitrates and higher quality video stream.

Infrastructure Mode Casting

Casting over Infrastructure can provide higher throughput but in a shared infrastructure there can be competing traffic and congestion. Miracast, AirPlay and Google Cast all use Real-time Transport Protocol (RTP) for the underlying transport protocol while casting. RTP can run over TCP or UDP and works in conjunction with RTP Streaming Protocol (RTSP) and RTP Control Protocol (RTCP). RTP does not have any specific QOS mechanism built in and leaves congestion mechanisms to be handled by the upper level application.

Casting Protocol Specifics

- Miracast MS-MICE mode uses RTSP to setup streaming and RTP via UDP port 4100 for streaming. Miracast also sets DSCP markings by default of CS5.
- AirPlay uses a HTTP server to setup streaming. Screen casting uses RTP over TCP port 7100. Apple sets a default DSCP marking by default of CS4.
- Google Cast uses RTP over UDP transferring over dynamic ports between 32768-61000. Googlecast traffic does not get DSCP markings by default.

Summary

All three casting protocols supported by the SW-510W operate slightly different, but they all support bit-rate adjustment to handle congestion. When these mechanisms aren't sufficient on their own, use the protocol specific information found above to classify and reserve bandwidth.

Reference Material

<https://tools.ietf.org/html/rfc7826#page-50>

Since RTSP messages are transmitted using reliable transport protocols, they MUST NOT be retransmitted at the RTSP level. Instead, the implementation must rely on the underlying transport to provide reliability. The RTSP implementation may use any indication of reception acknowledgment of the message from the underlying transport protocols to optimize the RTSP behavior.

<https://www.ietf.org/rfc/rfc3550.txt>

RTP Congestion Control

10. Congestion Control

All transport protocols used on the Internet need to address congestion control in some way [31]. RTP is not an exception, but because the data transported over RTP is often inelastic (generated at a fixed or controlled rate), the means to control congestion in RTP may be quite different from those for other transport protocols such as TCP. In one sense, inelasticity reduces the risk of congestion because the RTP stream will not expand to consume all available bandwidth as a TCP stream can. However, inelasticity also means that the RTP stream cannot arbitrarily reduce its load on the network to eliminate congestion when it occurs.

| | | |
|---------------------|-----------------|-----------|
| Schulzrinne, et al. | Standards Track | [Page 67] |
| RFC 3550 | RTP | July 2003 |

Since RTP may be used for a wide variety of applications in many different contexts, there is no single congestion control mechanism that will work for all. Therefore, congestion control SHOULD be defined in each RTP profile as appropriate. For some profiles, it may be sufficient to include an applicability statement restricting the use of that profile to environments where congestion is avoided by engineering. For other profiles, specific methods such as data rate adaptation based on RTCP feedback may be required.

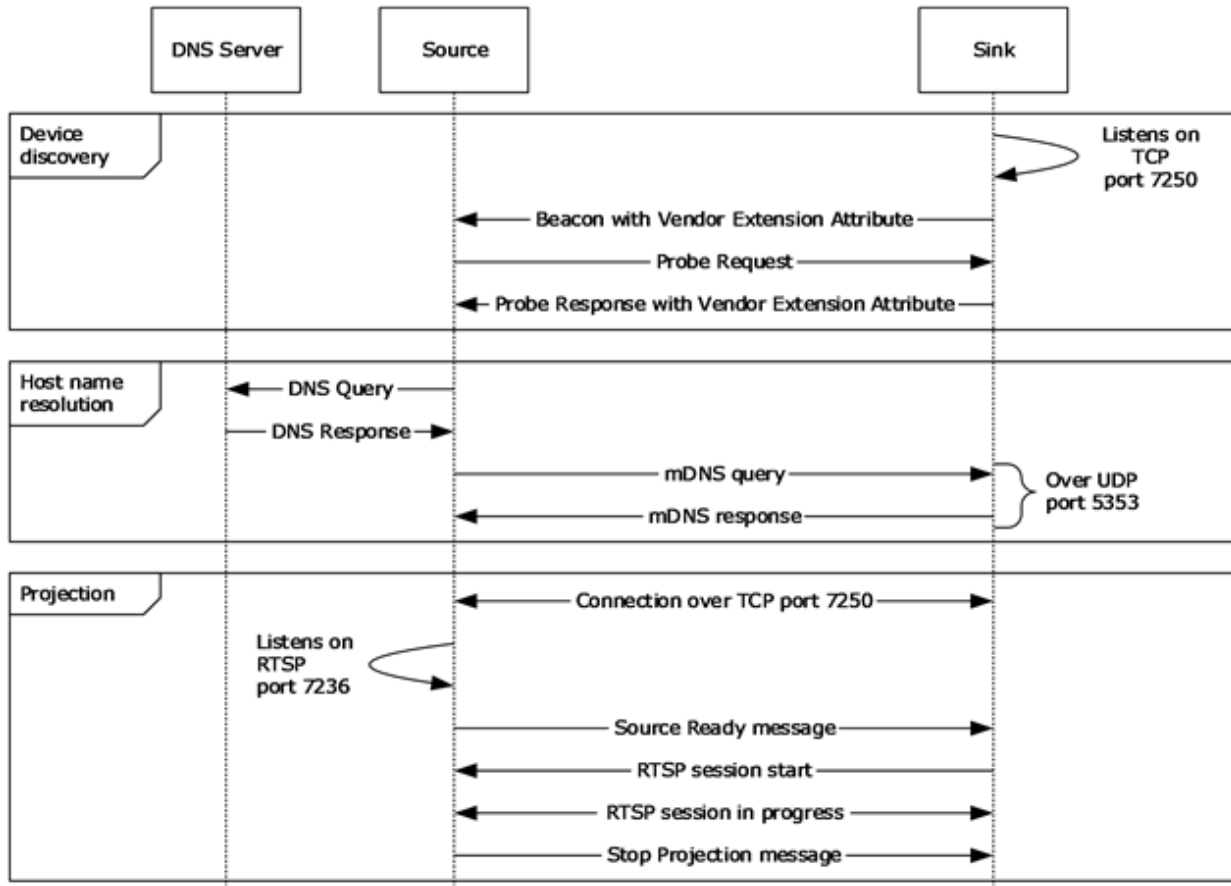
<https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/wireless-projection-receiver-manufacturers>

Microsoft real time bitrate modulation

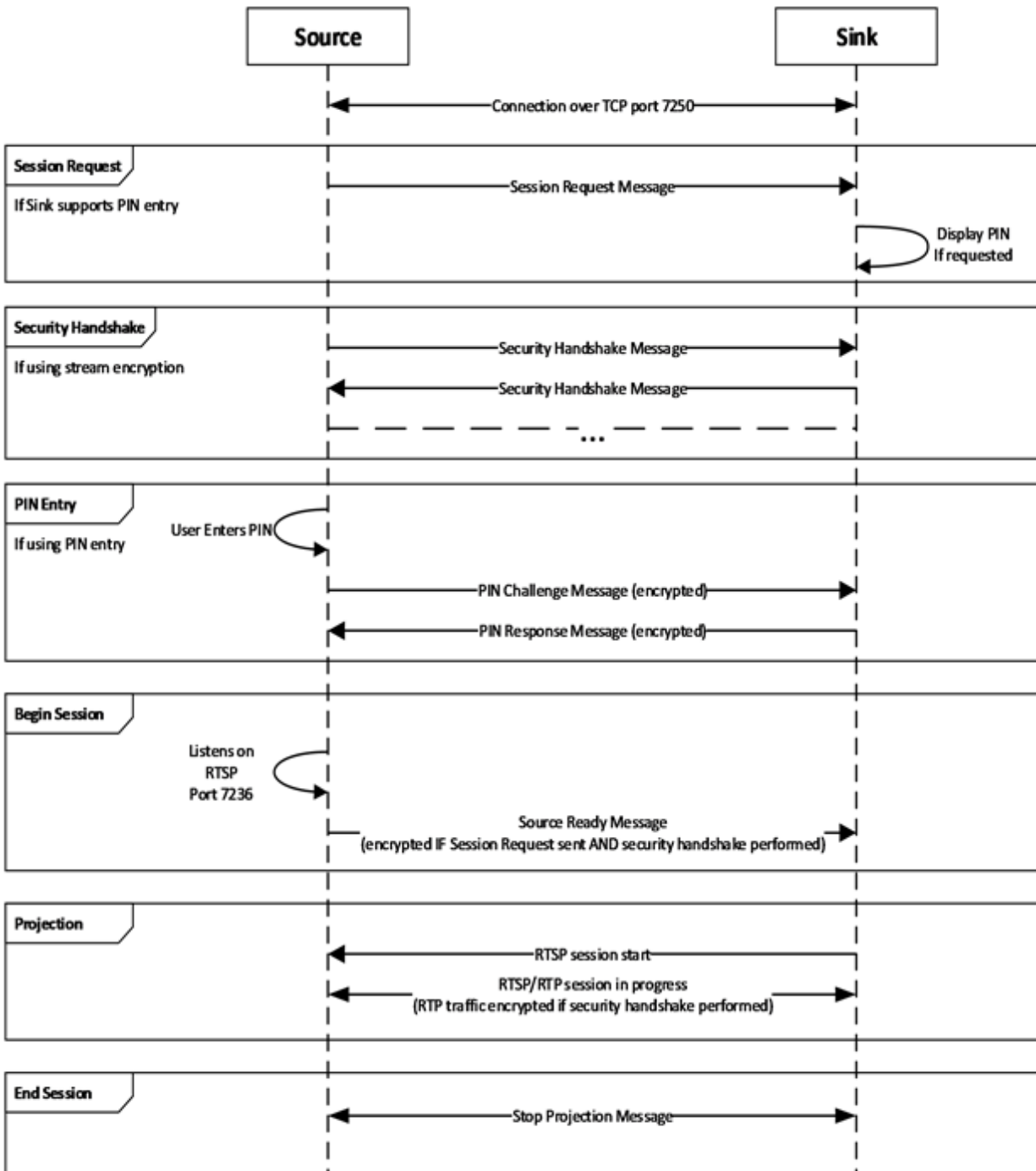
The Microsoft Miracast source supports RTCP to track a user's current network condition. Using packet information from RTCP in conjunction with format change capability, the Microsoft Miracast source modulates the bitrate to provide a smooth streaming experience even in poor network conditions. In addition, if a user's network conditions are good, the bitrate increases, providing a better-quality stream.

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-mice/940d808c-97f8-418e-a8a9-c471dc0d21bb

Microsoft Miracast over Infrastructure Connection Establishment (MS-MICE)



Projection Phase Detail



Source OPTIONS * RTSP/1.0\r\n
Sink RTSP/1.0 200 OK

Source GET_PARAMETER rtsp://localhost/wfd1.0 RTSP/1.0 (text/parameters)
Sink

OPTIONS * RTSP/1.0
Require: org.wfa.wfd1.0
CSeq: 1

RTSP/1.0 200 OK
Server: Reflector/2.6
Public: org.wfa.wfd1.0, SET_PARAMETER, GET_PARAMETER
CSeq: 1

OPTIONS * RTSP/1.0
Require: org.wfa.wfd1.0
CSeq: 2

RTSP/1.0 200 OK
Server: MSMiracastSource/10.00.18362.0657 guid/D090ABD8-EC1F-0005-379E-94D01FECD501
Public: org.wfa.wfd1.0, SETUP, TEARDOWN, PLAY, PAUSE, GET_PARAMETER, SET_PARAMETER
CSeq: 2

GET_PARAMETER rtsp://localhost/wfd1.0 RTSP/1.0
Content-Length: 673
Content-Type: text/parameters
CSeq: 2

wfd_video_formats
wfd_audio_codecs
wfd_client_rtp_ports
wfd_display_edid
wfd_connector_type
wfd_uibc_capability
wfd2_rotation_capability
wfd2_video_formats
wfd2_audio_codecs
wfd2_video_stream_control
wfd_content_protection
wfd_idr_request_capability
intel_friendly_name
intel_sink_manufacturer_name
intel_sink_model_name
intel_sink_version
intel_sink_device_URL
microsoft_latency_management_capability
microsoft_format_change_capability
microsoft_diagnostics_capability
microsoft_cursor
microsoft_rtcp_capability
microsoft_video_formats
microsoft_max_bitrate
microsoft_multiscreen_projection
microsoft_audio_mute
microsoft_color_space_conversion
RTSP/1.0 200 OK

Content-Type: text/parameters
Content-Length: 1245
CSeq: 1

wfd_client_rtp_ports: RTP/AVP/UDP;unicast 4100 0 mode=play
wfd_display_edid: 0001
00ffffffff00068c1120000000001150103801009780aee91a3544c99260f5054a108008180614045....
wfd_connector_type: 05
wfd_uibc_capability: none
wfd2_rotation_capability: none
wfd2_video_formats: 38 01 01 0010 0000000194a1 000005155555 000000000555 00 0000 001f
11, 01 02 0010 0000000194a1 000005155555 000000000555 00 0000 001f 11 00
wfd2_audio_codecs: LPCM 00000003 00
wfd2_video_stream_control: none
wfd_content_protection: none
wfd_idr_request_capability: 1
intel_friendly_name: huddle2
intel_sink_manufacturer_name: Atlona
intel_sink_model_name: SW-510
intel_sink_version: none
intel_sink_device_URL: http://www.atlona.com
microsoft_latency_management_capability: none
microsoft_format_change_capability: none
microsoft_diagnostics_capability: none
microsoft_cursor: none
microsoft_rtcp_capability: supported
microsoft_video_formats: none
microsoft_max_bitrate: none
microsoft_multiscreen_projection: none
microsoft_audio_mute: none
microsoft_color_space_conversion: none
SET_PARAMETER rtsp://localhost/wfd1.0 RTSP/1.0
Content-Length: 284
Content-Type: text/parameters
CSeq: 3

wfd2_video_formats: 00 01 04 0010 000000000080 000000000000 000000000000 00 0000 0000
00 00
wfd2_audio_codecs: LPCM 00000002 00
wfd_presentation_URL: rtsp://10.0.1.84/wfd1.0/streamid=0 none
wfd_client_rtp_ports: RTP/AVP/UDP;unicast 4100 0 mode=play
intel_overscan_comp: x=0, y=0
RTSP/1.0 200 OK
CSeq: 3

SET_PARAMETER rtsp://localhost/wfd1.0 RTSP/1.0
Content-Length: 27
Content-Type: text/parameters
CSeq: 4

wfd_trigger_method: SETUP
RTSP/1.0 200 OK
CSeq: 4

SETUP rtsp://10.0.1.84/wfd1.0/streamid=0 RTSP/1.0
Transport: RTP/AVP/UDP;unicast;client_port=4100-4101
CSeq: 3

```
RTSP/1.0 200 OK
Transport: RTP/AVP/UDP;unicast;client_port=4100-4101;server_port=51447-
7492;ssrc=b51791e6;rtcp-fb-ssrc=b51791e7
Server: MSMiracastSource/10.00.18362.0657 guid/D090ABD8-EC1F-0005-379E-94D01FECD501
Blocksize: 1450
Session: 1053406594
CSeq: 3
```

```
PLAY rtsp://10.0.1.84/wfd1.0/streamid=0 RTSP/1.0
session: 1053406594
CSeq: 4
```

```
RTSP/1.0 200 OK
Server: MSMiracastSource/10.00.18362.0657 guid/D090ABD8-EC1F-0005-379E-94D01FECD501
Date: Tue, 03 Mar 2020 01:03:45 GMT
Session: 1053406594
CSeq: 4
```

```
SET_PARAMETER rtsp://10.0.1.84/wfd1.0/streamid=0 RTSP/1.0
Content-Type: text/parameters
Session: 1053406594
CSeq: 5
Content-Length: 17
```

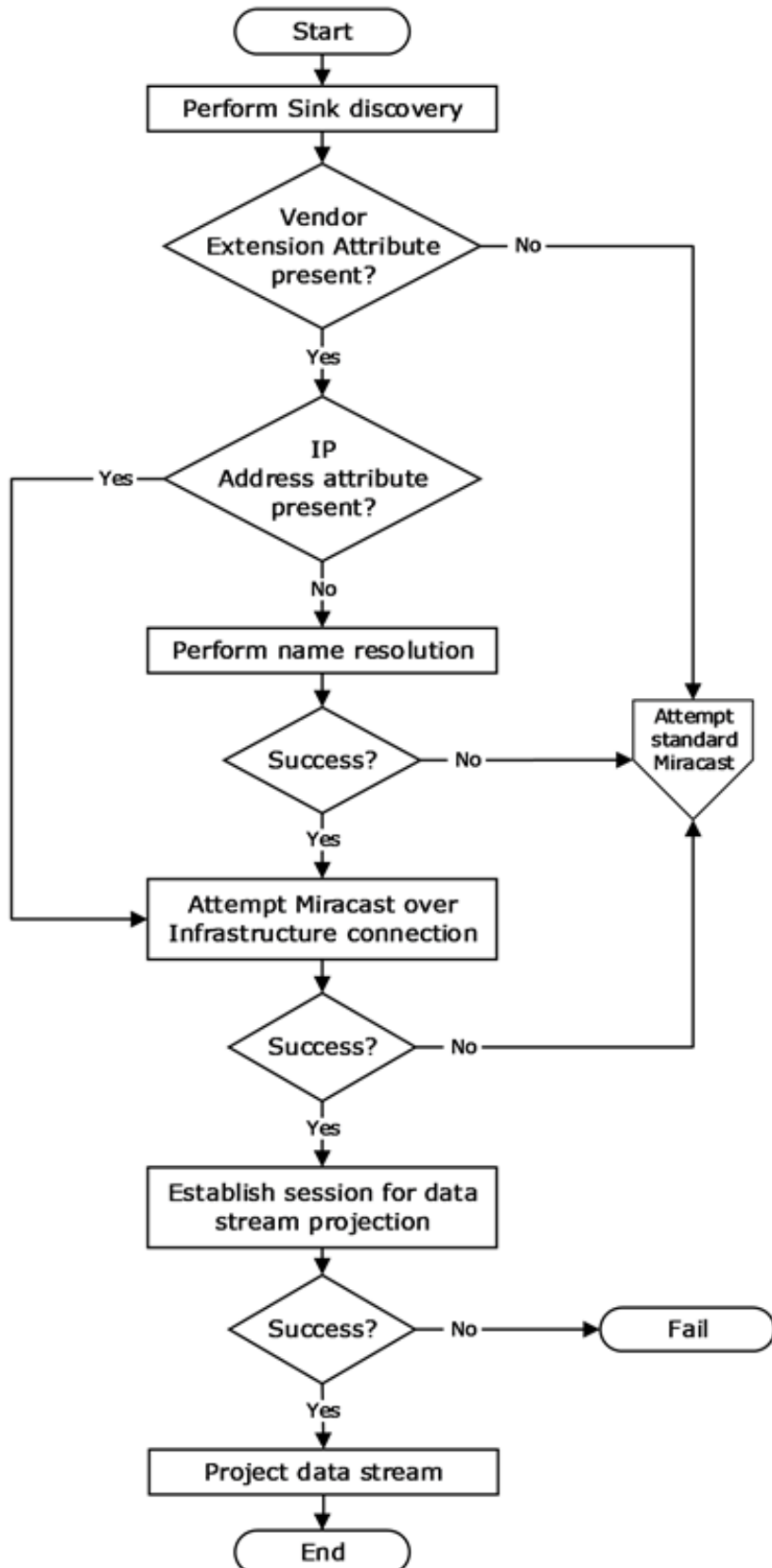
```
wfd_idr_request
RTSP/1.0 200 OK
Server: MSMiracastSource/10.00.18362.0657 guid/D090ABD8-EC1F-0005-379E-94D01FECD501
Session: 1053406594
CSeq: 5
```

Does RTP use congestion feedback mechanisms?

<https://www.cse.wustl.edu/~jain/books/ftp/rtp.pdf>

RTCP Protocol

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-mice/ab6341b7-4fc7-41fd-a74d-3fe023455482



Unofficial AirPlay Protocol Specification

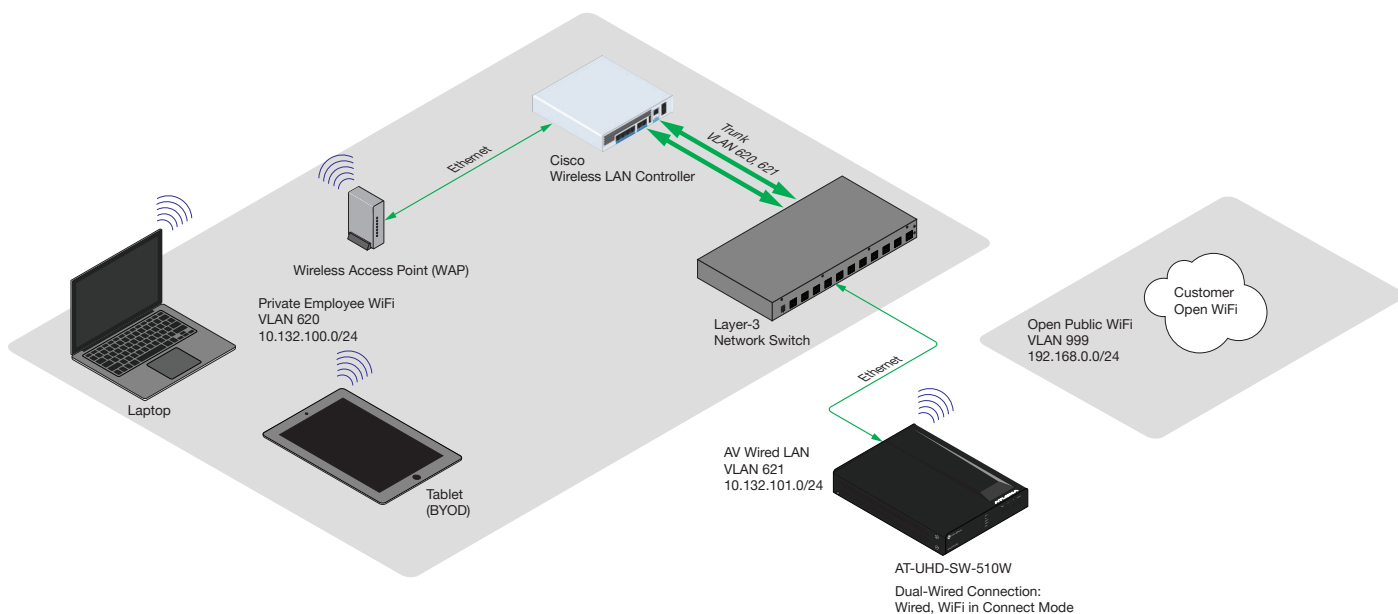
<https://nto.github.io/AirPlay.html>

RTSP RFC

<https://www.ietf.org/rfc/rfc2326.txt>

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

AT-UHD-SW-510W / AT-OME-MS52W 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 / AT-OME-MS52W 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 / AT-OME-MS52W 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 / AT-OME-MS52W 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 / AT-OME-MS52W 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.

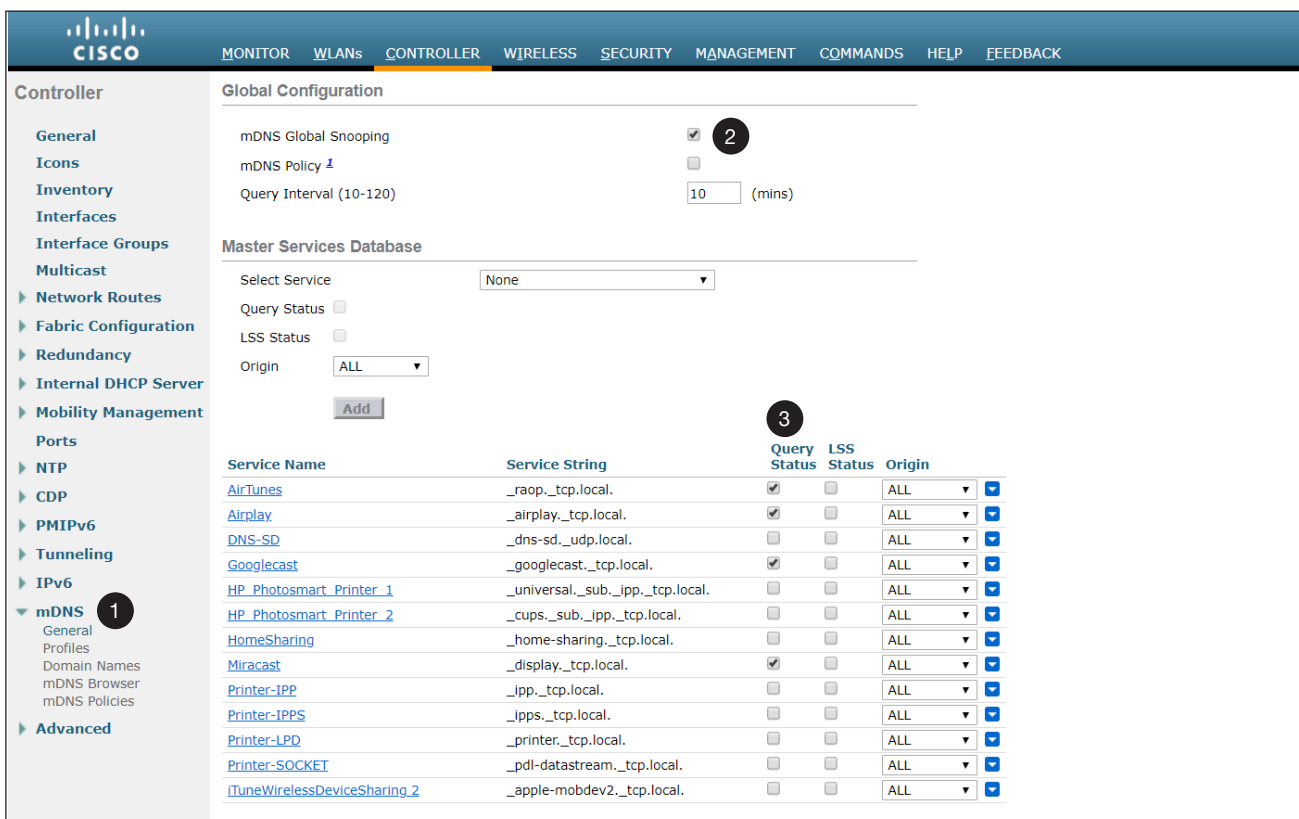
For this example, the following is given:

1. The wireless clients are on VLAN 620 and the AT-UHD-SW-510W / AT-OME-MS52W 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`



The screenshot shows the Cisco WLC configuration interface. The left-hand menu has 'mDNS' selected (marked with a '1'). The main content area is titled 'Global Configuration' and includes the following settings:

- mDNS Global Snooping: (marked with a '2')
- mDNS Policy:
- Query Interval (10-120): 10 (mins)

Below this is the 'Master Services Database' section, which includes a table with the following columns: Service Name, Service String, Query Status, LSS Status, and Origin. The table contains the following entries:

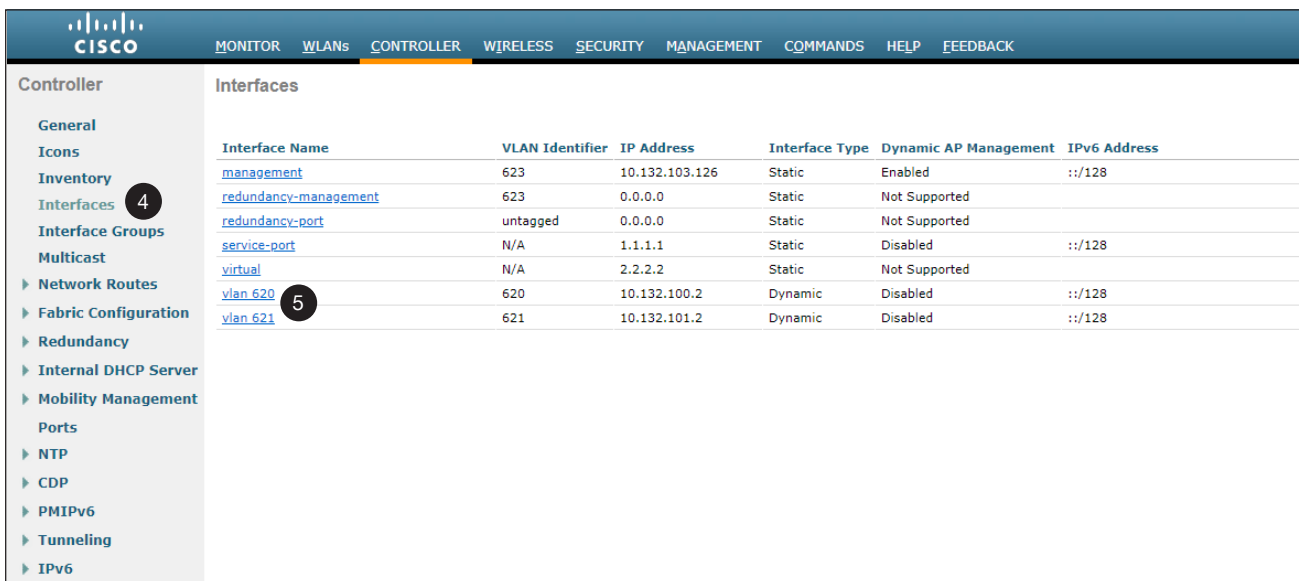
| Service Name | Service String | Query Status | LSS Status | Origin |
|--|--|-------------------------------------|--------------------------|--------|
| AirTunes | <code>_raop._tcp.local</code> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | ALL |
| Airplay | <code>_airplay._tcp.local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

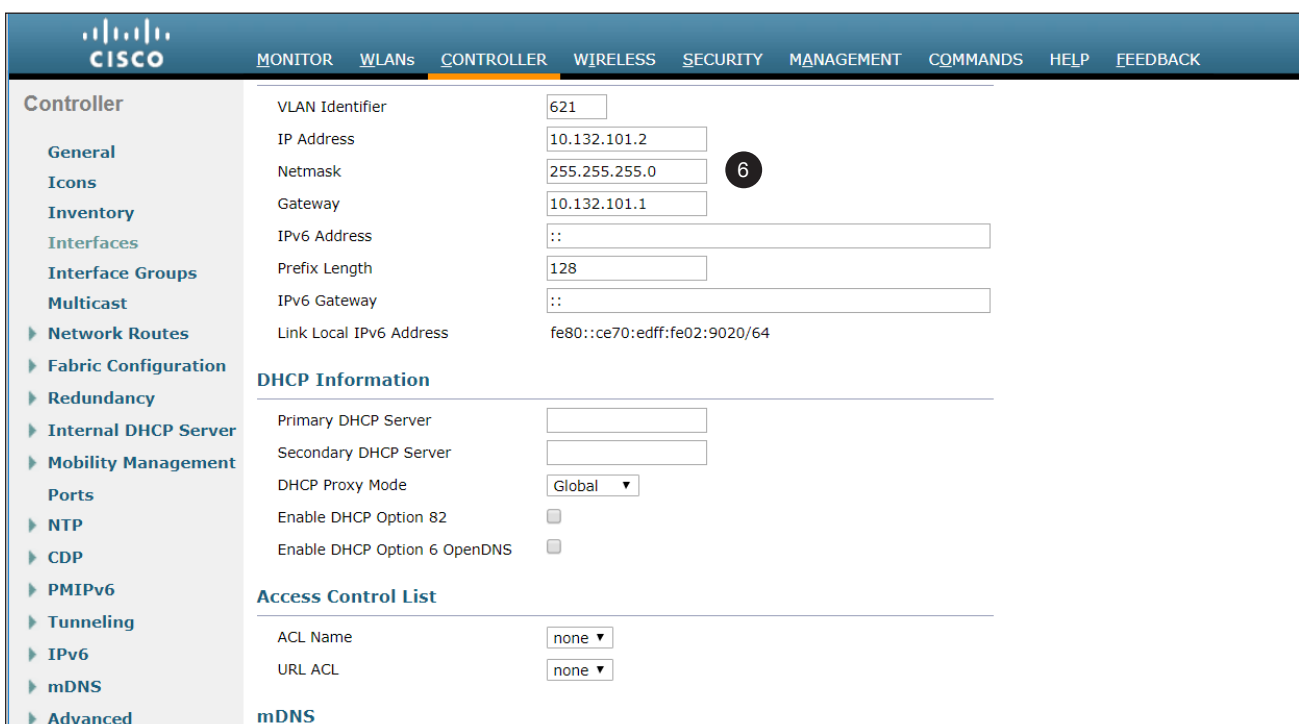
The WLC will need to have an interface created for VLAN 620 and VLAN 621. The WLC already had an interface on the working Wi-Fi network (VLAN 620), but it is necessary to create an interface on VLAN 621. In the example we did not assign an SSID to this VLAN as it is only used to forward mDNS announcements.

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 |
|---------------------------------------|-----------------|----------------|----------------|-----------------------|--------------|
| management | 623 | 10.132.103.126 | Static | Enabled | ::/128 |
| redundancy-management | 623 | 0.0.0.0 | Static | Not Supported | |
| redundancy-port | untagged | 0.0.0.0 | Static | Not Supported | |
| service-port | N/A | 1.1.1.1 | Static | Disabled | ::/128 |
| virtual | N/A | 2.2.2.2 | Static | Not Supported | |
| vlan_620 | 620 | 10.132.100.2 | Dynamic | Disabled | ::/128 |
| vlan_621 | 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

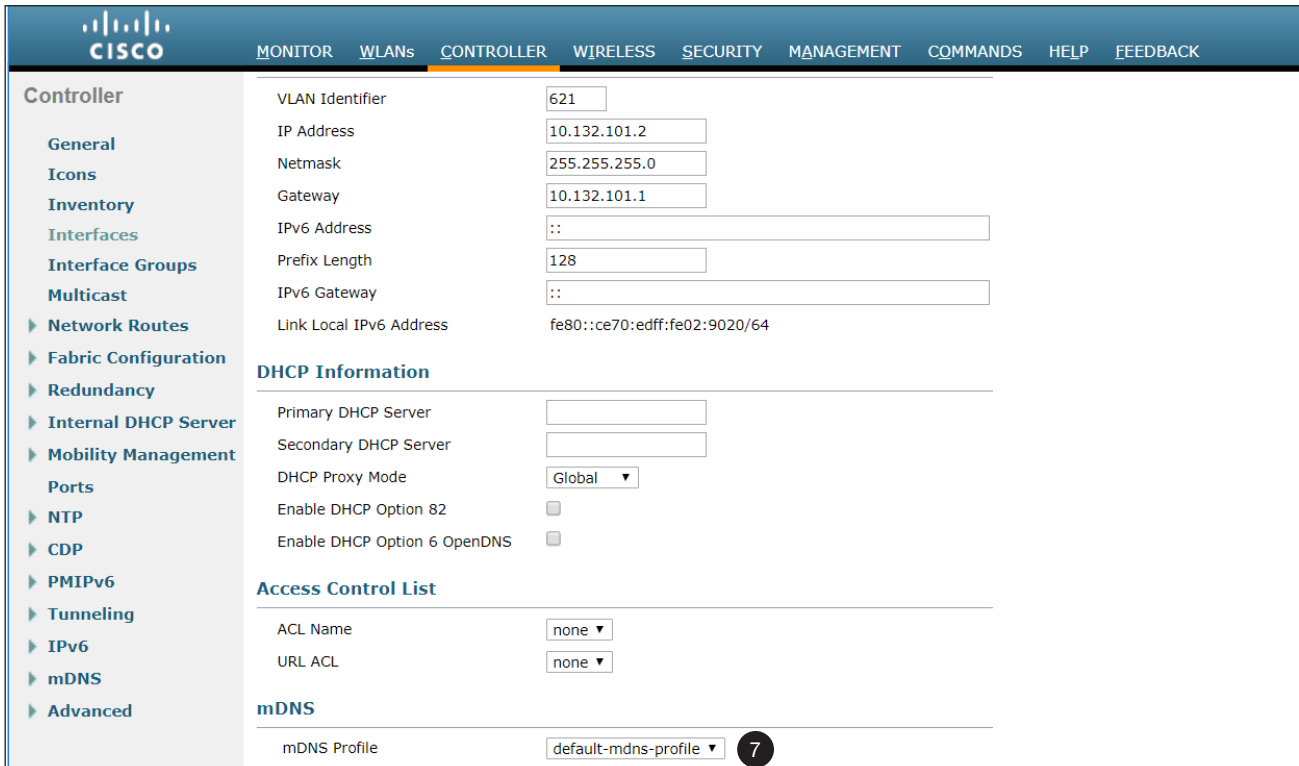
Primary DHCP Server:
 Secondary DHCP Server:
 DHCP Proxy Mode: Global
 Enable DHCP Option 82:
 Enable DHCP Option 6 OpenDNS:

Access Control List

ACL Name: none
 URL ACL: none

mDNS

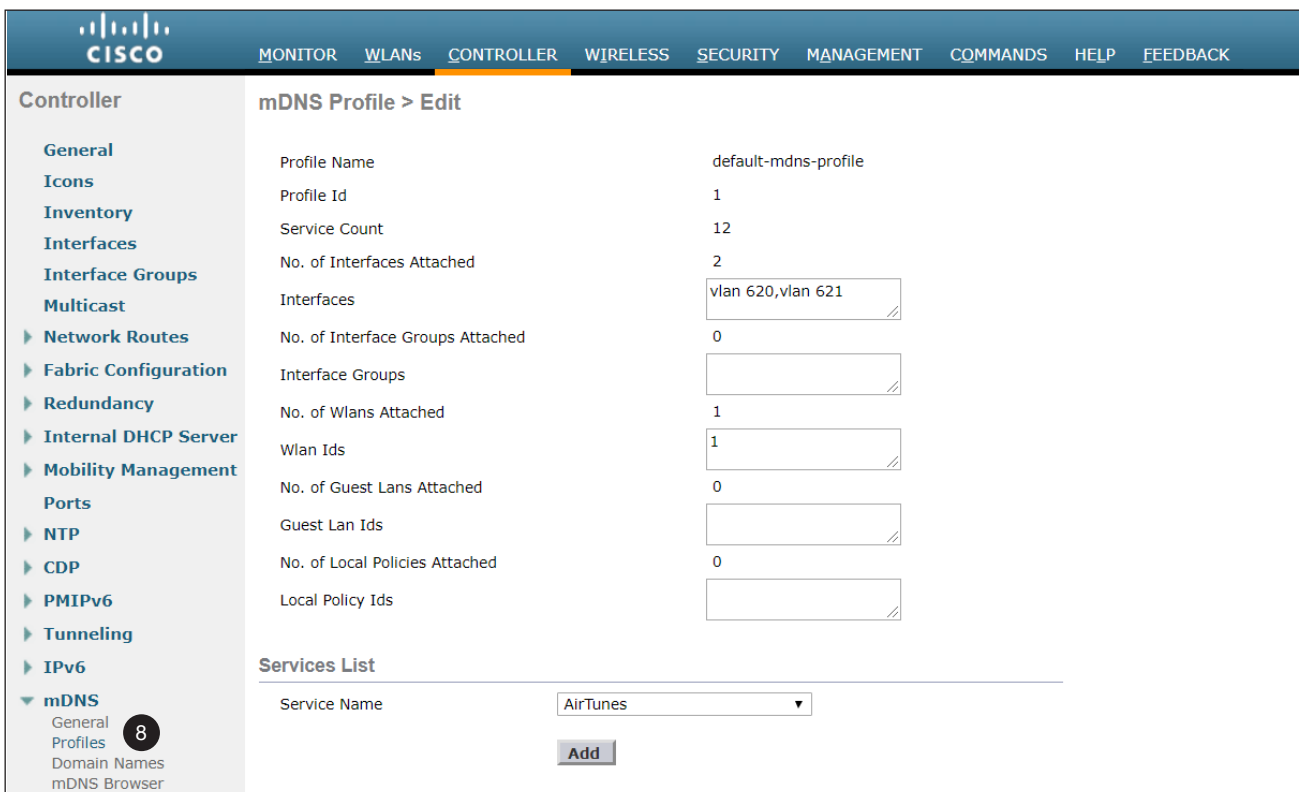
7. Enable mDNS on the interfaces. For each interface assign a mDNS profile to apply. Click the **mDNS Profile** drop-down list and select **default-mdns-profile** for interface VLAN 620 and VLAN 621.



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 > Profiles** selected, and **default-mdns-profile** 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 / AT-OME-MS52W 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 / AT-OME-MS52W 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

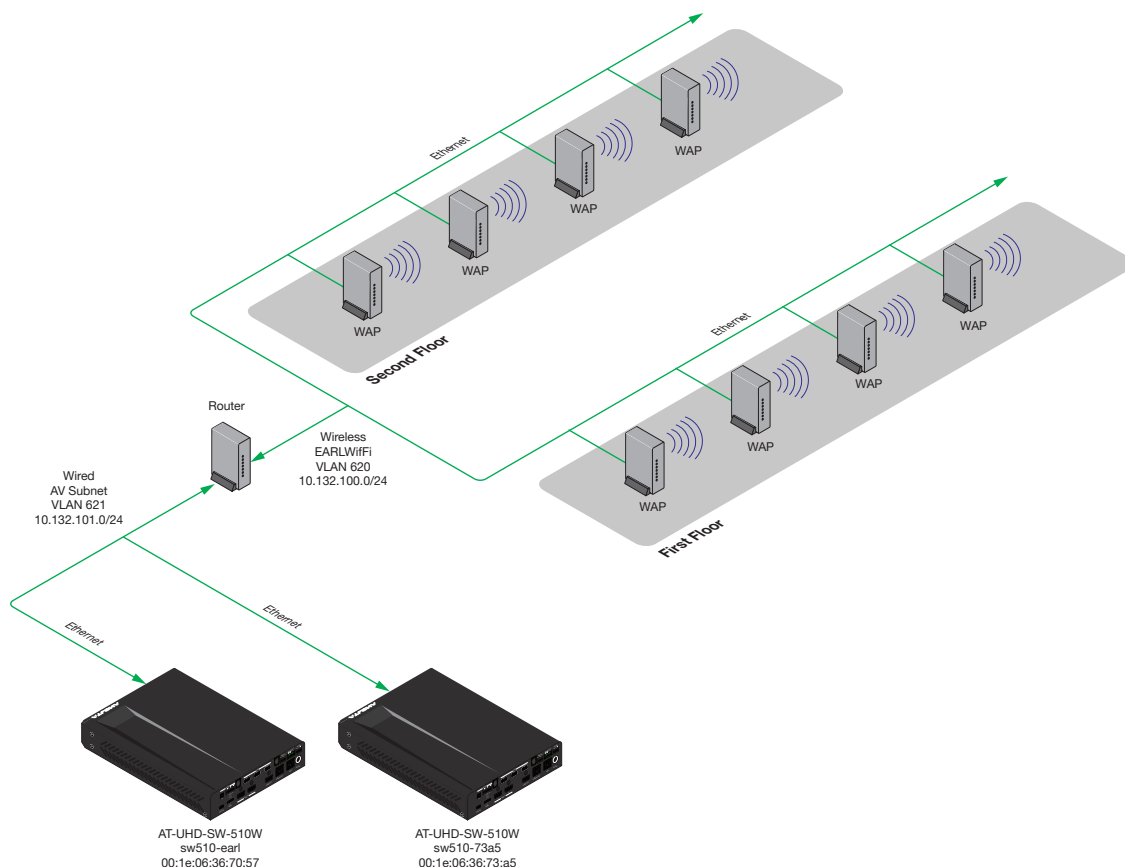
The AT-UHD-SW-510W / AT-OME-MS52W allows video and audio casting to several types of sources. Wireless networks using Cisco Wireless LAN Controllers(WLC) must be configured to forward mDNS announcements for both AirPlay and Google Cast service announcements, in order to be accessible on wireless client devices. In large enterprise networks environments with multiple AT-UHD-SW-510W / AT-OME-MS52W 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 / AT-OME-MS52W units through wireless clients.
- To restrict the AT-UHD-SW-510W / AT-OME-MS52W 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 / AT-OME-MS52W 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 / AT-OME-MS52W 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 / AT-OME-MS52W.



Important Wireless Coverage and Configuration Notice

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.

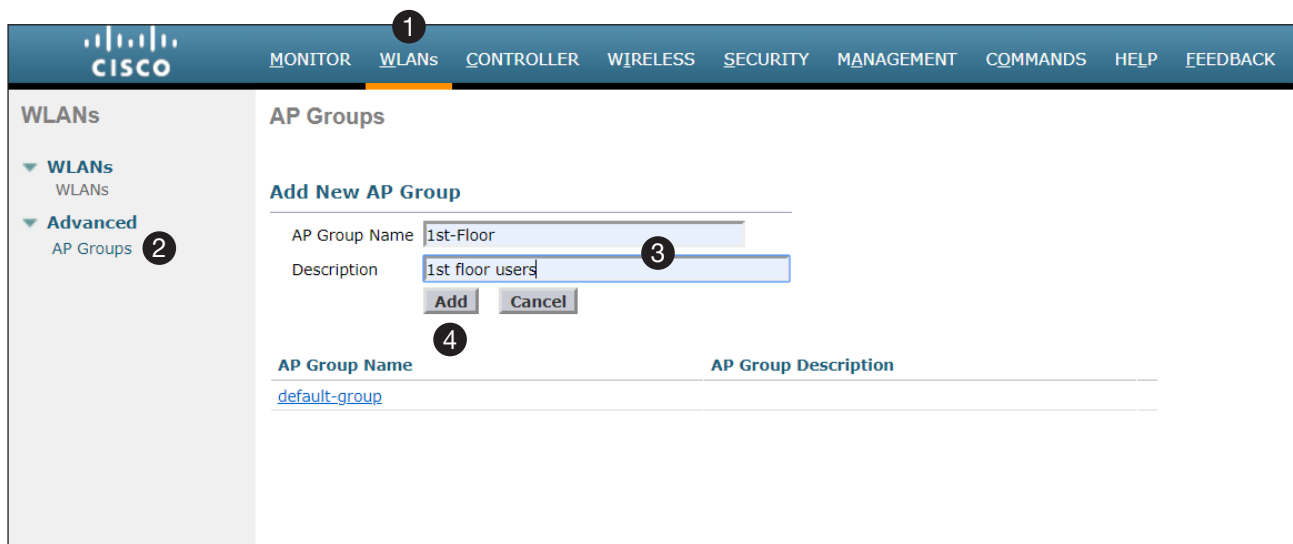
- Decrease power on the access points.
- Decrease the power on client devices.
- Disable lower data rates, globally, on the WLC.

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.

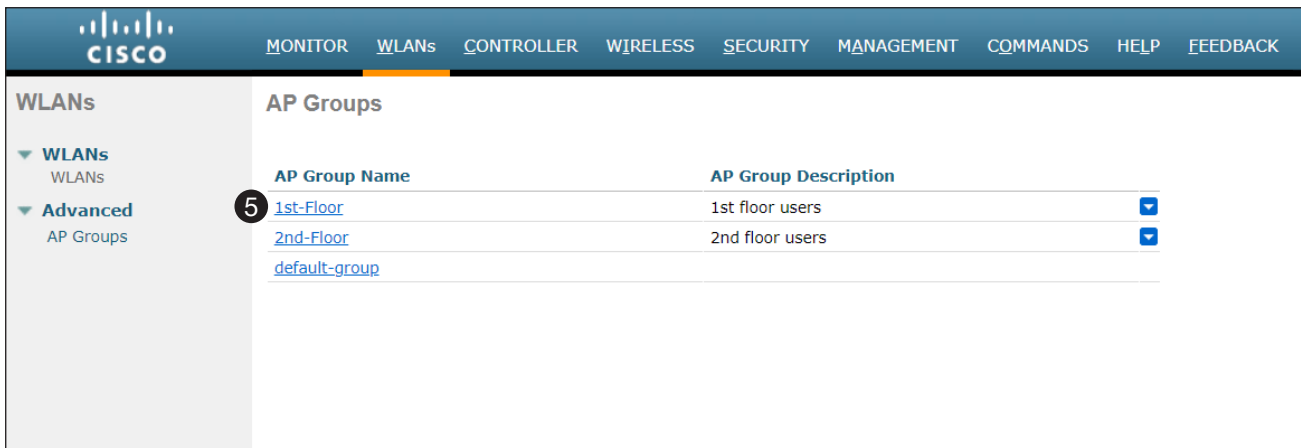
1. Connect to the controller through HTTPS, then click **WLANS** in the top menu system.
2. Click **Advanced > AP Groups > Add Group**.
3. Enter the name of the group in the **AP Group Name** and a description in the **Description** field.
4. Click the **Add** button to commit changes. Repeat steps 2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

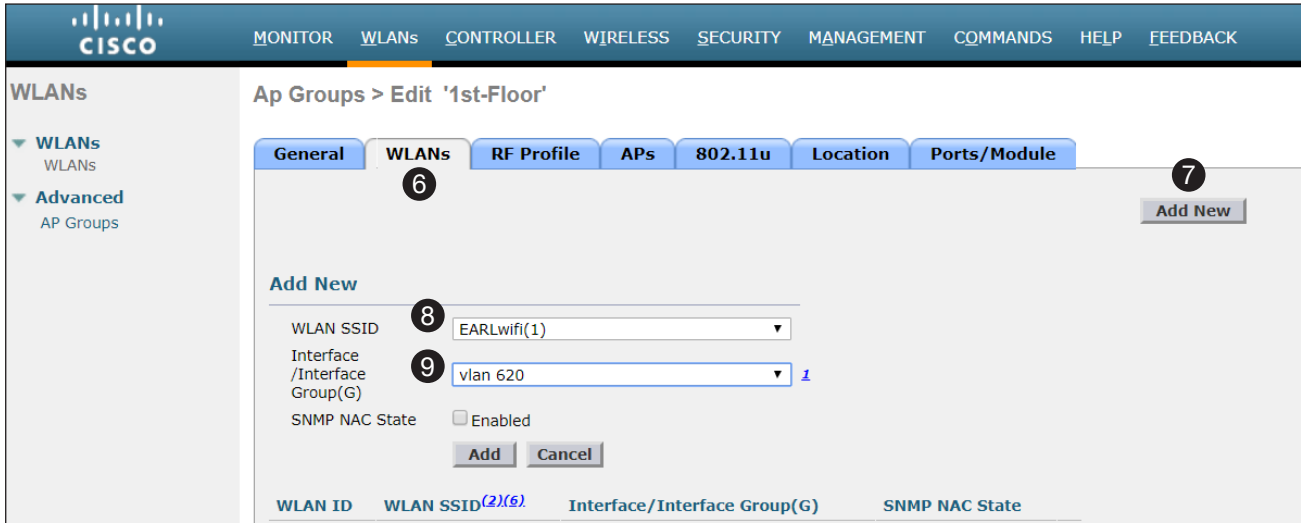
- Click on **1st-Floor** to edit the AP Group Name.



The screenshot shows the Cisco WLANs configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows WLANs and Advanced AP Groups. The main content area is titled 'AP Groups' and contains a table with the following data:

| AP Group Name | AP Group Description | |
|---------------|----------------------|-------------------------------------|
| 1st-Floor | 1st floor users | <input checked="" type="checkbox"/> |
| 2nd-Floor | 2nd floor users | <input checked="" type="checkbox"/> |
| default-group | | |

- 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.



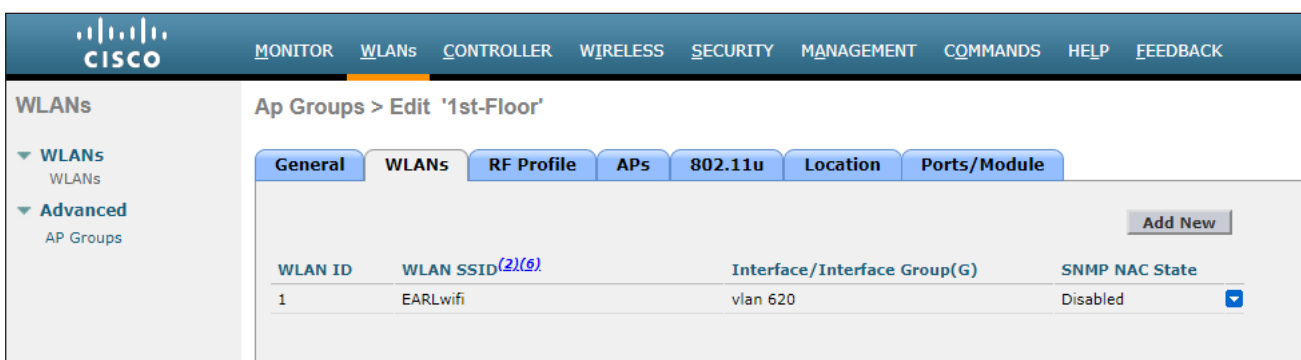
The screenshot shows the 'Ap Groups > Edit '1st-Floor'' configuration page. The 'WLANs' tab is selected, and the 'Add New' dialog is open. The dialog contains the following fields and options:

- WLAN SSID:** EARLwifi(1) (circled 8)
- Interface / Interface Group (G):** vlan 620 (circled 9)
- SNMP NAC State:** Enabled
- Buttons:** Add, Cancel

The 'Add New' button is circled 7. Below the dialog, a table shows the current state of the AP group:

| WLAN ID | WLAN SSID (2)(5) | Interface/Interface Group(G) | SNMP NAC State |
|---------|------------------|------------------------------|--|
| 1 | EARLwifi | vlan 620 | Disabled <input checked="" type="checkbox"/> |

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

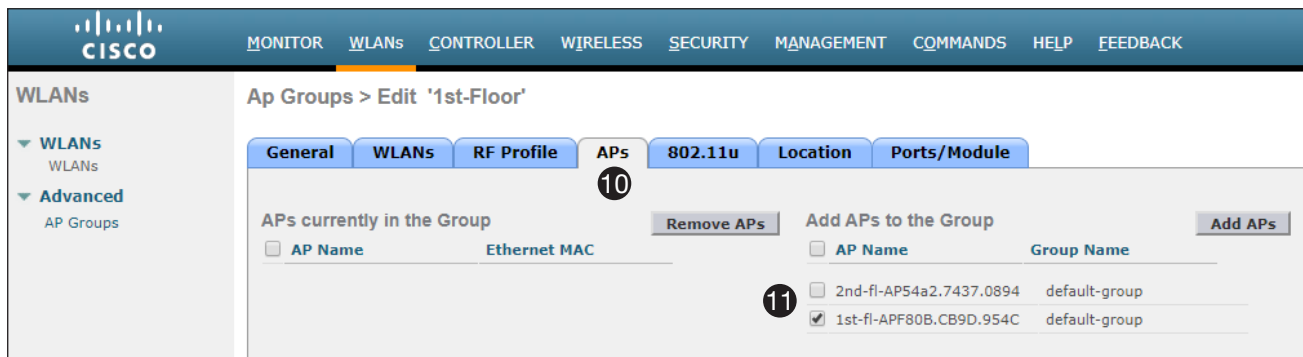


The screenshot shows the final state of the 'Ap Groups > Edit '1st-Floor'' configuration page. The 'WLANs' tab is selected, and the 'Add New' dialog is closed. The table below shows the final configuration:

| WLAN ID | WLAN SSID (2)(5) | Interface/Interface Group(G) | SNMP NAC State |
|---------|------------------|------------------------------|--|
| 1 | EARLwifi | vlan 620 | Disabled <input checked="" type="checkbox"/> |

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.

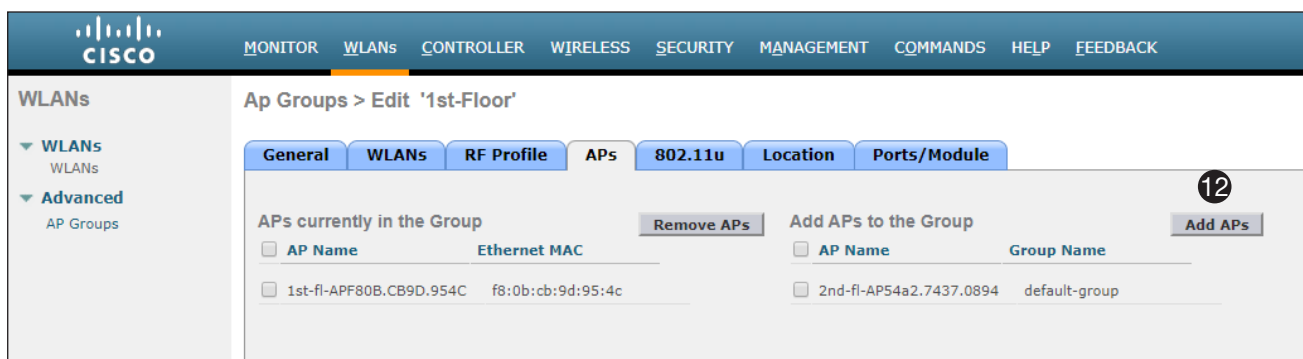


The screenshot shows the Cisco WLC interface for editing the '1st-Floor' AP Group. The 'APs' tab is selected, and the 'Add APs to the Group' section is visible. A circled '10' points to the 'APs' tab, and a circled '11' points to the checkbox next to the AP '1st-fl-APF80B.CB9D.954C' in the 'Add APs to the Group' table.

| AP Name | Ethernet MAC | Group Name |
|-------------------------------------|-------------------------|---------------|
| <input type="checkbox"/> | | |
| <input type="checkbox"/> | 2nd-fl-AP54a2.7437.0894 | default-group |
| <input checked="" type="checkbox"/> | 1st-fl-APF80B.CB9D.954C | default-group |

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.

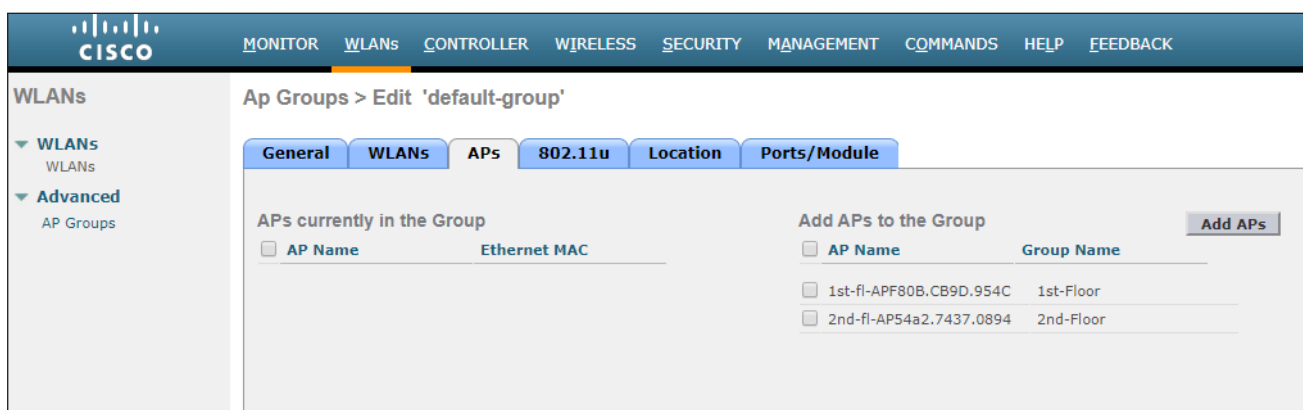


The screenshot shows the Cisco WLC interface for editing the '1st-Floor' AP Group. The 'Add APs to the Group' section now shows two APs. A circled '12' points to the 'Add APs' button.

| AP Name | Ethernet MAC | Group Name |
|--------------------------|-------------------------|-------------------|
| <input type="checkbox"/> | 1st-fl-APF80B.CB9D.954C | f8:0b:cb:9d:95:4c |
| <input type="checkbox"/> | 2nd-fl-AP54a2.7437.0894 | default-group |

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 / AT-OME-MS52W 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.



The screenshot shows the Cisco WLC interface for editing the 'default-group' AP Group. The 'Add APs to the Group' section shows two APs assigned to different groups.

| AP Name | Ethernet MAC | Group Name |
|--------------------------|-------------------------|------------|
| <input type="checkbox"/> | | |
| <input type="checkbox"/> | 1st-fl-APF80B.CB9D.954C | 1st-Floor |
| <input type="checkbox"/> | 2nd-fl-AP54a2.7437.0894 | 2nd-Floor |

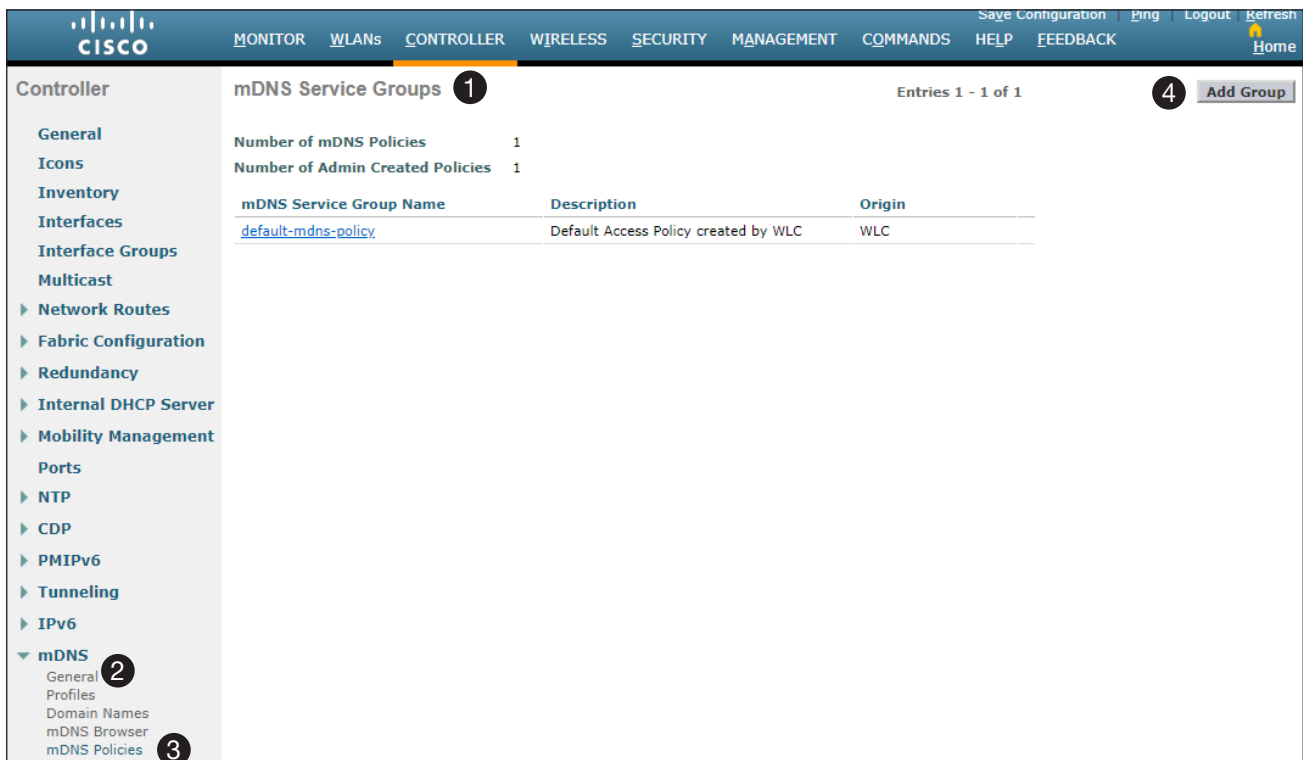
Configuring mDNS Policies

The mDNS policy is where limiting (fencing) which AP Groups can see which AT-UHD-SW-510W / AT-OME-MS52W 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.



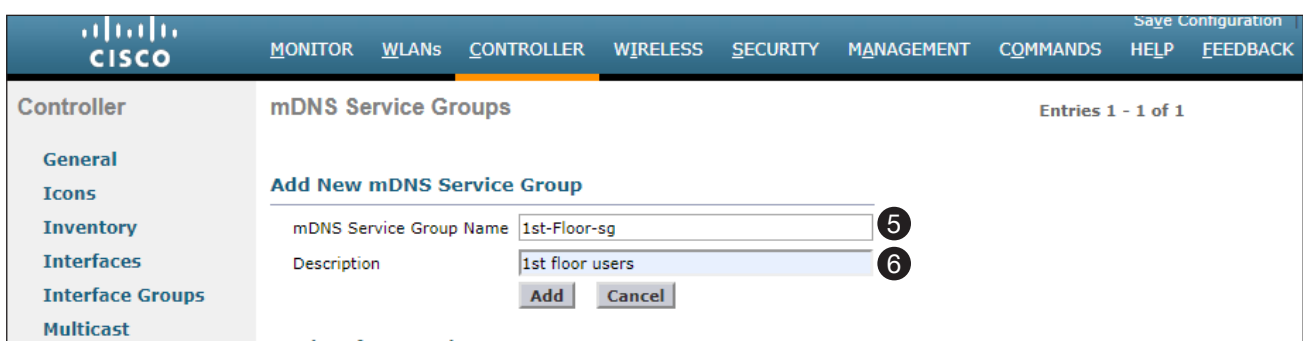
NOTE: It is important to note that the following procedure does not alter the mDNS profile. For example, the AP Group configuration was started using the `default-mdns-profile` to the wired and wireless interfaces. This profile is never changed.

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 for mDNS Service Groups. 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 shows 'mDNS Service Groups' with 'Entries 1 - 1 of 1'. A table lists one entry: 'default-mdns-policy' with description 'Default Access Policy created by WLC' and origin 'WLC'. An 'Add Group' button is visible in the top right corner.

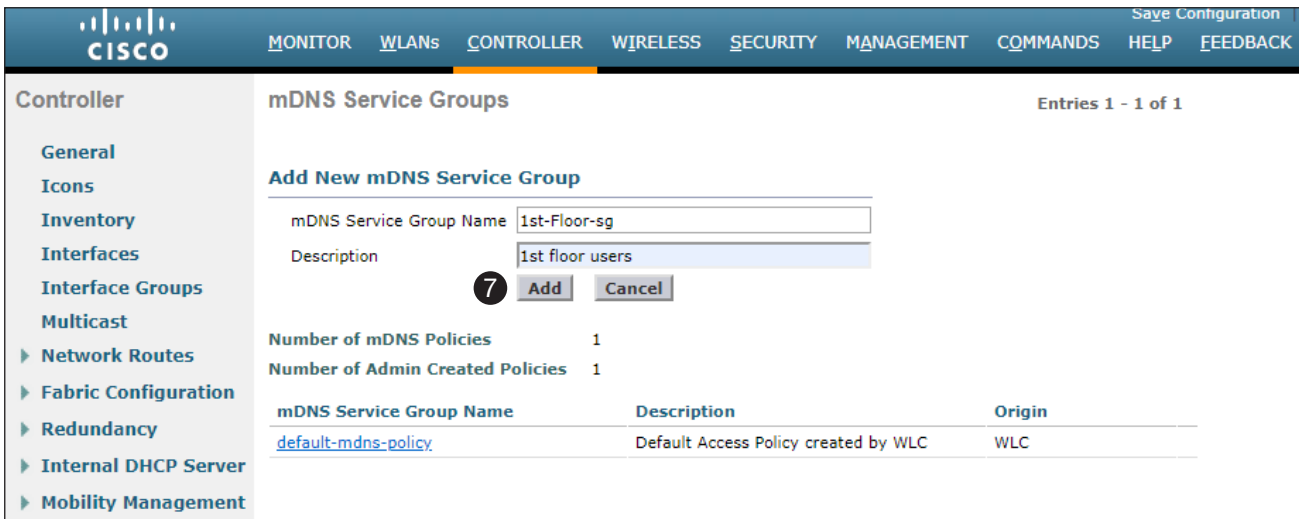
5. Enter new mDNS service group name in the **mDNS Service Group Name** field.
6. Enter the mDNS service group description in the **Description** field.



The screenshot shows the 'Add New mDNS Service Group' form in the Cisco Controller interface. The form has two input fields: 'mDNS Service Group Name' with the value '1st-Floor-sg' and 'Description' with the value '1st floor users'. Below the fields are 'Add' and 'Cancel' buttons. The top navigation bar and left-hand menu are the same as in the previous screenshot.

- 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`

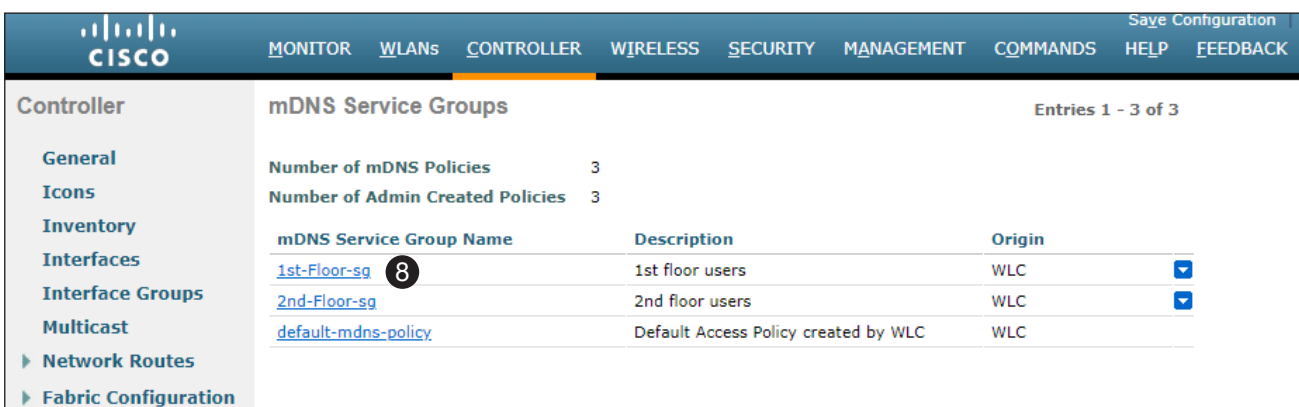
A circled '7' highlights the **Add** button. Below the form, the following statistics are shown:

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

| mDNS Service Group Name | Description | Origin |
|-------------------------------------|--------------------------------------|--------|
| default-mdns-policy | 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 / AT-OME-MS52W 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 / AT-OME-MS52W on the first floor.

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



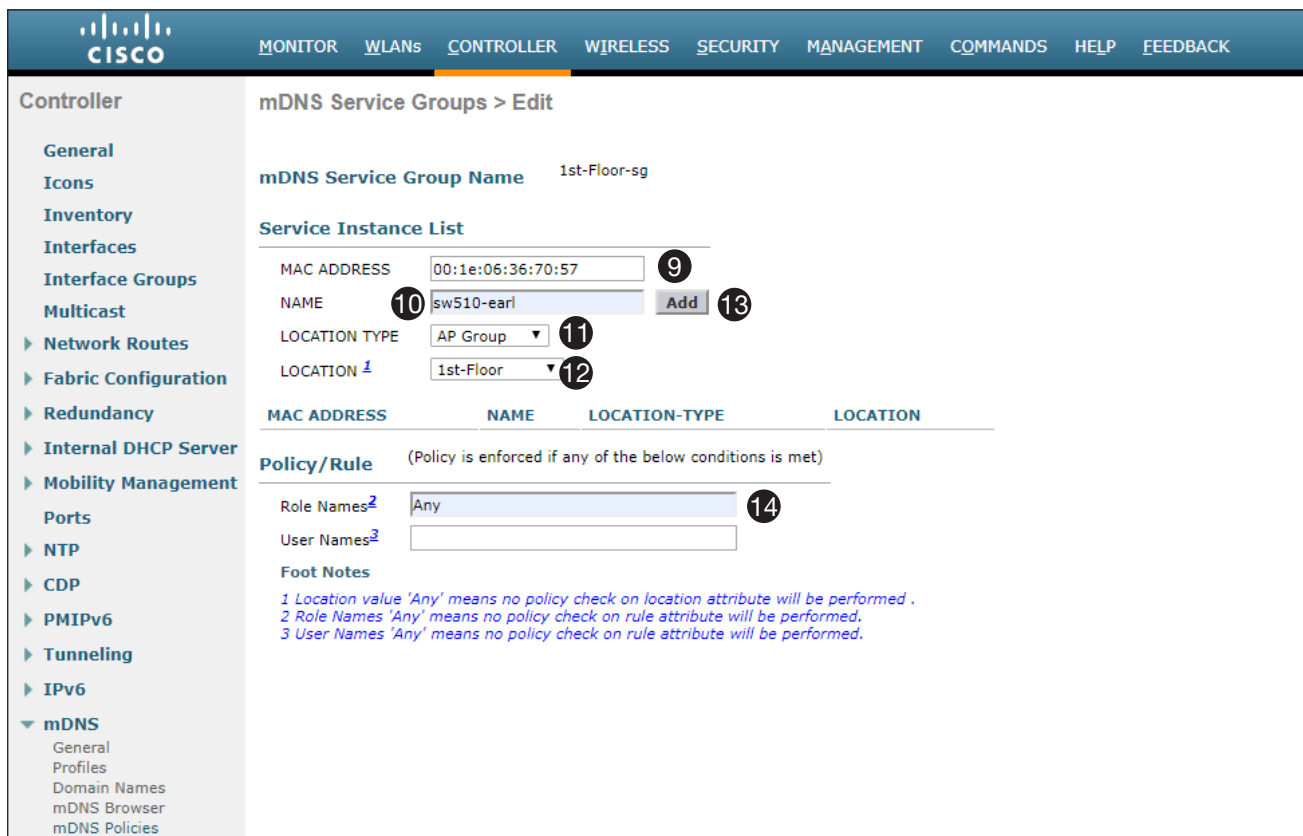
The screenshot shows the Cisco Controller interface for mDNS Service Groups. The list of service groups is displayed with the following statistics:

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

| mDNS Service Group Name | Description | Origin |
|--|--------------------------------------|--------|
| 1st-Floor-sg 8 | 1st floor users | WLC |
| 2nd-Floor-sg | 2nd floor users | WLC |
| default-mdns-policy | Default Access Policy created by WLC | WLC |

9. Enter the MAC address of the AT-UHD-SW-510W / AT-OME-MS52W in the **MAC ADDRESS** field. In this example, this refers to the AT-UHD-SW-510W / AT-OME-MS52W 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 breadcrumb is `mDNS Service Groups > Edit`. The `mDNS Service Group Name` is `1st-Floor-sg`. The `Service Instance List` table has the following entries:

| 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:

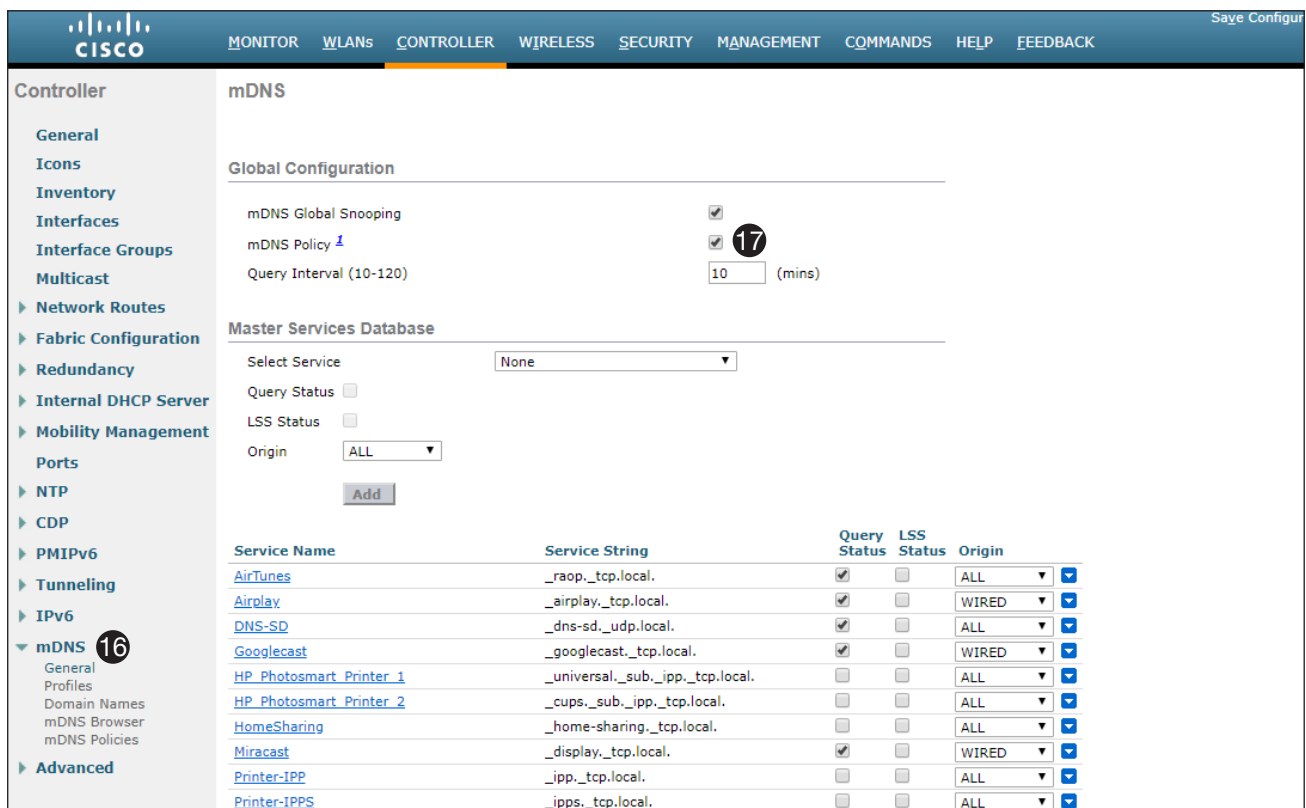
- `Role Names`: Any
- `User Names`: (empty)

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.
18. Configuration is complete.




The screenshot shows the Cisco Controller configuration page for mDNS. The left-hand menu has 'mDNS' expanded, with 'General' selected and highlighted with a red circle and the number 16. In the 'Global Configuration' section, the 'mDNS Policy' checkbox is checked and highlighted with a red circle and the number 17. The 'Query Interval' is set to 10 (mins). The 'Master Services Database' section shows a table of services with columns for Service Name, Service String, Query Status, LSS Status, and Origin.

| Service Name | Service String | Query Status | LSS Status | Origin |
|---|----------------------------------|-------------------------------------|--------------------------|--------|
| AirTunes | _raop._tcp.local. | <input checked="" type="checkbox"/> | <input type="checkbox"/> | ALL |
| Airplay | _airplay._tcp.local. | <input checked="" type="checkbox"/> | <input type="checkbox"/> | WIRED |
| DNS-SD | _dns-sd._udp.local. | <input checked="" type="checkbox"/> | <input type="checkbox"/> | ALL |
| Googlecast | _googlecast._tcp.local. | <input checked="" type="checkbox"/> | <input type="checkbox"/> | WIRED |
| HP Photosmart Printer 1 | _universal._sub._ipp._tcp.local. | <input type="checkbox"/> | <input type="checkbox"/> | ALL |
| HP Photosmart Printer 2 | _cups._sub._ipp._tcp.local. | <input type="checkbox"/> | <input type="checkbox"/> | ALL |
| HomeSharing | _home-sharing._tcp.local. | <input type="checkbox"/> | <input type="checkbox"/> | ALL |
| Miracast | _display._tcp.local. | <input checked="" type="checkbox"/> | <input type="checkbox"/> | WIRED |
| Printer-IPP | _ipp._tcp.local. | <input type="checkbox"/> | <input type="checkbox"/> | ALL |
| Printer-IPPS | _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 / AT-OME-MS52W in the first-floor conference room. Second-floor users should only access the AT-UHD-SW-510W / AT-OME-MS52W 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 / AT-OME-MS52W 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.

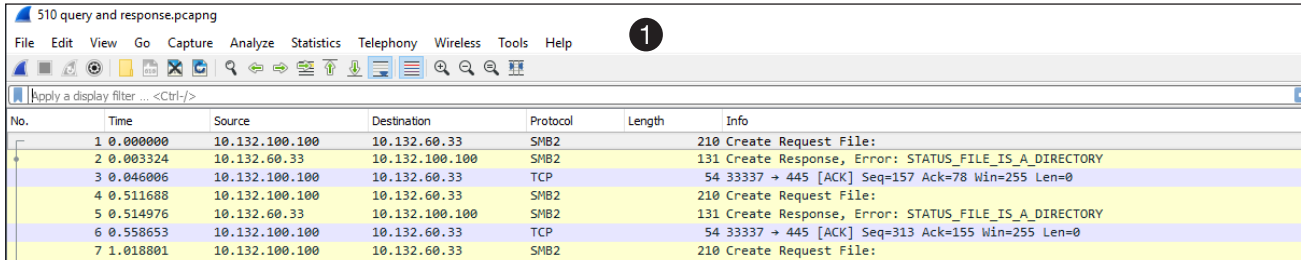
Solutions:

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

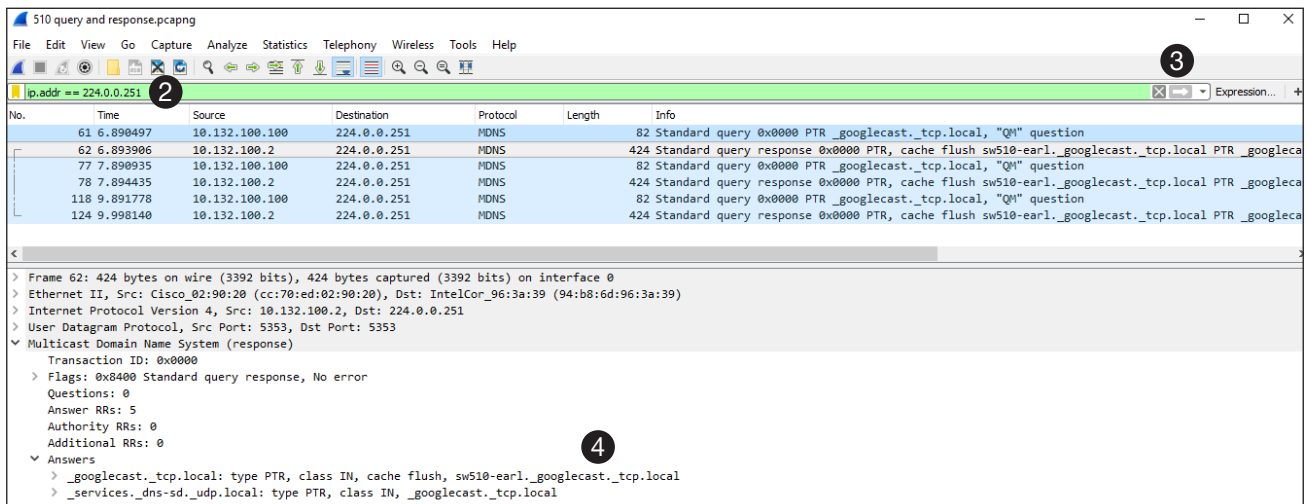
The best way to verify mDNS announcements is to perform a packet capture. The following example uses Wireshark, which is a free packet capture tool.

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



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|--|
| 1 | 0.000000 | 10.132.100.100 | 10.132.60.33 | SMB2 | | 210 Create Request File: |
| 2 | 0.003324 | 10.132.60.33 | 10.132.100.100 | SMB2 | | 131 Create Response, Error: STATUS_FILE_IS_A_DIRECTORY |
| 3 | 0.046006 | 10.132.100.100 | 10.132.60.33 | TCP | 54 | 33337 → 445 [ACK] Seq=157 Ack=78 Win=255 Len=0 |
| 4 | 0.511688 | 10.132.100.100 | 10.132.60.33 | SMB2 | | 210 Create Request File: |
| 5 | 0.514976 | 10.132.60.33 | 10.132.100.100 | SMB2 | | 131 Create Response, Error: STATUS_FILE_IS_A_DIRECTORY |
| 6 | 0.558653 | 10.132.100.100 | 10.132.60.33 | TCP | 54 | 33337 → 445 [ACK] Seq=313 Ack=155 Win=255 Len=0 |
| 7 | 1.018801 | 10.132.100.100 | 10.132.60.33 | SMB2 | | 210 Create Request File: |

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 / AT-OME-MS52W with the SSID of sw510-earl is responding with the `_googlecast._tcp.local` service.



Filter: `ip.addr == 224.0.0.251`

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|-------------|----------|--------|---|
| 61 | 6.898497 | 10.132.100.100 | 224.0.0.251 | MDNS | 82 | Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question |
| 62 | 6.893906 | 10.132.100.2 | 224.0.0.251 | MDNS | 424 | Standard query response 0x0000 PTR, cache flush sw510-earl._googlecast._tcp.local PTR _googleca |
| 77 | 7.890935 | 10.132.100.100 | 224.0.0.251 | MDNS | 82 | Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question |
| 78 | 7.894435 | 10.132.100.2 | 224.0.0.251 | MDNS | 424 | Standard query response 0x0000 PTR, cache flush sw510-earl._googlecast._tcp.local PTR _googleca |
| 118 | 9.891778 | 10.132.100.100 | 224.0.0.251 | MDNS | 82 | Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question |
| 124 | 9.998140 | 10.132.100.2 | 224.0.0.251 | MDNS | 424 | Standard query response 0x0000 PTR, cache flush sw510-earl._googlecast._tcp.local PTR _googleca |

Expanded packet details (Frame 62):

- Ethernet II, Src: Cisco_02:90:20 (cc:70:ed:02:90:20), Dst: IntelCor_96:3a:39 (94:b8:6d:96:3a:39)
- Internet Protocol Version 4, Src: 10.132.100.2, Dst: 224.0.0.251
- User Datagram Protocol, Src Port: 5353, Dst Port: 5353
- Multicast Domain Name System (response)
 - Transaction ID: 0x0000
 - Flags: 0x8400 Standard query response, No error
 - Questions: 0
 - Answer RRs: 5
 - Authority RRs: 0
 - Additional RRs: 0
 - Answers
 - _googlecast._tcp.local: type PTR, class IN, cache flush, sw510-earl._googlecast._tcp.local
 - _services-dns-sd._udp.local: type PTR, class IN, _googlecast._tcp.local
 - sw510-earl._googlecast._tcp.local: type SRV, class IN, cache flush, priority 0, weight 0, port 8000, target sw510-earl.local

