Primary AP Failover and Electing a new Primary

Cisco Mobility Express is supported on Cisco 1560, 1815I, 1815M, 1815W, 1830, 1850, 2800 and 3800 series Access Points. If you have a mix of these Access Points in a Cisco Mobility Express deployment, the Primary AP election process determines which of the supported Access Point will be elected to run Mobility Express controller function in case of a Failover of the Active Primary AP. VRRP is used to detect the failure of Primary AP which initiates the election of a new Primary.

Note Mobility Express uses MAC 00-00-5E-00-01-VRID where VRID is 1 so if there are other instances of VRRP running in the environment, use VRID other than 1 for those instances.

- Primary AP Failover, on page 1
- Electing a new Primary Access Point, on page 2
- Efficient AP Join for heterogeneous network, on page 3
- Schedule WLAN, on page 4
- Option 43 support for ME, on page 6
- mDNS support, on page 6
- FQDN support SFTP, on page 9
- Videostream support (MC2UC), on page 10
- Cisco RFID Tag support, on page 14

Primary AP Failover

To have redundancy in the Mobility Express network, it must have two or more Mobility Express capable Access Points. These Access Points should have AP Image type as MOBILITY EXPRESS IMAGE and AP Configuration as MOBILITY EXPRESS CAPABLE. In an event of a failure of Primary AP, another Mobility Express capable AP is elected as a Primary automatically. The newly elected Primary AP has the same IP and configuration as the original Primary AP.

Note Given Access Point models support different scale limits in terms of the number of Access Points supported, it is highly recommended to have at least two or more Access Points which support the same scale limits. For example, if you need to support scale of 100 Access Points, you should have at least two or more of either 3800, 2800 or a combination of both.

Note Access Points, which have the Mobility Express Image but **AP Configuration**, is **NOT MOBILITY EXPRESS CAPABLE**, will not participate in the Primary AP election process.

Electing a new Primary Access Point

Primary election process is based on a set of priorities. When an active Primary Access Point fails, the election process gets initiated and it elects the Access Point with the highest priority as the Primary AP.

Note During the Primary Election process, even though the Primary AP running the controller function is down, the remaining Access Points will fall into Standalone mode and will continue to service connected clients and switch data traffic locally. After the new Primary is elected, the Standalone Access points will move to connected mode.

As mentioned above, Primary Access Point election is based on a set of priorities. The priorities are as follows:

Procedure

Step 1 **User Defined Master**–User can select an Access Point to be the Primary Access Point. If such a selection is made, no new Primary will be elected in case of a failure of the active Primary. After five minutes, if the current Primary is still not active, it will be assumed dead and Primary Election will begin to elect a new Primary. To manually define a Primary, follow the procedure below:

a) Navigate to **Wireless Settings** > **Access Points**.
b) From the list of Access Points, click **Edit** icon of the Access Point which you would like to select as the Primary AP.
c) Under the **General** tab, click on **Make me Controller** button.
d) Click **Yes** on the Confirmation window.

Note The previous Primary will reboot and the selected Access Point will immediately launch the controller and become the active Primary.

Step 2 **Next Preferred Master**–Admin can configure the **Next Preferred Master** UI and CLI. When this is configured and the active Primary AP fails, the one configured as the **Next Preferred Master** will be elected as a Primary. To configure the **Next Preferred Master**, follow the procedure below:

Note Only one **Next Preferred Master** can be configured on Cisco Mobility Express.

a) Navigate to **Wireless Settings** > **Access Points.**
b) Edit the AP which you would like to make it as a **Next Preferred Master**
c) In the **Edit AP** window, enable the **Set as Preferred Master** toggle.
d) Click **Apply**.

To configure the **Next Preferred Master** from the controller CLI, please follow the steps below:

To configure the Next Preferred Master, execute the following CLI:

```
(Cisco Controller) >config ap next-preferred-master <Cisco AP>
       <Cisco AP> Enter the name of the Cisco AP
```

To see the Next Preferred Master, execute the following CLI:

```
(Cisco Controller) >show ap next-preferred-master
```

To clear the Next Preferred Master, execute the following CLI:

```
Cisco Controller) >clear ap next-preferred-master
```

Step 3 **Most Capable Access Point**– If the first two priorities are not configured, Primary AP election algorithm will select the new Primary based on the capability of the Access Point. For example, 3800 is the most capable followed by 2800, 1850, 1830 and finally the 1815 Series.

Note All 1815 Series Access Points have the same capability.

Step 4 **Least Client Load**– If here are multiple Access Points with the same capability i.e. multiple 3800 Access points, the one with least client load is elected as the Primary Access Point.

Step 5 **Lowest MAC Address**–If all of the Access Points are the same and have the same client load, then Access Point with the lowest MAC will be elected as a Primary.

Efficient AP Join for heterogeneous network

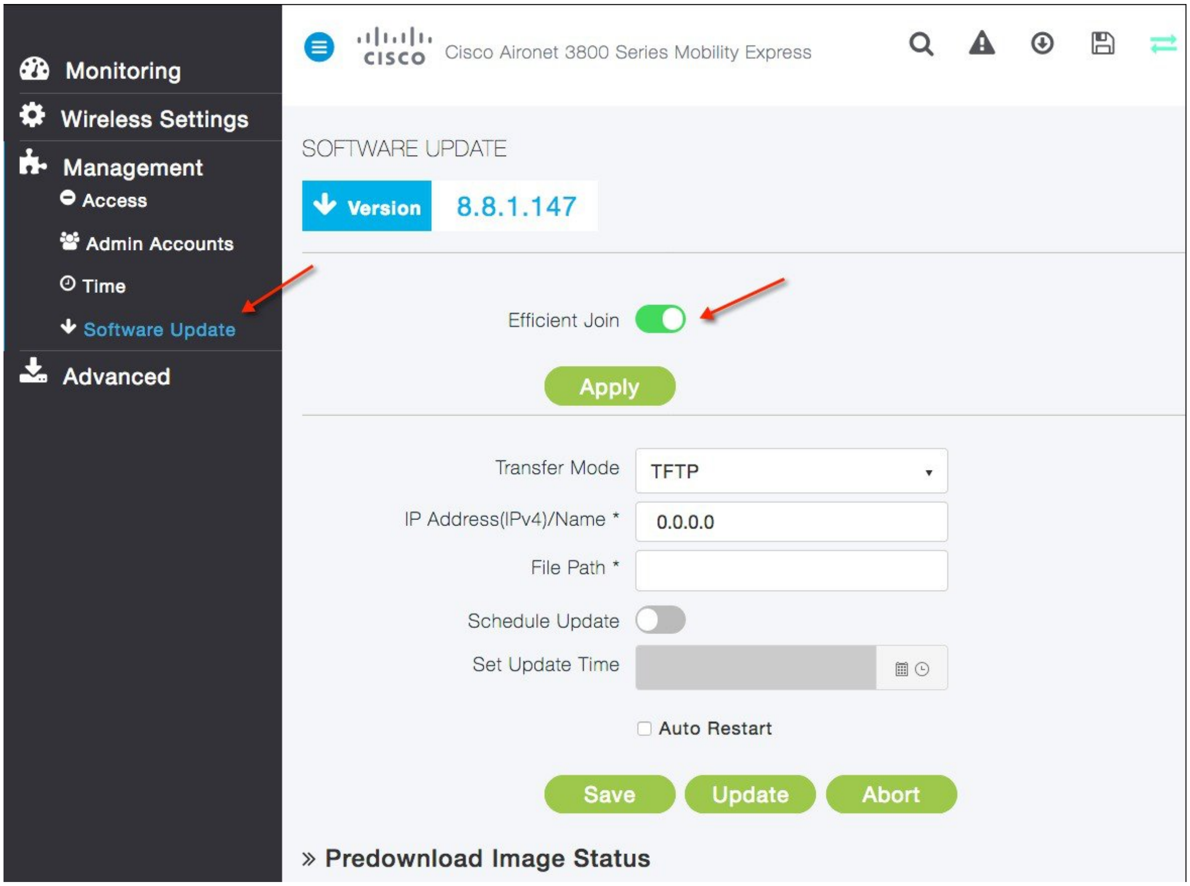
Efficient Join is a feature which enables downloading of the code from the Primary AP if the if the AP being added is of the same AP model as the Primary AP. For this feature, you do not need any external server to host the code running on the Primary AP.

Configuring Efficient Join

Procedure

Step 1 Navigate to **Management** > **Software Update**. Select **TFTP** or **SFTP** for **Transfer Mode** and configure the SFTP or TFTP Parameters

Step 2 Enable **Efficient Join** as shown below and click Apply.



SOFTWARE UPDATE

Version 8.8.1.147

Efficient Join: on

Transfer Mode: TFTP

IP Address(IPv4)/Name *: 0.0.0.0

File Path *:

Schedule Update: off

Set Update Time:

□ Auto Restart

Schedule WLAN

ME supports an option to schedule availability of each and every WLAN. By default, all WLANs are available 24/7 when they are initially created. Each WLAN would present the user options to create a scheduler as follows:

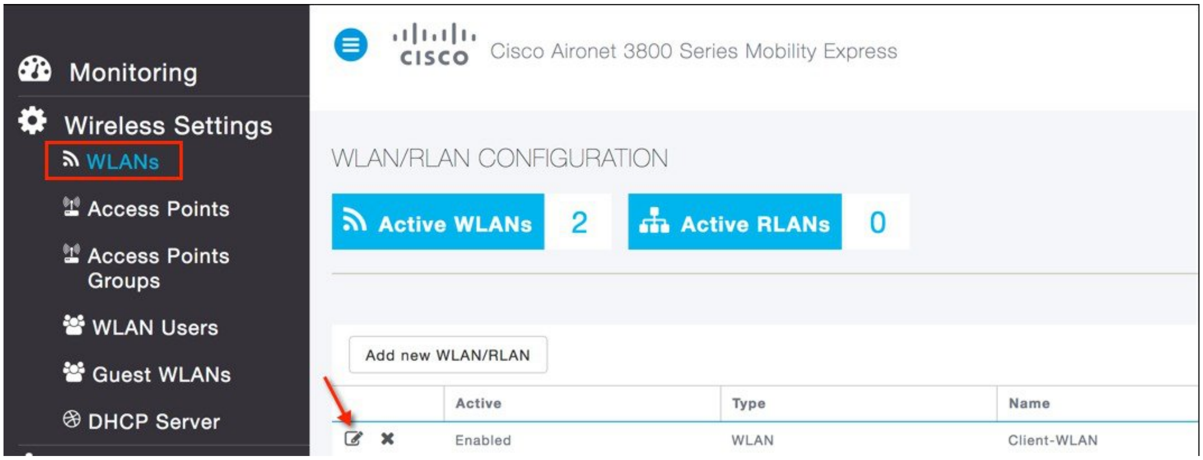
- Predefined:
  - Mon – Fri 8am to 5pm ON, all else OFF
  - Sat – Sun 8am to 8pm ON, all else OFF
- User-defined:
  - User can select each day of the week and check whether the WLAN would be ON for hourly intervals

Configuration can be defined from UI or CLI. Schedule WLAN configuration will also be included in configuration file that can be delivered to ME through PnP.

Scheduling WLAN

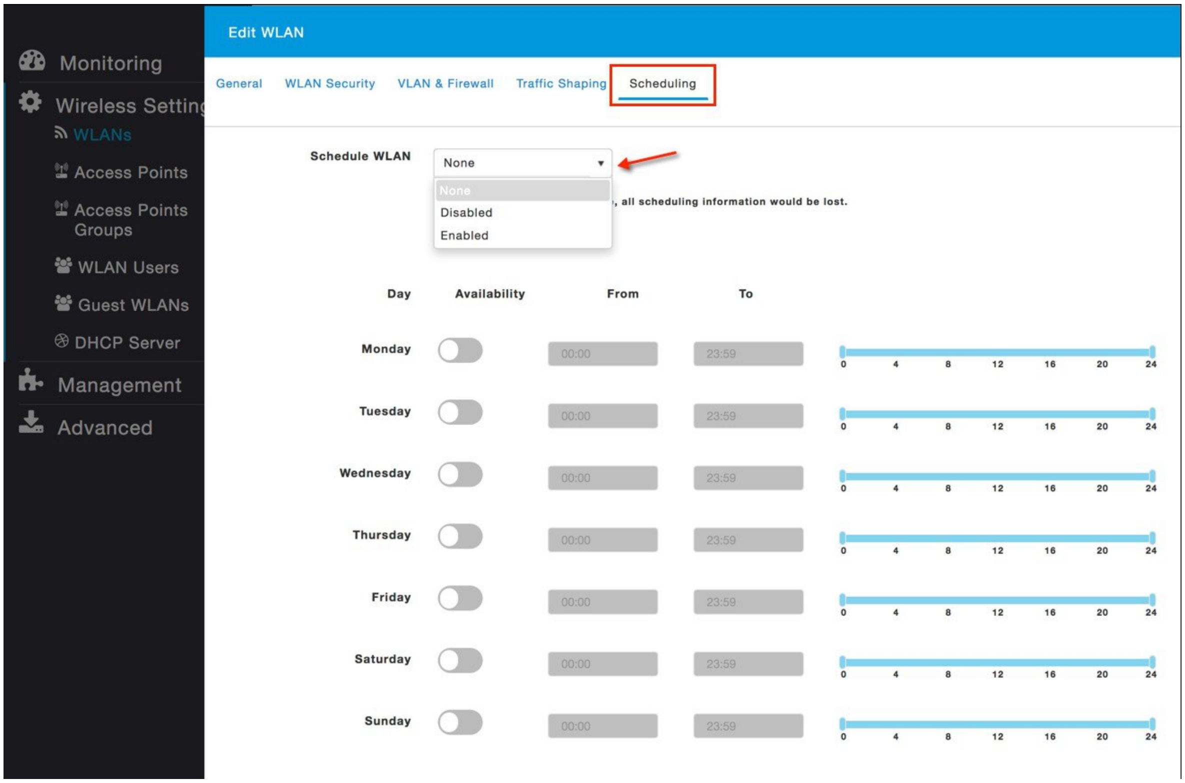
Procedure

Step 1 Navigate to **Wireless Settings** > **WLANs** and select WLAN required for setting WLAN schedule.



	Active	Type	Name
	Enabled	WLAN	Client-WLAN

Step 2 Click on the Scheduling tab you will have the option to Disable or Enable Schedule on the WLAN.

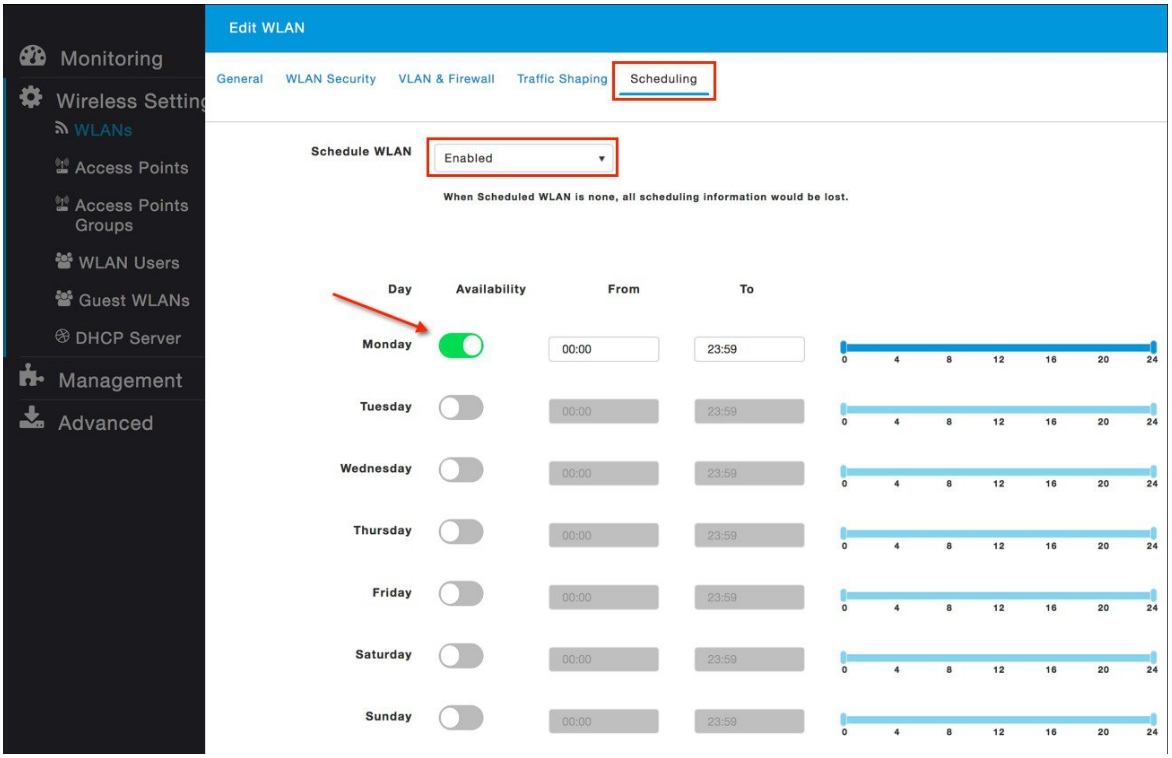


Schedule WLAN: None

, all scheduling information would be lost.

Day	Availability	From	To
Monday		00:00	23:59
Tuesday		00:00	23:59
Wednesday		00:00	23:59
Thursday		00:00	23:59
Friday		00:00	23:59
Saturday		00:00	23:59
Sunday		00:00	23:59

Step 3 In the screen shot below, an example of scheduling the WLAN to be enabled on Monday only is shown.



Edit WLAN

Schedule WLAN: Enabled

When Scheduled WLAN is none, all scheduling information would be lost.

Day	Availability	From	To
Monday	●	00:00	23:59
Tuesday	○	00:00	23:59
Wednesday	○	00:00	23:59
Thursday	○	00:00	23:59
Friday	○	00:00	23:59
Saturday	○	00:00	23:59
Sunday	○	00:00	23:59

Option 43 support for ME

DHCP option 43 is a vendor specific option and is used for providing WLC IP addresses to the Access Point. Without this option all Mobility Express APs will start the controller function but with this Option 43 with sub type option, one can have the Mobility Express AP convert to CAPWP and join a WLC appliance. After receiving the DHCP option 43 and sub type 0xF2 by the AP at bootup, it will convert the AP type to CAPWAP AP and follow the regular joining process.

DHCP Configuration on the switch is shown below.

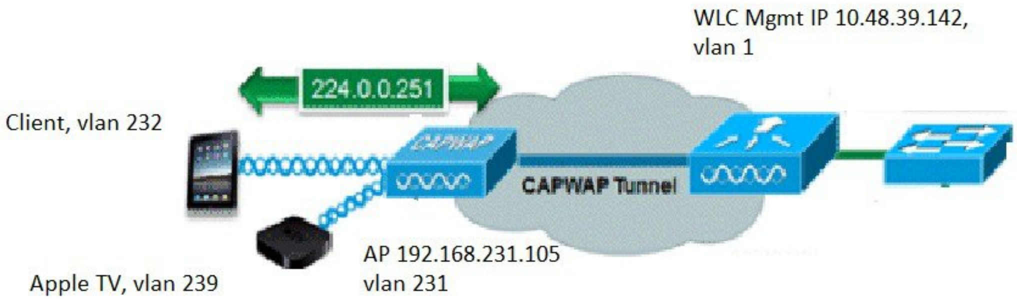
3750-SWITCH(dhcp-config)#option 43 hex F2056464645801

mDNS support

Bonjour protocol is an Apple service discovery protocol which locates devices and services on a local network with the use of multicast Domain Name System (mDNS) service records. The Bonjour protocol operates on service announcements and service queries. Each query or advertisement is sent to the Bonjour multicast address ipv4 224.0.0.251 (ipv6 FF02::FB). This protocol uses mDNS on UDP port 5353.

The address used by the Bonjour protocol is link-local multicast address and therefore is only forwarded to the local L2 network. Routers cannot use multicast routing to redirect the traffic because the time to live (TTL) is set to 1. This meant that all the service providers/sources (which advertise the service) and Bonjour clients(which ask for service) had to be in the same subnet. This lead to scalability problems.

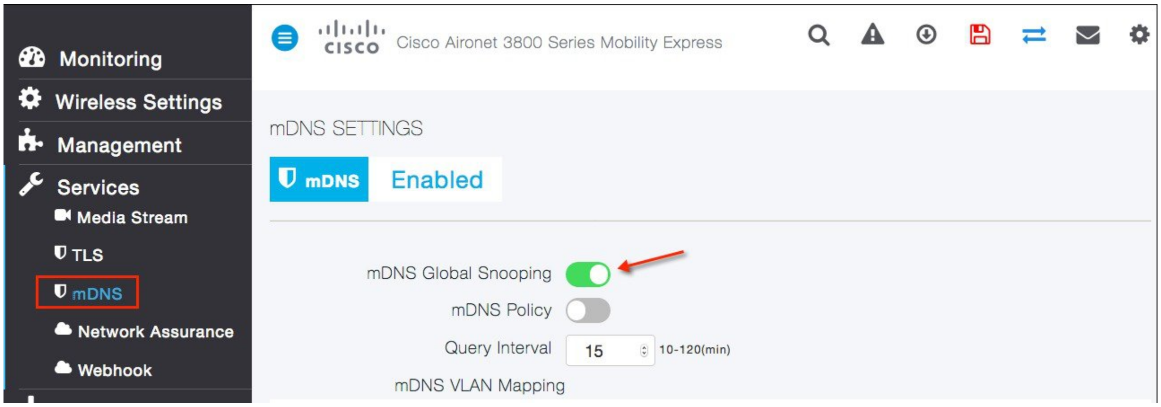
In order to address this issue, the Cisco Wireless LAN Controller (WLC) acts as a Bonjour Gateway. The WLC listens for Bonjour services, caches these Bonjour advertisements (AirPlay, AirPrint etc.) from the source/host. For example, Apple TV and responds back to Bonjour clients when they ask/request for a service. This way you can have the sources and clients in different subnets.



Cisco WLC works as a Bonjour gateway in local mode today. The WLC listens for Bonjour services and by caching those Bonjour Advertisements (AirPlay, AirPrint etc.) from the source/host e.g. AppleTV and responding back to Bonjour clients when they ask/request for a service.

Procedure

Step 1 Navigate to **Services** > **mDNS** and Enable **mDNS Global Snooping** as shown below.



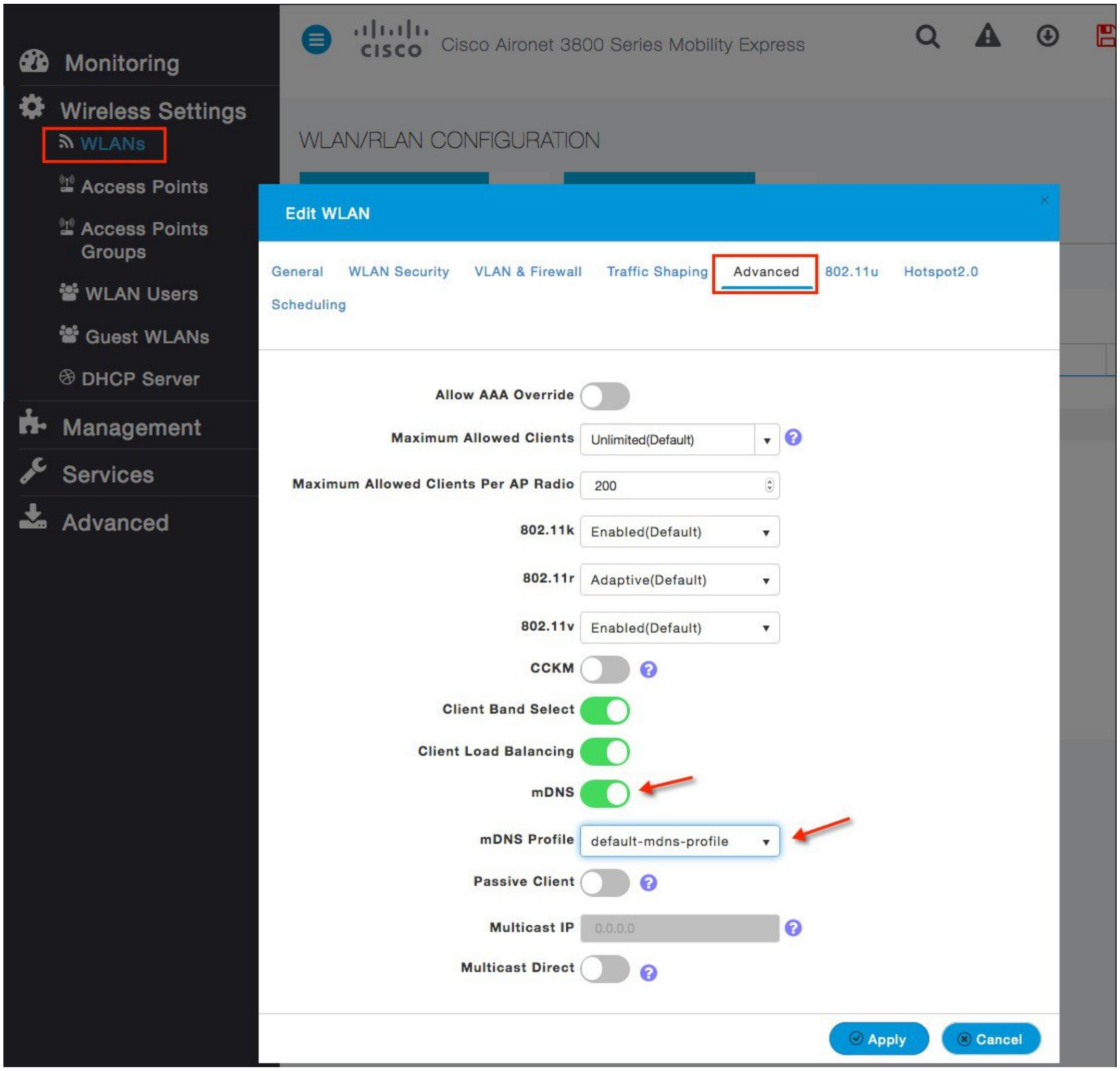
mDNS Global Snooping: on

mDNS Policy: off

Query Interval: 15 10-120(min)

mDNS VLAN Mapping

Step 2 Navigate to **Wireless Setting** > **WLANs** and create a WLAN for clients with any security type and Enable mDNS on the WLAN. By default mDNS Profile set as the default-mdns-profile to allow the Bonjour services that you require to be advertised on a particular WLAN.

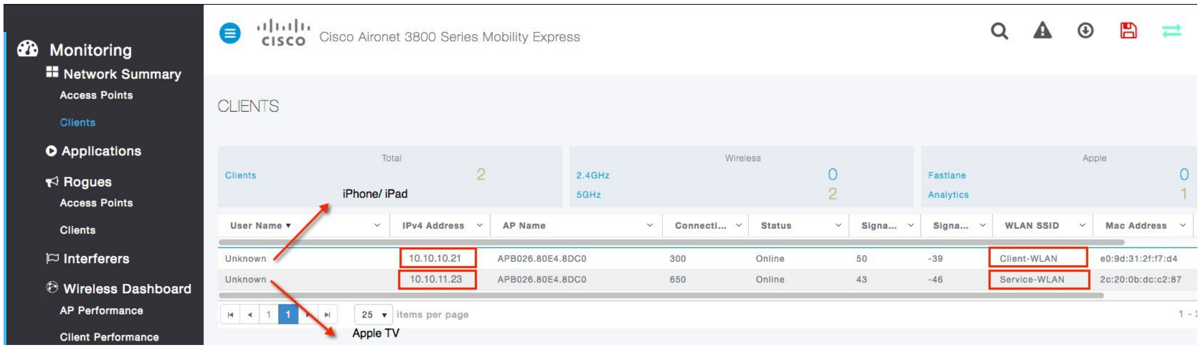


Allow AAA Override
Maximum Allowed Clients: Unlimited(Default)
Maximum Allowed Clients Per AP Radio: 200
802.11k: Enabled(Default)
802.11r: Adaptive(Default)
802.11v: Enabled(Default)
CCKM
Client Band Select
Client Load Balancing
mDNS
mDNS Profile: default-mdns-profile
Passive Client
Multicast IP: 0.0.0.0
Multicast Direct

```
(Cisco Controller) >config wlan mdns enable <wlan ID>
```

Step 3 Create another WLAN for services as shown and enable mDNS as we dids in step 2.

Step 4 Check if ipad/iphone and Apple TV are connected to the correct SSIDs and make sure they have ip addresses assigned from two different subnets.



Total		Wireless		Apple	
Clients	2	2.4GHz	0	Fastlane	0
		5GHz	2	Analytics	1

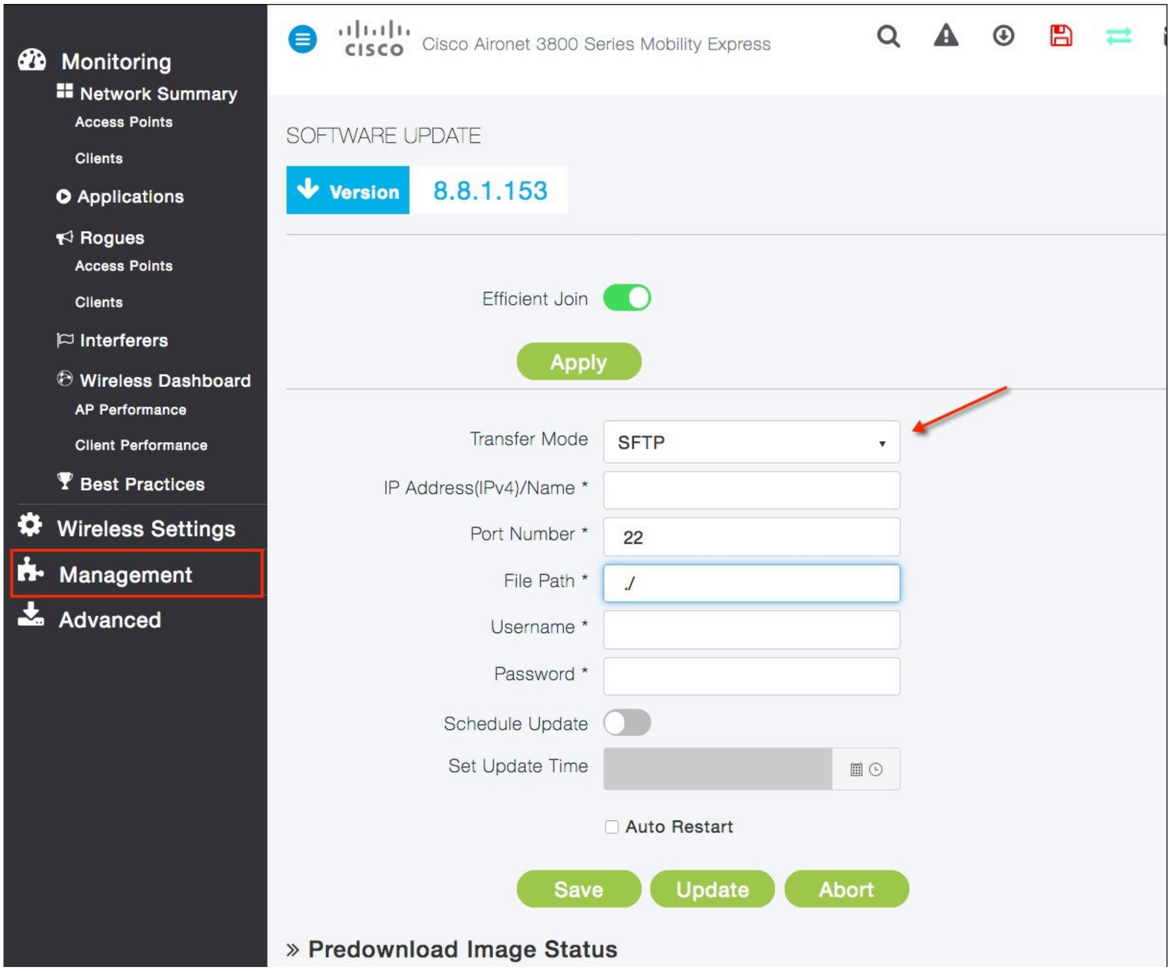
User Name	IPv4 Address	AP Name	Connecti...	Status	Signa...	Signa...	WLAN SSID	Mac Address
Unknown	10.10.10.21	APB026.80E4.8DC0	300	Online	50	-39	Client-WLAN	e0:9d:31:2f:f7:d4
Unknown	10.10.11.23	APB026.80E4.8DC0	650	Online	43	-46	Service-WLAN	2c:20:0b:dc:c2:87

FQDN support SFTP

User provided domain name of the SFTP server is resolved and used for transfer download method. In this release we added the support domain name along with ipv4 address for the SFTP server configuration.

Configuring SFTP

Navigate to management and select SFTP as your transfer method. Specify SFTP ip address and username/password configured.



SOFTWARE UPDATE

Version 8.8.1.153

Efficient Join

Transfer Mode SFTP

IP Address(IPv4)/Name *

Port Number * 22

File Path * ./

Username *

Password *

Schedule Update

Set Update Time

□ Auto Restart

Videostream support (MC2UC)

Cisco Unified Wireless Network (CUWN) release 8.0 introduces a new feature—VideoStream for Local Switching, for branch office deployments. This feature enables the wireless architecture to deploy multicast video streaming across the branches, just like it is currently possible for enterprise deployments. This feature recompenses the drawbacks that degrade the video delivery as the video streams and clients scale in a branch network. VideoStream makes video multicast to wireless clients more reliable and facilitates better usage of wireless bandwidth in the branch.

Multicast to Unicast

By enabling 802.11n data rates and providing packet error correction, multicast-to-unicast capabilities of Cisco VideoStream enhances reliability of delivering streaming video over Wi-Fi beyond best-effort features of traditional wireless networks. A wireless client application subscribes to an IP multicast stream by sending an IGMP join message. With reliable multicast, this request is snooped by the infrastructure, which collects data from the IGMP messages. The AP checks the stream subscription and configuration. A response is sent to the wireless client attached to the AP in order to initiate reliable multicast once the stream arrives. When the multicast packet arrives, the AP replicates the multicast frame and converts it to 802.11 unicast frames. Finally, a reliable multicast service delivers the video stream as unicast directly to the client.

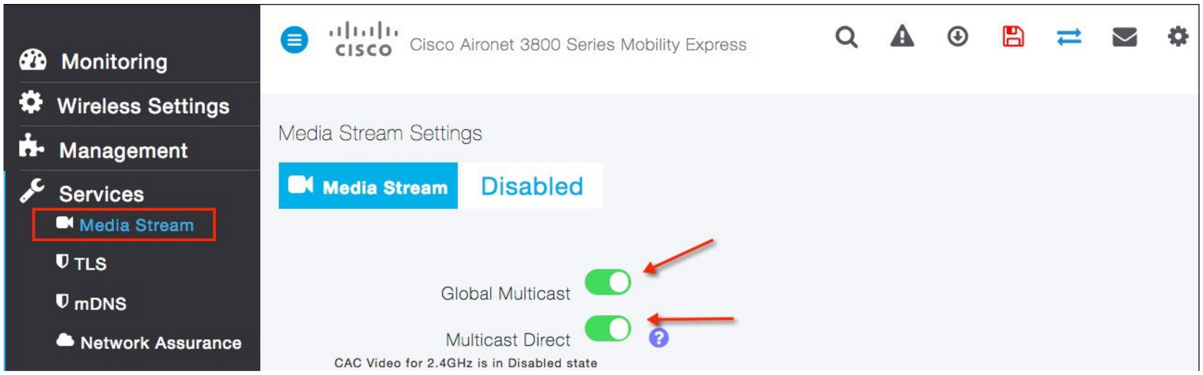
Higher Video Scaling on Clients

With Cisco VideoStream technology, all of the replication is done at the edge (on the AP), thus utilizing the overall network efficiently. At any point in time, there is only the configured media stream traversing the network, because the video stream is converted to unicast at the APs based on the IGMP requests initiated by the clients. Some other vendor implementations do a similar conversion of multicast to unicast, but do it inefficiently as evidenced by the load put on the wired network to support the stream.

Configuring Videostream

Procedure

Step 1 Navigate to **Services** > **Media Stream** and enable Global Multicast mode and Multicast Direct as shown below



Media Stream Settings

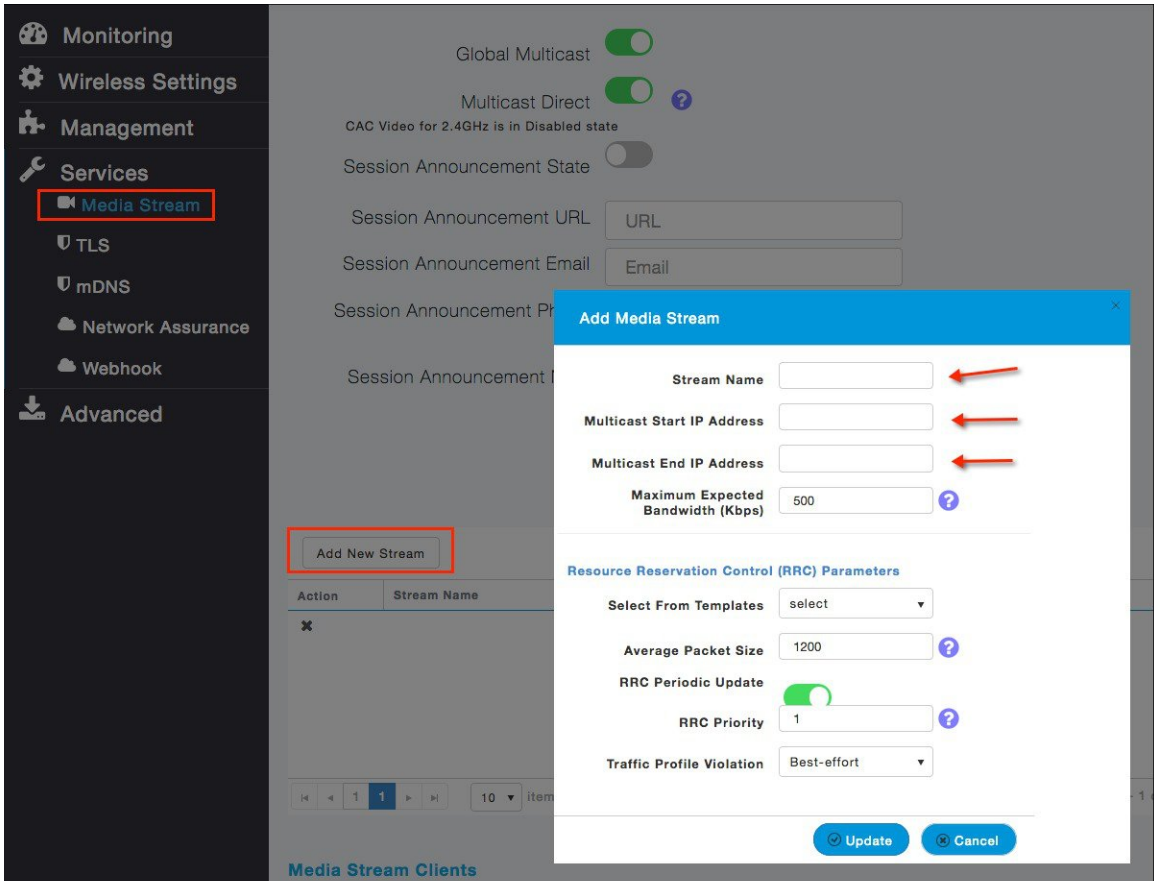
Media Stream Disabled

Global Multicast

Multicast Direct

CAC Video for 2.4GHz is in Disabled state

Step 2 Click on Add new Stream to add multicast stream to controller. Choose Stream Name and select multicast range.



Global Multicast

Multicast Direct

CAC Video for 2.4GHz is in Disabled state

Session Announcement State

Session Announcement URL: URL

Session Announcement Email: Email

Session Announcement Ph

Session Announcement I

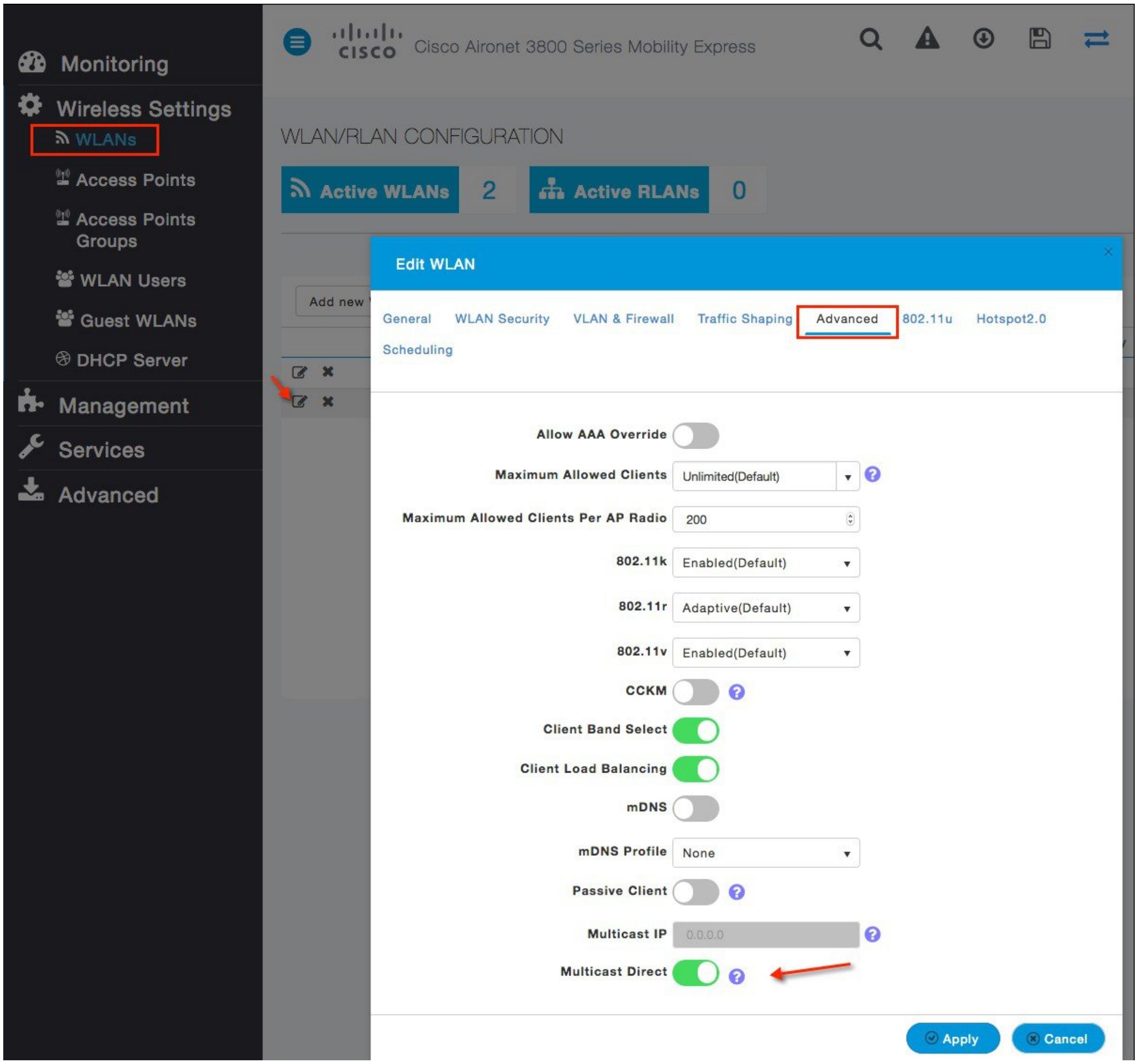
Add Media Stream

Stream Name	
Multicast Start IP Address	
Multicast End IP Address	
Maximum Expected Bandwidth (Kbps)	500

Resource Reservation Control (RRC) Parameters

Select From Templates	select
Average Packet Size	1200
RRC Periodic Update	
RRC Priority	1
Traffic Profile Violation	Best-effort

Step 3 To enable VideoStream on WLAN One or all WLANs/SSIDs configured can be enabled for streaming video with VideoStream. This is another configuration step that can control the enabling of the VideoStream feature. Enabling or disabling the VideoStream feature is non-disruptive.

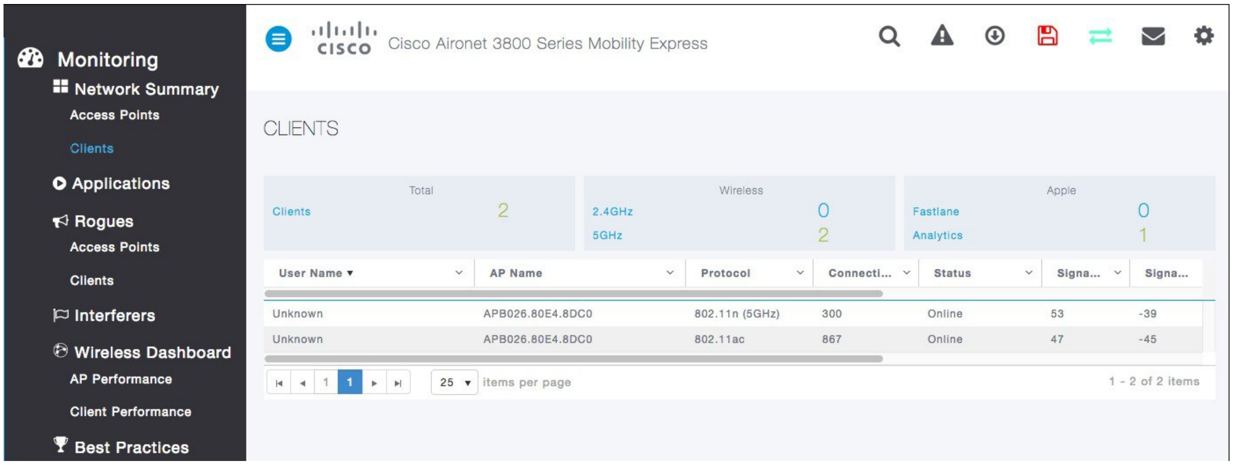


Allow AAA Override
Maximum Allowed Clients: Unlimited(Default)
Maximum Allowed Clients Per AP Radio: 200
802.11k: Enabled(Default)
802.11r: Adaptive(Default)
802.11v: Enabled(Default)
CCKM
Client Band Select
Client Load Balancing
mDNS
mDNS Profile: None
Passive Client
Multicast IP: 0.0.0.0
Multicast Direct

All wireless clients requesting to join a stream will be assigned video QoS priority on admission.

Wireless client streaming video prior to enabling the feature on the WLAN will be streaming using normal multicast. Enabling the feature switch the clients to multicast-direct automatically on the next IGMP snooping interval. Legacy multicast can be enabled on the WLAN by not checking the Multicast Direct feature. This will show that wireless clients streaming video are in Normal Multicast mode.

Step 4 Make sure the wireless clients are associated to the access point(s), and are configured for a correct interface. As seen in the Figure , there are two clients associated to one AP. The two clients have an IP address from VLAN X (SSID name—enjoy).The associated clients have an IP address and good uplink connectivity to the AP.



Total		Wireless		Apple	
Clients	2	2.4GHz	0	Fastlane	0
		5GHz	2	Analytics	1

User Name	AP Name	Protocol	Connecti...	Status	Signa...	Signa...
Unknown	APB026.80E4.8DC0	802.11n (5GHz)	300	Online	53	-39
Unknown	APB026.80E4.8DC0	802.11ac	867	Online	47	-45

Enable streaming on the wired side by connecting a video server with a configured multicast address 229.77.77.28. Refer the following link to know how to stream from a Video Sever: https://wiki.videolan.org/Documentation:Streaming_HowTo_New/#Streaming_using_the_GUI

The Wireshark capture on the client shows the Multicast to Unicast Video Stream. The Ethernet header contains the MAC address of the client as the Destination MAC address, for example, 7c:d1:c3:86:7e:dc.

Cisco RFID Tag support

The Cisco ME supports tracking of active RFIDs. This helps customers track valued assets. When the active RFID is in range the WLC will add information to its database. With Cisco Aironet 4800, 3800, and 2800 Series APs, you can track up to 2000 active RFIDs. With all the other applicable Cisco APs, you can track up to 1000 active RFIDs.

Configuring Cisco RFID Tag

Procedure

Step 1 RFID Tag data Collection is enabled by default, CLI shown below should show default configuration.

```
RFID Tag data Collection......................... Enabled
   RFID  timeout................................. 1200 seconds
   RFID mobility..................................
  RFID  Rate limit............................... 1000
```

Step 2 Place RFID tag near AP, “show rfid summary” should show RFID tags.

```
(Cisco Controller) >show rfid summary

Total Number of RFID    : 2
----------------- -------- ------------------ ------ ---------------------
     RFID ID       VENDOR       Closest AP      RSSI  Time Since Last Heard
----------------- -------- ------------------ ------ ---------------------
```

```
00:0c:cc:4f:5b:62 Aerosct  APB026.80E4.8DC0    -52      456 seconds ago
00:12:b8:0a:c5:f6 G2       APB026.80E4.8DC0    -37     1011 seconds ago
```

Step 3 To show RFID details, use CLI as shown below:

```
“show rfid detail <mac>” should show RFID tag details
(Cisco Controller) >show rfid detail 00:0c:cc:0b:c0:79
RFID address.................................... 00:0c:cc:0b:c0:79
Vendor.......................................... Aerosct Last
Heard....................................... 24 seconds ago
Packets Received................................ 7 Bytes
Received................................. 399
Detected Polling Interval....................... 35 seconds Cisco
Type.....................................
Content Header
=================
CCX Tag Version................................. 1
Tx Power........................................ 19 dBm
Channel......................................... 11
Reg Class....................................... 6
Burst Length.................................... 2
CCX Payload ===========
Last Sequence Control........................... 0
Payload length.................................. 22
Payload Data Hex Dump
00 02 00 33 02 07 42 02 80 00 00 00 e1 04 07 00 0c cc 00 00 13 00
Nearby AP Statistics: APA0EC.F96C.D510(slot 0, chan 11) 23 se.... -66 dBm
```