Cisco Wireless LAN Controller Bonjour Phase III Deployment Guide, Release 8.0

Last Updated: August, 2014

For configuration and information on the previously released Bonjour features, refer to the following deployment guides:

http://www.cisco.com/c/en/us/td/docs/wireless/technology/bonjour/Bonjour74.html

http://www.cisco.com/c/en/us/td/docs/wireless/technology/bonjour/7-5/Bonjour_Gateway_Phase-2_WLC_software_release_7-5.html

Overview

Bonjour is an Apple service discovery protocol, which locates devices such as printers, other computers, and the services that those devices offer on a local network using multicast Domain Name System (mDNS) service records. The Bonjour protocol operates on service announcements and service queries, which allow devices to ask and advertise specific applications such as:

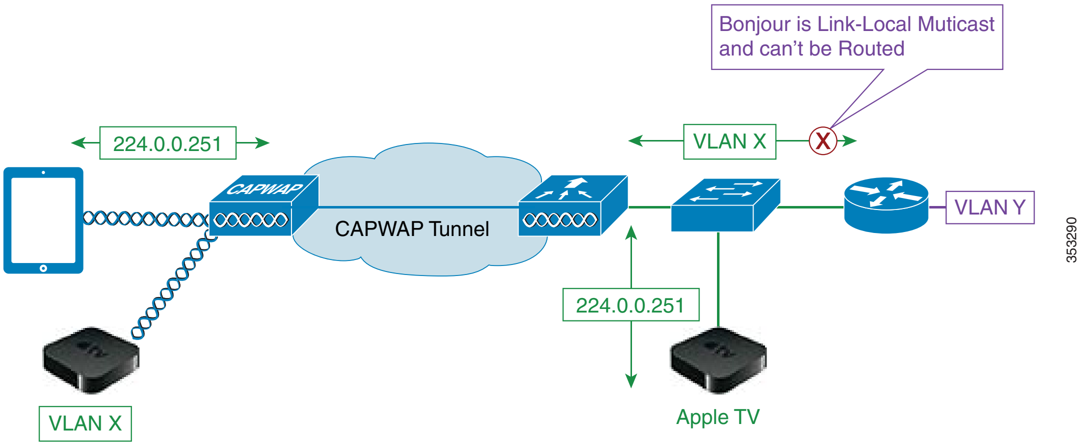
- Printing Services
- File Sharing Services
- Remote Desktop Services
- iTunes File Sharing
- iTunes Wireless iDevice Syncing (in Apple iOS v5.0+)
- AirPlay offering the following streaming services:
  - Music broadcasting in iOS v4.2+
  - Video broadcasting in iOS v4.3+
  - Full screen mirroring in iOS v5.0+ (iPad2, iPhone4S or later)

Each query or advertisement is sent to the Bonjour multicast address for delivery to all clients on the subnet. Apple's Bonjour protocol relies on mDNS operating at UDP port 5353 and sent to the following reserved group addresses:

Cisco Systems, Inc.
www.cisco.com

- IPv4 Group Address – 224.0.0.251
- IPv6 Group Address – FF02::FB

The addresses used by the Bonjour protocol are link-local multicast addresses, and thus are only forwarded to the local L2 domain. Routers cannot use multicast routing to redirect the traffic because the time to live (TTL) is set to one, and link-local multicast is meant to stay local by design.



Bonjour Services in Phase I and II — Release 7.4-7.6

Prior to release 8.0, the following features were introduced in the Phase 1 and 2 of the Bonjour services support on the CUWN. These features include the following:

- Controller mDNS gateway
- Controller mDNS snooping
- Bonjour profiles on WLAN
- Location Specific Services (LSS) for wireless service
- mDNS-AP (enhance VLAN visibility at WLC for non-layer 2 VLANs)
- Priority MAC support
- Origin based service discovery
- Bonjour browser
- Bonjour SSO
- Bonjour debugging

Table 1 lists the services that are offered in phases 1, 2 and 3.

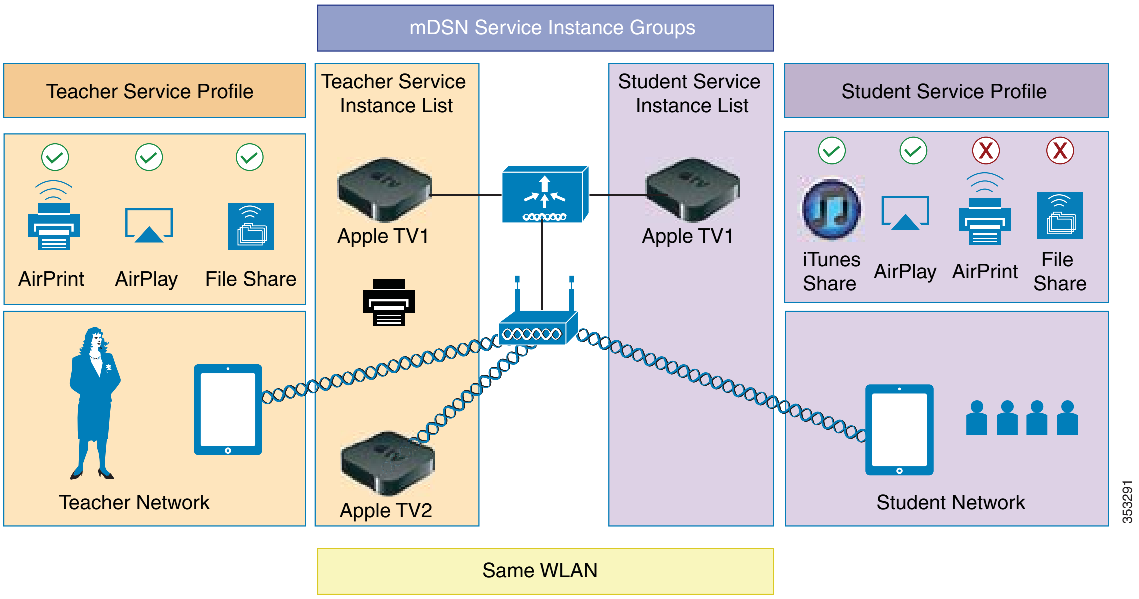
Table 1 Summary of Services in Phase 1, 2, and 3

Bonjour - 7.4 (Phase 1)	Bonjour - 7.5 (Phase 2)	Bonjour - 8.0 (Phase 3)
• Bonjour service with mDNS gateway for wired and wireless services • Bonjour service policy applied per interface or per WLAN • mDNS services cached on the controller • Bonjour services available on all controller seen L2 domains • Bonjour services supported on the Anchor controller • Bonjour services supported with L2 and L3 roaming • 100 services and 64 service providers per service type • Support of Flex Connect APs in central and local mode	• Support of mDNS services across L3 domains • Introduction of mDNS AP for Bonjour service snooping on 10 wired VLANs • LSS – Location Specific Services • Priority MAC of Bonjour service • Origin based service discovery • 6400 services and service providers per service type	• Bonjour GW with access policy controlled service discovery • Device service mapping to access policy • Bonjour group and single access policy management • Bonjour profile control by local policy • Introduction of Bonjour administrator to manage specific Bonjour services from Cisco Prime

Introduction to Bonjour Policies and New Requirements

Enterprise credentials of Bonjour are poor and hence the advent of Bonjour gateway. Bonjour gateway snoops and caches Bonjour services across VLANs and periodically refreshes the same. WLC acts as a proxy for all Bonjour services published by wireless and wired devices. Bonjour gateway as of release prior to 8.0 had inadequate capabilities to filter cached wired / wireless service instances based on the credentials of the querying client and its location.

With introduction of the Bonjour policies in the release 8.0, the administrator can configure to identify who uses the Bonjour service instances and in what location (all this applies to the same WLAN). With introduction of the Bonjour policies, the administrator does not need to create multiple WLANs to select which services are allowed or should be used on specific WLAN. Based on user 802.1x authentication, the AAA server or ISE can be configured to return USER-ROLE or BONJOUR-PROFILE in the form of the “CISCO-AV-PAIR”. This value gets plumbed into the policy created on the wireless controller. Based on the user authentication, a configured policy and profile are applied to a specific user on the same WLAN.



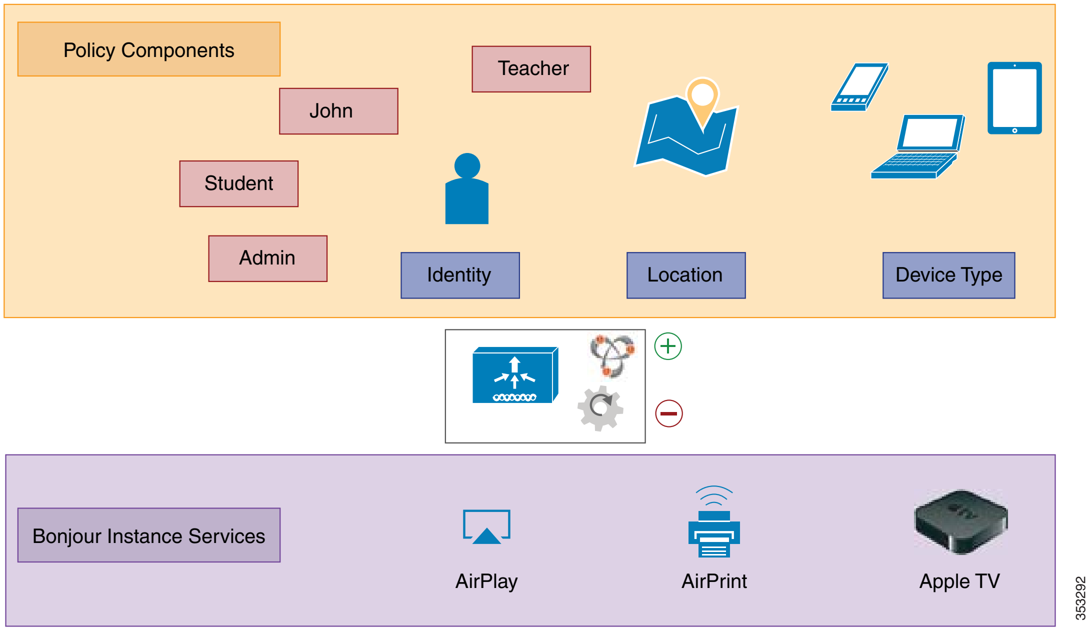
As mentioned in the figure above, improvements to Bonjour services are made, and Bonjour policies are introduced to allow per service instance (MAC address) configuration that mandates how the service instance is shared, which is articulated as follows:

- Service instance is shared with whom (user-id).
- Service instance is shared with which role/s (client-role).
- What is the location allowed to access the service instance (client location).

This configuration can be applied to wired and wireless service instances, and the response to any query will solely be based on the policy configured for each service instance. This allows selective sharing of service instances based on the location, user-id, or role. Since most service publishing devices are wired, this allows filtering of wired services at par with wireless service instances. While mDNS profile associated with the client checks for service type being queried before responding to the query, the access policy further allows filtering of specific service instances based on querying client location, role, or user-id.

With Bonjour access policy, there are two levels of filtering the client queries, which are as follows:

- At the service type level by using the mDNS profile.
- At the service instance level using the access policy associated with the service each instance.



A service instance or a set of service instances discovered and cached by the WLC can be associated with an access policy filter, which acts like a lens that determines which clients and what kind of client context (role or user-id) can see and access the service instance.

Note Service instances that are not configured with any access policy will be mapped to the default access policy, which allows only the administrator user role, by default, to receive the service instances. Additional users can be configured and added in the default policy.

- Bonjour access policy filters can be configured for specific service instances identified by the MAC address of the devices publishing the services.
- Bonjour access policy is associated with a service group name that contains one or more MAC addresses of the devices publishing the Bonjour services.
- The service group name is then attached to the service instance when it is discovered and cached at the WLC.
- While traversing the list of service instances in response to a client query, each instance will be evaluated to verify if the querying client location, role, or user-id are allowed access to the service instance before including the same in the response.

If the same MAC address is configured in multiple service groups, it means the service instance will be associated with all the service group names that are configured with this MAC address, and all the access policies associated with the MAC addressee's service group names will be evaluated until the verdict is to include the service instance. Currently, a maximum of five service groups are supported for a single MAC address. Service group configurations can be done even when mDNS snooping is disabled or offline, and the access-policy comes into effect when the services are discovered. It can also be done dynamically when snooping is already enabled.

Bonjour Service Groups

A service group name can be associated with a set of MAC addresses, and the maximum MAC addresses that can be configured for any service group is limited by the platform dependent global maximum number of service instances that can be discovered, that is,

Service limit: 6400 on 2500, 5508, WiSM2 and vWLC and 16000 services on 7510 and 8510 UC Controllers.

Each MAC address is configured with a unique name, which can be the service instance name, and the location of the MAC address for both wired and or wireless.

1. Since flexibility is desired when configuring the location using the AP-NAME, AP-GROUP, or AP-LOCATION, the administrator has to configure the type of location that is desired. This configuration implies that only clients from the same location as that of the device publishing the service can access the service. As long as the global maximum limit of MAC addresses is not exceeded, any service group can configure as many MAC addresses as desired.

   In case of wireless service instances, the device location can change. Yet, if you want only those devices whose location is same as that of the service instance, the keyword "same" could be configured for such wireless service providers.

   In case of wired services, the same location does not apply because wired clients do not get associated to the AP.

2. If the keyword "Any" is configured for location, it implies that there is no location based filtering for the clients trying to access the device. This means the clients from any location can access the service subject to role and user-id credentials being allowed by the policy associated with the service group for that MAC address.

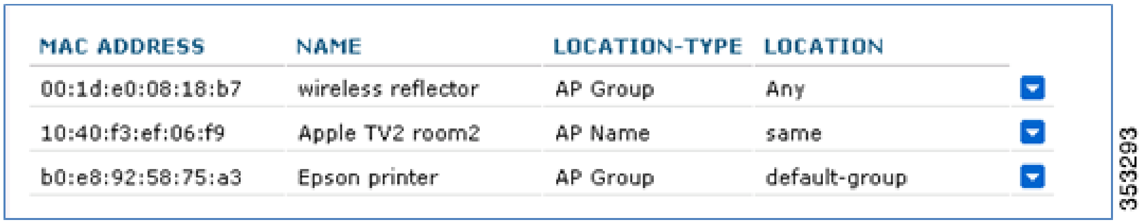
3. If the keyword "ap-name" is used, only clients associated to that AP can access the service instance.

Note Location validation is implicit and will be the first level of access policy filtering even before ROLE and USER-ID credentials of the client are verified.

Table 2 depicts a possible policy configuration with the service group named AppleTV-teachers.

Table 2 Example for Policy Configuration with the Service Group Name

Service Group Name	MAC Address	Service Name	Location Type	Location
AppleTV-teachers	e8:b7:48:9b:f0:20	AppleTV-class1	AP-GROUP	6-FLR
	e8:b7:48:9b:f0:21	AppleTV-class2	AP-NAME	AP4403.a740.bc97
	—	—	—	—
	e2:34:23:11:32:eb	AppleTV-class9	AP-NAME	same
	—	—	—	—
	e8:c7:38:9c:f1:32	AppleTV -class3	AP-GROUP	any



MAC ADDRESS	NAME	LOCATION-TYPE	LOCATION
00:1d:e0:08:18:b7	wireless reflector	AP Group	Any
10:40:f3:ef:06:f9	Apple TV2 room2	AP Name	same
b0:e8:92:58:75:a3	Epson printer	AP Group	default-group

Device Access Policy Constructs and Rules

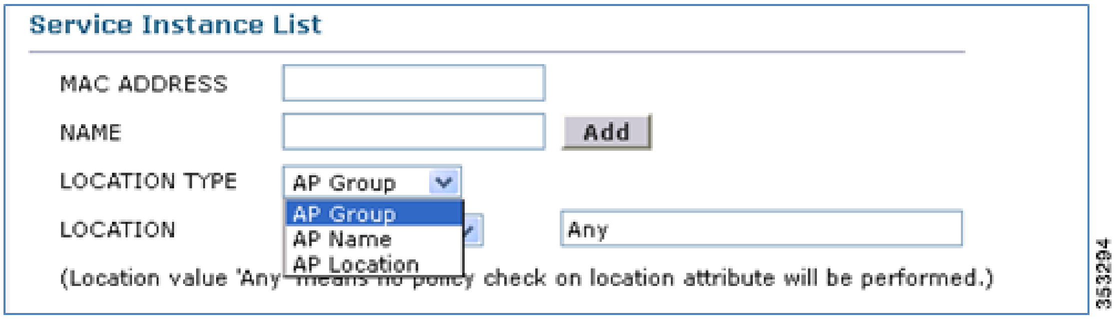
This section explains the access policy in terms of the client context attributes, its constructs, the rule components that make up of the policy, and how the rules and hence the policies are evaluated. This helps in deciding whether the given service instance should be included or not in the mDNS response for the client that made the mDNS query. Further, if multiple service instances are mapped to the same access policy, for a given mDNS query, the policy will be evaluated only once for all those instances which have the same access policy mapping to optimize the policy evaluation overhead for a given query.

Client Context Attributes in an mDNS Policy

Any client initiating an mDNS query can be associated with a set of attributes that describe the context of the client. The attributes, for example location, can change dynamically when the clients move to a different location. Only these enumerated attributes will be used to articulate a Bonjour access policy rule. The list of attributes and how they are fetched are detailed in Table 3. The user can formulate a rule by combining these attributes with logical OR operations and attach the rule to the policy. A policy is composed of a single rule, even though multiple rules can be provisioned.

Table 3 Attributes and Their Usage

S.No	Attribute name	Description	When used in configuration
1	ROLE	Is a string like "teacher" or "student" and plumbed into the DB of the client. ISE or AAA can associate a role to a client.	Administrator must add the role name and user_id to create a rule.
2	LOCATION	Location of the client is a string, which is the "ap-location" of the client's AP.	When this is used to configure a rule, the user could mention any of the below three to specify location: • ap-location • ap-name • ap-group name
3	USER-ID	Uniquely identifies whether the client is plumed into the client DB by AAA or ISE during 802.1x authentication.	Exactly same string name must be used by user, while configuring a policy that uses user-id.



Service Instance List

MAC ADDRESS

NAME

LOCATION TYPE AP Group

LOCATION Any

(Location value 'Any' means no policy check on location attribute will be performed.)

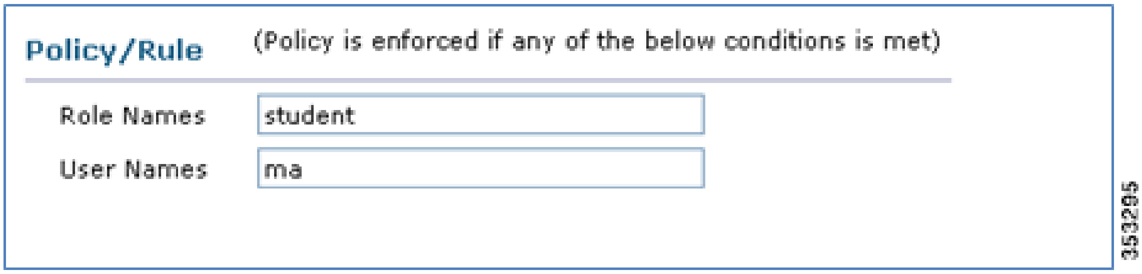
Access Policy Rules

An access policy service group is identified by a name and is associated with just one rule.

The rule is defined using the role or user-id (comma separated list). It implies that, a client, making an mDNS query, whose role is one of those listed in the policy roles or the client user-id is one of those listed in the user-id list, then access to the service instances is granted.

RULE is defined as,

[ROLE=teacher, student] AND [USER-ID = John, Mike]



Policy/Rule (Policy is enforced if any of the below conditions is met)

Role Names student

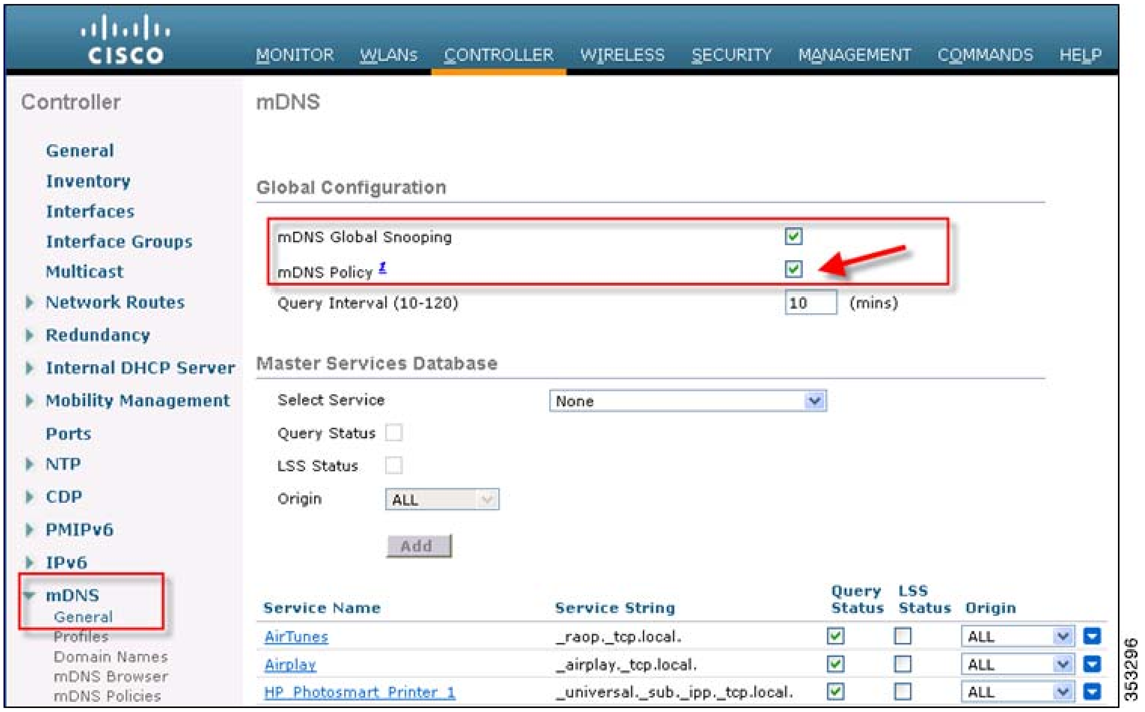
User Names ma

Configuring mDNS Bonjour Policies

To configure the mDNS Bonjour policy on the controller, perform the following steps:

Step 1 On the Controller tab, in the left pane, click **mDNS > General**.

Step 2 In the right pane, in the Global Configuration area, check the **mDNS Global Snooping** and **mDNS Policy** check boxes.



mDNS

Global Configuration

mDNS Global Snooping ☑

mDNS Policy [1] ☑

Query Interval (10-120) 10 (mins)

Master Services Database

Select Service None

Query Status □

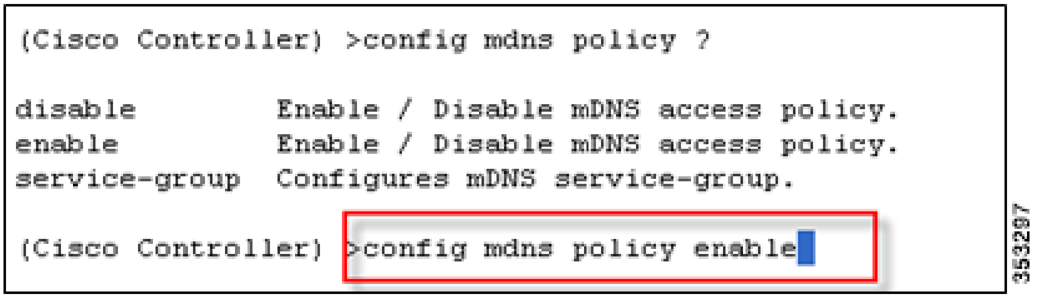
LSS Status □

Origin ALL

Service Name	Service String	Query Status	LSS Status	Origin
AirTunes	_raop._tcp.local.	☑	□	ALL
Airplay	_airplay._tcp.local.	☑	□	ALL
HP_Photosmart_Printer_1	_universal._sub._ipp._tcp.local.	☑	□	ALL

The same operation can be accomplished from the CLI with the command:

```
Wlc > config mdns policy enable
```



```
(Cisco Controller) >config mdns policy ?

disable          Enable / Disable mDNS access policy.
enable           Enable / Disable mDNS access policy.
service-group    Configures mDNS service-group.

(Cisco Controller) >config mdns policy enable
```

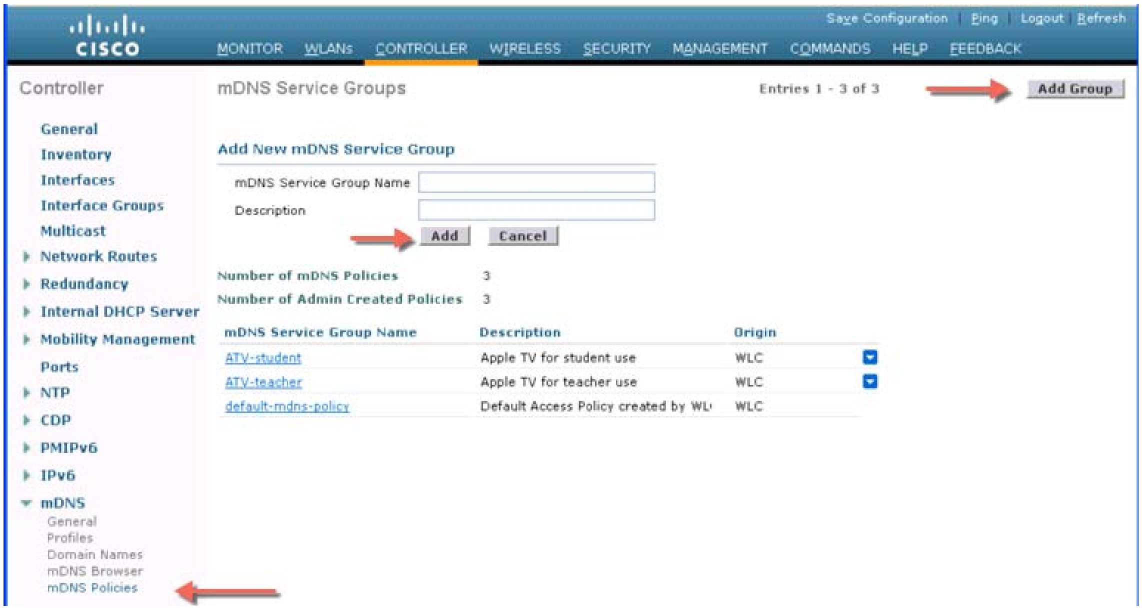
Step 3 To configure the mDNS Service group, do the following:

a. On the Controller tab, in the left pane, click **mDNS > mDNS policies**.

b. In the right pane, click **Add Group**.

c. In the Add New mDNS Service Group area, enter the group name and description for the mDNS service group.

d. Click **Add**.



mDNS Service Groups

Entries 1 - 3 of 3

Add New mDNS Service Group

mDNS Service Group Name

Description

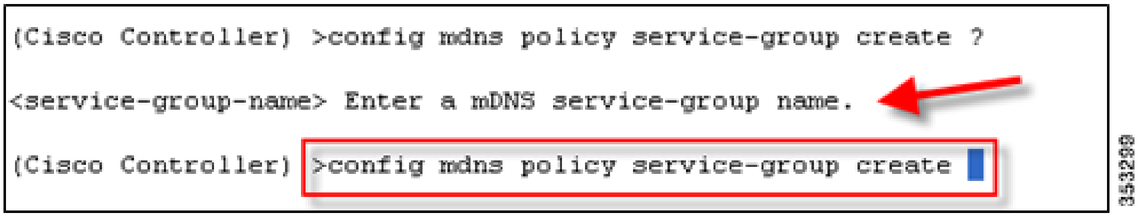
Number of mDNS Policies 3

Number of Admin Created Policies 3

mDNS Service Group Name	Description	Origin
ATV-student	Apple TV for student use	WLC
ATV-teacher	Apple TV for teacher use	WLC
default-mdns-policy	Default Access Policy created by WL(	WLC

The same operation can be accomplished from the CLI with the command:

```
Wlc> config mdns service-group create
```



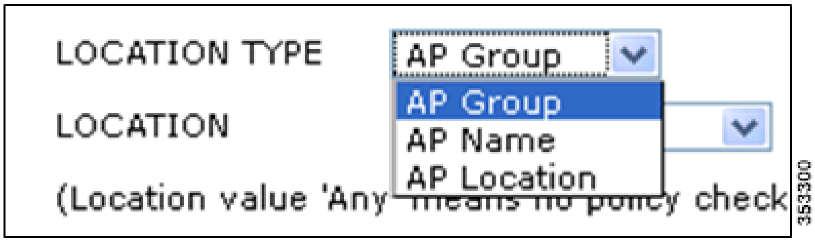
```
(Cisco Controller) >config mdns policy service-group create ?

<service-group-name> Enter a mDNS service-group name.

(Cisco Controller) >config mdns policy service-group create
```

Step 4 Once the service group is created, configure the service group with service instances in that group, such as who can use those services and in what location. See examples of configuration from GUI where ATV-teacher group is configured.

You can choose Location Type by AP Group, AP Name or AP Location.

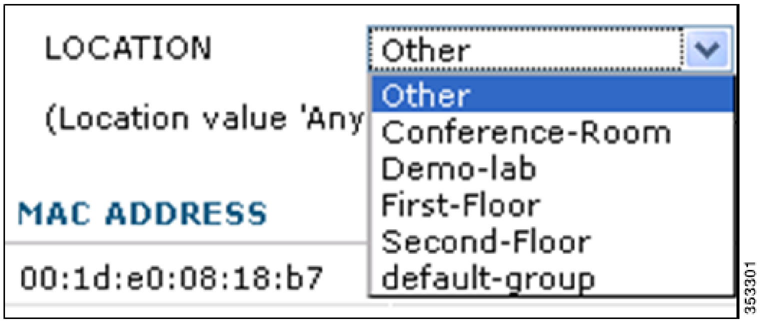


LOCATION TYPE AP Group

LOCATION

(Location value 'Any' means no policy check

Step 5 Configure Location as ANY, SAME or by AP-NAME. Location AP can selected based on the AP Name configured as shown in the following example.



LOCATION Other

(Location value 'Any

MAC ADDRESS

00:1d:e0:08:18:b7

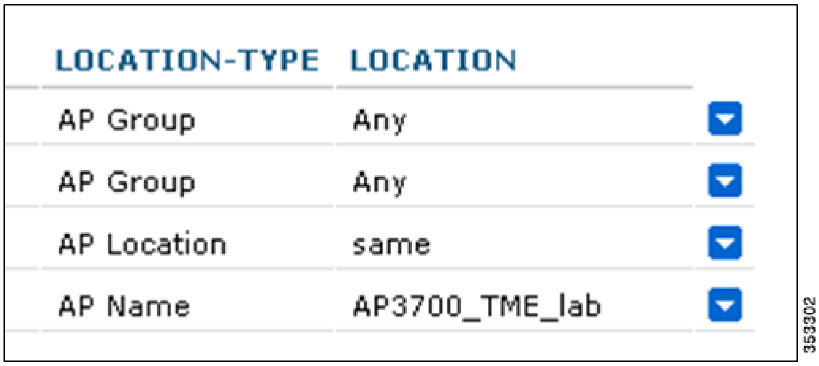
1. If keyword Same is selected, it implies that only clients from the same location as that of the device publishing the service can access the service. As long as the global maximum limit of MAC addresses is not exceeded, any service group can configure as many MAC addresses as desired.

   In case of wireless service instances, since the device location can change, and yet we want only those devices whose location is same as that of the service instance, the keyword Same could be configured for such wireless service providers.

   In case of wired services, the same location does not apply because wired clients do not get associated to the AP.

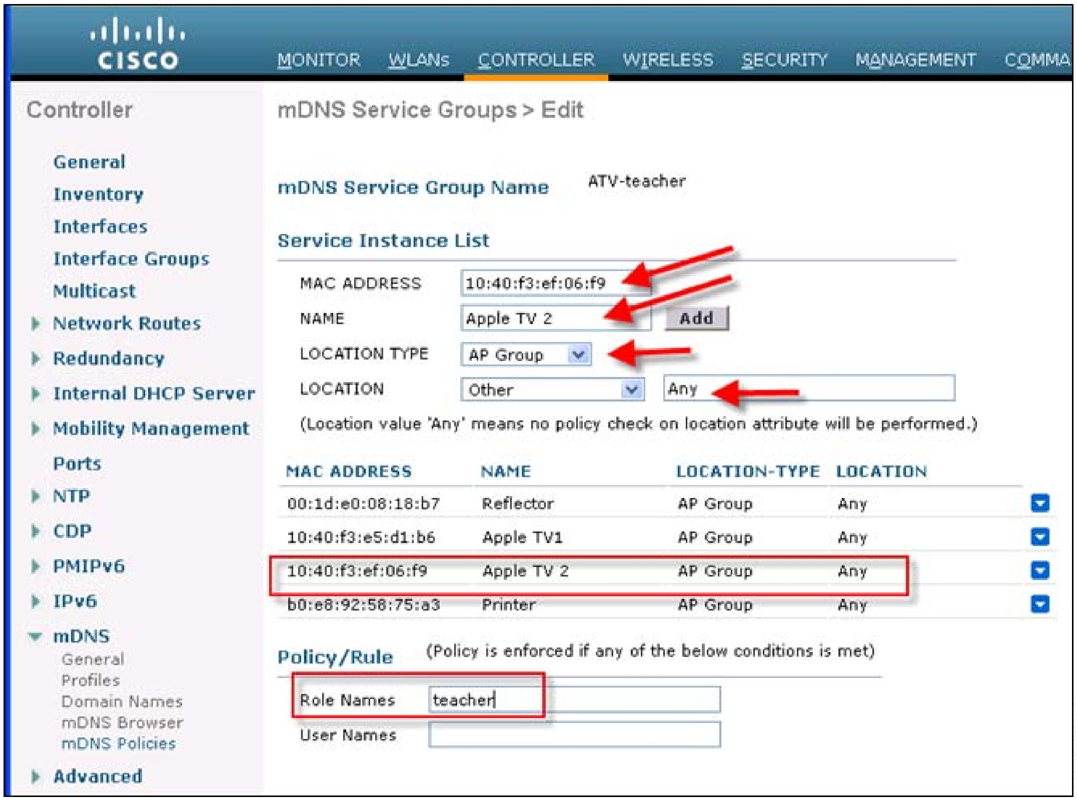
2. If the keyword Any is configured for location, it implies that there is no location based filtering for the clients trying to access the device. Meaning, clients from any location can access the service subject to role and user-id credentials being allowed by the policy associated with the service group for the mentioned MAC address.

3. If the keyword AP-Name is used, only clients associated to that AP can access the service instance.



LOCATION-TYPE	LOCATION
AP Group	Any
AP Group	Any
AP Location	same
AP Name	AP3700_TME_lab

Finally, as explained, the policy rule must be configured with users Role and optionally with user-id. Also, the user ROLE has to be configured to match the ROLE av-pair string that will be returned from the AAA server upon user's successful authentication. As shown in the example below, the Role Name teacher has to be matched to use that service group.



mDNS Service Groups > Edit

mDNS Service Group Name ATV-teacher

Service Instance List

MAC ADDRESS 10:40:f3:ef:06:f9

NAME Apple TV 2

LOCATION TYPE AP Group

LOCATION Other Any

(Location value 'Any' means no policy check on location attribute will be performed.)

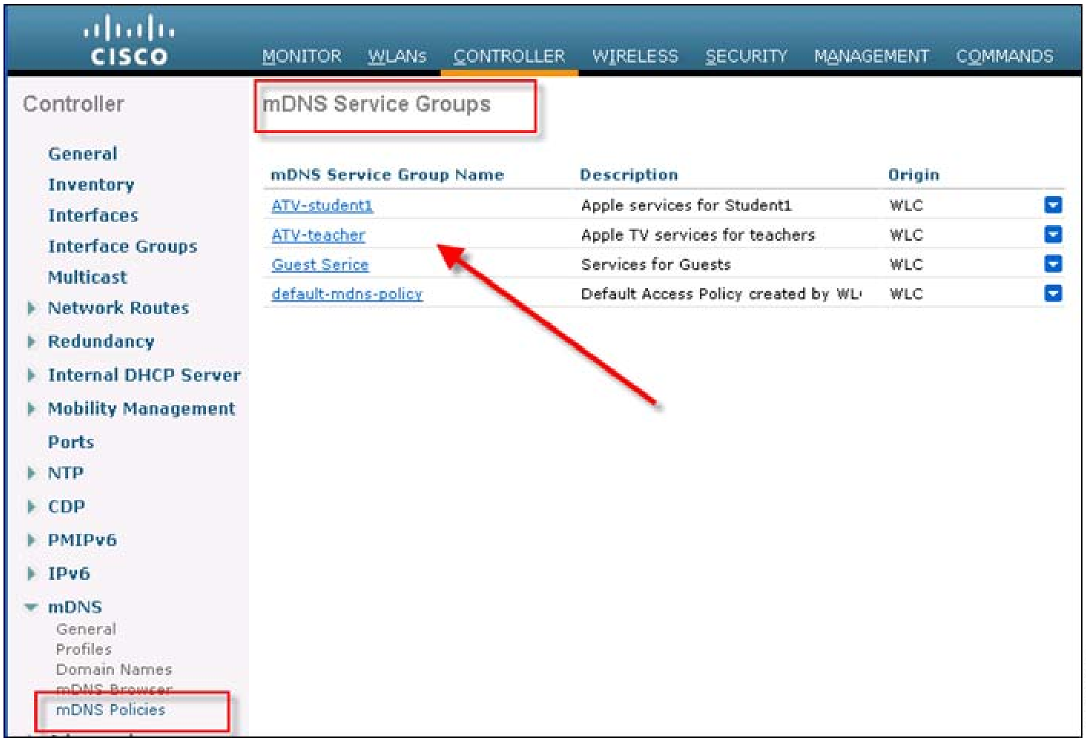
MAC ADDRESS	NAME	LOCATION-TYPE	LOCATION
00:1d:e0:08:18:b7	Reflector	AP Group	Any
10:40:f3:e5:d1:b6	Apple TV1	AP Group	Any
10:40:f3:ef:06:f9	Apple TV 2	AP Group	Any
b0:e8:92:58:75:a3	Printer	AP Group	Any

Policy/Rule (Policy is enforced if any of the below conditions is met)

Role Names teacher

User Names

The mDNS service groups are listed after being created.



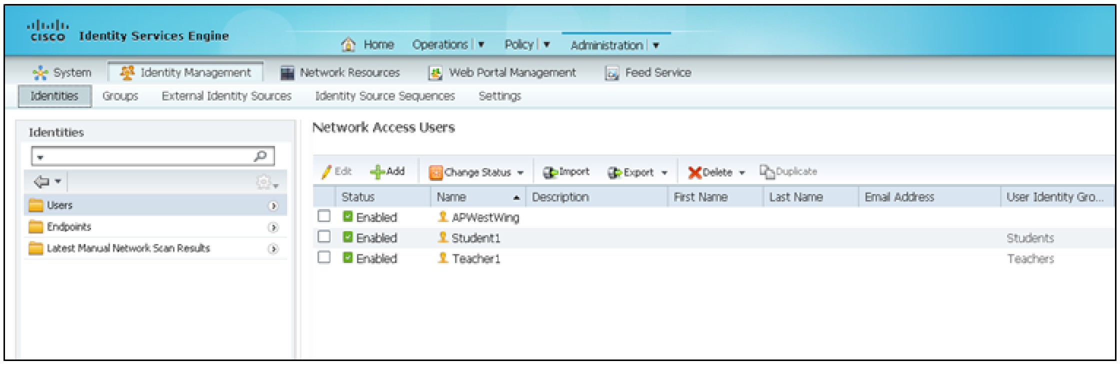
mDNS Service Groups

mDNS Service Group Name	Description	Origin
ATV-student1	Apple services for Student1	WLC
ATV-teacher	Apple TV services for teachers	WLC
Guest Serice	Services for Guests	WLC
default-mdns-policy	Default Access Policy created by WL	WLC

Note There is a default-mdns-policy group that contains all the service instances that are not configured in all other groups. Only the administrator has access to those instant services unless other users are added in the default mDNS policy.

Step 6 Configure the AAA server or ISE to allow users to be 802.1x authenticated and have the AAA server send the ROLE string back to the wireless controller.

As illustrated below, on ISE, configure users, that is, teacher1 and student1. and groups, that is, group teachers and students.

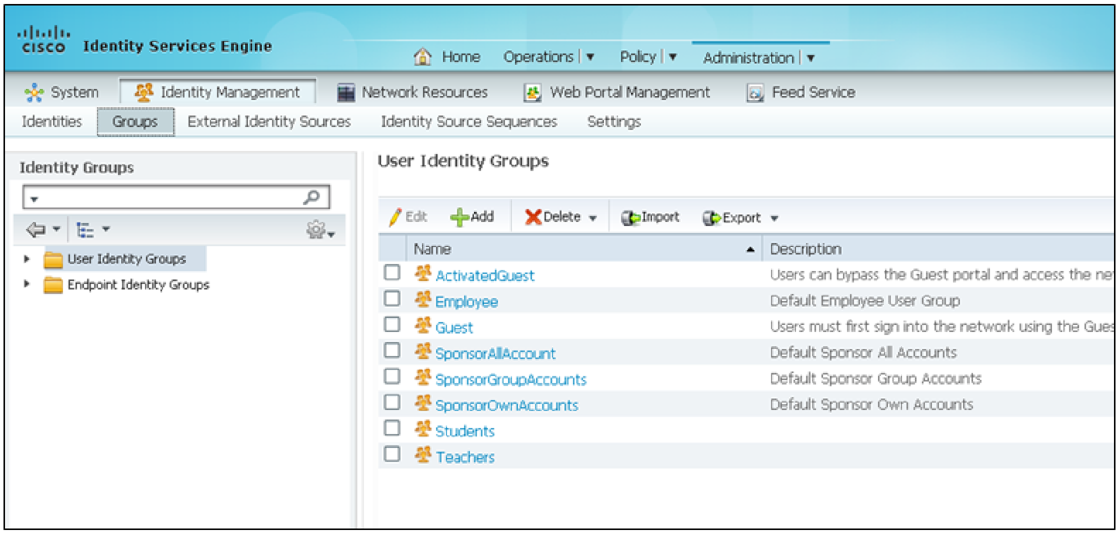


Network Access Users

	Status	Name	Description	First Name	Last Name	Email Address	User Identity Gro...
☐	Enabled	APWestWing					
☐	Enabled	Student1					Students
☐	Enabled	Teacher1					Teachers

353305

Also configure groups, that is, group teachers and students.

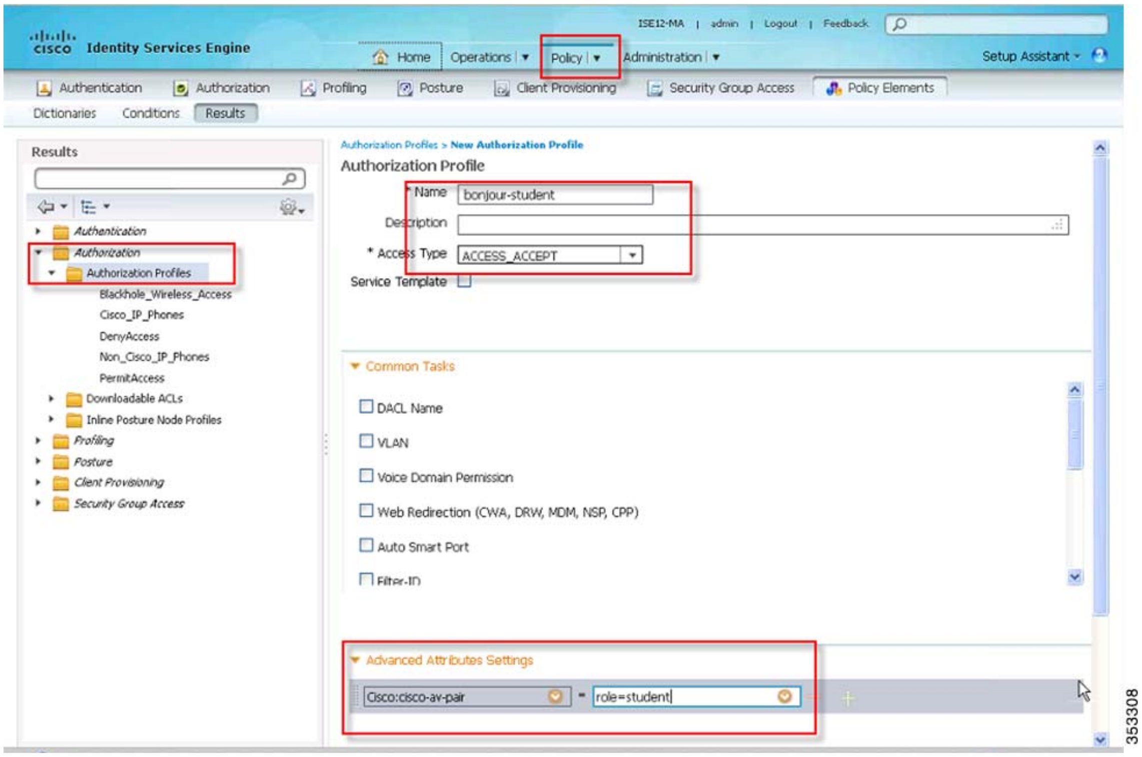


User Identity Groups

	Name	Description
☐	ActivatedGuest	Users can bypass the Guest portal and access the ne
☐	Employee	Default Employee User Group
☐	Guest	Users must first sign into the network using the Gues
☐	SponsorAllAccount	Default Sponsor All Accounts
☐	SponsorGroupAccounts	Default Sponsor Group Accounts
☐	SponsorOwnAccounts	Default Sponsor Own Accounts
☐	Students	
☐	Teachers	

353307

Step 7 Create an ISE policy for a specific group of users with a desired role, that is, student or teacher.



Authorization Profile

* Name: bonjour-student

Description:

* Access Type: ACCESS_ACCEPT

Service Template □

Common Tasks

□ DACL Name

□ VLAN

□ Voice Domain Permission

□ Web Redirection (CWA, DRW, MDM, NSP, CPP)

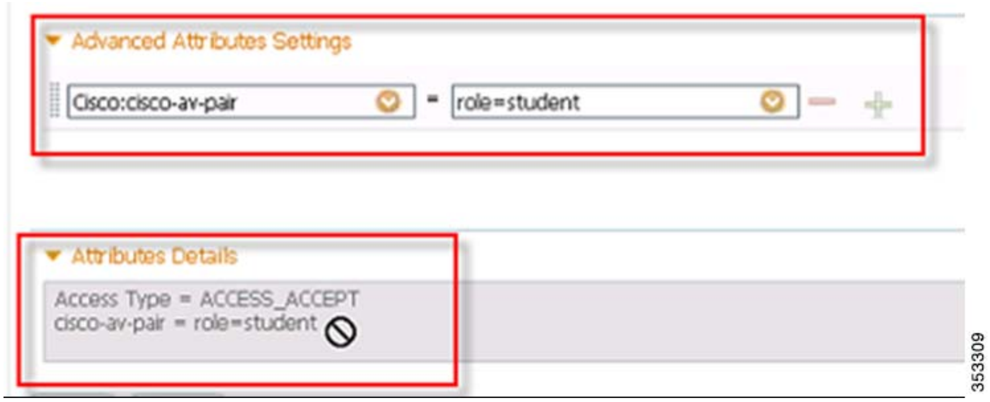
□ Auto Smart Port

□ Filter-ID

Advanced Attributes Settings

Cisco:cisco-av-pair = role=student

This creates a cisco-av-pair with a role attribute as student or teacher. Below is an illustration of the cisco-av-pair with a role attribute "student" that has been created.



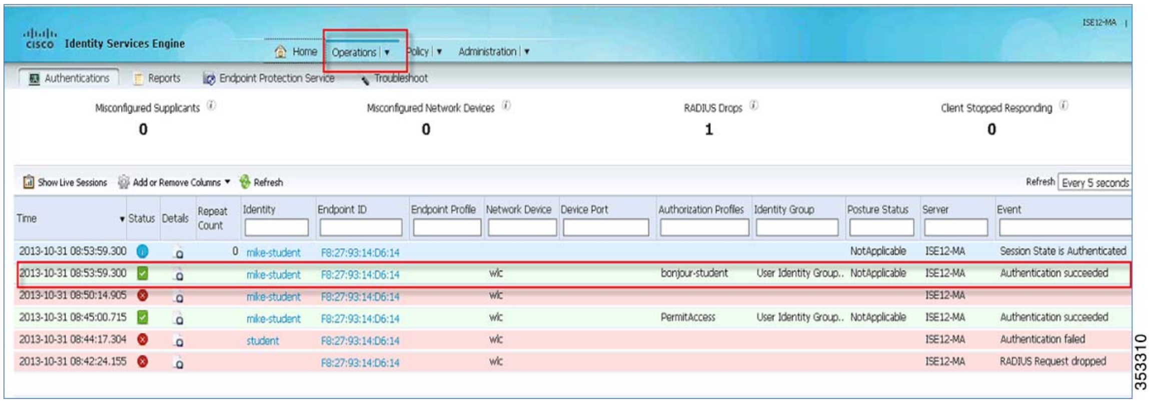
Advanced Attributes Settings

Cisco:cisco-av-pair = role=student

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = role=student

As a result, a user with "role = student" will be allowed to use service instances, that is, "bonjour-student" but other would not be able to access the service instances. Also, a user with "role = teacher" will be allowed to use service instances configured in the mDNS Service group with role = teacher or student.

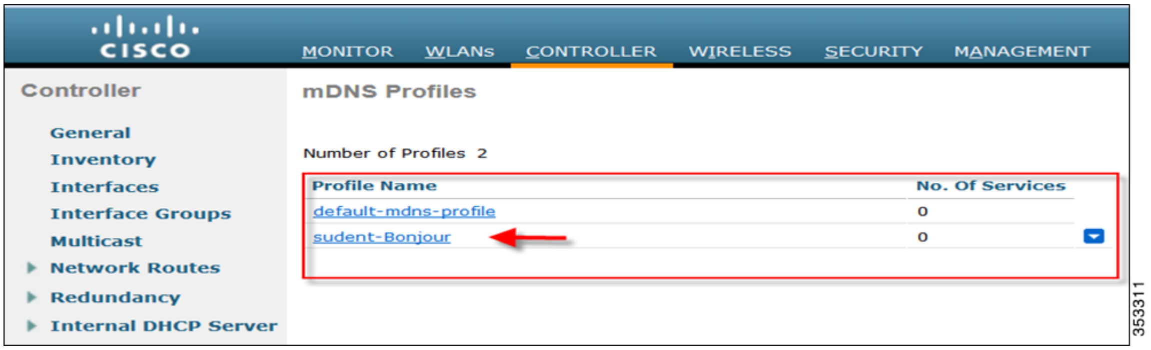


Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding
0	0	1	0

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Server	Event
2013-10-31 08:53:59.300	ⓘ		0	mike-student	F8:27:93:14:D6:14						NotApplicable	ISE12-MA	Session State is Authenticated
2013-10-31 08:53:59.300	✓			mike-student	F8:27:93:14:D6:14		wlc		bonjour-student	User Identity Group..	NotApplicable	ISE12-MA	Authentication succeeded
2013-10-31 08:50:14.905	✗			mike-student	F8:27:93:14:D6:14		wlc					ISE12-MA	
2013-10-31 08:45:00.715	✓			mike-student	F8:27:93:14:D6:14		wlc		PermitAccess	User Identity Group..	NotApplicable	ISE12-MA	Authentication succeeded
2013-10-31 08:44:17.304	✗			student	F8:27:93:14:D6:14		wlc					ISE12-MA	Authentication failed
2013-10-31 08:42:24.155	✗				F8:27:93:14:D6:14		wlc					ISE12-MA	RADIUS Request dropped

Step 8 The administrator can also create multiple mDNS profiles on the WLC and override them based on user authentication. The mDNS profile can be user specific and be overridden with AAA “av-pair=mDNS-profile-name” returned to WLC from AAA server that overrides default profile.

The following figure illustrates profile names that are configured on the wireless controller.

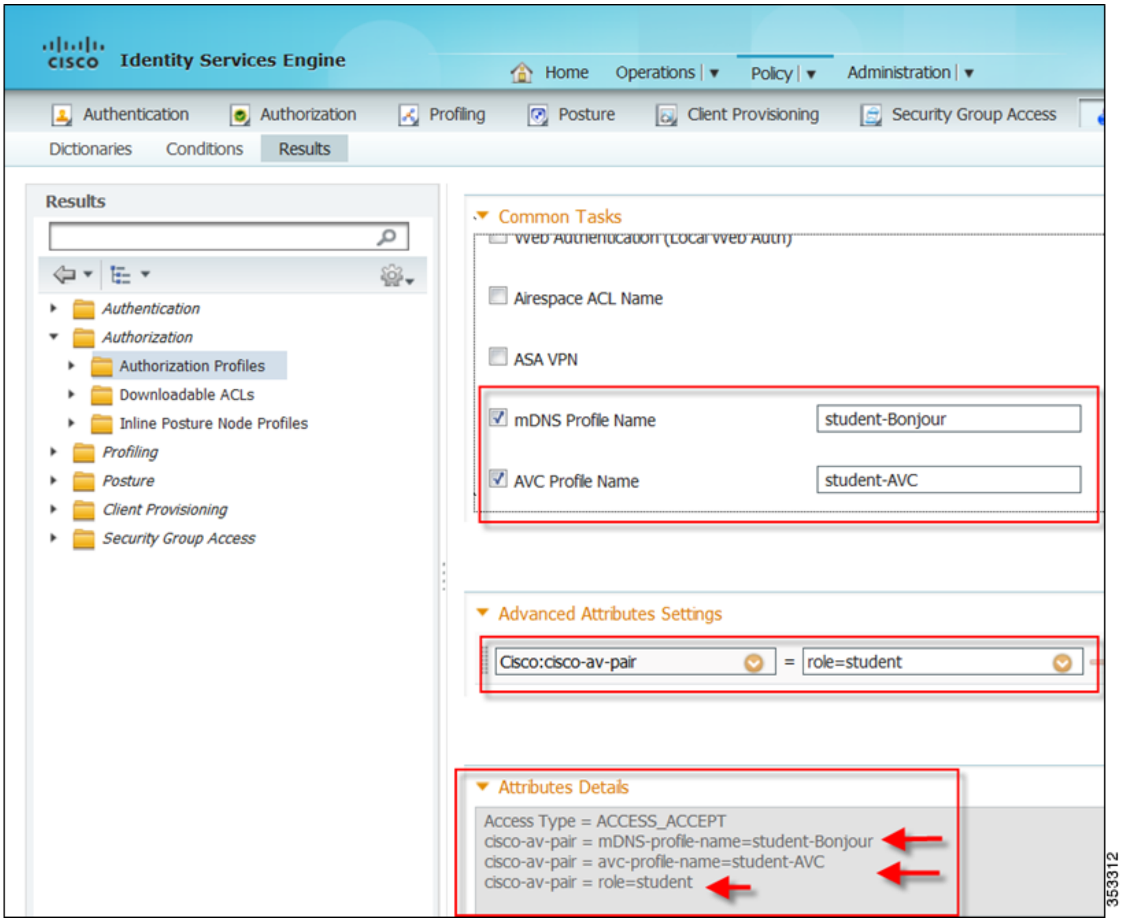


mDNS Profiles

Number of Profiles 2

Profile Name	No. Of Services
default-mdns-profile	0
sudent-Bonjour	0

The profile names can be overwritten with a profile based on a configuration for a specific user per their AAA credentials as illustrated below in the ISE configuration example.



Common Tasks

□ Web Authentication (Local Web Auth)

□ Airespace ACL Name

□ ASA VPN

☑ mDNS Profile Name: student-Bonjour

☑ AVC Profile Name: student-AVC

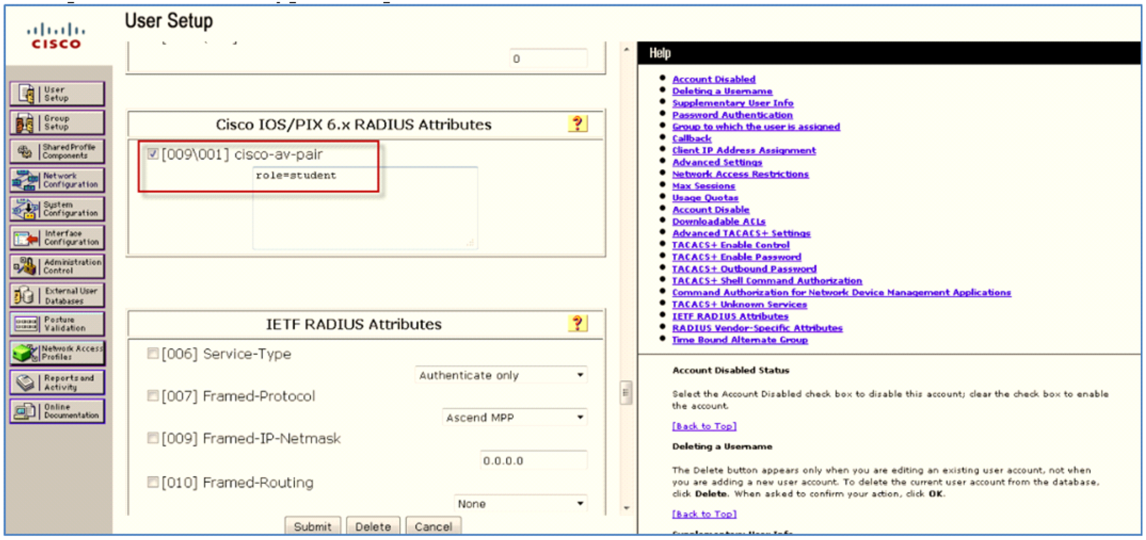
Advanced Attributes Settings

Cisco:cisco-av-pair = role=student

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = mDNS-profile-name=student-Bonjour
cisco-av-pair = avc-profile-name=student-AVC
cisco-av-pair = role=student
```

The figure below shows the ACS server configuration.



0

Cisco IOS/PIX 6.x RADIUS Attributes

☑ [009\001] cisco-av-pair

```
role=student
```

IETF RADIUS Attributes

□ [006] Service-Type: Authenticate only

□ [007] Framed-Protocol: Ascend MPP

□ [009] Framed-IP-Netmask: 0.0.0.0

□ [010] Framed-Routing: None

Help

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes
- Time Bound Alternate Group

Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[Back to Top]

Deleting a Username

The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click **Delete**. When asked to confirm your action, click **OK**.

[Back to Top]

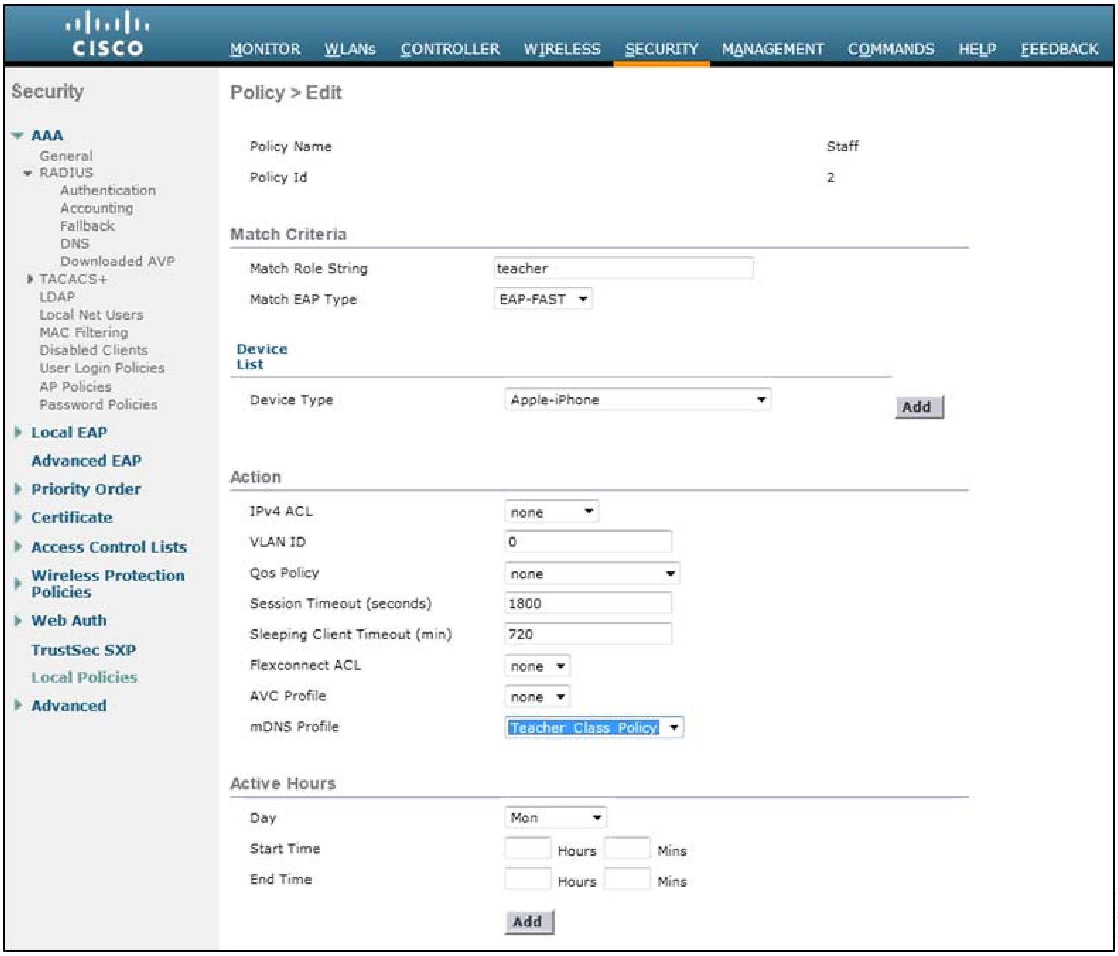
mDNS Profile Attached to Local Policies

Just like all clients associated with a WLAN pick the same Bonjour profile and allow the services configured for the profile, a Bonjour profile can be attached to a local policy for a client with a particular device type and ensure that each policy can be configured with a different mDNS profile name to restrict the policy from being able to use the services allowed by the profile. Eventually, the device gets access to the service instance based on the access policy tagged to the specific service instance. So there are two levels of filtering:

- Local policy just decides / controls if the service type is allowed or not.
- Bonjour access policy for the specific service instance will eventually decide if the client can use the service.

The administrator has an option to bind or enforce a specific profile to a local policy. Bonjour profile can be attached to a local policy for a client with a particular device type. This allows each local policy to be configured with a different mDNS profile name and to restrict the user from being able to use the services allowed by the profile.

In the example shown below – Local Policy limits the users with role "teacher" to using Service Group instances on the Apple iPhone devices.



Policy > Edit

Policy Name Staff

Policy Id 2

Match Criteria

Match Role String teacher

Match EAP Type EAP-FAST

Device List

Device Type Apple-iPhone Add

Action

IPv4 ACL none

VLAN ID 0

Qos Policy none

Session Timeout (seconds) 1800

Sleeping Client Timeout (min) 720

Flexconnect ACL none

AVC Profile none

mDNS Profile Teacher_Class_Policy

Active Hours

Day Mon

Start Time Hours Mins

End Time Hours Mins

Add

Use Cases for mDNS Bonjour Policies Deployments

In order to better understand the new Bonjour Policies introduced for the controller release 8.0 and their deployments, several use cases have been created to demonstrate deployment examples of the new policies implementation. The profiles can be created and applied to the WLAN, but all rules applied in the profile are applied to all users regardless of their roles or location. With introduction of policies, the administrator can configure different rules to be applied for the 802.11x authenticated users based on their Role, Name, Location or Device they are using.

For the purposes of the configuration, let us use the following examples of the Use Cases.

Table 4 Use Cases

Teacher, Student, and Guest same Service Set Identification (SSID) with WPA2/802.1x	Teacher authenticates and gets access to AirPrint, AirPlay TV1, and Apple TV2 any location.
	Student authenticates and gets access to only Apple TV1 in any location.
	Guest authenticates and gets no access to any Bonjour service.
Teacher, Student, and Guest same SSID with WPA2/802.1x	Teacher and another user by name authenticate and get access to Apple TV 1and TV2 and only if in the same room.
	Student authenticates and gets access to Apple TV2 only if in the same room as teacher.
	Guest authenticates and gets access to Air Print in any location.

USE Case #1 Deployment

Teacher, Student, and Guest on the same SSID with WPA2/802.1x.

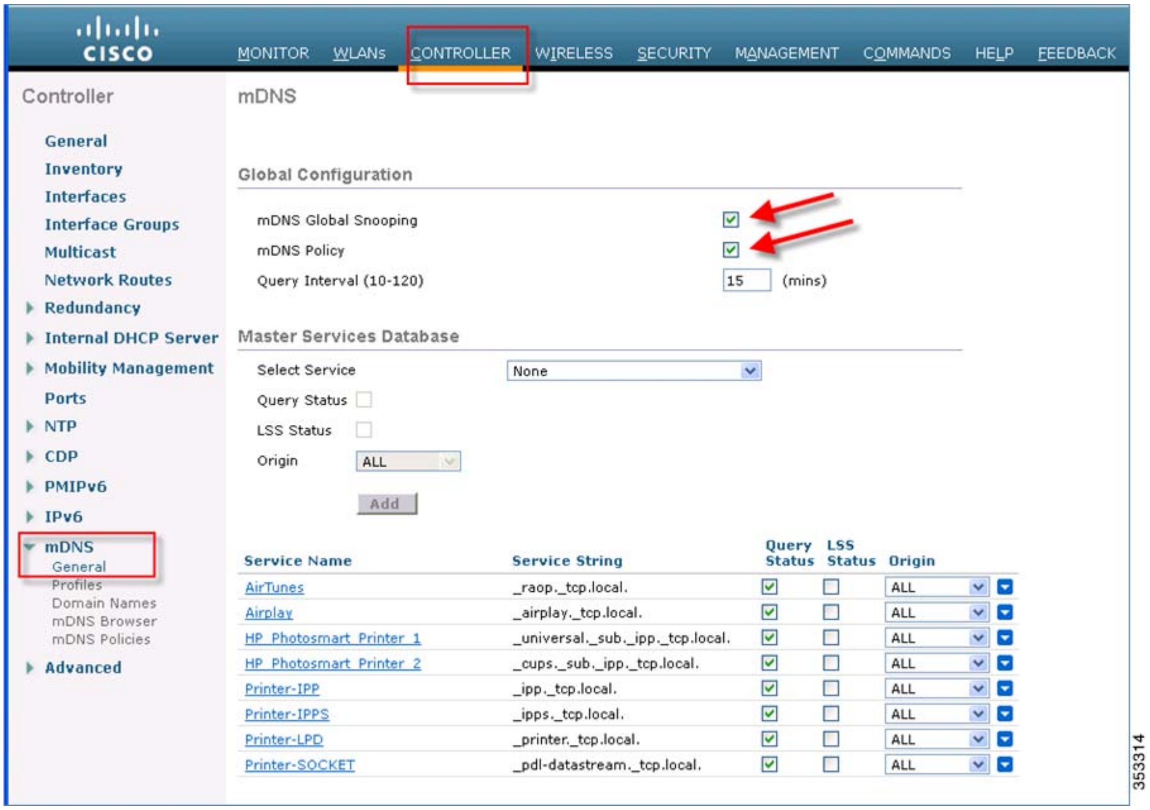
Table 5 Use Case #1

Teacher authenticates and gets access to AirPrint, AirPlay TV1 and Apple TV2 any location.
Student authenticates and gets access to only Apple TV1 in any location.
Guest authenticates and gets no access to any Bonjour service.

As mentioned in the Configuring mDNS Bonjour Policies section, do the following to deploy the use case:

Step 1 On the Controller tab, in the left pane, click **mDNS > General**.

Step 2 In the right pane, in the Global Configuration area, check the **mDNS Global Snooping** and **mDNS Policy** check boxes to enable the mDNS gateway services on the controller. This enables the Bonjour policies on the controller. Also, under services, ensure to enable desired Apple services for the controller to snoop.



mDNS

Global Configuration

mDNS Global Snooping	☑
mDNS Policy	☑
Query Interval (10-120)	15 (mins)

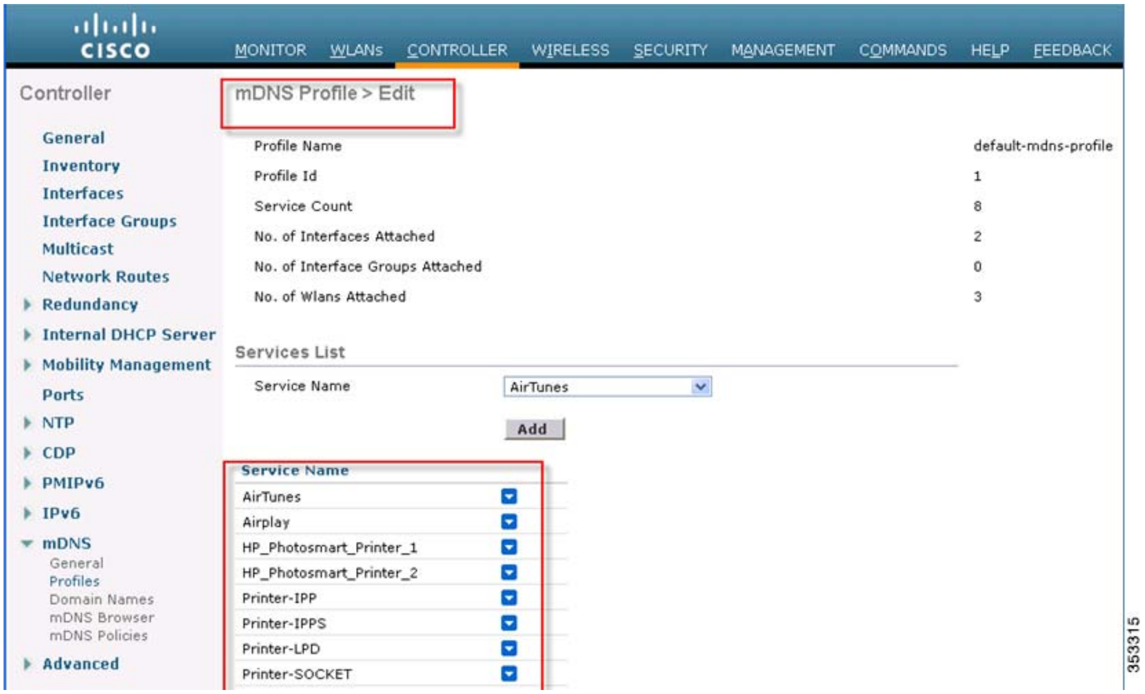
Master Services Database

Select Service	None
Query Status	☐
LSS Status	☐
Origin	ALL

Service Name	Service String	Query Status	LSS Status	Origin
AirTunes	_raop._tcp.local.	☑	☐	ALL
Airplay	_airplay._tcp.local.	☑	☐	ALL
HP_Photosmart_Printer_1	_universal._sub._ipp._tcp.local.	☑	☐	ALL
HP_Photosmart_Printer_2	_cups._sub._ipp._tcp.local.	☑	☐	ALL
Printer-IPP	_ipp._tcp.local.	☑	☐	ALL
Printer-IPPS	_ipps._tcp.local.	☑	☐	ALL
Printer-LPD	_printer._tcp.local.	☑	☐	ALL
Printer-SOCKET	_pdl-datastream._tcp.local.	☑	☐	ALL

Step 3 On the Controller tab, in the left pane, click **mDNS > Profiles**, and check that at least one mDNS profile is available.

Note The "default-mdns-profile" is configured with all main Apple services. As indicated in the earlier section, only one mDNS profile can be enabled per WLAN.



mDNS Profile > Edit

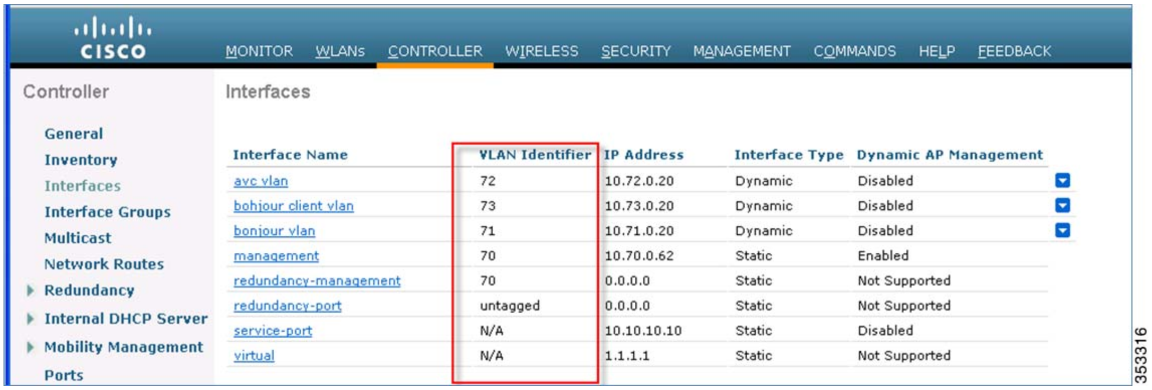
Profile Name	default-mdns-profile
Profile Id	1
Service Count	8
No. of Interfaces Attached	2
No. of Interface Groups Attached	0
No. of Wlans Attached	3

Services List

Service Name: AirTunes

Service Name
AirTunes
Airplay
HP_Photosmart_Printer_1
HP_Photosmart_Printer_2
Printer-IPP
Printer-IPPS
Printer-LPD
Printer-SOCKET

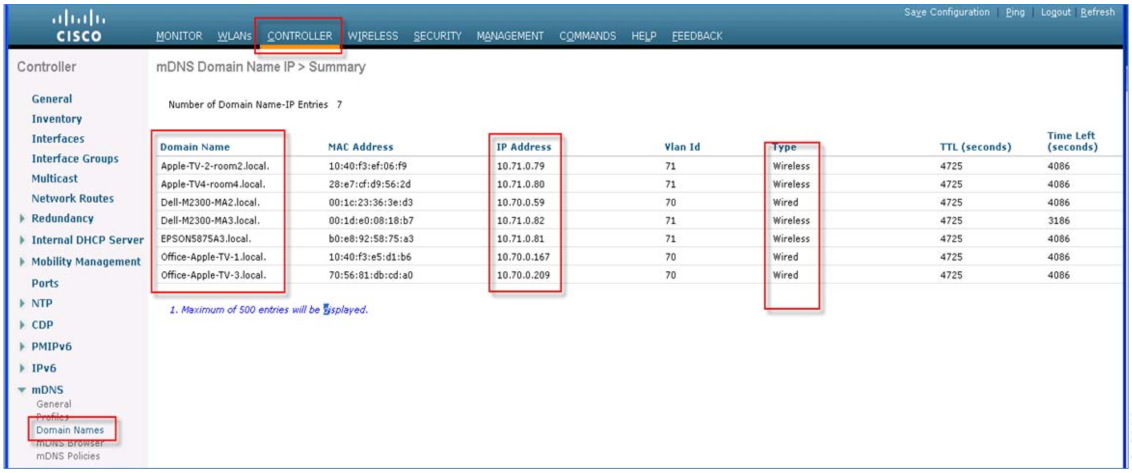
Step 4 On the Controller tab, in the left pane, click **Interfaces,** create dynamic interfaces, and map services to those interfaces or VLANs. Ensure that you have Apple services on the interface other than management.



Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
avc vlan	72	10.72.0.20	Dynamic	Disabled
bohjour client vlan	73	10.73.0.20	Dynamic	Disabled
bonjour vlan	71	10.71.0.20	Dynamic	Disabled
management	70	10.70.0.62	Static	Enabled
redundancy-management	70	0.0.0.0	Static	Not Supported
redundancy-port	untagged	0.0.0.0	Static	Not Supported
service-port	N/A	10.10.10.10	Static	Disabled
virtual	N/A	1.1.1.1	Static	Not Supported

Step 5 After connecting Bonjour services such as Apple TV, Printers, and Reflector services, check that all the services are listed in the **Domain Names** area on the **Controller** tab.



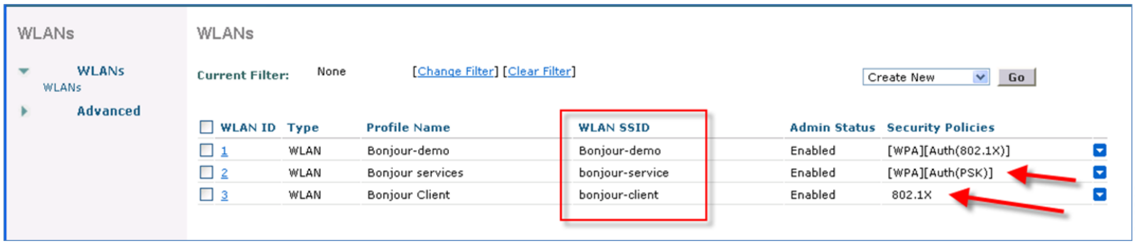
mDNS Domain Name IP > Summary

Number of Domain Name-IP Entries 7

Domain Name	MAC Address	IP Address	Vlan Id	Type	TTL (seconds)	Time Left (seconds)
Apple-TV-2-room2.local.	10:40:f3:ef:06:f9	10.71.0.79	71	Wireless	4725	4086
Apple-TV4-room4.local.	28:e7:cf:d9:56:2d	10.71.0.80	71	Wireless	4725	4086
Dell-M2300-MA2.local.	00:1c:23:36:3e:d3	10.70.0.59	70	Wired	4725	4086
Dell-M2300-MA3.local.	00:1d:e0:08:18:b7	10.71.0.82	71	Wireless	4725	3186
EPSON5875A3.local.	b0:e8:92:58:75:a3	10.71.0.81	71	Wireless	4725	4086
Office-Apple-TV-1.local.	10:40:f3:e5:d1:b6	10.70.0.167	70	Wired	4725	4086
Office-Apple-TV-3.local.	70:56:81:db:cd:a0	10.70.0.209	70	Wired	4725	4086

1. Maximum of 500 entries will be displayed.

Step 6 Configure WLAN for services with WPA / PSK and also another WLAN for clients with 802.1x, activate the AAA server or ISE.

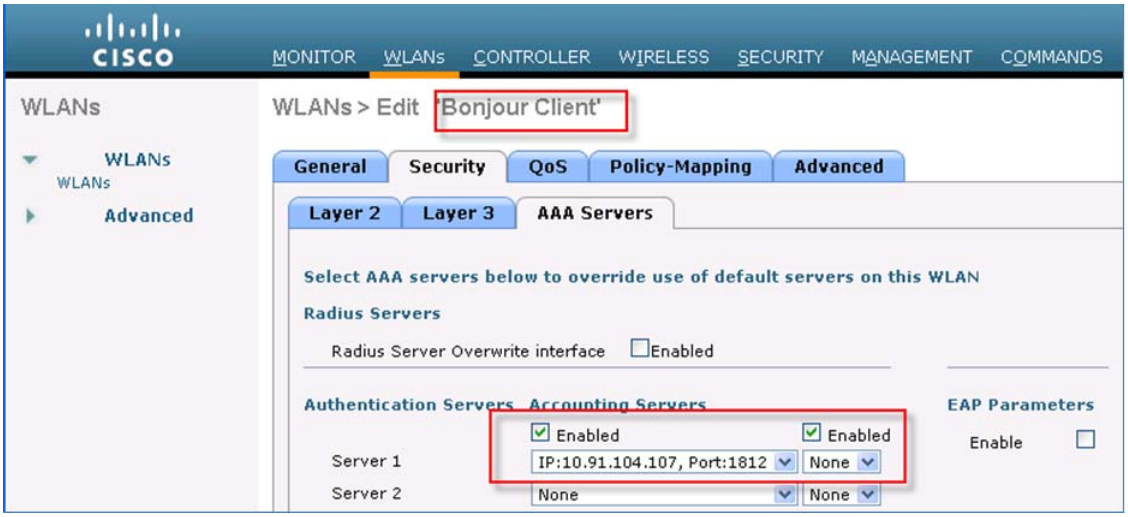


WLANs

Current Filter: None

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	Bonjour-demo	Bonjour-demo	Enabled	[WPA][Auth(802.1X)]
2	WLAN	Bonjour services	bonjour-service	Enabled	[WPA][Auth(PSK)]
3	WLAN	Bonjour Client	bonjour-client	Enabled	802.1X

Step 7 Enable the AAA server.



WLANs > Edit 'Bonjour Client'

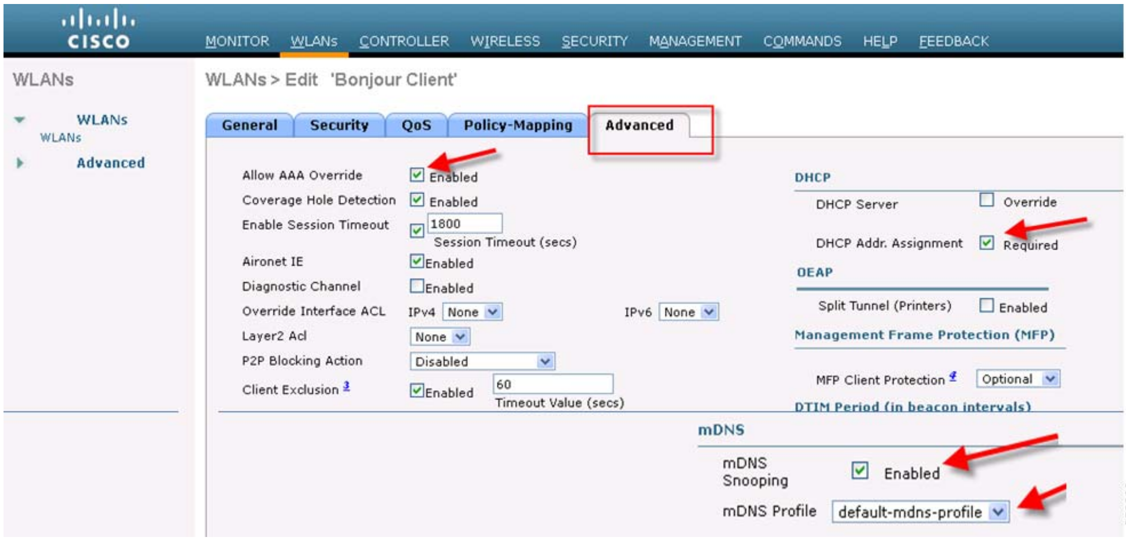
Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overwrite interface □Enabled

	Authentication Servers	Accounting Servers	EAP Parameters
	☑ Enabled	☑ Enabled	Enable □
Server 1	IP:10.91.104.107, Port:1812	None	
Server 2	None	None	

Step 8 Enable mDNS snooping on the WLAN and bind it to an mDNS profile.


cisco
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
General Security QoS Policy-Mapping Advanced
353320

WLANs > Edit 'Bonjour Client'

Allow AAA Override ☑ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel □ Enabled
Override Interface ACL IPv4 None IPv6 None
Layer2 Acl None
P2P Blocking Action Disabled
Client Exclusion [3] ☑ Enabled 60 Timeout Value (secs)

DHCP
DHCP Server □ Override
DHCP Addr. Assignment ☑ Required

OEAP
Split Tunnel (Printers) □ Enabled

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

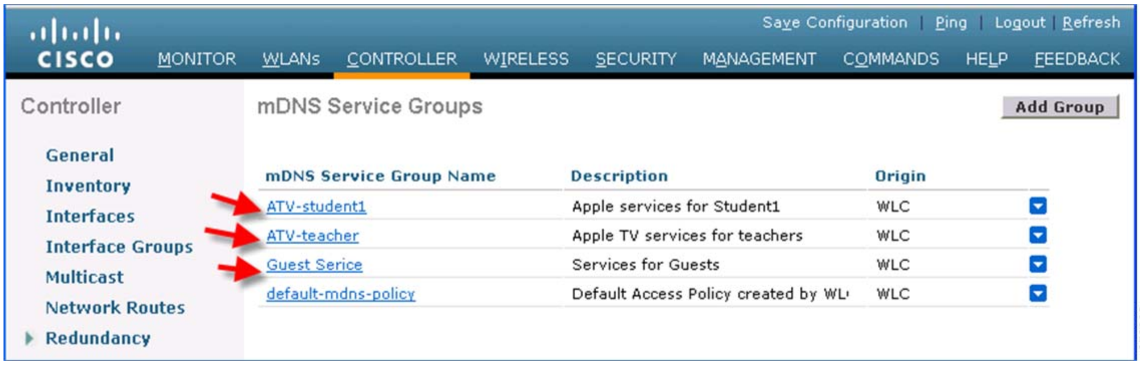
DTIM Period (in beacon intervals)

mDNS
mDNS Snooping ☑ Enabled
mDNS Profile default-mdns-profile

Step 9 After general configurations for the mDNS are complete, configure Bonjour policy so that the following occurs upon users authentication:

1. Teacher authenticates and gets access to Reflector, Apple TV1, and Apple TV2 in any location.
2. Student authenticates and gets access to only Apple TV1 in any location.
3. Guest authenticates and gets no access to any Bonjour service.

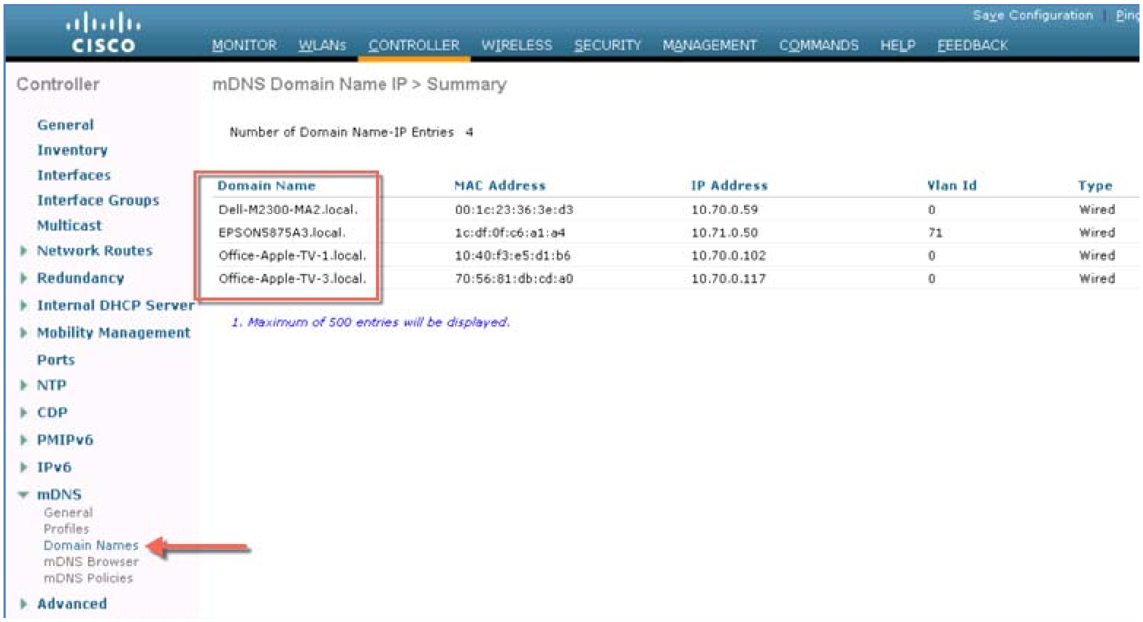
Step 10 Create mDNS service groups under **Controller > mDNS Policies**.


Save Configuration | Ping | Logout | Refresh
cisco
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Controller
General
Inventory
Interfaces
Interface Groups
Multicast
Network Routes
Redundancy
Add Group
353323

mDNS Service Groups

mDNS Service Group Name	Description	Origin
ATV-student1	Apple services for Student1	WLC
ATV-teacher	Apple TV services for teachers	WLC
Guest Serice	Services for Guests	WLC
default-mdns-policy	Default Access Policy created by WL	WLC

Step 11 Create Bonjour policy for teachers as required in the case study. To add service instances to the list, use the Domain Names area to obtain MAC addresses for each specific service.

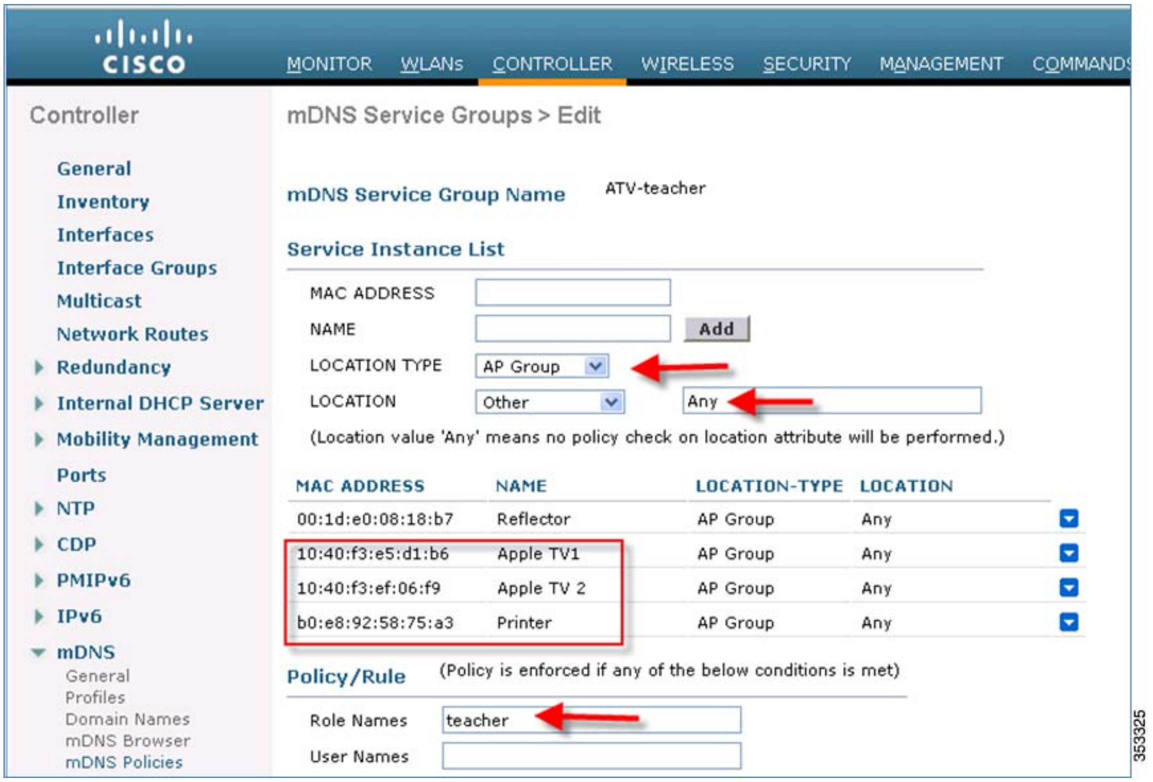


mDNS Domain Name IP > Summary

Number of Domain Name-IP Entries 4

Domain Name	MAC Address	IP Address	Vlan Id	Type
Dell-M2300-MA2.local.	00:1c:23:36:3e:d3	10.70.0.59	0	Wired
EPSON5875A3.local.	1c:df:0f:c6:a1:a4	10.71.0.50	71	Wired
Office-Apple-TV-1.local.	10:40:f3:e5:d1:b6	10.70.0.102	0	Wired
Office-Apple-TV-3.local.	70:56:81:db:cd:a0	10.70.0.117	0	Wired

1. Maximum of 500 entries will be displayed.



mDNS Service Groups > Edit

mDNS Service Group Name ATV-teacher

Service Instance List

MAC ADDRESS

NAME

LOCATION TYPE AP Group

LOCATION Other Any

(Location value 'Any' means no policy check on location attribute will be performed.)

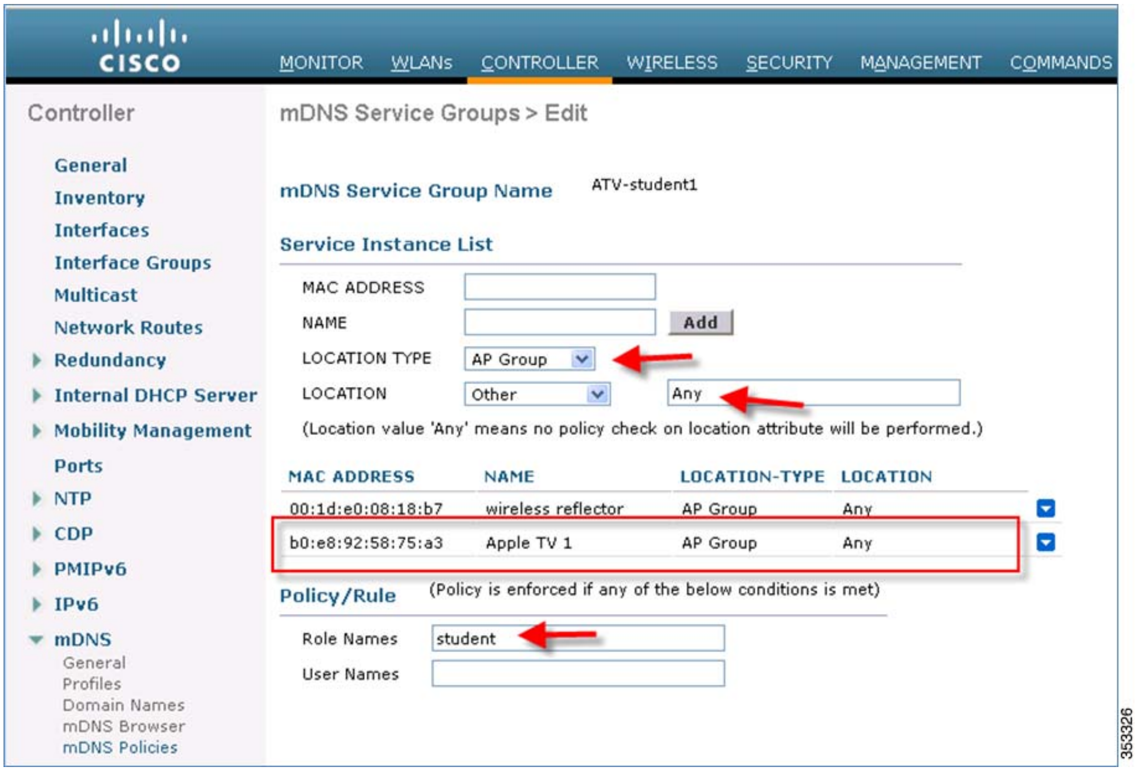
MAC ADDRESS	NAME	LOCATION-TYPE	LOCATION
00:1d:e0:08:18:b7	Reflector	AP Group	Any
10:40:f3:e5:d1:b6	Apple TV1	AP Group	Any
10:40:f3:ef:06:f9	Apple TV 2	AP Group	Any
b0:e8:92:58:75:a3	Printer	AP Group	Any

Policy/Rule (Policy is enforced if any of the below conditions is met)

Role Names teacher

User Names

Step 12 Create Bonjour policy for students as required in the case study #1.



mDNS Service Groups > Edit

mDNS Service Group Name ATV-student1

Service Instance List

MAC ADDRESS

NAME

LOCATION TYPE AP Group

LOCATION Other Any

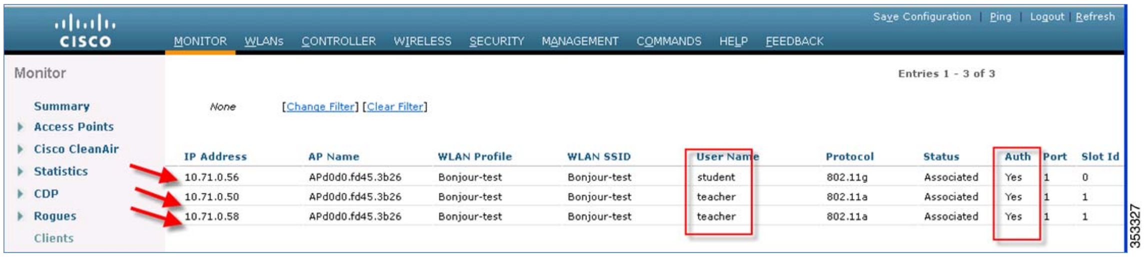
(Location value 'Any' means no policy check on location attribute will be performed.)

MAC ADDRESS	NAME	LOCATION-TYPE	LOCATION
00:1d:e0:08:18:b7	wireless reflector	AP Group	Any
b0:e8:92:58:75:a3	Apple TV 1	AP Group	Any

Policy/Rule (Policy is enforced if any of the below conditions is met)

Role Names student

User Names



Entries 1 - 3 of 3

None [Change Filter] [Clear Filter]

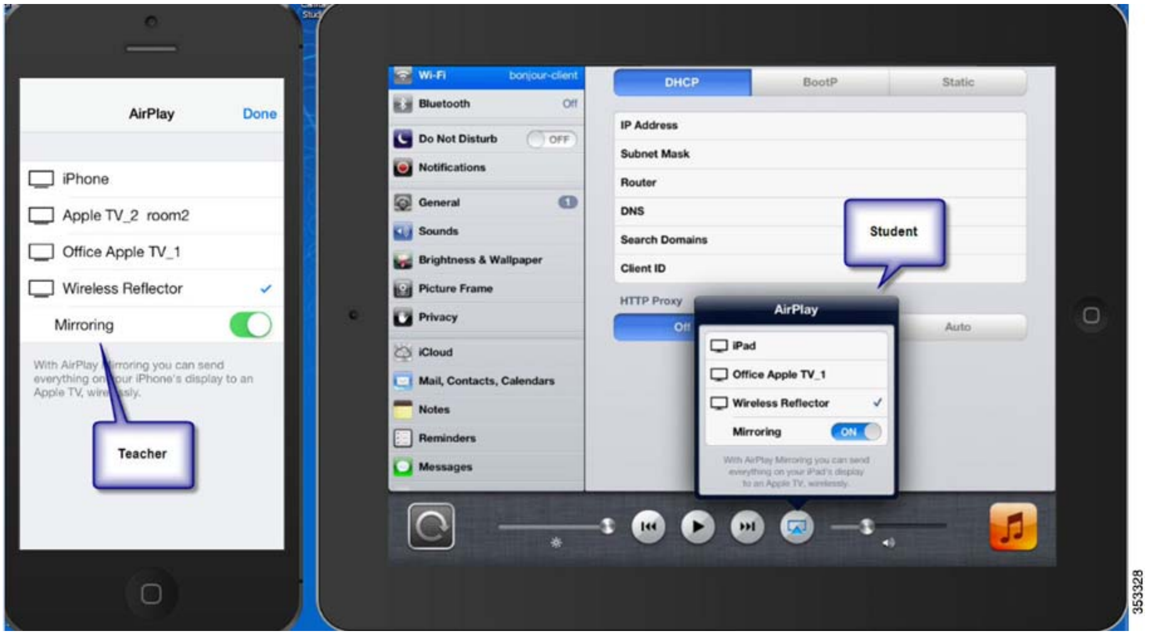
IP Address	AP Name	WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth	Port	Slot Id
10.71.0.56	APd0d0.fd45.3b26	Bonjour-test	Bonjour-test	student	802.11g	Associated	Yes	1	0
10.71.0.50	APd0d0.fd45.3b26	Bonjour-test	Bonjour-test	teacher	802.11a	Associated	Yes	1	1
10.71.0.58	APd0d0.fd45.3b26	Bonjour-test	Bonjour-test	teacher	802.11a	Associated	Yes	1	1

Summary

As shown in this use case, the teacher will have access to Apple TV 1, Apple TV 2, and Printer.

Student, based on the policy designed, will have only access to the Apple TV1.

Guest User will not have access to any services on this WLAN.



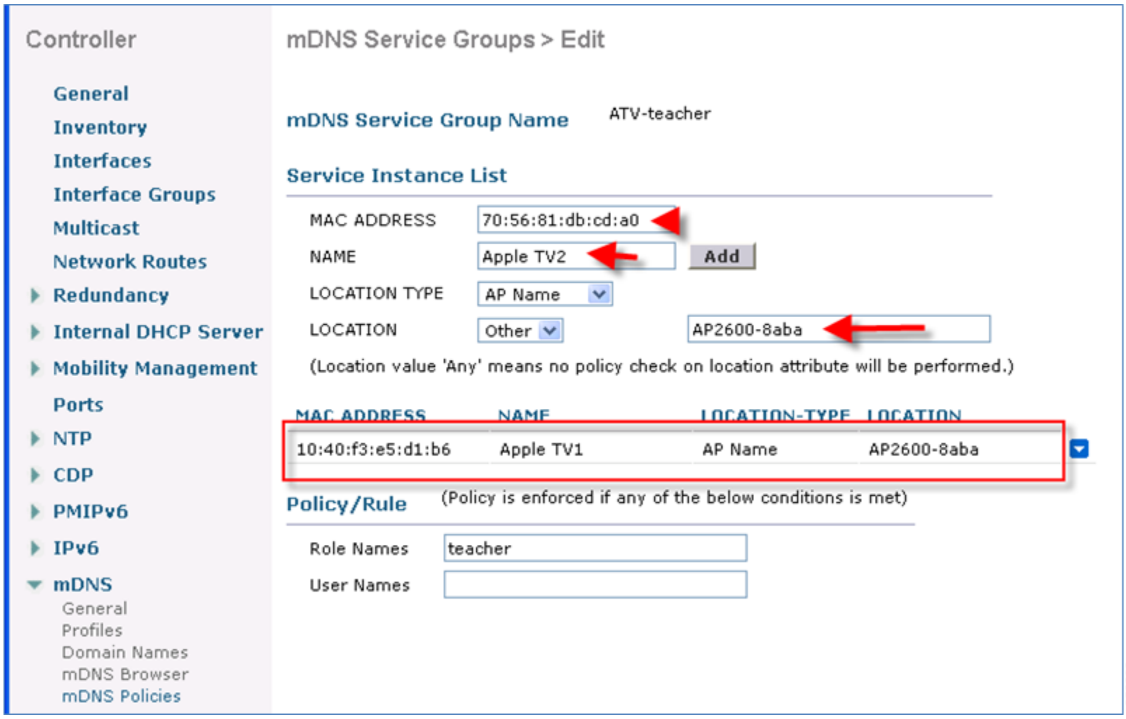
Use Case #2 Deployment

Table 6 Use case #2

Teacher and Another User by name authenticate and get access to Apple TV 1 and TV2 and only if in the same room.
Student authenticates and gets access to Apple TV2 only if in the same room as teacher.
Guest authenticates and gets access to Air Print in any location.

To configure the policy, perform the following steps:

Step 1 Configure a policy for the teacher to be able to access Apple TV1 and Apple TV2 only in one location next to one specific AP. In this case, the AP name is AP2600-8aba.



mDNS Service Groups > Edit

mDNS Service Group Name ATV-teacher

Service Instance List

MAC ADDRESS 70:56:81:db:cd:a0

NAME Apple TV2

LOCATION TYPE AP Name

LOCATION Other AP2600-8aba

(Location value 'Any' means no policy check on location attribute will be performed.)

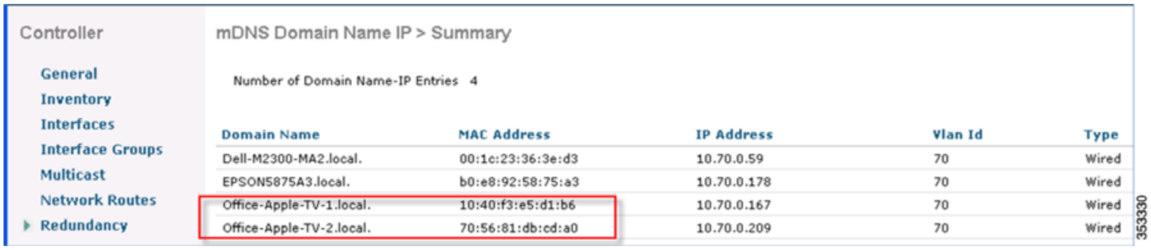
MAC ADDRESS	NAME	LOCATION-TYPE	LOCATION
10:40:f3:e5:d1:b6	Apple TV1	AP Name	AP2600-8aba

Policy/Rule (Policy is enforced if any of the below conditions is met)

Role Names teacher

User Names

Step 2 Choose the MAC addresses of both Apple TVs from the domain name summary, and manually enter them as shown in the figure above.

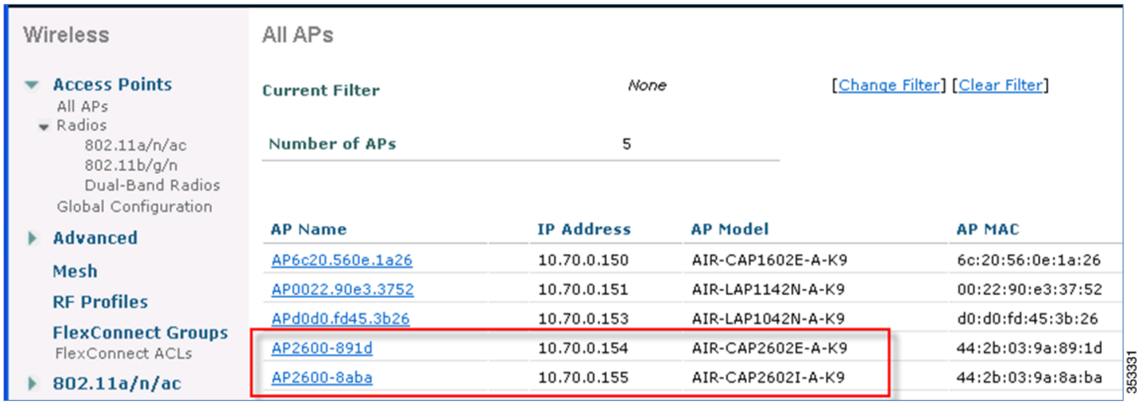


mDNS Domain Name IP > Summary

Number of Domain Name-IP Entries 4

Domain Name	MAC Address	IP Address	Vlan Id	Type
Dell-M2300-MA2.local.	00:1c:23:36:3e:d3	10.70.0.59	70	Wired
EPSON5875A3.local.	b0:e8:92:58:75:a3	10.70.0.178	70	Wired
Office-Apple-TV-1.local.	10:40:f3:e5:d1:b6	10.70.0.167	70	Wired
Office-Apple-TV-2.local.	70:56:81:db:cd:a0	10.70.0.209	70	Wired

Step 3 Also choose APs, that is AP names, from the list of the APs in the desired location. Only wireless clients connected to these selected APs will have access to the desired Apple TV services.



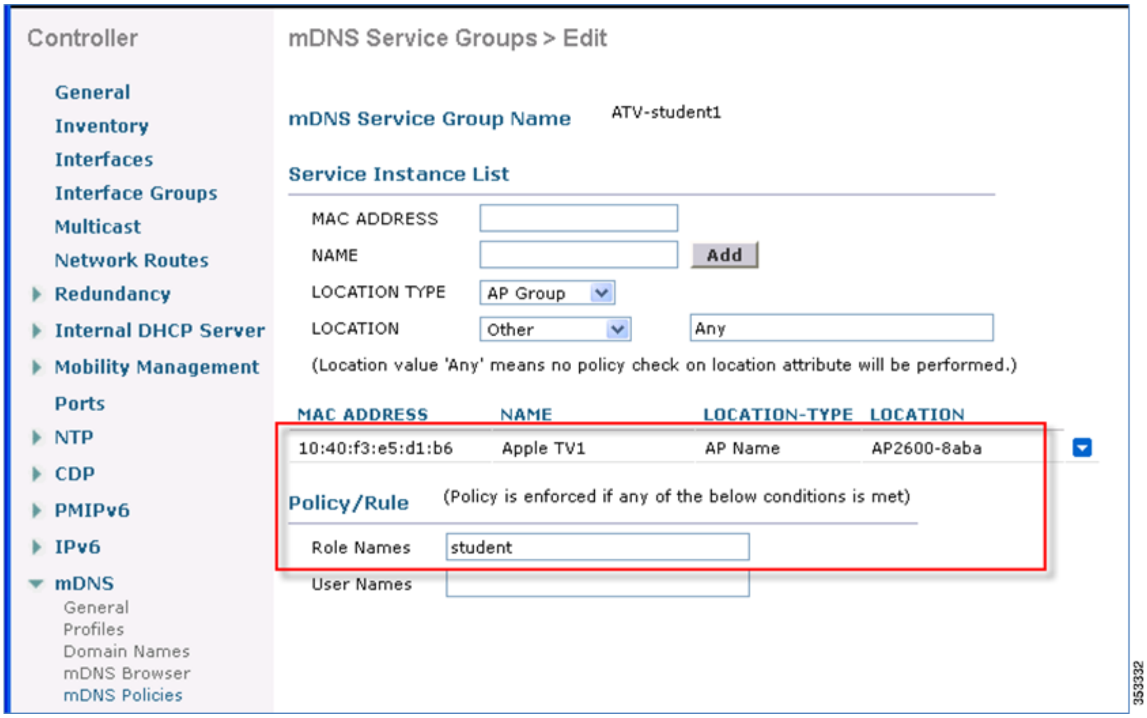
All APs

Current Filter None

Number of APs 5

AP Name	IP Address	AP Model	AP MAC
AP6c20.560e.1a26	10.70.0.150	AIR-CAP1602E-A-K9	6c:20:56:0e:1a:26
AP0022.90e3.3752	10.70.0.151	AIR-LAP1142N-A-K9	00:22:90:e3:37:52
APd0d0.fd45.3b26	10.70.0.153	AIR-LAP1042N-A-K9	d0:d0:fd:45:3b:26
AP2600-891d	10.70.0.154	AIR-CAP2602E-A-K9	44:2b:03:9a:89:1d
AP2600-8aba	10.70.0.155	AIR-CAP2602I-A-K9	44:2b:03:9a:8a:ba

Once the configurations of the two policies for this use case are completed, they will look as in the figures below.



mDNS Service Groups > Edit

mDNS Service Group Name ATV-student1

Service Instance List

MAC ADDRESS

NAME

LOCATION TYPE AP Group

LOCATION Other Any

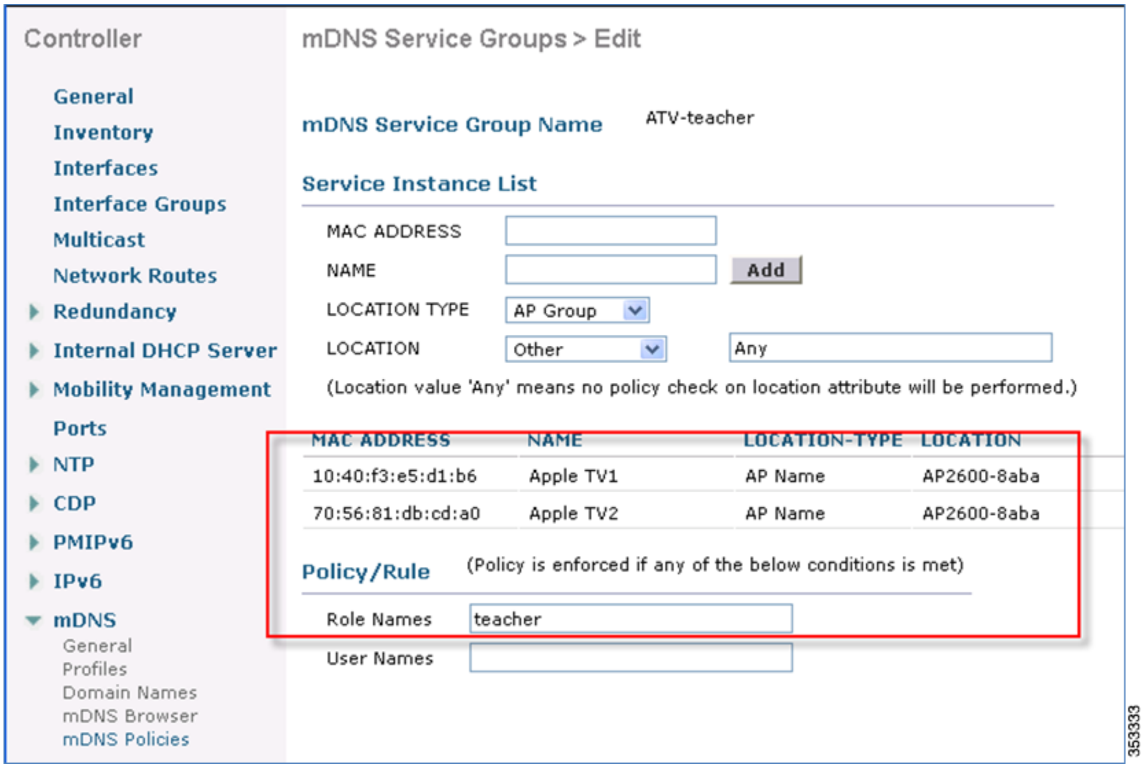
(Location value 'Any' means no policy check on location attribute will be performed.)

MAC ADDRESS	NAME	LOCATION-TYPE	LOCATION
10:40:f3:e5:d1:b6	Apple TV1	AP Name	AP2600-8aba

Policy/Rule (Policy is enforced if any of the below conditions is met)

Role Names student

User Names



mDNS Service Groups > Edit

mDNS Service Group Name ATV-teacher

Service Instance List

MAC ADDRESS

NAME

LOCATION TYPE AP Group

LOCATION Other Any

(Location value 'Any' means no policy check on location attribute will be performed.)

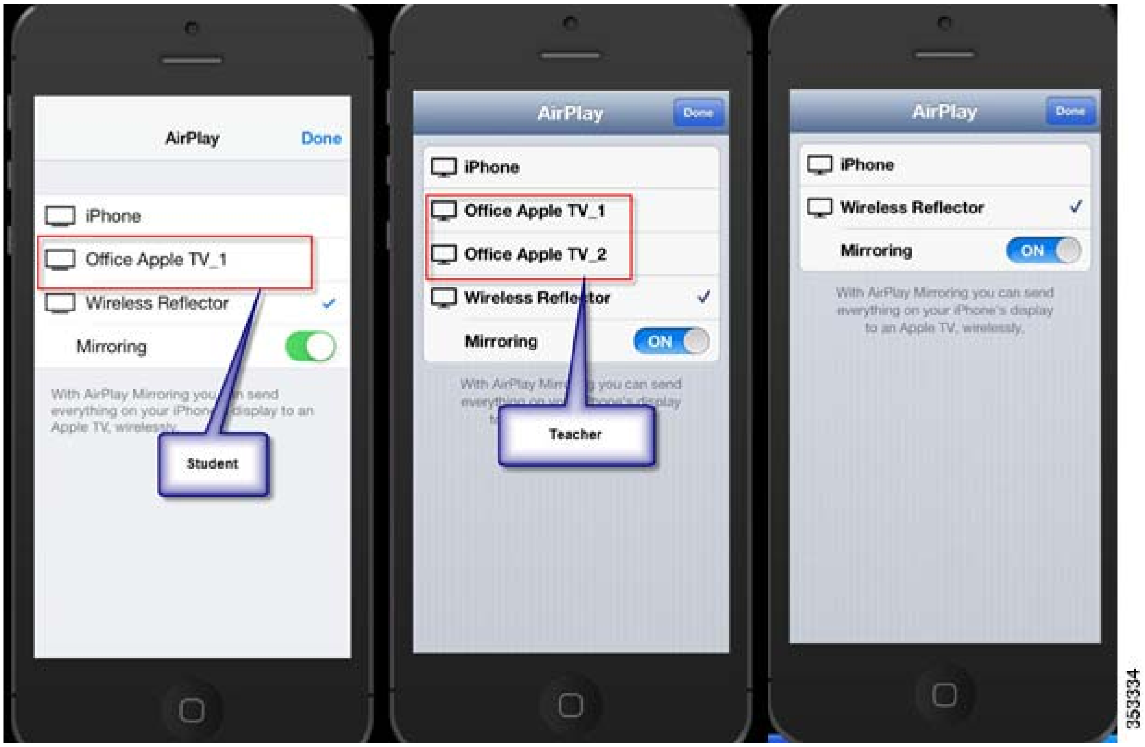
MAC ADDRESS	NAME	LOCATION-TYPE	LOCATION
10:40:f3:e5:d1:b6	Apple TV1	AP Name	AP2600-8aba
70:56:81:db:cd:a0	Apple TV2	AP Name	AP2600-8aba

Policy/Rule (Policy is enforced if any of the below conditions is met)

Role Names teacher

User Names

When the teachers login and only attached to the AP2600, they will see the services available to them in that specific location only. The below services also show Reflector service – it was done just for the purpose of taking screenshots. Last example is for the Guest user.



With AirPlay Mirroring you can send everything on your iPhone's display to an Apple TV, wirelessly.

Summary

As shown in this use case, the teacher has access to Apple TV 1 and Apple TV 2 in specific location. Student, based on the policy designed, has access to only Apple TV2 in specific location. Guest User does not have access to any services on this WLAN.

Debugging Bonjour

Following are the commands to debug Bonjour:

- debug mdns error enable
- debug mdns message enable
- debug mdns detail enable
- debug mdns all enable

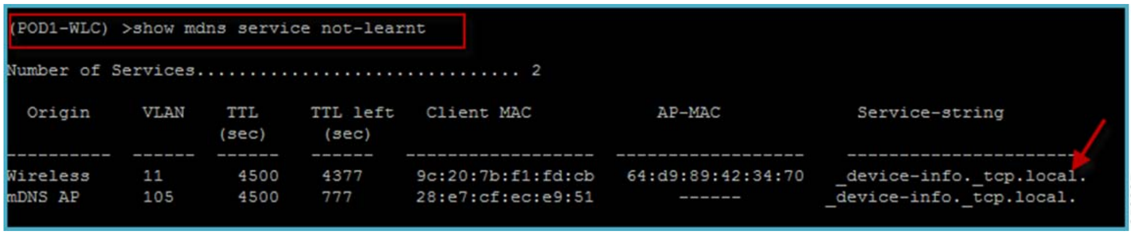
The above debugs are enhanced for the new features also.

Bonjour browser and "show mdns service not-learnt" could be used as a debug tool as well.

Bonjour browser

- Bonjour browser is a cache of all the service advertisements seen at the WLC and not discovered because configuration did not allow learning.
- Service advertisements across all VLANs and ORIGIN types that are not learnt are displayed.
- Bonjour browser is a cache of top 500 entries.

- The user can add services by picking them from the Bonjour browser instead of typing the string.



```
(POD1-WLC) >show mdns service not-learnt

Number of Services.............................. 2

  Origin     VLAN    TTL     TTL left   Client MAC           AP-MAC             Service-string
                    (sec)     (sec)
----------  ------  ------  ------   ------------------  ------------------   ----------------------
Wireless     11       4500    4377     9c:20:7b:f1:fd:cb   64:d9:89:42:34:70   _device-info._tcp.local.
mDNS AP      105      4500    777      28:e7:cf:ec:e9:51        ------        _device-info._tcp.local.
```

Bonjour SSO

Any mDNS configuration performed on the Active WLC will be synced up on the standby WLC besides the mDNS AP configuration. For mDNS AP, no sync up is needed on standby as the AP configuration information is always stored on AP.

Show Commands on WLC

- WLC > show mdns profile summary
- WLC > show mdns profile detail <profile-name>
- WLC > show mdns service summary
- WLC > show mdns service detail <service-name>
- WLC > show mdns domain-name-ip summary
- WLC > Show interface detail <interface-name>
- WLC > Show interface group detail <interface-group-name>
- WLC > Show wlan <wlan-id>
- WLC > Show client detail <mac-address>
- WLC > Show network summary

Clear commands

To clear the mDNS database learned dynamically per service.

WLC > clear mdns service-database <service-name / all>

Show commands on AP CLI

AP3600#show capwap mcast mdns