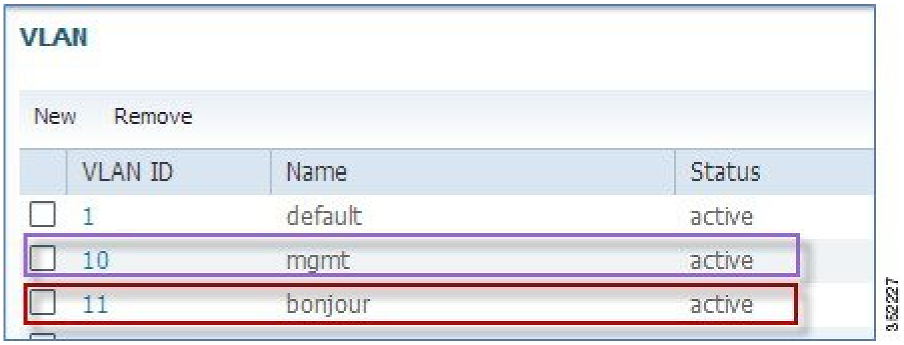
Configuration

The following topics are covered under this chapter:

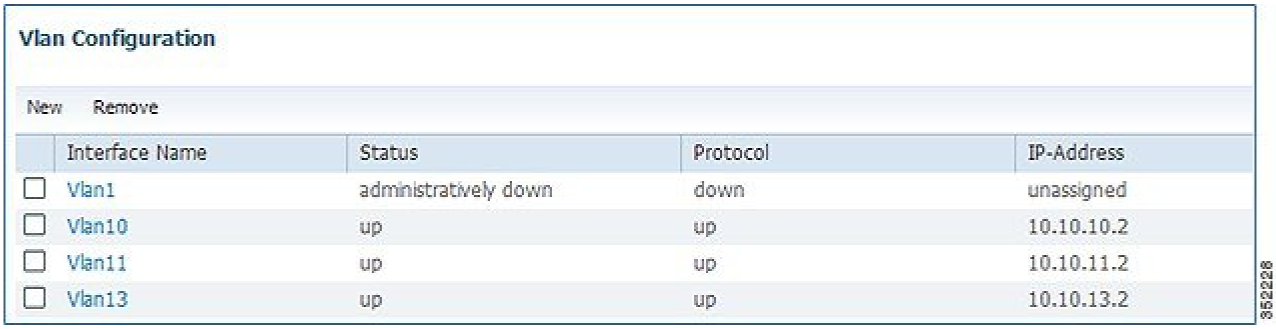
Initial Configuration for Service Discovery Gateway (SDG)

To configure and demonstrate the Service Discovery gateway/mDNS feature on WLC, users can create a VLAN interface for Bonjour Services on a separate VLAN than the Client VLAN.

Here is an example showing different interfaces and VLANs for Clients (VLAN10) and AppleTV (VLAN11):



	VLAN ID	Name	Status
□	1	default	active
□	10	mgmt	active
□	11	bonjour	active

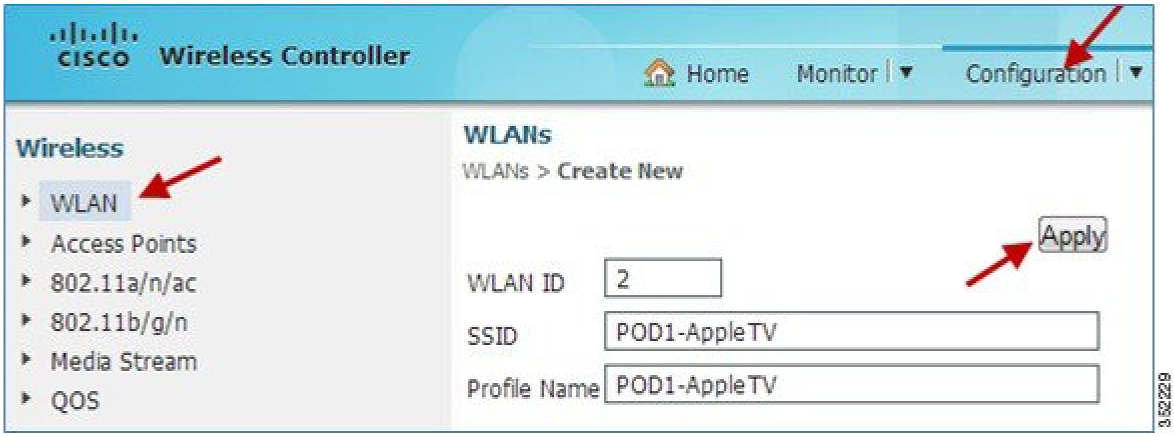


Vlan Configuration

New Remove

	Interface Name	Status	Protocol	IP-Address
□	Vlan1	administratively down	down	unassigned
□	Vlan10	up	up	10.10.10.2
□	Vlan11	up	up	10.10.11.2
□	Vlan13	up	up	10.10.13.2

Step 1 Create one WLAN for clients with any security type and another WLAN for AppleTV with security set to WPA2-PSK. Map the WLANs to the respective interfaces. The example below is of WLAN for AppleTV.



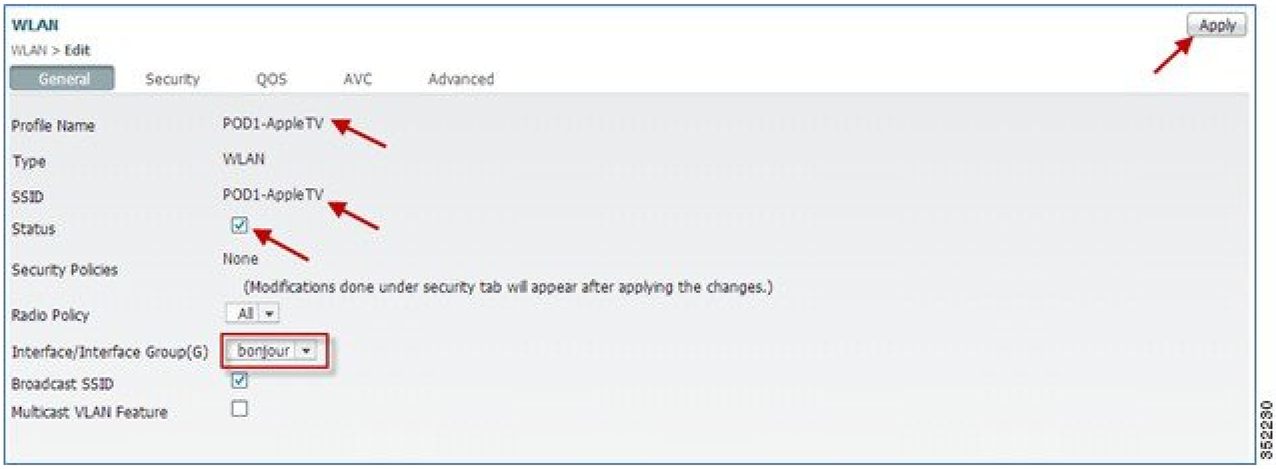
WLANs

WLANs > Create New

WLAN ID 2

SSID POD1-AppleTV

Profile Name POD1-AppleTV



WLAN

WLAN > Edit

Profile Name POD1-AppleTV

Type WLAN

SSID POD1-AppleTV

Status ☑

Security Policies None

(Modifications done under security tab will appear after applying the changes.)

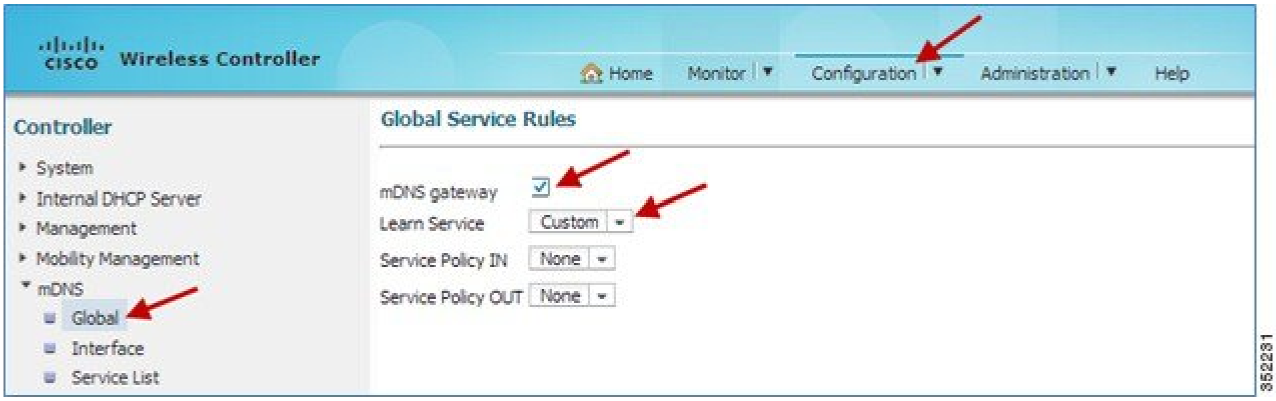
Radio Policy All

Interface/Interface Group(G) bonjour

Broadcast SSID ☑

Multicast VLAN Feature □

Step 2 Enable Service Discovery Gateway—Now, to enable the Bonjour services, navigate to **Configuration** > **Controller** > **mDNS** > **Global**. Under **Global Service Rules**, enable **mDNS gateway** by checking the **mDNS gateway** checkbox because it is disabled by default. Also, from the **Learn Service** drop-down menu, select **Enable** and click **Apply**.



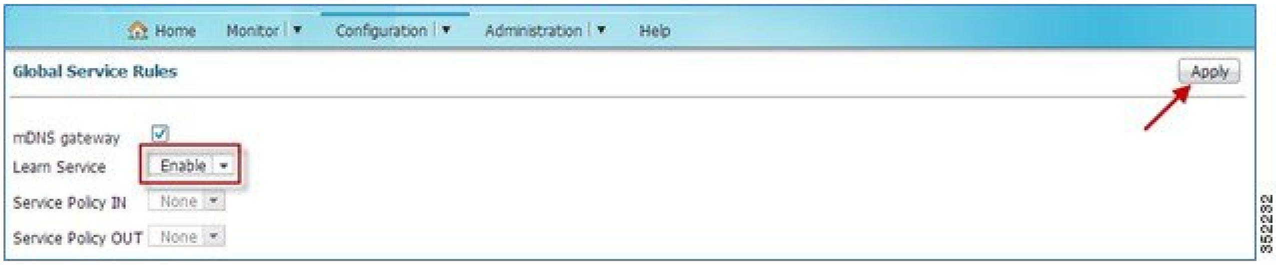
Global Service Rules

mDNS gateway ☑

Learn Service: Custom

Service Policy IN: None

Service Policy OUT: None



Global Service Rules

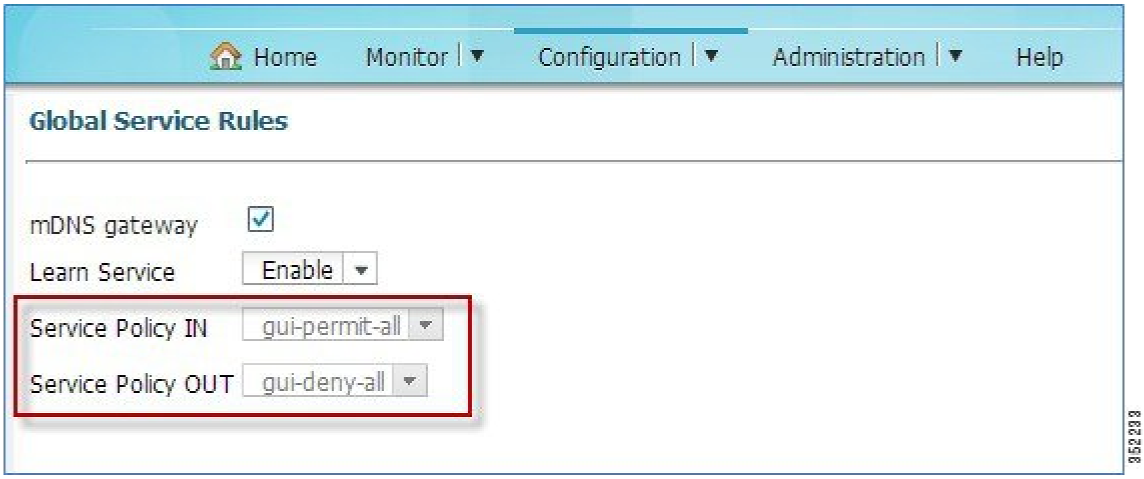
mDNS gateway ☑

Learn Service: Enable

Service Policy IN: None

Service Policy OUT: None

Once the **Learn Service** is enabled, the default service policies are created and applied. The **gui-permit-all** for **Service Policy IN** and **gui-deny-all** for **Service Policy OUT**.



Global Service Rules

mDNS gateway ☑

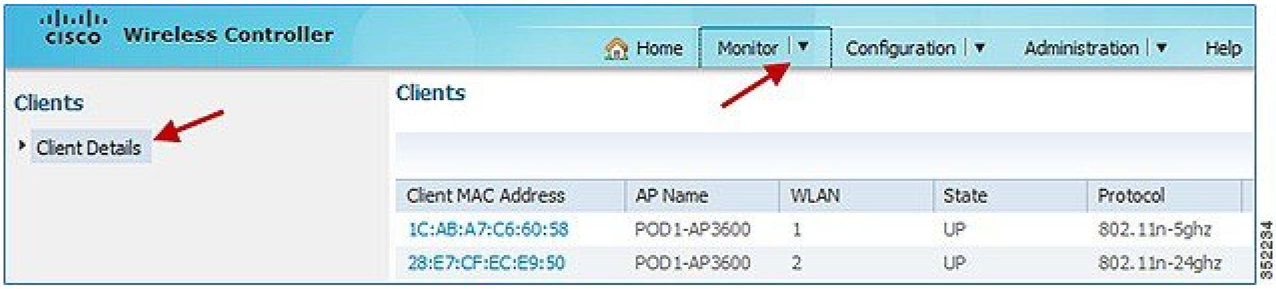
Learn Service: Enable

Service Policy IN: gui-permit-all

Service Policy OUT: gui-deny-all

Note The default Service Policy helps discover and cache the mDNS services on the WLC without them being advertised on the network.

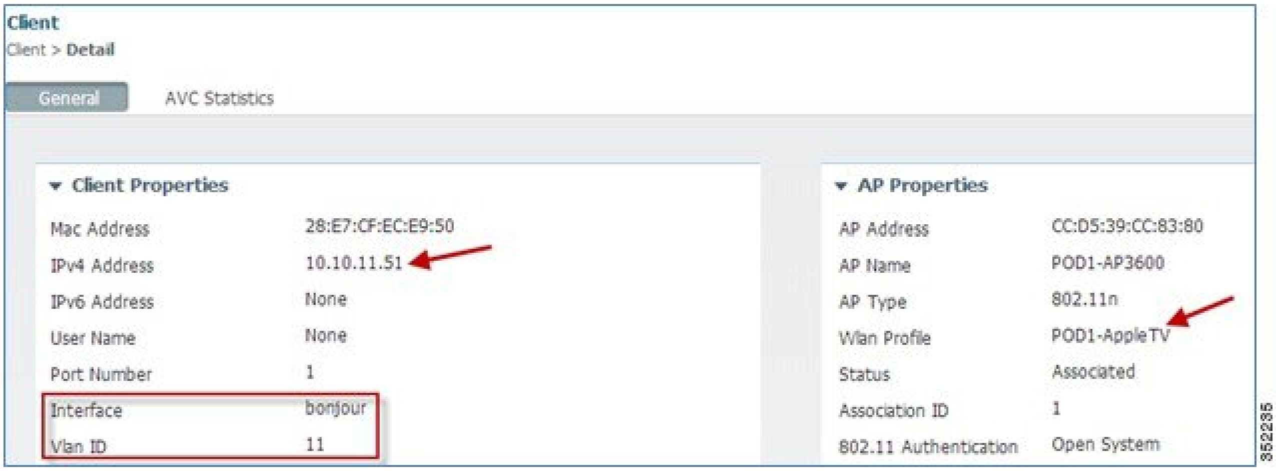
Step 3 Now, connect the Apple TV to the SSID for Bonjour services and the Bonjour client (iPad/iPhone) to SSID for Clients. Navigate to **Monitor > Clients** and you will see that the Bonjour servicing the Apple TV and the Bonjour Client (your iPad/IPhone) are associated to two different SSIDs as shown below.



Clients

Client MAC Address	AP Name	WLAN	State	Protocol
1C:AB:A7:C6:60:58	POD1-AP3600	1	UP	802.11n-5ghz
28:E7:CF:EC:E9:50	POD1-AP3600	2	UP	802.11n-24ghz

Apple TV:



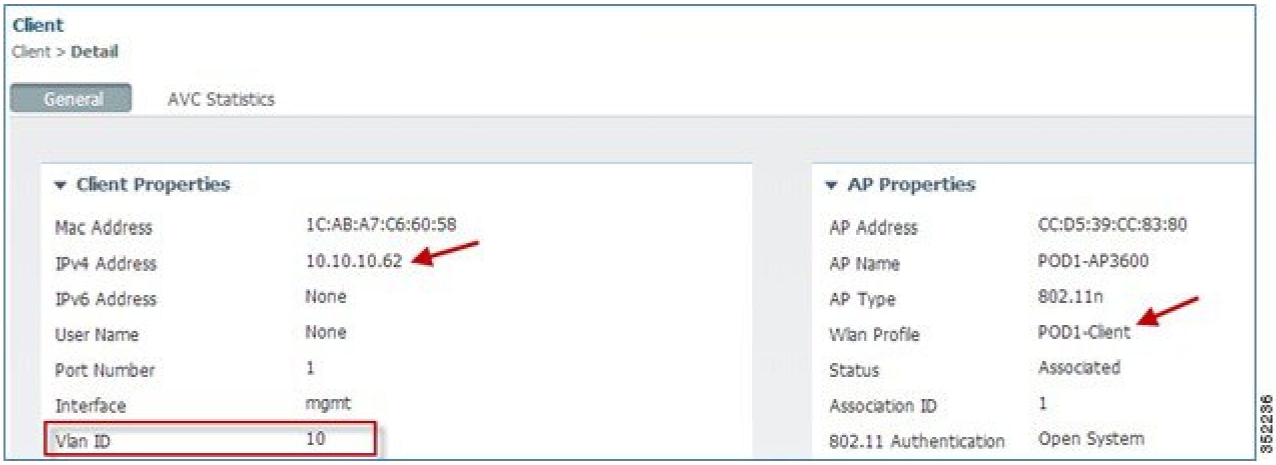
Client Properties

Mac Address	28:E7:CF:EC:E9:50
IPv4 Address	10.10.11.51
IPv6 Address	None
User Name	None
Port Number	1
Interface	bonjour
Vlan ID	11

AP Properties

AP Address	CC:D5:39:CC:83:80
AP Name	POD1-AP3600
AP Type	802.11n
Wlan Profile	POD1-AppleTV
Status	Associated
Association ID	1
802.11 Authentication	Open System

iOS Client:



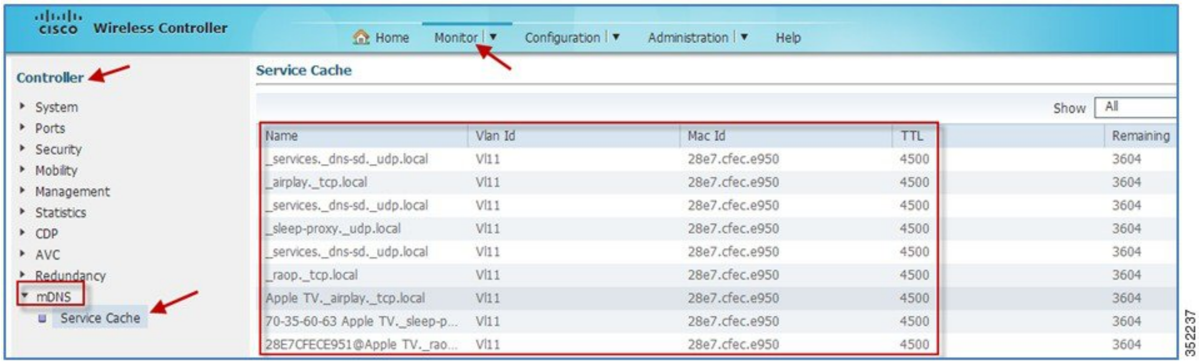
Client Properties

Mac Address	1C:AB:A7:C6:60:58
IPv4 Address	10.10.10.62
IPv6 Address	None
User Name	None
Port Number	1
Interface	mgmt
Vlan ID	10

AP Properties

AP Address	CC:D5:39:CC:83:80
AP Name	POD1-AP3600
AP Type	802.11n
Wlan Profile	POD1-Client
Status	Associated
Association ID	1
802.11 Authentication	Open System

Step 4 Once the clients are connected and the Global mDNS has been enabled, you can confirm which mDNS services are discovered and cached by navigating to **Monitor > Controller > mDNS > Service Cache**.

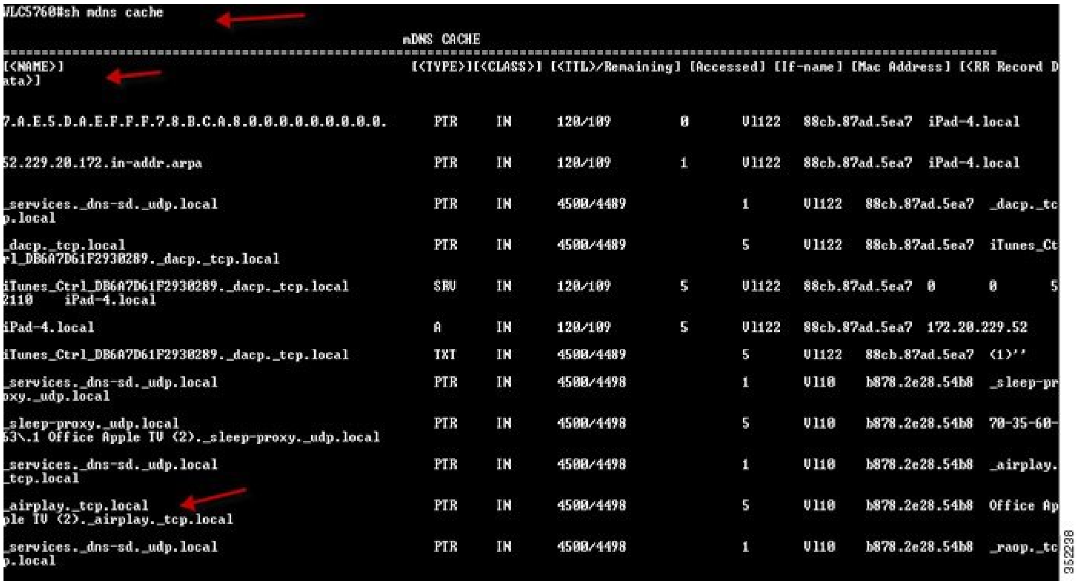


Service Cache

Name	Vlan Id	Mac Id	TTL	Remaining
_services._dns-sd._udp.local	Vl11	28e7.cfec.e950	4500	3604
_airplay._tcp.local	Vl11	28e7.cfec.e950	4500	3604
_services._dns-sd._udp.local	Vl11	28e7.cfec.e950	4500	3604
_sleep-proxy._udp.local	Vl11	28e7.cfec.e950	4500	3604
_services._dns-sd._udp.local	Vl11	28e7.cfec.e950	4500	3604
_raop._tcp.local	Vl11	28e7.cfec.e950	4500	3604
Apple TV._airplay._tcp.local	Vl11	28e7.cfec.e950	4500	3604
70-35-60-63 Apple TV._sleep-p...	Vl11	28e7.cfec.e950	4500	3604
28E7CFECE951@Apple TV._rao...	Vl11	28e7.cfec.e950	4500	3604

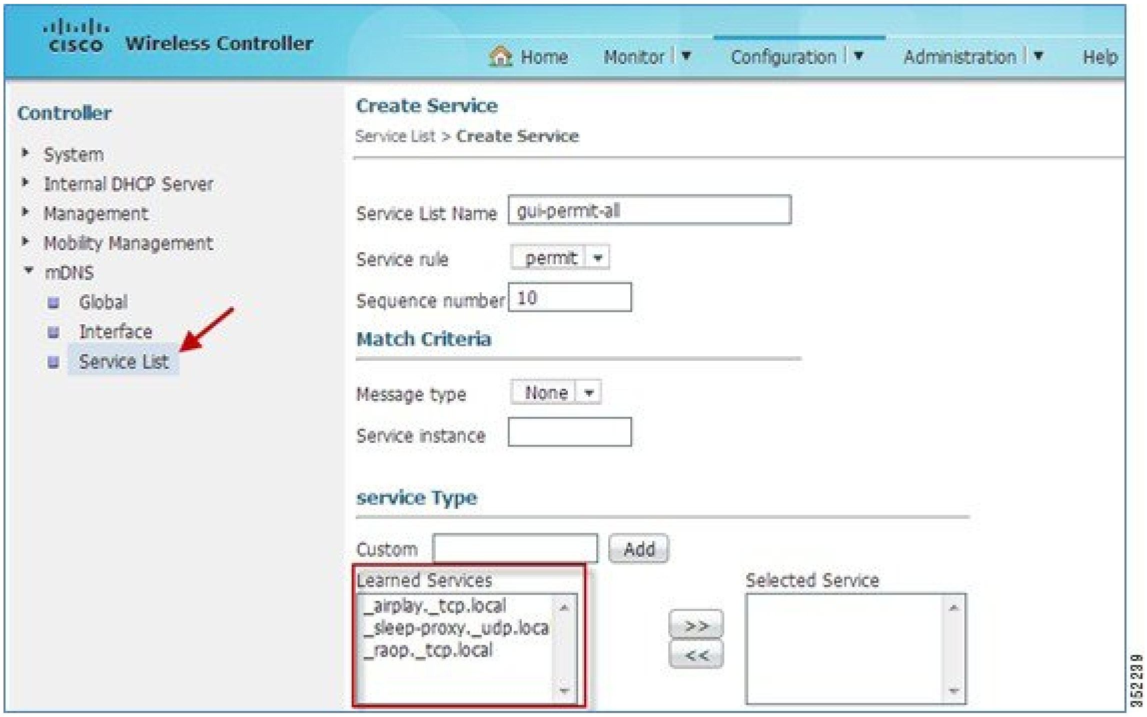
You can also check if the Bonjour services are being discovered in the IOS controller by issuing the following command from the CLI:

```
show mdns cache
```



```
WLC5760#sh mdns cache

                                                   mDNS CACHE
=========================================================================================================================================
[<NAME>]                                                    [<TYPE>][<CLASS>] [<TTL>/Remaining] [Accessed] [If-name] [Mac Address] [<RR Record D
ata>]

7.A.E.5.D.A.E.F.F.F.7.8.B.C.A.8.0.0.0.0.0.0.0.0.0.0.0.0.     PTR     IN      120/109         0       Vl122    88cb.87ad.5ea7  iPad-4.local

52.229.20.172.in-addr.arpa                                   PTR     IN      120/109         1       Vl122    88cb.87ad.5ea7  iPad-4.local

_services._dns-sd._udp.local                                 PTR     IN      4500/4489               1        Vl122    88cb.87ad.5ea7  _dacp._tc
p.local

_dacp._tcp.local                                             PTR     IN      4500/4489               5        Vl122    88cb.87ad.5ea7  iTunes_Ct
rl_DB6A7D61F2930289._dacp._tcp.local

iTunes_Ctrl_DB6A7D61F2930289._dacp._tcp.local                SRV     IN      120/109         5       Vl122    88cb.87ad.5ea7  0        0        5
2110    iPad-4.local

iPad-4.local                                                 A       IN      120/109         5       Vl122    88cb.87ad.5ea7  172.20.229.52

iTunes_Ctrl_DB6A7D61F2930289._dacp._tcp.local                TXT     IN      4500/4489               5        Vl122    88cb.87ad.5ea7  (1)''

_services._dns-sd._udp.local                                 PTR     IN      4500/4498               1        Vl10     b878.2e28.54b8  _sleep-pr
oxy._udp.local

_sleep-proxy._udp.local                                      PTR     IN      4500/4498               5        Vl10     b878.2e28.54b8  70-35-60-
63\.1 Office Apple TV (2)._sleep-proxy._udp.local

_services._dns-sd._udp.local                                 PTR     IN      4500/4498               1        Vl10     b878.2e28.54b8  _airplay.
_tcp.local

_airplay._tcp.local                                          PTR     IN      4500/4498               5        Vl10     b878.2e28.54b8  Office Ap
ple TV (2)._airplay._tcp.local

_services._dns-sd._udp.local                                 PTR     IN      4500/4498               1        Vl10     b878.2e28.54b8  _raop._tc
p.local
```

Step 5 Customize mDNS global configuration so that the cached mDNS services can be accessible to the clients which are requesting the services. To check what services are available in the default list, navigate to **mDNS > Service list** and click **gui-permit-all**.



Create Service

Service List > Create Service

Service List Name: gui-permit-all

Service rule: permit

Sequence number: 10

Match Criteria

Message type: None

Service instance:

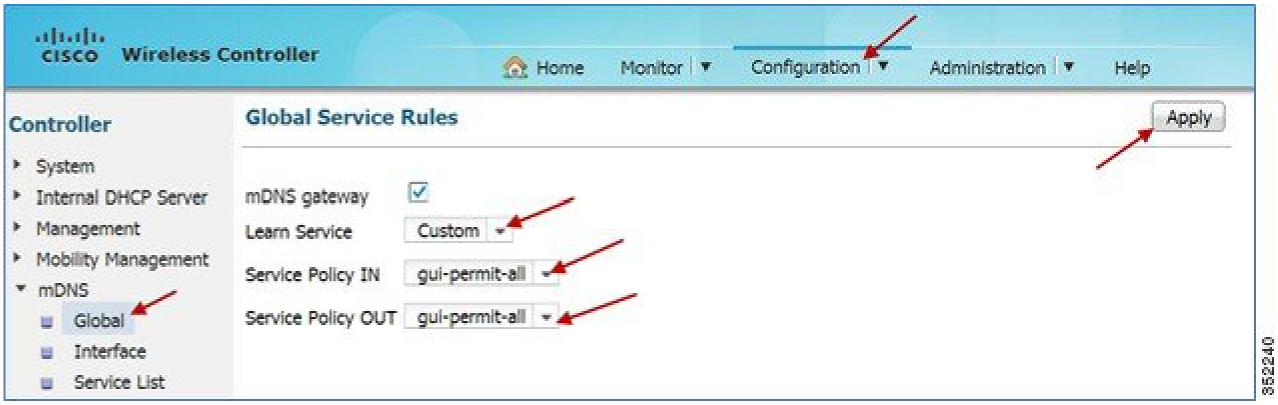
service Type

Custom:

Learned Services: _airplay._tcp.local, _sleep-proxy._udp.loca, _raop._tcp.local

Selected Service:

Step 6 Now, navigate to **Configuration > Controller > mDNS > Global** and from the **Learn Service** drop-down menu, select **Custom**. From the **Service Policy IN** drop-down menu, select the **gui-permit-all** option. Do the same for **Service Policy OUT**.



Global Service Rules

mDNS gateway ☑

Learn Service: Custom

Service Policy IN: gui-permit-all

Service Policy OUT: gui-permit-all

Service Lists: **gui-permit-all** and **gui-deny-all** are the default lists. You can create a customized Service List and define a service rule and service type as well. These rules are available to control the mDNS messages coming into and going out from the cache.

Note Service filters must be specified to allow records into and out of the cache because there is a 'deny any' policy installed by default. In other words, if no explicit filter policy is installed either globally or per interface, no records will make it into the cache and the cache will not answer to any queries.

Active Queries Configuration

Active Queries are specific filters that actively query for services attached to local segments. This helps to keep services ‘fresh’ in the cache. If a device queries for a specific service, the cache already holds a valid record and it does not need to proxy the service query to the attached network segments, but can respond immediately. This also helps to quickly detect the removal of a service (For example: A device is turned off without proper announcement of the service removal).

Currently, the GUI is not available to configure the active query. From the WLC CLI prompt, users can configure an active query by issuing the following command:

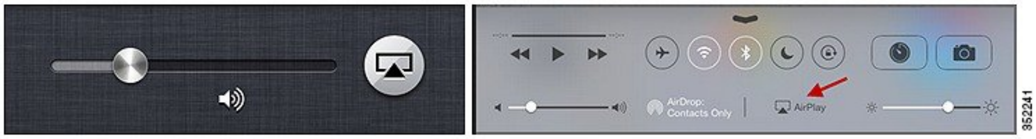
```
service-list mdns-sd <name> query
service-type <service type string>
```

For example:

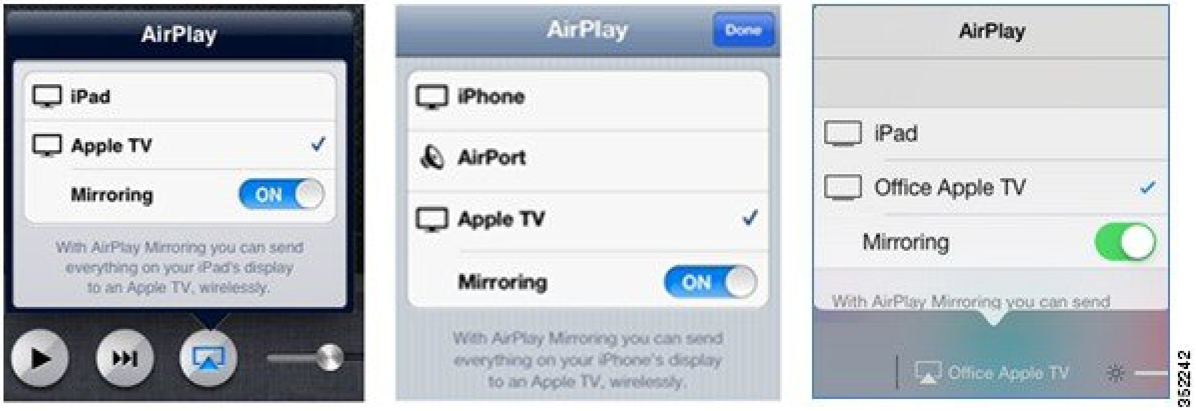
```
service-list mdns-sd active-query query
 service-type _airplay._tcp.local
 service-type _scanner._tcp.local
 service-type _printer._tcp.local
 service-type _raop._tcp.local
 service-type _ipp._tcp.local
!
service-routing mdns-sd
 service-policy-query active-query 60
```

Accessing Bonjour

- Once the mDNS is enabled and Bonjour services are being cached as shown in above steps, proceed with testing to see if the Bonjour services are routed across the VLANs.
- Make sure your Apple (iPhone/iPad) client is connected to the SSID for **Clients** and the Apple TV is connected to the SSID for Bonjour services.
- Ensure that the Apple TV has **AirPlay** enabled by checking the **Settings > AirPlay** menu from the home screen using the TV remote for the Monitor. An optional passcode can be set for security.
- On your Apple iOS device, double-click the home button to reveal the multi-tasking view. If you are using iOS7, swipe up the screen to see the options.
- Swipe left to right (twice for iPhone, once for iPad) to reveal a menu with the AirPlay icon as depicted in the below screenshot for iOS6 and iOS7 respectively.



- Select the Apple TV from the list, and enable mirroring.

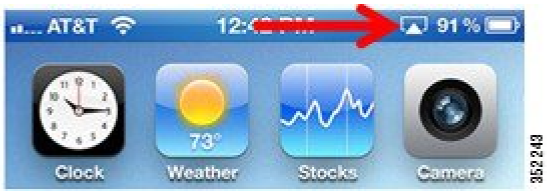


With AirPlay Mirroring you can send everything on your iPad's display to an Apple TV, wirelessly.

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

With AirPlay Mirroring you can send

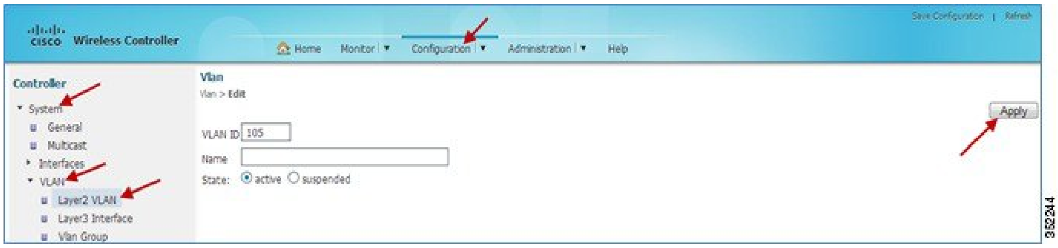
- The status bar of the Apple device will turn blue along with adding an icon for AirPlay, signifying that you are broadcasting your screen on the Apple TV.



Accessing Bonjour Printer Service

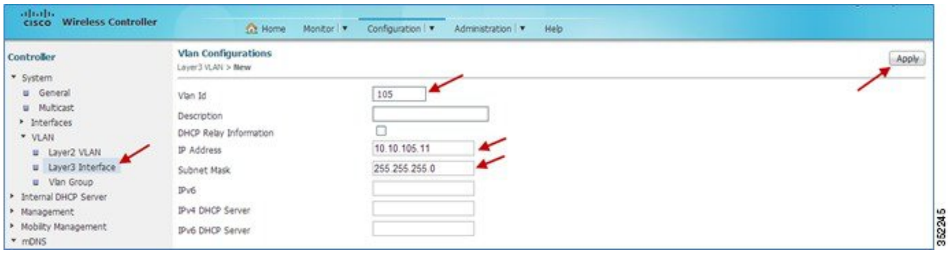
In most scenarios, printers are connected through wires on the network. The printer might be on the same network as other Bonjour services or on a different network. To showcase and verify that the Air Print Services are accessible to users:

1 Create a VLAN interface on the WLC on which the Bonjour Printer is connected (In this example, it is VLAN 105) by navigating to **Configuration > Controller > System > VLAN > Layer2 VLAN** and click **New**. Assign the VLAN ID and click **Apply**.



VLAN ID 105
Name
State: ● active ○ suspended

2 Similarly, create a L3 interface by navigating to **Configuration > Controller > System > VLAN > Layer3 Interface** and click **New**. Assign the **VLAN Id** and **IP Address** and click **Apply**.

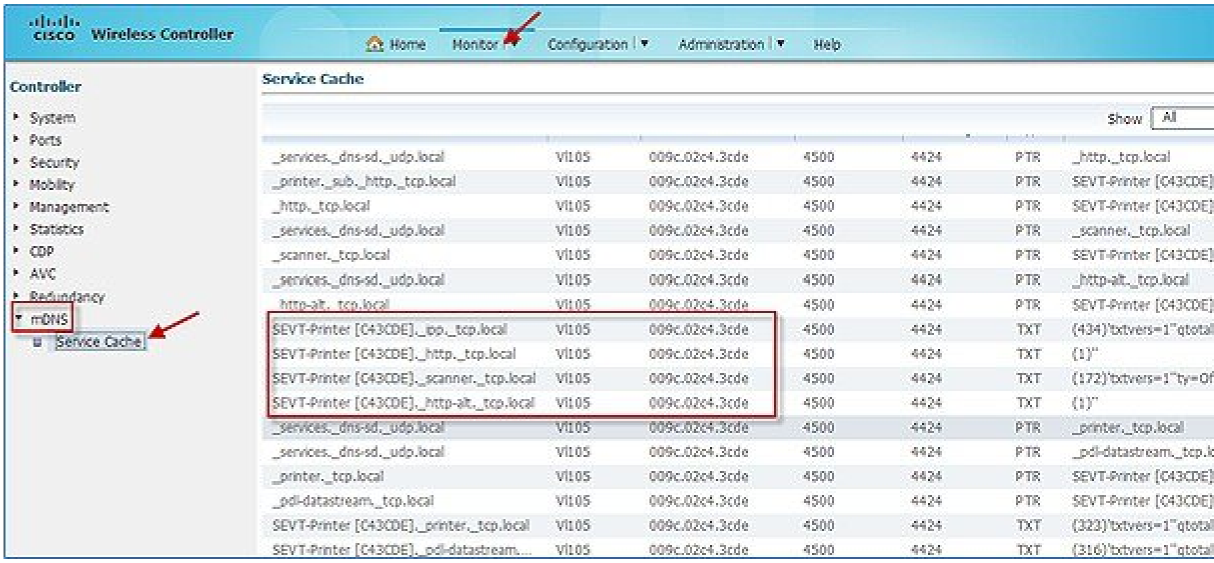


Vlan Configurations

Layer3 VLAN > New

Vlan Id	105
Description	
DHCP Relay Information	□
IP Address	10.10.105.11
Subnet Mask	255.255.255.0
IPv6	
IPv4 DHCP Server	
IPv6 DHCP Server	

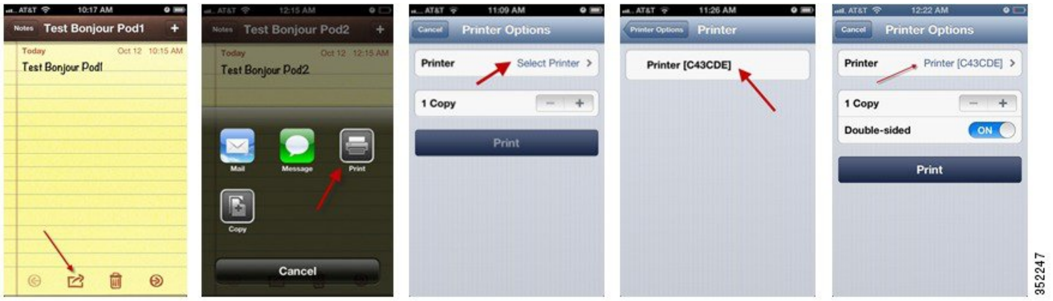
3 To check if the Bonjour Printer service is being discovered and cached by the WLC, navigate to **Monitor > Controller > mDNS > Service Cache** and you will see the printer being discovered and cached as shown below.



Service Cache

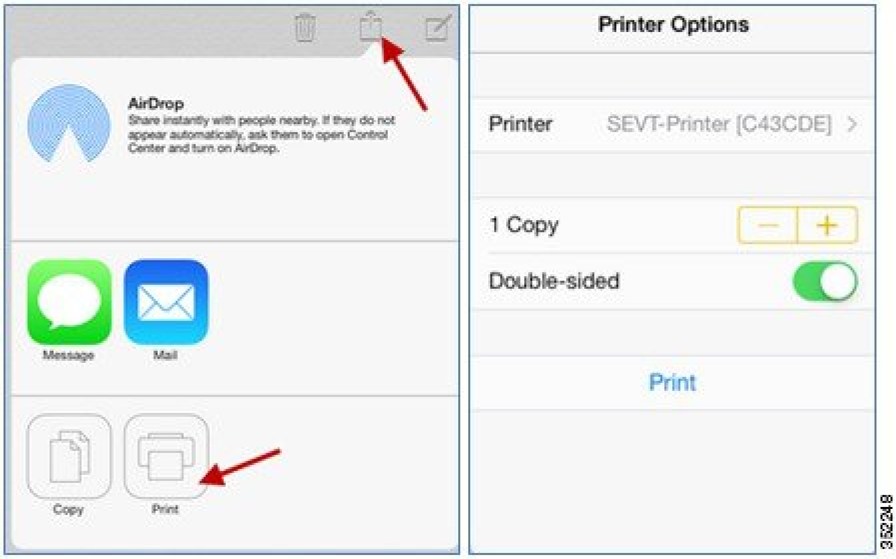
_services._dns-sd._udp.local	Vl105	009c.02c4.3cde	4500	4424	PTR	_http._tcp.local
_printer._sub._http._tcp.local	Vl105	009c.02c4.3cde	4500	4424	PTR	SEVT-Printer [C43CDE]
_http._tcp.local	Vl105	009c.02c4.3cde	4500	4424	PTR	SEVT-Printer [C43CDE]
_services._dns-sd._udp.local	Vl105	009c.02c4.3cde	4500	4424	PTR	_scanner._tcp.local
_scanner._tcp.local	Vl105	009c.02c4.3cde	4500	4424	PTR	SEVT-Printer [C43CDE]
_services._dns-sd._udp.local	Vl105	009c.02c4.3cde	4500	4424	PTR	_http-alt._tcp.local
_http-alt._tcp.local	Vl105	009c.02c4.3cde	4500	4424	PTR	SEVT-Printer [C43CDE]
SEVT-Printer [C43CDE]._ipp._tcp.local	Vl105	009c.02c4.3cde	4500	4424	TXT	(434)'txtvers=1''qtotal
SEVT-Printer [C43CDE]._http._tcp.local	Vl105	009c.02c4.3cde	4500	4424	TXT	(1)''
SEVT-Printer [C43CDE]._scanner._tcp.local	Vl105	009c.02c4.3cde	4500	4424	TXT	(172)'txtvers=1''ty=Of
SEVT-Printer [C43CDE]._http-alt._tcp.local	Vl105	009c.02c4.3cde	4500	4424	TXT	(1)''
_services._dns-sd._udp.local	Vl105	009c.02c4.3cde	4500	4424	PTR	_printer._tcp.local
_services._dns-sd._udp.local	Vl105	009c.02c4.3cde	4500	4424	PTR	_pdl-datastream._tcp.l
_printer._tcp.local	Vl105	009c.02c4.3cde	4500	4424	PTR	SEVT-Printer [C43CDE]
_pdl-datastream._tcp.local	Vl105	009c.02c4.3cde	4500	4424	PTR	SEVT-Printer [C43CDE]
SEVT-Printer [C43CDE]._printer._tcp.local	Vl105	009c.02c4.3cde	4500	4424	TXT	(323)'txtvers=1''qtotal
SEVT-Printer [C43CDE]._pdl-datastream....	Vl105	009c.02c4.3cde	4500	4424	TXT	(316)'txtvers=1''qtotal

4 In your iOS device, open an application such as Safari, Note, or Photos. If you are using iOS6, click the Print icon as shown below. This should show the bonjour printer which is discovered by the device.



5

In iOS7, from the application, click the icon and then click **Print**. Select the **Printer** under **Printer Options** as shown below.



AirDrop
Share instantly with people nearby. If they do not appear automatically, ask them to open Control Center and turn on AirDrop.

Printer Options

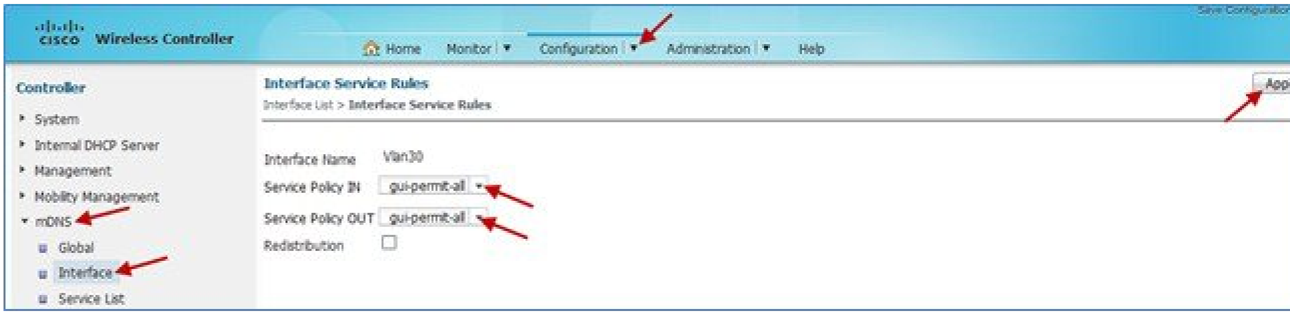
Printer SEVT-Printer [C43CDE]

1 Copy

Double-sided

Configuring Service Policy on Interface

Service policy can be applied on an interface as well. On the WLC main menu, navigate to **Controller > mDNS > Interface** and then click the desired interface name on which you want the service policy to be enabled. From the **Service Policy IN/OUT** drop-down menu, select the Service Policy and click **Apply**. Here we have selected the default service policy **gui-permit-all** for Service Policy IN and Service Policy OUT.



Interface Service Rules

Interface List > Interface Service Rules

Interface Name Vlan30

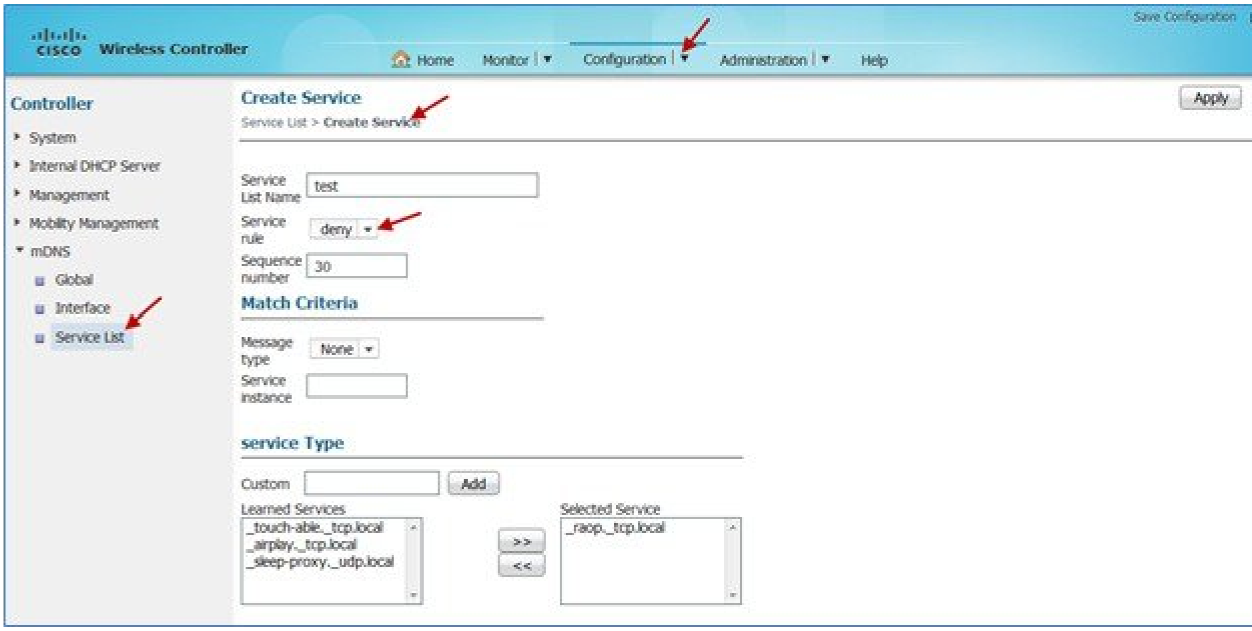
Service Policy IN gui-permit-all

Service Policy OUT gui-permit-all

Redistribution □

Creating Service List

You can create a Service List, define a service rule (Permit or Deny), and select a service type as shown below.



Service List Name: test
Service rule: deny
Sequence number: 30
Message type: None
Service instance:
Learned Services: _touch-able._tcp.local, _airplay._tcp.local, _sleep-proxy._udp.local
Selected Service: _raop._tcp.local

Note Currently on WLC GUI, only one service can be selected from **Learned Services** to **Selected Service**. You can add more services to the Service Policy List from the WLC CLI.

Service lists are configured to permit or deny statements matching a certain part of the mDNS record which make up the filter. These use regular expression for string match (e.g. service type match or instance name match).

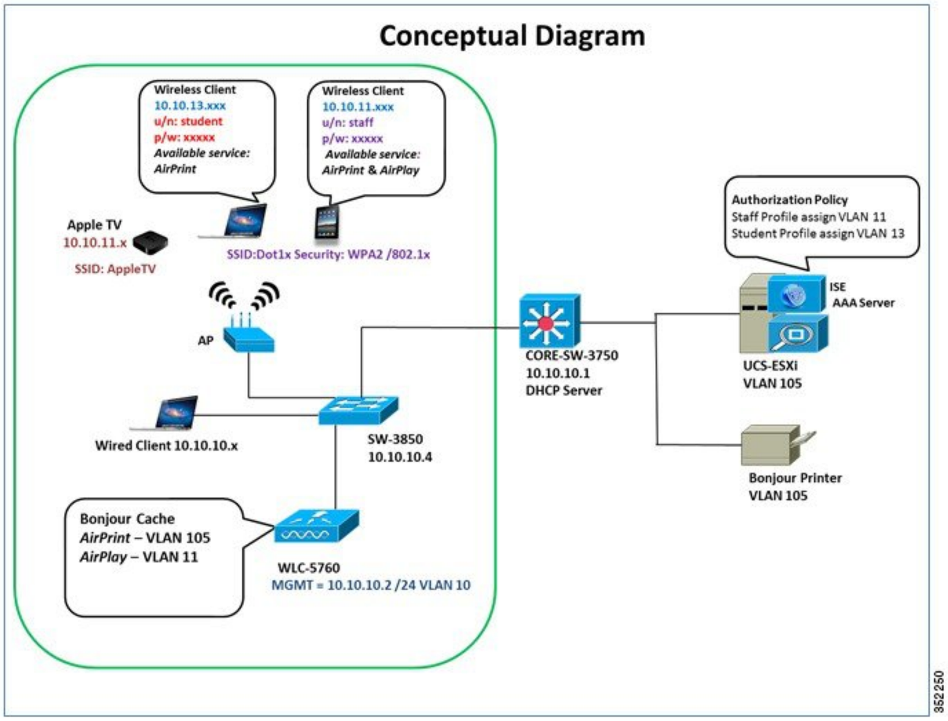
You can have different filters based on your network requirements:

- Filtering of certain services from certain subnets (for example, no Music sharing across subnet boundaries).
- Exclusion of specific services from being visible on the network.

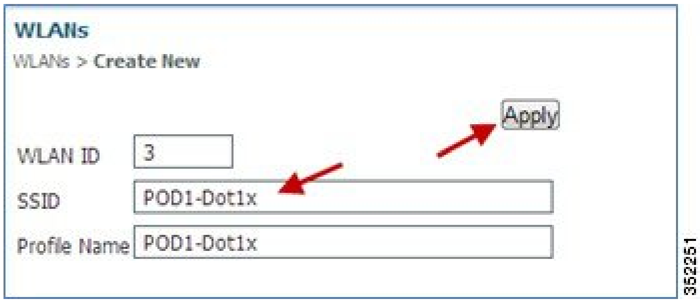
Configuring mDNS Service Filtering on an Interface with AAA Override

In the example shown below we will deny AirPlay service (AppleTV) to certain users (which belong to group Student) and permit AirPlay and AirPrint (Bonjour Printer) services for other users (group Staff).

It is assumed that the user has pre-configured the controller for AAA authentication (802.1x authentication).



Step 1 To configure and demonstrate the service filtering of specific service on a particular interface, we created another WLAN with L2 Security set to WPA2/802.1x which is mapped to the management interface as shown in example below.



WLANs

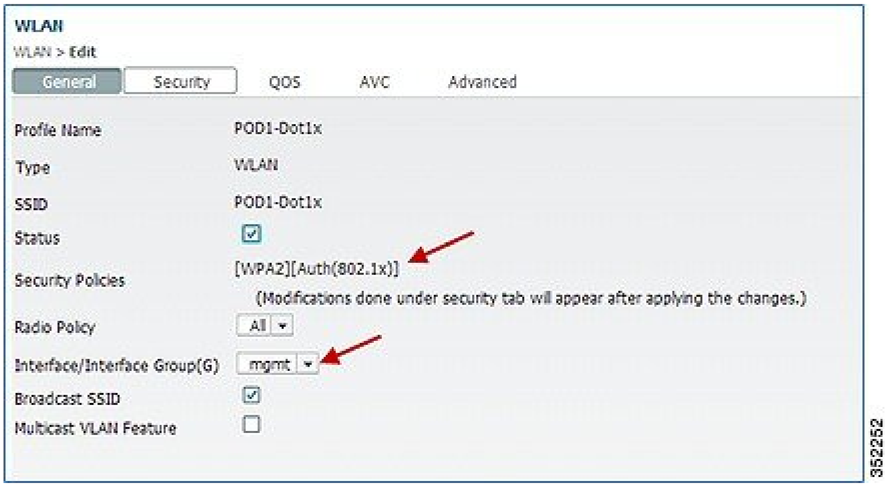
WLANs > Create New

Apply

WLAN ID: 3

SSID: POD1-Dot1x

Profile Name: POD1-Dot1x



WLAN

WLAN > Edit

General | Security | QOS | AVC | Advanced

Profile Name: POD1-Dot1x

Type: WLAN

SSID: POD1-Dot1x

Status: ☑

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

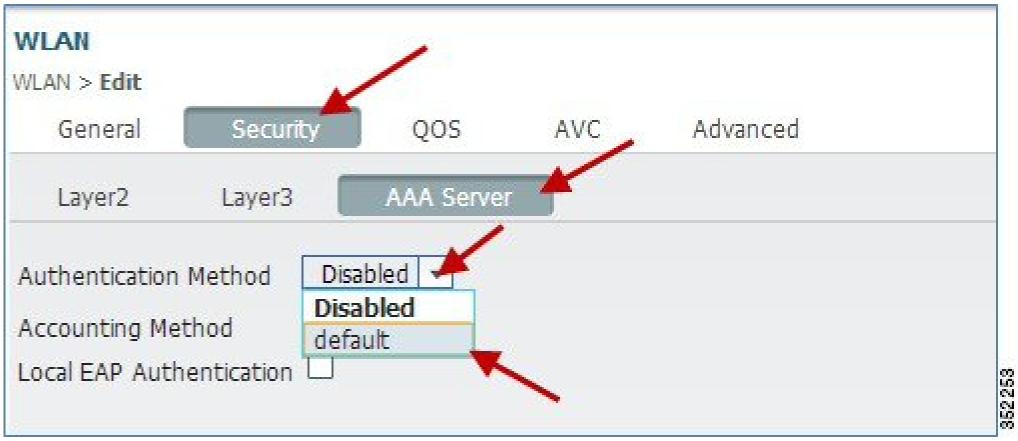
Radio Policy: All

Interface/Interface Group(G): mgmt

Broadcast SSID: ☑

Multicast VLAN Feature: □

Now, navigate to **Security > AAA Server** and from the **Authentication Method** drop-down menu select the Authentication method.



WLAN

WLAN > Edit

General | Security | QOS | AVC | Advanced

Layer2 | Layer3 | AAA Server

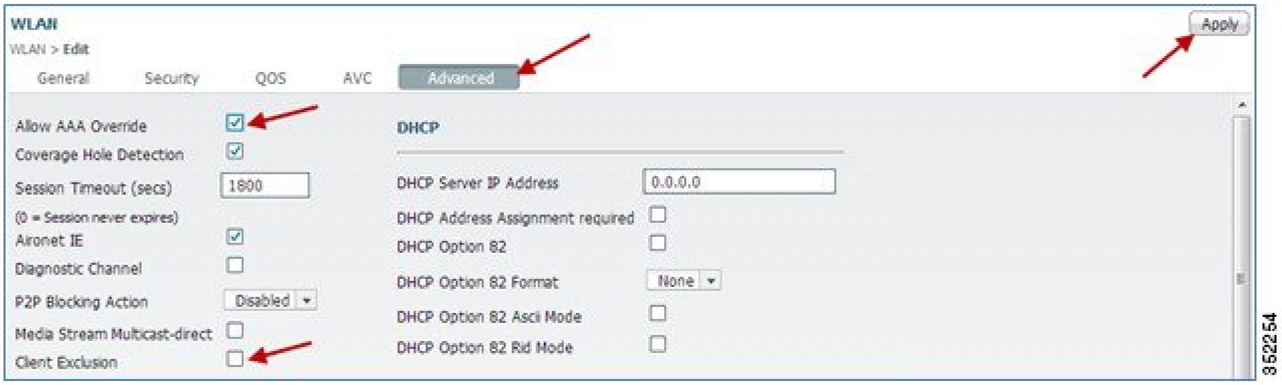
Authentication Method: Disabled
Disabled
default

Accounting Method

Local EAP Authentication: □

Note The default Authentication Method is the Method List Name which we have already configured. It can be different according to user configuration. Please refer to the WLC5760 deployment guide for AAA configuration. http://www.cisco.com/en/US/docs/wireless/technology/5760_deploy/CT5760_Controller_Deployment_Guide.pdf

From the WLAN **Advanced** tab, enable **Allow AAA Override**.



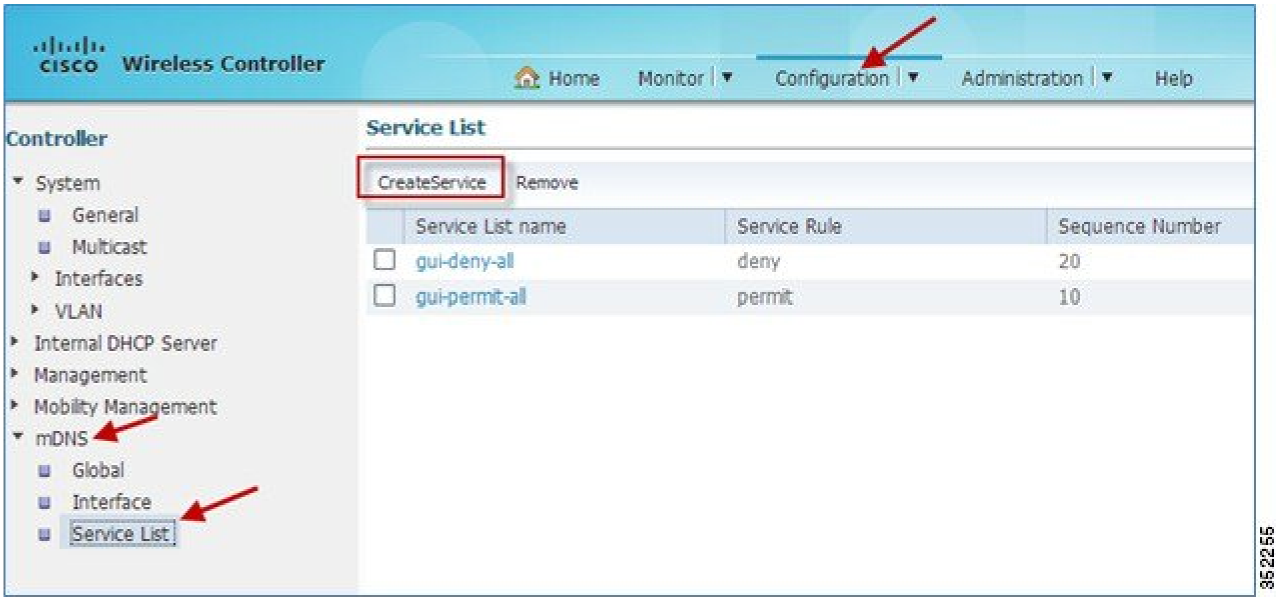
Allow AAA Override	☑
Coverage Hole Detection	☑
Session Timeout (secs)	1800
(0 = Session never expires)	
Aironet IE	☑
Diagnostic Channel	□
P2P Blocking Action	Disabled
Media Stream Multicast-direct	□
Client Exclusion	□

DHCP Server IP Address	0.0.0.0
DHCP Address Assignment required	□
DHCP Option 82	□
DHCP Option 82 Format	None
DHCP Option 82 Ascii Mode	□
DHCP Option 82 Rid Mode	□

In this scenario, we have a single SSID (Security WPA2/dot1x) with two user profiles/groups. The users for "Staff" and "Student" is already configured on ISE server (AAA server). The "Staff" users should be able to access all the bonjour services i.e AppleTV and bonjour printer while "Student" users should only have access to the bonjour printer.

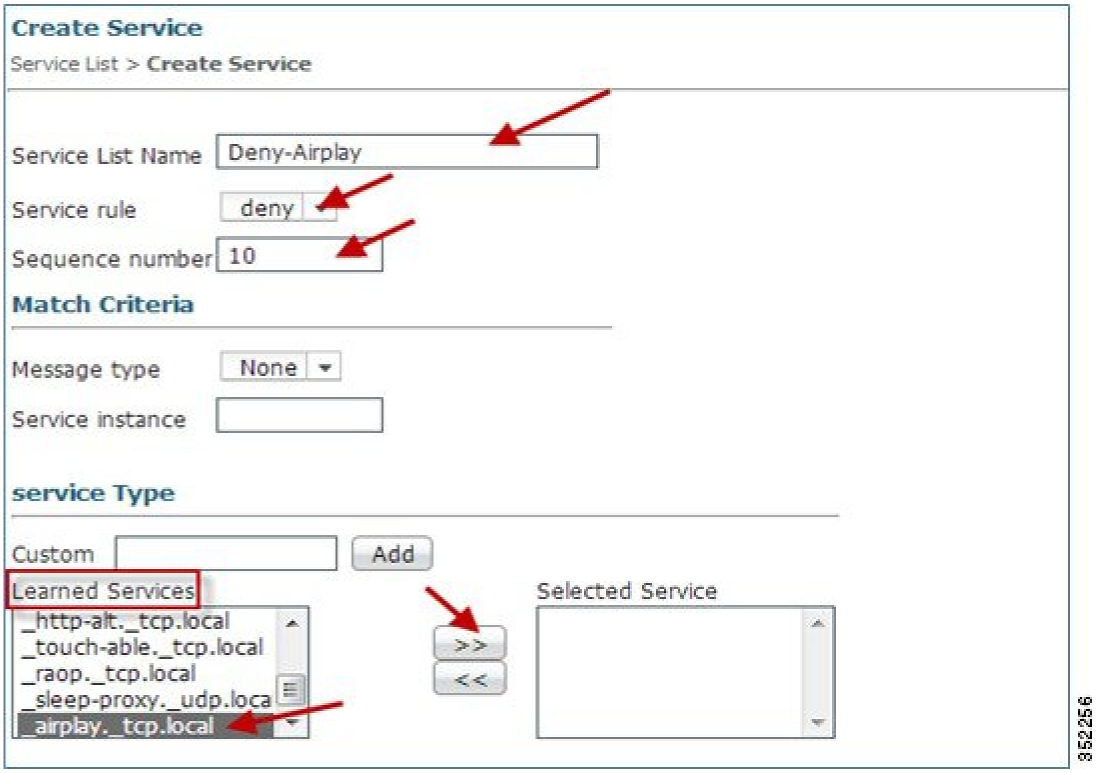
In order to implement this scenario, we need to configure the Service list which should deny AppleTV/Airplay services and only allow the Printer services on the VLAN which is tied to the profile 'Student'.

Step 2 Navigate to **Configuration** > **Controller** > **mDNS** > **Service List** and click the **CreateService** tab.



Service List name	Service Rule	Sequence Number
□ gui-deny-all	deny	20
□ gui-permit-all	permit	10

Step 3 Now, configure the **Service List Name**, users can assign any intuitive name to configure the service list. Here, we are naming it as **Deny-Airplay**. From the **Service rule** drop-down menu, select **deny** and add a **Sequence number** *(sequence number can be from 0-100)*. Under **service Type** there are two options available, you can leave the **Custom** option as is and choose the service you want to deny from the **Learned Services** list and add it to the **Selected Service** list.



Create Service

Service List > Create Service

Service List Name: Deny-Airplay

Service rule: deny

Sequence number: 10

Match Criteria

Message type: None

Service instance:

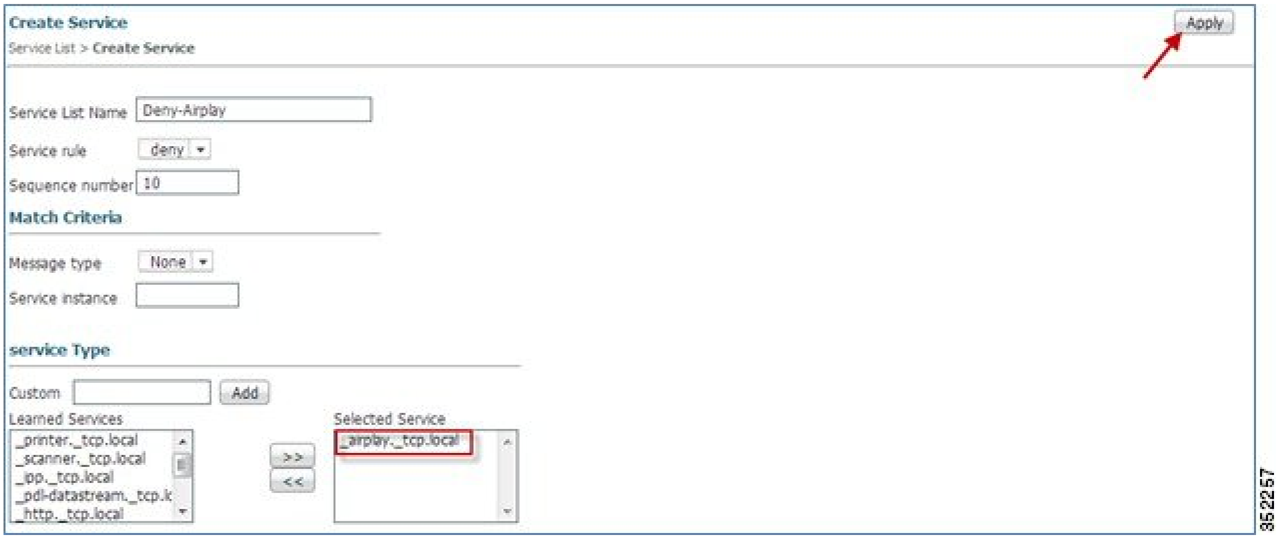
service Type

Custom:

Learned Services:
- _http-alt._tcp.local
- _touch-able._tcp.local
- _raop._tcp.local
- _sleep-proxy._udp.loca
- _airplay._tcp.local

Selected Service:

In our case it is airplay service which we want to deny, so select **_airplay._tcp.local** and then click **Apply**.



Create Service

Service List > Create Service

Service List Name: Deny-Airplay

Service rule: deny

Sequence number: 10

Match Criteria

Message type: None

Service instance:

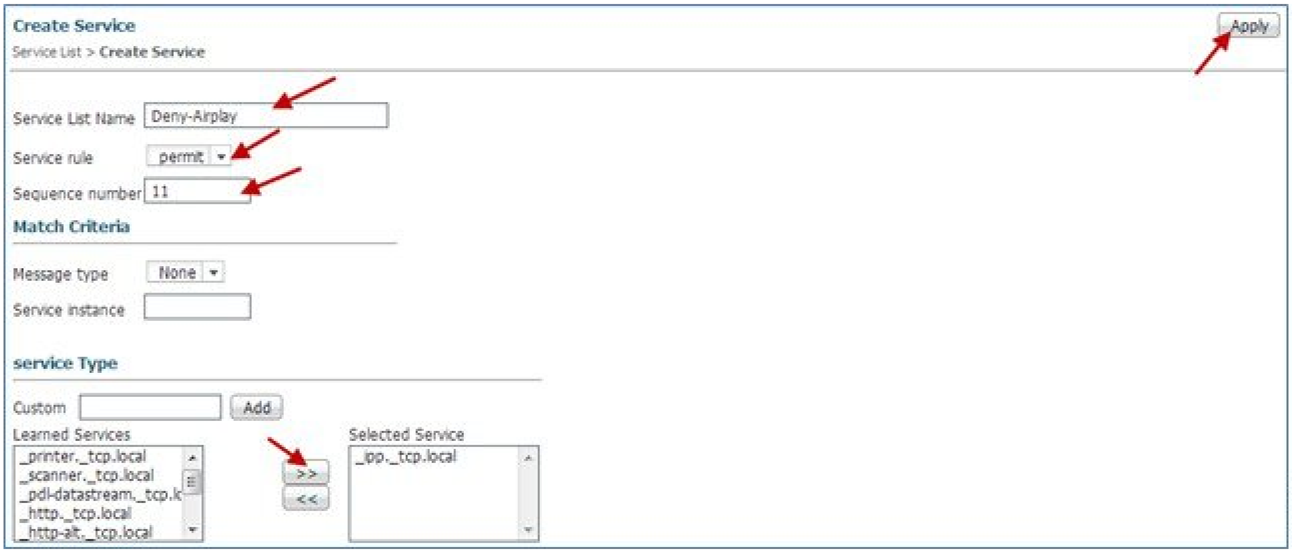
service Type

Custom:

Learned Services:
- _printer._tcp.local
- _scanner._tcp.local
- _ipp._tcp.local
- _pdl-datastream._tcp.lc
- _http._tcp.local

Selected Service:
- _airplay._tcp.local

Similarly, to permit bonjour printer services, create a **Service List** permit rule with the same list name **Deny-Airplay**, but with a higher **Sequence Number**. Select the **_ipp._tcp.local** from the **Learned Services** list as shown in example below to allow printer service.



Create Service

Service List > Create Service

Apply

Service List Name: Deny-Airplay

Service rule: permit

Sequence number: 11

Match Criteria

Message type: None

Service instance:

service Type

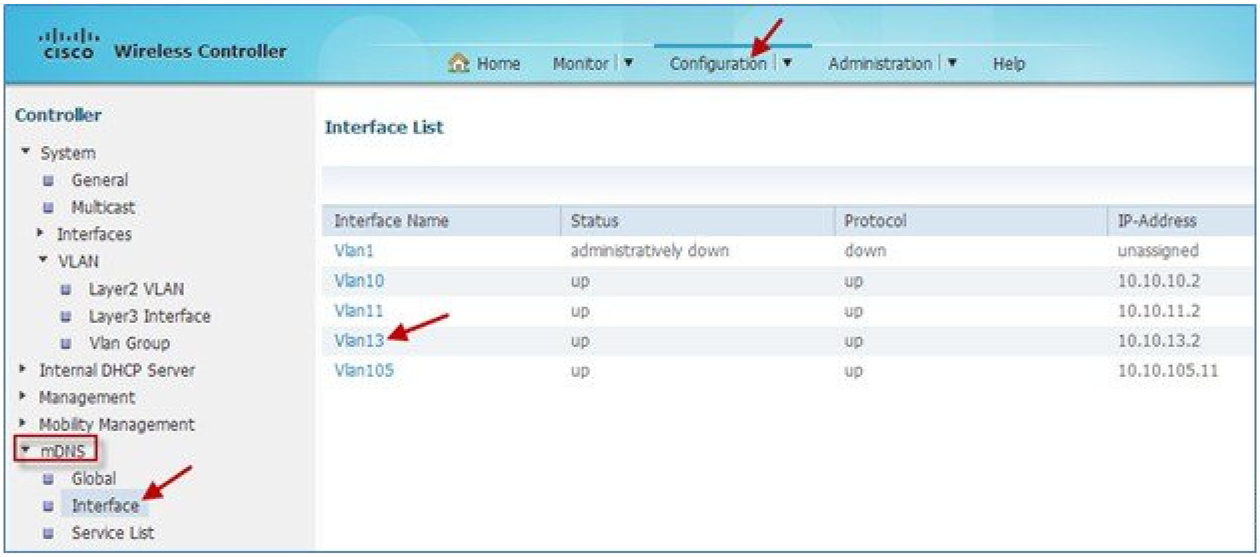
Custom: Add

Learned Services:
_printer._tcp.local
_scanner._tcp.local
_pdl-datastream._tcp.lc
_http._tcp.local
_http-alt._tcp.local

Selected Service:
_ipp._tcp.local

352258

Step 4 Once the Service List is created, we need to apply it on the interface for it to take effect. Navigate to **mDNS > Interface** and click the VLAN on which you want to apply this rule. In this example we are using the VLAN interface (VLAN13) to implement this policy.

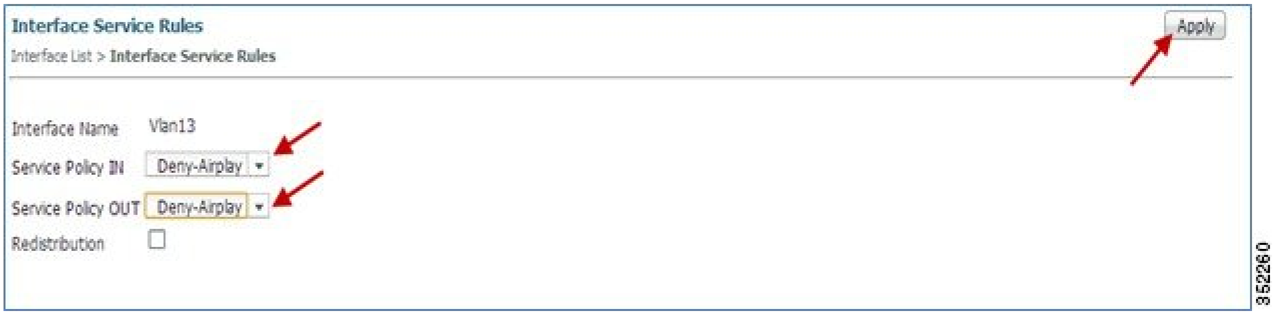


Interface List

Interface Name	Status	Protocol	IP-Address
Vlan1	administratively down	down	unassigned
Vlan10	up	up	10.10.10.2
Vlan11	up	up	10.10.11.2
Vlan13	up	up	10.10.13.2
Vlan105	up	up	10.10.105.11

352259

From the **Service Policy IN** drop-down menu, select the rule created above i.e Deny-Airplay and select the same for **Service Policy OUT** as well. The Service List rule with the lower sequence number will be processed first.



Interface Service Rules

Interface List > Interface Service Rules

Interface Name Vlan13

Service Policy IN Deny-Airplay

Service Policy OUT Deny-Airplay

Redistribution □

Note Redistribution is the process of forwarding service announcements to other segments. This is turned off by default. If a service is announced on one segment it will be recorded in the cache. However, other segments will not ‘see’ this service instance unless the service is actively queried. If the service should be visible on other segments at the time of its original announcement on the originating segment, redistribution must be enabled.

Step 5 Now, to ensure if the Service list rule is being applied correctly, connect an iOS client to Dot1x SSID, when prompted for username/password, enter the credentials.

Note Before accessing bonjour services on your client, go to the WLC to check if the mDNS cache has an entry for those services.

Step 6 After the client is authenticated as a "Staff" user, try accessing bonjour services as shown earlier in this guide. The Staff user should be able to access AppleTV and Printer services.

Similarly, connect with student credentials to the same SSID and verify that the student is placed on the desired VLAN (i.e. VLAN13 in our example), you will see that only printer service is available for that user profile.

Service Discovery Gateway Summary

- AIR-CT5760 (14K services), WS-C3850 (14K services) and WS-3650 (8K services) in IOS-XE 3.3.
- Supported with Centralized and Converged Access mode.
- Detect wired and wireless services on VLANs that are L2 adjacent to the WLC.
- Each Bonjour service has an advertised Time To Live (TTL). The controller will ask the device for an update at 85% of this TTL.