



Service Discovery Gateway Deployment Guide, Cisco IOS-XE Release 3.3

Last Modified: January 25, 2014

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

CHAPTER 1

Introduction 1

CT5760 Controller 1

Service Discovery Gateway (mDNS Gateway) 2

CHAPTER 2

Configuration 5

Initial Configuration for Service Discovery Gateway (SDG) 5

Active Queries Configuration 11

Accessing Bonjour Printer Service 12

Configuring Service Policy on Interface 14

Configuring mDNS Service Filtering on an Interface with AAA Override 15

Service Discovery Gateway Summary 21

CHAPTER 3

mDNS CLI Configuration 23



Introduction

This guide introduces release 3.3 deployment guide for the Cisco Converged Access CT5760 and Cat3850 products. This guide is designed to help you deploy and monitor new features introduced in release 3.3.

The document builds on previous releases with the assumption that users are familiar with the Converged Access products. Please refer to both the [CT5760 Controller Deployment Guide](#) and the [Cisco Catalyst 3850 Switch Deployment Guide](#) for released features not covered in this guide.

The following topics are covered under this chapter:

- [CT5760 Controller, page 1](#)
- [Service Discovery Gateway \(mDNS Gateway\), page 2](#)

CT5760 Controller

CT5760 is an innovative UADP ASIC based wireless controller deployed as a centralized controller in the next generation unified wireless architecture. CT5760 controllers are specifically designed to function as Unified model central wireless controllers. They also support newer Mobility functionality with Converged Access switches in the wireless architecture.



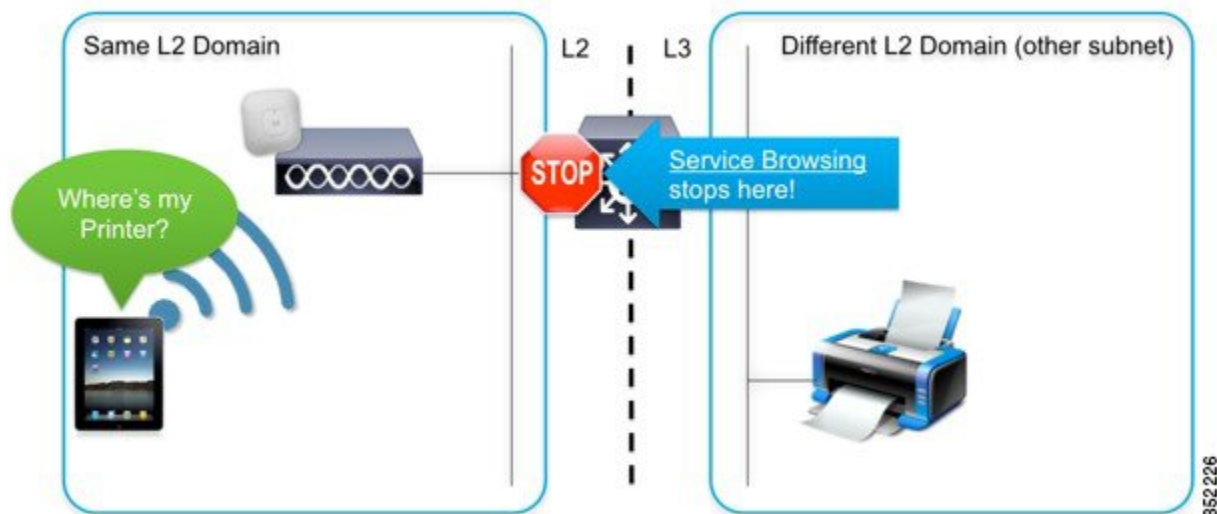
CT5760 controllers are deployed behind a core switch/router. The core switch/router is the only gateway into the network for the controller. The uplink ports connected to the core switch are configured as EtherChannel trunk to ensure port redundancy.

This new controller is an extensible and high performing wireless controller, which can scale up to 1000 access points and 12000 clients. The controller has 6 to 10 Gbps data ports.

As a component of the Cisco Unified Wireless Network, the 5760 series works in conjunction with Cisco Aironet access points, the Cisco Prime infrastructure, and the Cisco Mobility Services Engine to support business-critical wireless data, voice, and video applications.

Service Discovery Gateway (mDNS Gateway)

Cisco's Service Discovery Gateway is an IOS component that implements the Zeroconf suite of technologies in IOS. Zeroconf is a widely used standard for plug-and-play service discovery, including Apple Bonjour® services. Zeroconf has been designed with the local network in mind and operates only in its local network. However, due to the huge success of the BYOD device in enterprises and educational institutions, the need to support Zeroconf enabled services beyond the boundaries of a local subnet has become top of mind.



Cisco's Service Discovery Gateway allows for controlled and secure access to services and devices across subnets. It listens to service announcements on all configured network segments and builds a cache of services and addresses. It proxies these requests to other segments and can also apply filters based on various service attributes. These filters can limit what services will be requested or advertised.



Configuration

The following topics are covered under this chapter:

- [Initial Configuration for Service Discovery Gateway \(SDG\), page 5](#)
- [Active Queries Configuration, page 11](#)
- [Accessing Bonjour Printer Service, page 12](#)
- [Configuring Service Policy on Interface, page 14](#)
- [Configuring mDNS Service Filtering on an Interface with AAA Override, page 15](#)
- [Service Discovery Gateway Summary, page 21](#)

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):

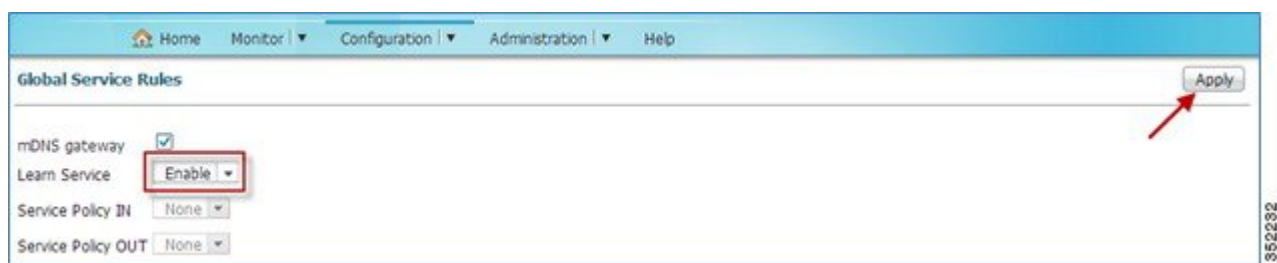
VLAN			
New Remove			
	VLAN ID	Name	Status
<input type="checkbox"/>	1	default	active
<input type="checkbox"/>	10	mgmt	active
<input type="checkbox"/>	11	bonjour	active

Vlan Configuration				
New Remove				
<input type="checkbox"/>	Interface Name	Status	Protocol	IP-Address
<input type="checkbox"/>	Vlan1	administratively down	down	unassigned
<input type="checkbox"/>	Vlan10	up	up	10.10.10.2
<input type="checkbox"/>	Vlan11	up	up	10.10.11.2
<input type="checkbox"/>	Vlan13	up	up	10.10.13.2

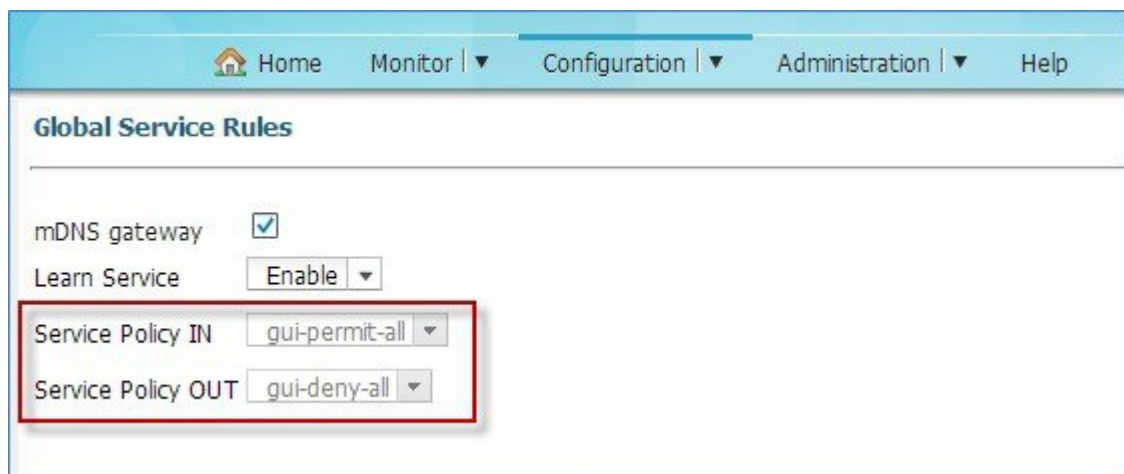
Step 1 Create one WLAN for clients with any security type and another WLAN for AppleTV with security set to WPA2-PSK. Map the WLANs to the respective interfaces. The example below is of WLAN for AppleTV.

The figure shows two screenshots of the Cisco Wireless Controller configuration interface. The top screenshot shows the 'WLANs > Create New' page. The 'WLAN ID' is set to 2, the 'SSID' is 'POD1-AppleTV', and the 'Profile Name' is 'POD1-AppleTV'. The 'Apply' button is highlighted with a red arrow. The bottom screenshot shows the 'WLAN > Edit' page for the 'POD1-AppleTV' profile. The 'Type' is 'WLAN', the 'SSID' is 'POD1-AppleTV', and the 'Status' checkbox is checked. The 'Interface/Interface Group(s)' is set to 'bonjour'. The 'Apply' button is also highlighted with a red arrow.

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**.



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**.



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.

The screenshot shows the Cisco Wireless Controller interface. The top navigation bar includes 'Home', 'Monitor', 'Configuration', 'Administration', and 'Help'. The 'Monitor' tab is selected. On the left sidebar, under 'Clients', the 'Client Details' link is highlighted. The main content area displays a table of connected 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:

The screenshot shows the 'Client > Detail' page for an Apple TV. The 'General' tab is selected. The 'Client Properties' section shows the following details:

- 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

The 'AP Properties' section shows the following details:

- 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:

The screenshot shows the 'Client > Detail' page for an iOS Client. The 'General' tab is selected. The 'Client Properties' section shows the following details:

- 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

The 'AP Properties' section shows the following details:

- 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**.



```
show mdns cache
```

```
WLC5760#sh ndns cache
```

352238

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**.

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**.

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.



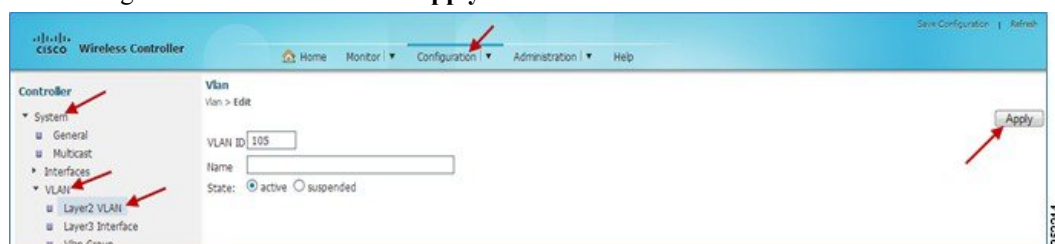
- The status bar of the Apple device will turn blue along with adding an icon for AirPlay, signifying that you are broadcasting your screen on the Apple TV.



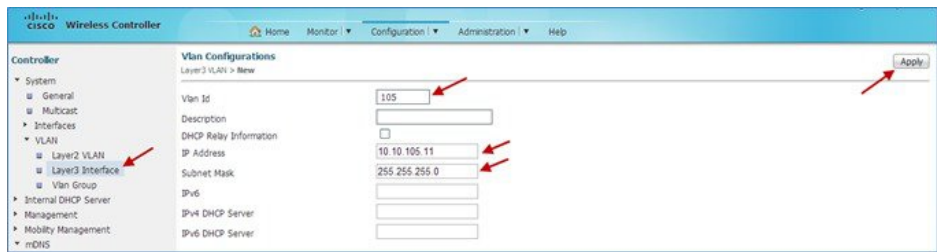
Accessing Bonjour Printer Service

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:

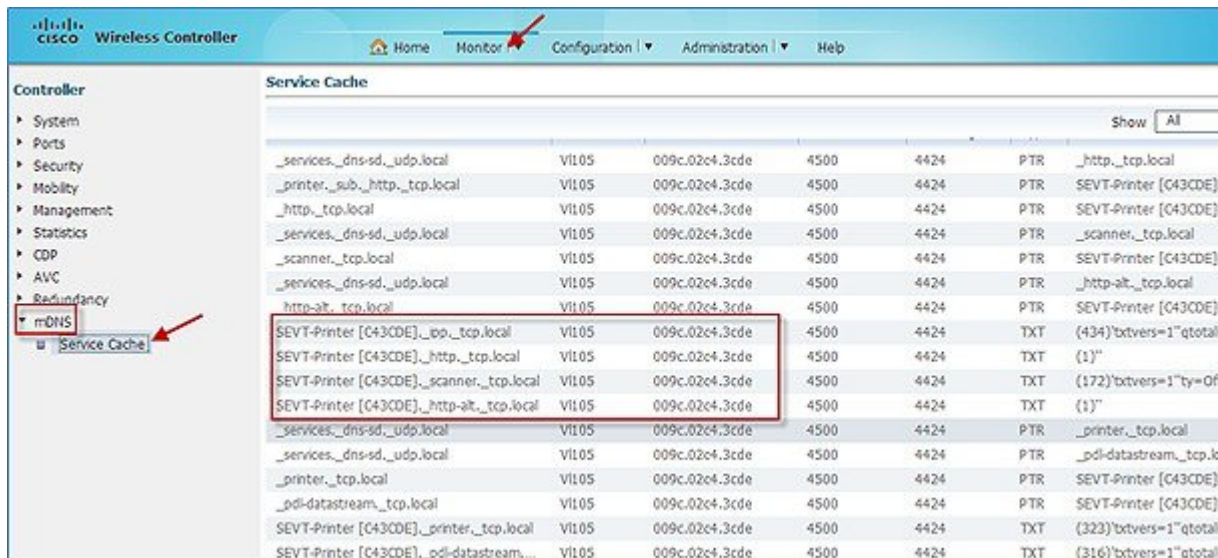
- 1 Create a VLAN interface on the WLC on which the Bonjour Printer is connected (In this example, it is VLAN 105) by navigating to **Configuration > Controller > System > VLAN > Layer2 VLAN** and click **New**. Assign the VLAN ID and click **Apply**.




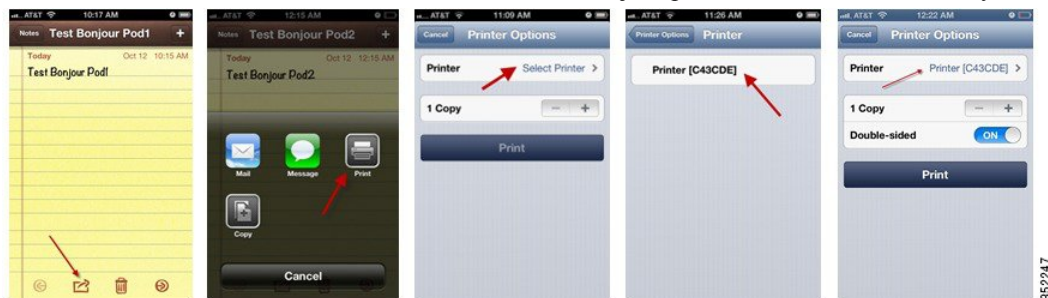
- 2 Similarly, create a L3 interface by navigating to **Configuration > Controller > System > VLAN > Layer3 Interface** and click **New**. Assign the **VLAN Id** and **IP Address** and click **Apply**.



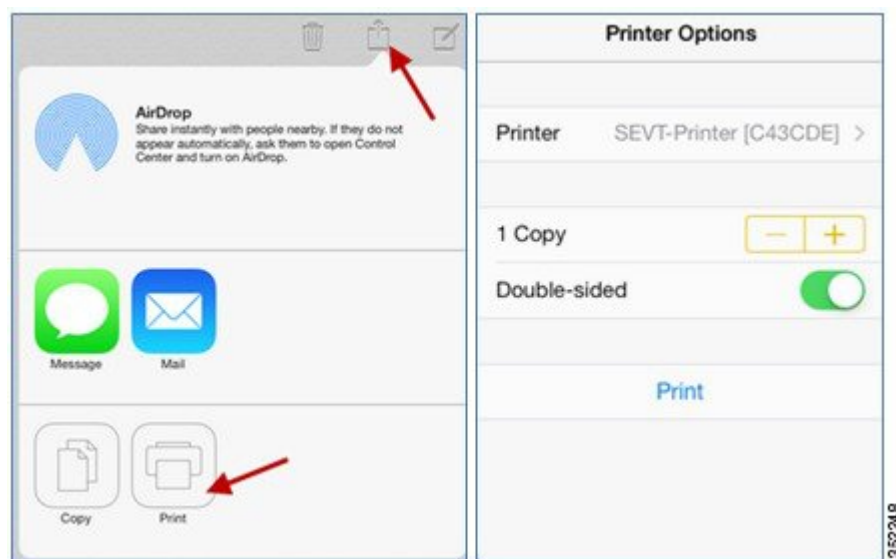
- 3 To check if the Bonjour Printer service is being discovered and cached by the WLC, navigate to **Monitor > Controller > mDNS > Service Cache** and you will see the printer being discovered and cached as shown below.



- 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.

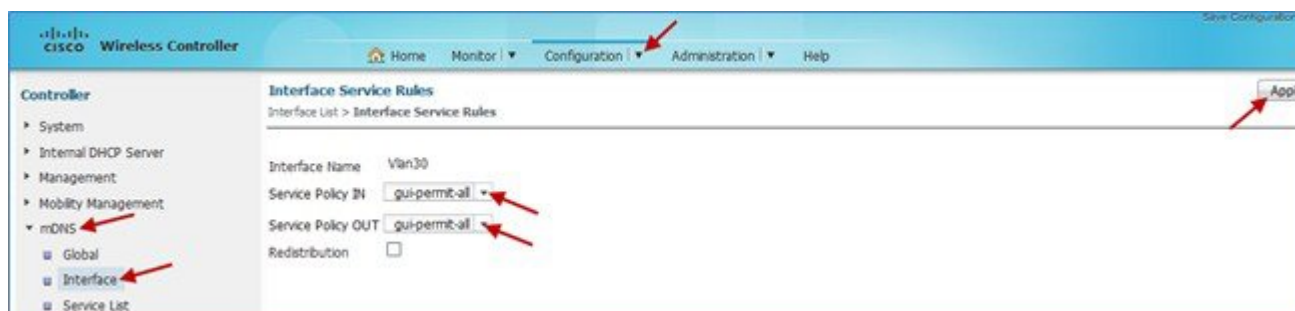


- 5 In iOS7, from the application, click the icon  and then click **Print**. Select the **Printer** under **Printer Options** as shown below.



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.



Creating Service List

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

**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).

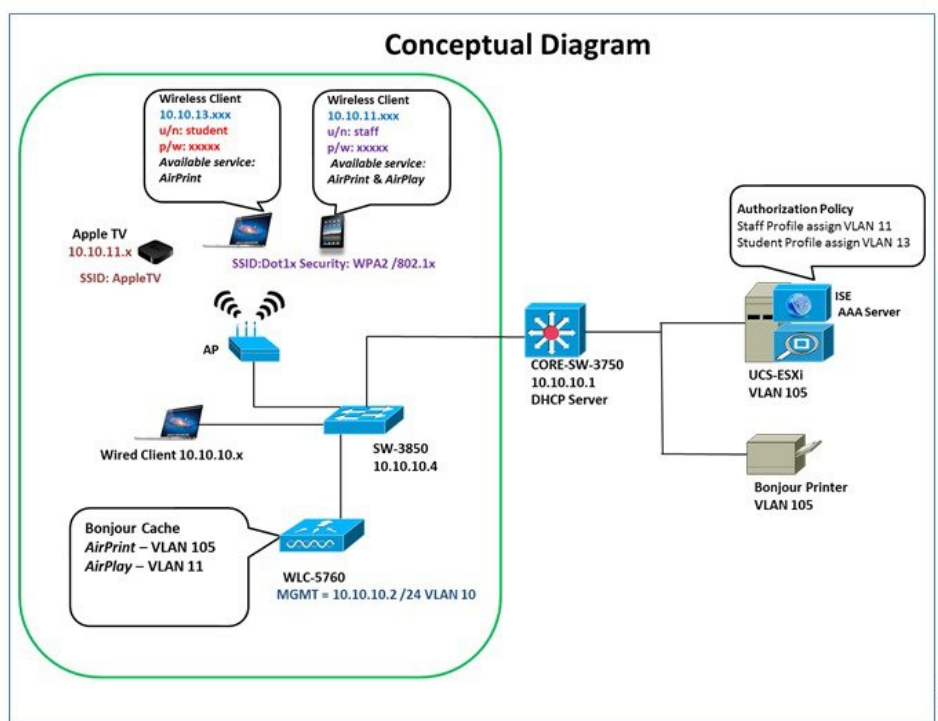
You can have different filters based on your network requirements:

- 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

WLAN ID

SSID

Profile Name

352251

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 ☐

352252

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

Accounting Method Disabled

Local EAP Authentication ☐

352253

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**.

WLAN
WLAN > Edit

General Security QOS AVC **Advanced**

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
 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 ☐

Apply

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.

CISCO Wireless Controller

Home Monitor Configuration Administration Help

Controller

- System
 - General
 - Multicast
 - Interfaces
 - VLAN
 - Internal DHCP Server
 - Management
 - Mobility Management
 - mDNS**
 - Global
 - Interface
 - Service List**

Service List

CreateService Remove

	Service List name	Service Rule	Sequence Number
<input type="checkbox"/>	gui-deny-all	deny	20
<input type="checkbox"/>	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:

Service rule:

Sequence number:

Match Criteria

Message type:

Service instance:

service Type

Custom:

Learned Services

- _http-alt._tcp.local
- _touch-able._tcp.local
- _raop._tcp.local
- _sleep-proxy._udp.local
- _airplay._tcp.local**

Selected Service

352256

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:

Service rule:

Sequence number:

Match Criteria

Message type:

Service instance:

service Type

Custom:

Learned Services

- _printer._tcp.local
- _scanner._tcp.local
- _ipp._tcp.local
- _pdf-datastream._tcp.local
- _http._tcp.local

Selected Service

_airplay._tcp.local

352257

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

Service List Name:

Service rule:

Sequence number:

Match Criteria

Message type:

Service instance:

service Type

Custom: Add

Learned Services:

- _printer._tcp.local
- _scanner._tcp.local
- _pdl-datastream._tcp.local
- _http._tcp.local
- _http-alt._tcp.local

Selected Service:

- _ipp._tcp.local

Apply

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.

Controller

- System
 - General
 - Multicast
- Interfaces
 - VLAN
 - Layer2 VLAN
 - Layer3 Interface
 - Vlan Group
 - Internal DHCP Server
 - Management
 - Mobility Management
 - mDNS
 - Global
 - Interface
 - Service List

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

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: ☐

Apply

362260

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.



mDNS CLI Configuration

Below is a list of commands to enable Bonjour Gateway solution on the Converged access products through CLI.

To enable mDNS gateway, issue the following CLI in global-config mode:

```
Service-routing mdns-sd
```

Creating Service Lists and Filters

Service filters are available to control the mDNS messages coming into and going out from the cache. Service filters can contain several permit or deny statements matching a certain part of the mDNS record which make up the filter. Service filters use regular expressions for string matching (e.g. service type matching or instance name matching).



Note

Service filters must be specified to allow records into and out of the cache since 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.

Elements of a service filter are numbered and either deny or permit the service record based on a match. There is an implicit 'deny anything' at the end of the list.

To apply a filter for incoming and outgoing mDNS messages, issue the following CLI in global-config or interface-config mode:

```
service-list mdns-sd <name>{permit|deny} <sequence_number> ( from 0-100)
    match message-type {query|announcement|any}
    match service-instance <instance-name>
    match service-type <DNS service type string>
```

Below is an example of Service Filter, which denies service type AirPlay and allows service type AirPrint.

```
service-list mdns-sd Deny-AirPlay deny 10
    match service-type _airplay._tcp.local

service-list mdns-sd Deny-AirPlay permit 20
    match service-type _ipp._tcp.local
```

Applying Service Policy on Interface

The service policy can be applied per interface as shown below:

Example:

```
interface Vlan30
ip address 10.10.30.2 255.255.255.0
ip helper-address 10.10.30.1
```

```

service-routing mdns-sd
  service-policy gui-permit-all IN
  service-policy gui-permit-all OUT

```

To redistribute service announcements received on one interface over all the interfaces or over a specific interface, issue the following CLI on the respective interface on which you want to enable redistribution.

Example:

```

interface Vlan30
ip address 10.10.30.2 255.255.255.0
ip helper-address 10.10.30.1
service-routing mdns-sd
  service-policy gui-permit-all IN
  service-policy gui-permit-all OUT
redistribute mdns-sd

```

Enabling Active Queries

Because there are devices that do not send unsolicited announcements, and to force learning of services and keeping them refreshed in the cache, the active query feature is added which ensures that services listed in the active query list will be queried.

```

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

```

The service list of queries thus created can be applied under global service routing mdns-sd to start active browsing of the services as shown below:

```

Service-routing mdns-sd
service-policy-query <service-list name> periodicity <in seconds>

```

Maintenance and Troubleshooting

This section primarily consists of the various show commands and the ability to clear the cache or associated counters as outlined above. In addition, a 'debug mdns' command is available to debug various aspects of the SDG subsystem as shown here:

```

mdns-iol#debug mdns ?
  all      MDNS all debugs
  api      MDNS api enter/exit log
  error    MDNS error debugs
  event    MDNS event debugs
  packet   MDNS packet dumps debug
  verbose  MDNS Verbose debug

```

Show Commands

```

Router#show mdns cache
Shows mDNS cache records

```

```

Router#show mdns cache ?
  interface  Enter the Interface
  name       Record Name
  type       Record Type

```

```

Router#show mdns requests
Shows mDNS Requests Pending

```

```

Router#show mdns statistics all
Shows all mDNS stats

```

```

Router#show mdns statistics ?
  all          Displays Statistics of all
  service-list Entire Service list details in cache
  service-policy Show service-policy statistics

```

mDNS Clear Commands

```
Router#clear mdns ?
  cache          Clear MDNS feature
  statistics     MDNS stats
```

