Managing Bonjour Services for BYOD

Revised: August 7, 2013

Executive Summary

This chapter focuses on how to use the Cisco Wireless LAN Controller software Bonjour Gateway feature to manage Apple's Bonjour protocol in a BYOD enterprise context.

Bonjour is Apple's zero-configuration protocol for advertising, discovering, and connecting to network services like file sharing, print sharing, media sharing, etc. The Bonjour protocol was originally designed for home network use and utilizes Multicast Domain Name Services (mDNS) via link-local multicasting to share network services. While this approach works well in home networks, a limitation of link-local multicasting is that these network services will only be shared within a single Layer 2 domain (such as a VLAN or WLAN). In a BYOD enterprise scenario, different WLANs and VLANs are used for different classes of devices, including corporate devices, employee devices, personal devices, and guest devices (as well as quarantine WLANs for unapproved devices). As such, basic Bonjour operations—such as printing to a wired printer from a wireless LAN—may not be natively supported.

To address this limitation and to facilitate the user demand of BYOD for Apple devices within the enterprise, Cisco has developed the Bonjour Gateway feature for its Wireless LAN Controllers (WLCs). This feature was introduced in Cisco WLC software version 7.4 and solves the Layer 2 domain limitation for Bonjour by allowing the WLC to snoop, cache, and proxy-respond to Bonjour service requests that may reside on different Layer 2 domains. Additionally, these responses may be selectively controlled by administrative policies, so that only certain Bonjour services will be permitted in specific Layer 2 domains.

This chapter provides an overview of the Bonjour protocol and shows how the Bonjour Gateway feature functions, as well as how it can be practically deployed in an enterprise BYOD context to manage Bonjour services. To this end, step-by-step configuration guidance and verification commands are presented, both for the Cisco WLC GUI as well as the Command Line Interface (CLI).

Why Bonjour?

Bonjour is Apple's implementation of a suite of zero-configuration networking protocols and is supported on both Mac OS X devices (such as laptops and desktops), as well as on Apple iOS devices (such as iPhones and iPads). Bonjour is designed to make network configuration easier for users.

For example, consider enabling IP-based print services. Each printer needs a unique IP address, whether statically assigned or dynamically assigned (by a DHCP server). Since dynamically-assigned addresses can change, most printers are manually configured with a static address so that computers on the network can reach them using the same address every time. In this case, each client device must know the statically configured IP address of the printer(s) in order to use these. To make the process more user friendly, network administrators may configure DNS records so that clients can access printers by name, rather than by specific IP addresses. Even so, the clients must know the specific DNS name of each printer they are trying to access. Thus, the seemingly minor task of enabling IP-based printing can require significant client and server configuration. Additionally, in a home network environment, people who do not fit the traditional role of the network administrator often set up networks (e.g., families connecting their laptops and personal devices to the Internet over a shared router). As such, this level of configuration simply is not practical in such a setting.

Consider the same example in a network running Bonjour. Bonjour lets you connect a printer to your network without assigning it a specific IP address or manually entering that address into each computer. With zero-configuration networking, nearby computers can discover its existence and automatically determine the printer's IP address. If that address is a dynamically assigned address that changes, they can automatically discover the new address in the future.

Bonjour functionality is not limited to printing and includes:

- File Sharing Services
- Remote Desktop Services
- Full screen Mirroring (Apple iOS v5.0+ for iPad2, iPhone4S, or later)
- iTunes Services:
  - iTunes File Sharing
  - iTunes Wireless iDevice Syncing (Apple iOS v5.0+)
  - Music broadcasting (Apple iOS v4.2+)
  - Video broadcasting (Apple iOS v4.3+)

Bonjour's zero-configuration networking services benefit not only users (who will no longer have to assign IP addresses or host names to access network services), but also applications (as applications can leverage Bonjour to automatically detect required services or to interact with other applications to allow for automatic connection, communication, and data exchange, all without any user configuration).

Bonjour Overview

Bonjour offers zero-configuration solutions for three areas of IP networking:

- Addressing (allocating IP addresses to hosts)—Bonjour Addressing
- Naming (using names to refer to hosts instead of IP addresses)—Bonjour Naming
- Service discovery (finding services on the network automatically)—Bonjour Service Discovery

Each of these areas is discussed in turn, as well as how Bonjour optimizes the delivery of these solutions.

Bonjour Addressing

Bonjour solves the addressing problem of allocating IP addresses to hosts by leveraging self-assigned link-local addressing. Link-local addressing uses a range of addresses reserved for the local network and is achieved differently by IPv6 and IPv4:

- IPv6 includes self-assigned link-local addressing as part of the protocol
- IPv4 self-assigned addressing works by picking a random IP address in the link-local range and testing it. If the address is not in use, it becomes the local address. If it is already in use, the computer or other device chooses another address at random and tries again.

Any user or service on a computer or iOS device that supports link-local addressing benefits from this feature automatically. When a host computer joins a local network, it finds an unused local address and adopts it. No user action or configuration is required.

Bonjour Naming

Bonjour leverages Multicast DNS (mDNS) for name-to-address translation, which sends DNS-format queries over the local network using an IP multicast address. Because these DNS queries are sent to a multicast address, no single DNS server with global knowledge is required to answer the queries. Each service or device can provide its own DNS capability—when it sees a query for its own name, it provides a DNS response with its own address.

Actually, Bonjour goes a bit further than basic mDNS functionality by including a responder that handles mDNS queries for any network service on the host computer or iOS device. This relieves an application of the need to interpret and respond to mDNS messages. Once a service is registered with the Bonjour process, Bonjour automatically advertises the availability of the service so that any queries for it are directed to the correct IP address and port number automatically.

Note Registration is performed using one of the Bonjour APIs. This functionality is available only to services running on the host OS X computer or iOS device. Services running on other devices, such as printers, need to implement a simple mDNS responder daemon that handles queries for services provided by that device (which is included on printers supporting the Apple AirPrint feature).

Bonjour also provides built-in support for the NAT port mapping protocol (NAT-PMP). If the upstream router supports this protocol, OS X and iOS applications can create and destroy port mappings to allow hosts on the other side of the firewall to connect to the provided services.

For name-to-address translation to work properly, a unique name on the local network is necessary. Unlike conventional DNS host names, the local name only has significance on the local network or LAN segment. A local name can be assigned much the same way as a self-assigned a local address: a name is chosen and if it is not already in use, it gets used. If it is unavailable, then the name can be modified slightly and re-tested for availability. For example, if a printer with the default name XYZ-LaserPrinter.local attaches to a local network with two other identical printers already installed, it tests for XYZ-LaserPrinter.local, then XYZ-LaserPrinter-**2**.local, then XYZ-LaserPrinter-**3**.local, which is unused and which becomes its name.

Bonjour Naming Rules

This section explains the Bonjour local "domain" and the naming rules for Bonjour service instances and service types. These service names are snooped by and presented within the Cisco WLC and as such are helpful for an administrator to understanding.

Bonjour protocols deal primarily with local link service advertisements. A host's link-local network includes itself and all other hosts that can exchange packets without IP header data being modified (i.e., hosts sharing a single layer 2 domain/VLAN). In practice, this includes all hosts not separated by a router. On Bonjour systems, "local." is used to indicate a name that should be looked up using an mDNS query on the local IP network.

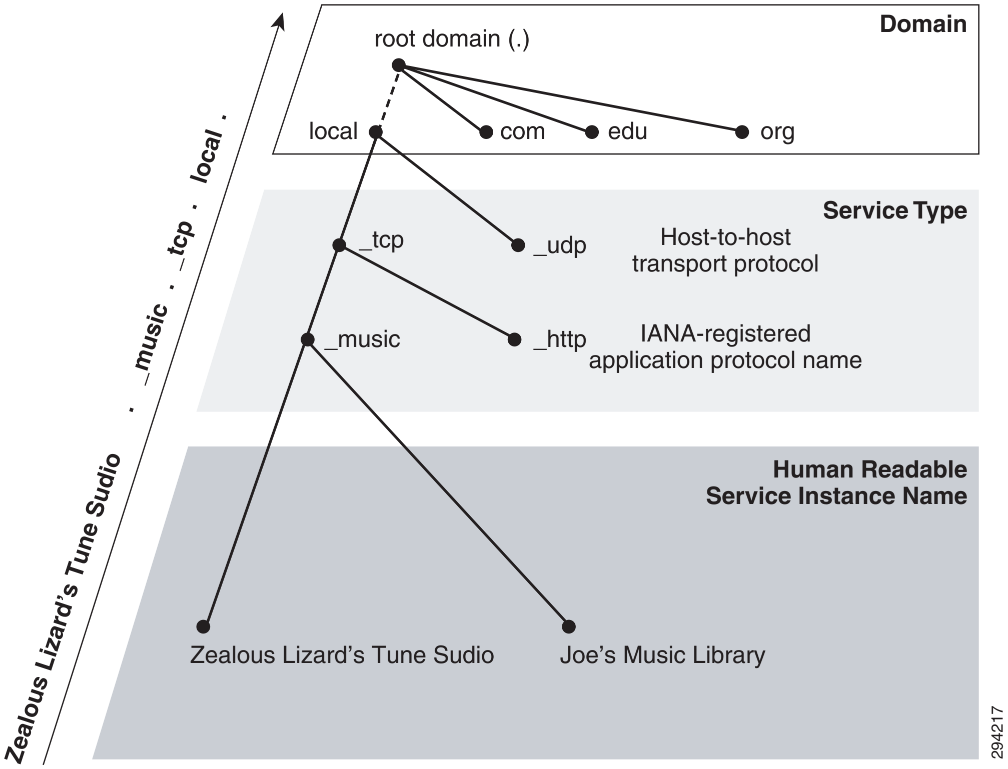
Note that “local.” is not really a domain, but rather a pseudo-domain. It differs from conventional DNS domains in a fundamental way: names within DNS domains are globally unique; link-local domain names are not. As such, local names are useful only on the local network. In many cases this is adequate, as these provide a way to refer to network devices using names instead of IP numbers and of course they require less effort to coordinate and administer as compared to globally unique names.

Locally unique names are particularly useful on networks that have no connection to the global Internet, either by design or because of interruption, and on small, temporary networks, such as a pair of computers linked by a crossover cable or a few people playing network games using laptops on the wireless network of a home or cafe.

Note If a name collision on the local network occurs, a Bonjour host finds a new name automatically (in the case of an iOS device) or by asking the user (in the case of an OS X personal computer).

Bonjour service instance names are intended to be user-readable strings with descriptive names. Figure 25-1 illustrates the organization of the name of a Bonjour service instance. At the top level of the tree is the domain, such as “local.” for the local network. Below the domain is the registration type, which consists of the service type preceded by an underscore (_music) and the transport protocol, also preceded by an underscore (_tcp). At the bottom of the tree is the human-readable service instance name, such as Zealous Lizard's Tune Studio. The complete name is a path along the tree from bottom to top, with each component separated by a dot.

Figure 25-1 ***Bonjour Service Name Hierarchy and Organization***



Other Bonjour service name suffixes include:

- _ipp._tcp.local. for AirPrint Printers
- _printer._tcp.local. for generic IP Printers

- _airplay._tcp.local. for AppleTV

Bonjour Service Discovery

The final element of Bonjour is service discovery. Service discovery allows applications to find all available instances of a particular type of service and to maintain a list of named services and port numbers. The application can then resolve the service hostname to a list of IPv4 and IPv6 addresses, as previously described.

The list of named services provides a layer of indirection between a service and its current DNS name and port number. Indirection allows applications keep a persistent list of available services and resolve an actual network address just prior to using a service. The list allows services to be relocated dynamically without generating a lot of network traffic announcing the change.

Service discovery in Bonjour is accomplished by "browsing." An mDNS query is sent out for a given service type and domain, and any matching services reply with their names. The result is a list of available services to choose from.

This is very different from the traditional device-centric paradigm of network services, which describes services in terms of physical hardware. In a device-centric view, the network consists of a number of devices or hosts, each with a set of services. In a device-centric browsing scheme, a client queries the server for what services it is running, gets back a list (FTP, HTTP, print-services and so on), and decides which service to use. The interface reflects the way the physical system is organized. But this is not necessarily what the user logically wants or needs.

On the other hand, a service-centric paradigm is typically more logical and efficient from a user-perspective. Users typically want to accomplish a certain task, not query a list of devices to find out what services are running. It makes far more sense for a client to ask a single question, "What print services are available?" than to query each available device with the question, "What services are you running?" and sift through the results looking for printers. The device-centric approach is not only time-consuming, but it also generates a significant amount of irrelevant network traffic. In contrast, the service-centric approach sends a single query, generating only relevant replies.

Bonjour takes the service-oriented view. Queries are made according to the type of service needed, not the hosts providing them. Applications store service instance names, not addresses, so if the IP address, port number, or even host name has changed, the application can still connect. By concentrating on services rather than devices, the user's browsing experience becomes more relevant and efficient.

Bonjour Optimization

Server-free addressing, naming, and service discovery have the potential to create a significant amount of excess network traffic, but Bonjour uses several mechanisms to reduce this traffic to a minimum to avoid unnecessary "chattiness", including:

- Caching
- Suppression of Duplicate Responses
- Exponential Back-Off and Service Announcement

Each of these Bonjour optimization mechanisms is briefly described in the following sections.

Caching

Bonjour uses a cache of mDNS records to prevent hosts from requesting information that has already been requested. For example, when one host requests, say, a list of print spoolers, the list of printers comes back via multicast, so all local hosts see it. The next time a host needs a list of print spoolers, it already has the list in its cache and does not need to reissue the query.

Suppression of Duplicate Responses

To prevent repeated answers to the same query, Bonjour service queries include a list of known answers. For example, if a host is browsing for printers, the first query includes no print services and gets, say, twelve replies from available print servers. The next time the host queries for print services, the query includes a list of known servers. Print servers already on the list do not respond.

Bonjour also suppresses duplicate responses in another way. If a host is about to respond, and notices that another host has already responded with the same information, the host suppresses its response.

Exponential Back-off and Service Announcement

When a host is browsing for services, it does not continually send queries to see if new services are available. Instead, the host issues an initial query and sends subsequent queries exponentially less often, for example: after 1 second, 3 seconds, 9 seconds, 27 seconds, and so on, up to a maximum interval of one hour.

This does not mean that it can take over an hour for a browser to see a new service. When a service starts up on the network, it announces its presence a few times using a similar exponential back-off algorithm. This way, network traffic for service announcement and discovery is kept to a minimum, but new services are seen very quickly.

Cisco Bonjour Gateway Solution in WLC 7.4+

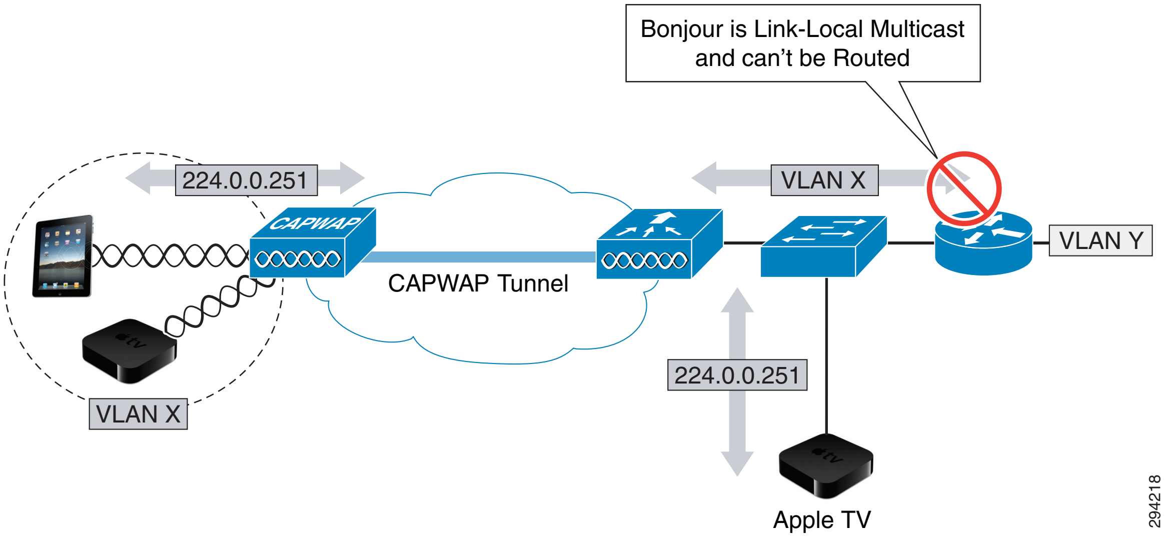
As previously discussed, the Bonjour protocol uses mDNS queries. These queries are sent over UDP port 5353 to the reserved group addresses listed below:

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

However it should be noted that the mDNS addresses used by Bonjour are link-local multicast addresses and are only forwarded within the local Layer 2 domain, as link-local multicast is meant to stay local by design. Furthermore, routers cannot even use multicast routing to redirect the mDNS queries, because the time-to-live (TTL) of these packets is set to 1.

Bonjour was originally developed with home networks in mind. As such, since most home networks consist of a single Layer 2 domain, this link-local limitation of mDNS rarely posed any practical deployment constraints. However in an enterprise context, where large numbers of (wired and wireless) Layer 2 domains exist, this limitation severely handicaps Bonjour functionality, as Bonjour clients would only see locally-hosted services and would not be able to see or connect to services hosted on other subnets. This link-local multicast limitation of Bonjour mDNS is illustrated in Figure 25-2.

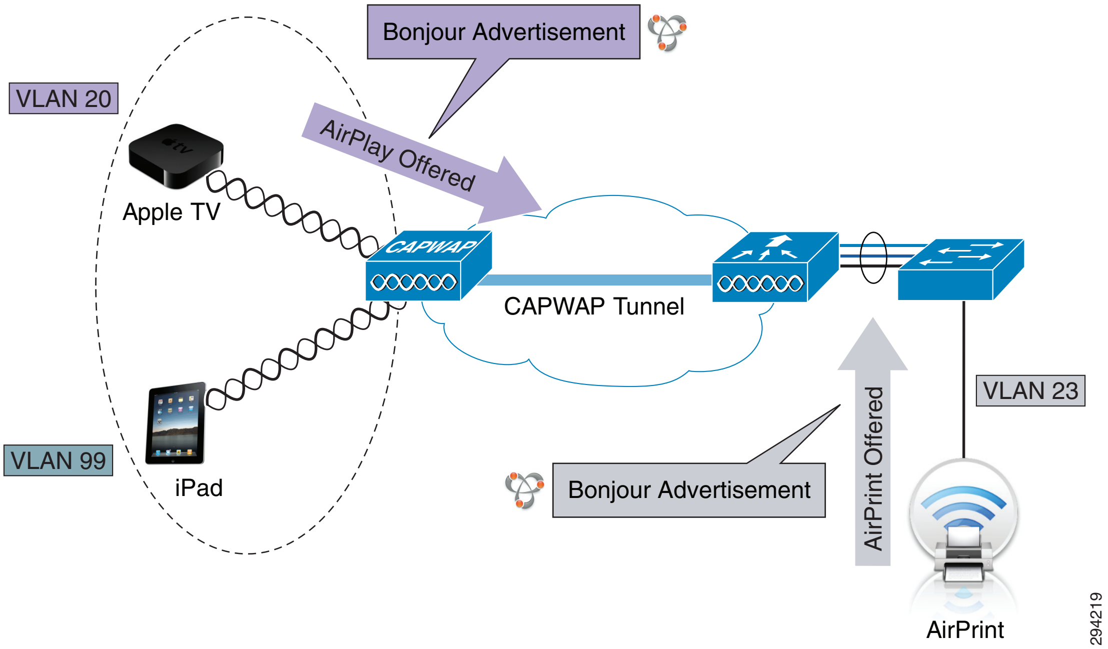
Figure 25-2 Bonjour Deployment Limitation in Enterprise Networks



To address this limitation and to facilitate BYOD functionality on enterprise networks, Cisco released a Bonjour Gateway feature in WLC 7.4+ software. The Bonjour Gateway feature (technically speaking a mDNS gateway feature, but most relevantly applied to Bonjour) snoops and caches all Bonjour service advertisements across multiple VLANs and can be configured to (selectively) reply to Bonjour queries. Figure 25-3 through Figure 25-5 illustrate the operation of the Bonjour Gateway.

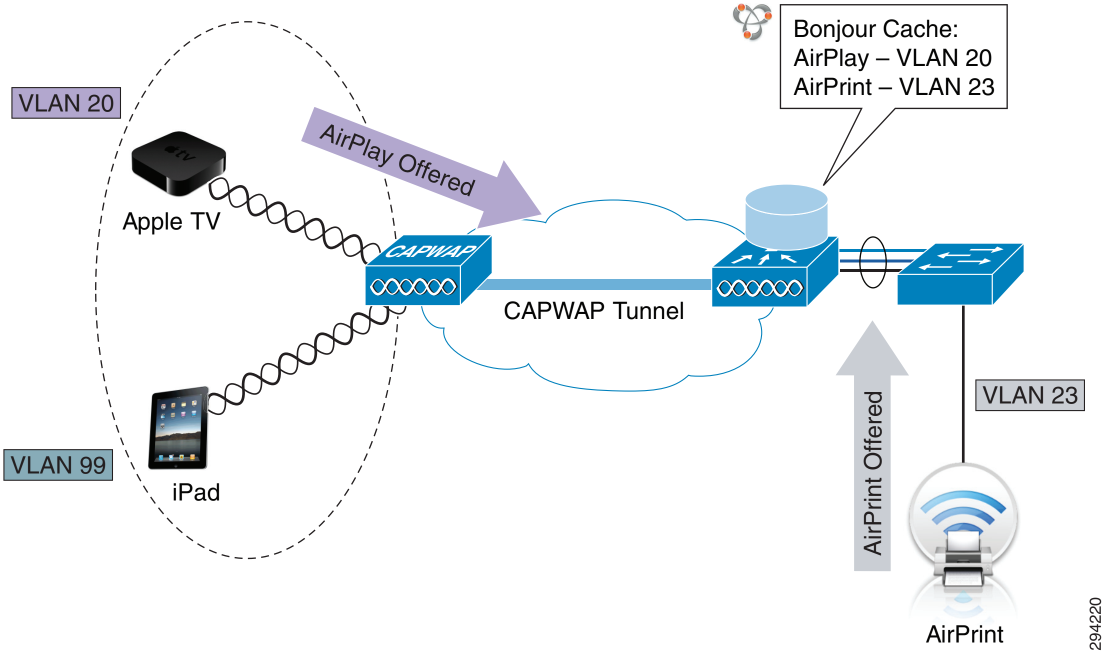
In Figure 25-3, the Bonjour Gateway listens/snoops all Bonjour advertisements.

Figure 25-3 Cisco WLC Bonjour Gateway Operation—Step 1—Bonjour Service Advertisement Snooping



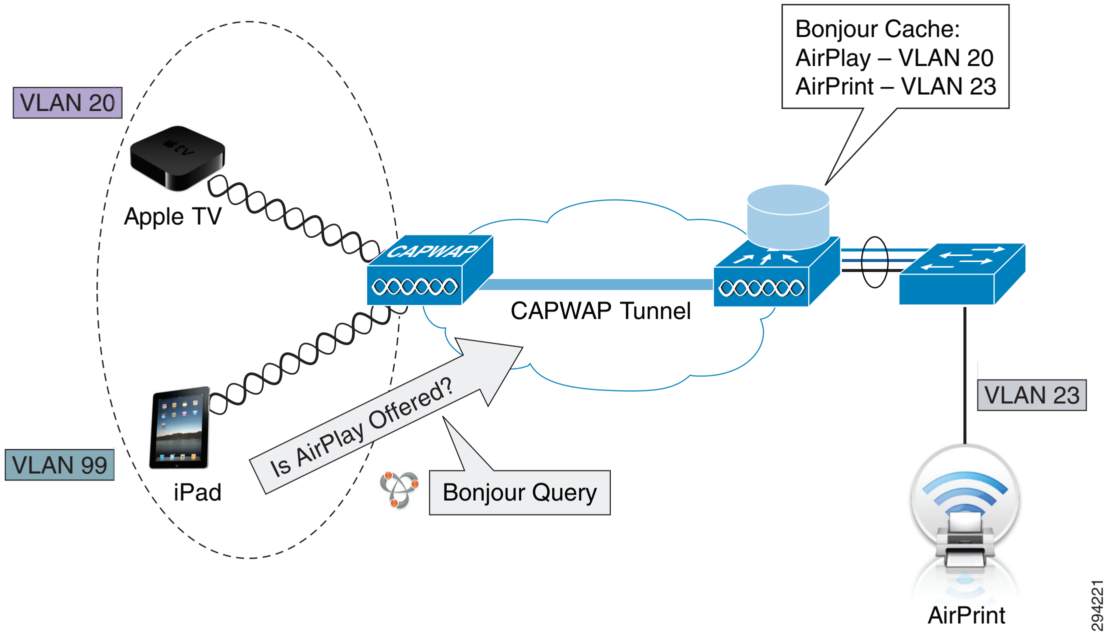
Next, the Bonjour Gateway caches all these service advertisements, as shown in Figure 25-4. Incidentally, the WLC 7.4 release supports up to 64 services and 100 service providers per service type. Each service provider is registered in the WLC as its domain name. Additionally, each Bonjour service has an advertised TTL (which is different from a packet's TTL) and the controller asks the device for an update at 85% of this TTL.

Figure 25-4 Cisco WLC Bonjour Gateway Operation—Step 2—Service Advertisement Caching



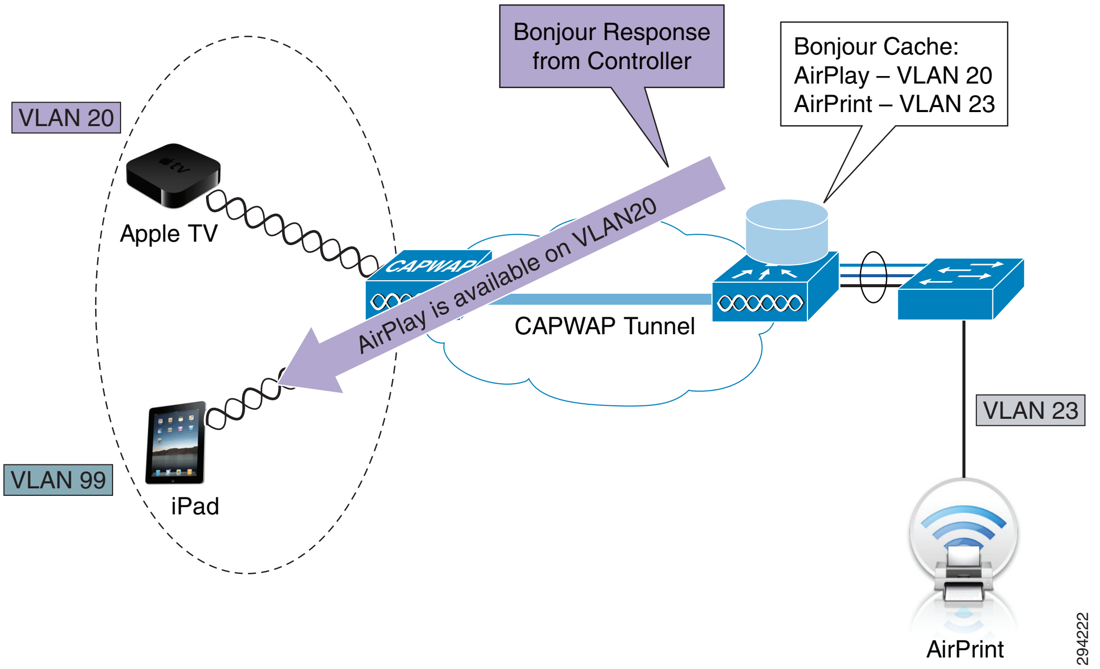
In addition to listening to service advertisements, the WLC is always listening for client queries for services, as illustrated in Figure 25-5.

Figure 25-5 Cisco WLC Bonjour Gateway Operation—Step 3—Bonjour Query Snooping



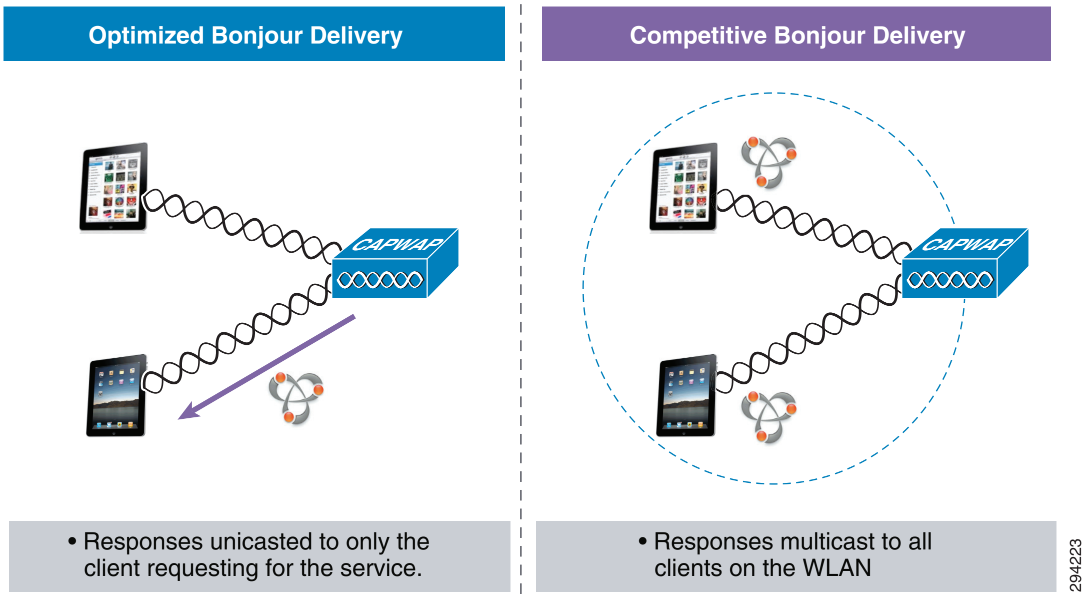
Clients that request locally-hosted services will receive unicast replies from the service provider; however clients that request services that may be hosted on other VLANs will receive unicast responses from the WLC, as shown in Figure 25-6.

Figure 25-6 Cisco WLC Bonjour Gateway Operation—Step 4—Bonjour Query Response (from Cache)



And finally, the Bonjour Gateway service can serve to further optimize Bonjour traffic by unicasting replies directly to clients requesting a given service (as opposed to multicasting replies like some competitive solutions), making more efficient use of network resources, as shown in Figure 25-7.

Figure 25-7 Cisco WLC Bonjour Gateway Operation versus Competitive Offering Operation


Optimized Bonjour Delivery
Competitive Bonjour Delivery
CAPWAP
CAPWAP
• Responses unicasted to only the client requesting for the service.
• Responses multicast to all clients on the WLAN
294223

Bonjour Gateway Service Policy Deployment Options

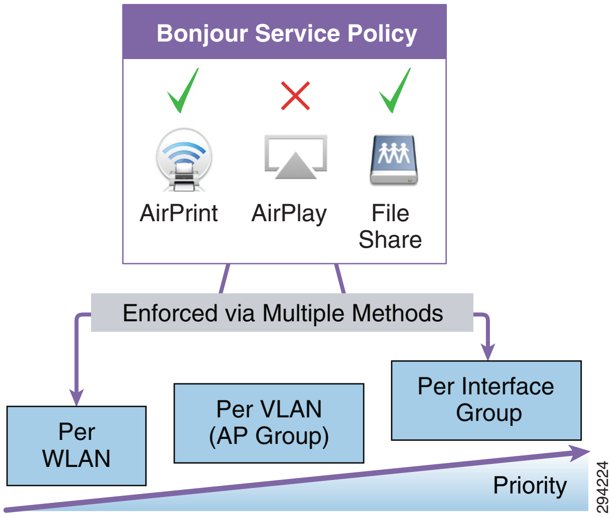
A key functional advantage of the Bonjour Gateway is that it can be configured to selectively reply to Bonjour service requests, thus allowing for administrative control of Bonjour services within the enterprise. Bonjour policies can be applied on the following basis:

- Per WLAN
- Per VLAN
- Per Interface/Interface-Group

Note Per-User Bonjour policy application is planned for a future release via RADIUS AAA-Override.

These Bonjour service policy options are illustrated in Figure 25-8.

Figure 25-8 Cisco WLC Bonjour Gateway Service Policy Deployment Options

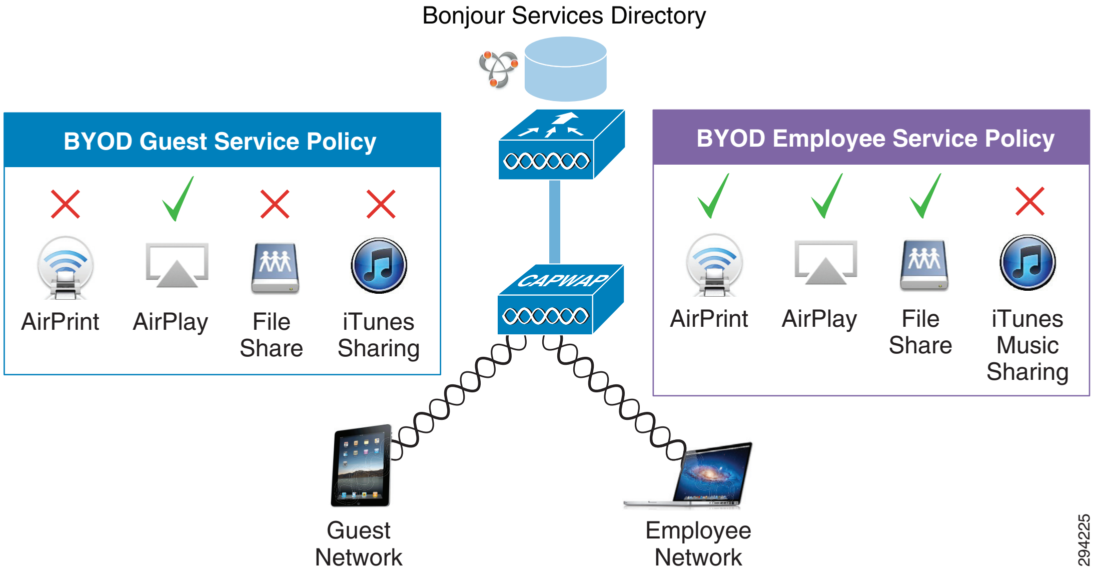


Consider a few examples of how such Bonjour service policies may be deployed. For instance, in an BYOD enterprise context, you can configure Bonjour policies such that employees can take advantage of Bonjour services that enhance productivity (such as AirPrint, AirPlay, and File Sharing), but block entertainment-oriented Bonjour services (such as iTunes Sharing).

Additionally, stricter limitations could be placed on Guest WLANs. For example, inter-domain Bonjour services could be limited to AirPlay only—such that guest devices may be allowed to connect to (wired or wireless) AppleTVs that reside on the production network—so that guests could share presentations, videos, demonstrations, etc.

These example Bonjour service policies for an enterprise BYOD deployment context are illustrated in Figure 25-9.

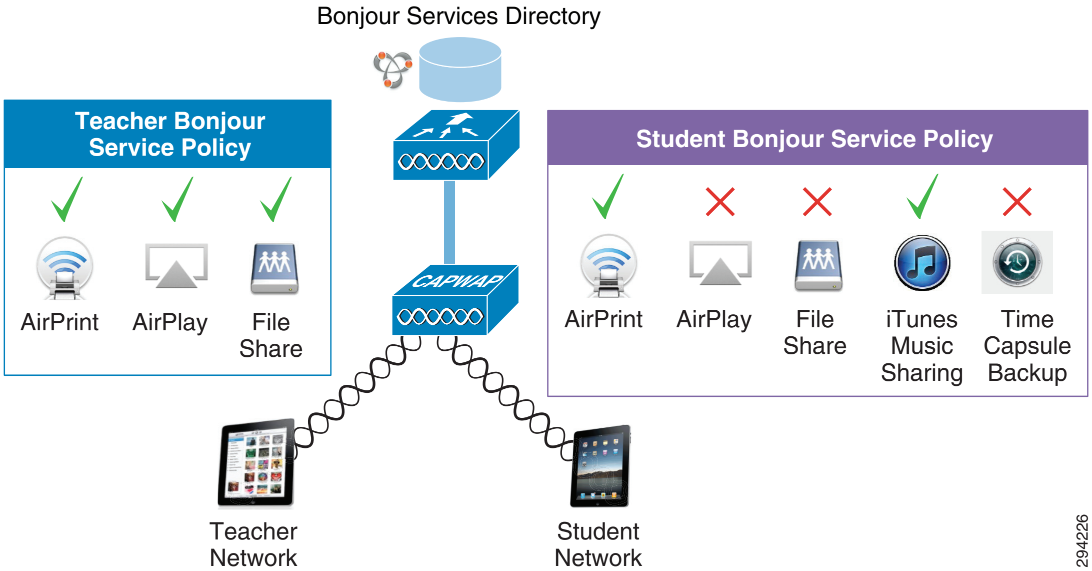
Figure 25-9 Cisco WLC Bonjour Gateway Service Policy Deployment Example 1—A BYOD Enterprise



It is important to note that these Bonjour service policy examples are not a one-size-fits-all solution. The policy-specifics will likely vary according to deployment contexts. As a second example consider a college/university deployment context. In this example, assume separate WLANs for teachers and students. Teachers would likely have all Bonjour productivity-oriented services enabled, such as AirPrint, AirPlay, and File Sharing. However you may wish to limit AirPlay on student networks, as this may prevent significant volumes of traffic traversing different WLANs as students may host full-length HD movies on one network while streaming them to devices on another. Similarly, Time Capsule traffic may be another service to limit from spanning WLANs—again due to the significant traffic loads these typically entail. However, consideration may be extended students by permitting iTunes Music Sharing (as music files are significantly smaller than videos or Time-Capsule backups).

These example Bonjour service policies for a university BYOD deployment context are illustrated in Figure 25-10.

Figure 25-10 Cisco WLC Bonjour Gateway Service Policy Deployment Example 2—A BYOD University



While the specifics of a Bonjour service policy may differ according to deployment context, there are two broad use cases for Bonjour Gateway deployments that are discussed next.

Bonjour Gateway BYOD Use Cases and Configuration Examples

There are effectively two general use cases for Bonjour Gateway service policy deployments:

- Wireless-to-Wired Bonjour Gateway Service Policies—The primary use case is enabling wireless BYOD devices to print to wired AirPrint printers.
- Wireless-to-Wireless Bonjour Gateway Service Policies—Enables Bonjour services to be shared among devices in separate WLANs; an example use case would be to allow guest devices to access wireless AppleTVs to share presentations (even though these devices may reside in different WLANs).

Bonjour service policies on Cisco WLCs can be configured using one of two approaches:

- Editing the default mDNS profile

- Creating new mDNS profiles

Also, mDNS profiles can be applied directly to:

- Interfaces/Interface-Groups
- VLANs
- WLANs

To highlight deployment options, the examples that follow utilize a variety of these options.

Design configuration are presented both via the Cisco WLC GUI and the Cisco WLC CLI. CLI examples show both the general syntax of a command (which is highlighted in **blue**) and the specific variation needed in the design example (which is highlighted in **red**).

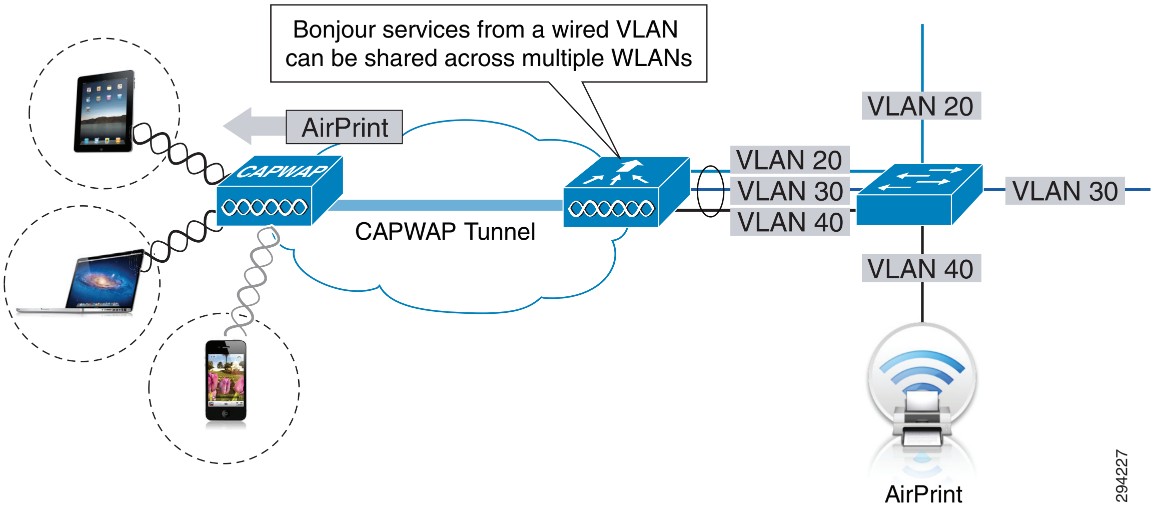
Note In these design examples, it is assumed that the network infrastructure and WLC have been configured in accordance with the best-practice BYOD designs presented in this CVD.

Use Case 1—Wireless-to-Wired Bonjour Gateway Service Policy—BYOD Employee AirPrint Example

In this primary Bonjour Gateway use case, wireless BYOD employee devices are permitted to access AirPrint-enabled printers that are deployed on separate wired networks. Incidentally, this design will also support wireless printing from wireless clients across separate WLANs.

A prerequisite of this design is that the wired VLANs hosting AirPrint printers must be trunked to the Cisco WLC controller, as shown in Figure 25-11.

Figure 25-11 Use-Case 1—Cisco WLC Bonjour Gateway Wireless-to-Wired Design Example



Multiple design and configuration options exist to enable Bonjour service policies. In this example, Bonjour service policies will be configured by:

- Step 1—Globally enabling mDNS snooping
- Step 2—Editing the default mDNS profile
- Step 3—Applying the default profile to an interface

Each of these steps is detailed in turn (with additional design options being presented in the following example).

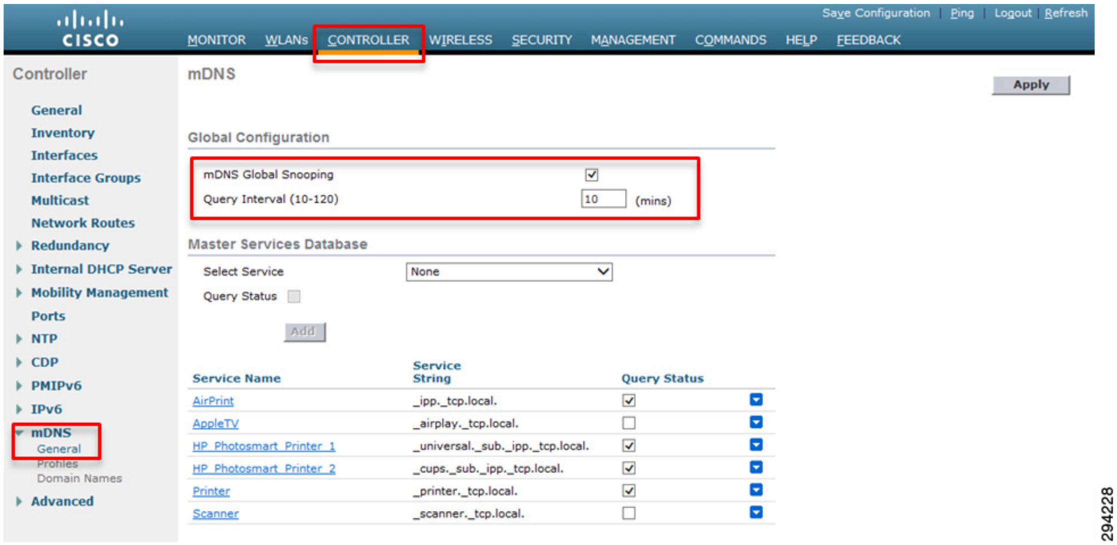
Step 1—Enable mDNS Global Snooping

The first step is to globally enable mDNS snooping by doing the following:

1. Open a web browser to the Cisco WLC IP address via HTTPS and login.
2. Click the **CONTROLLER** heading-bar and expand the **mDNS** link on the lower left and click **General**.
3. Under the **Global Configuration** heading, select the checkbox to enable **mDNS Global Snooping**.
4. Optionally the mDNS Snooping **Query Interval** can be tuned (from 10 min. to 120 min.).

These steps are shown in Figure 25-12.

Figure 25-12 Use-Case 1—Step 1—Enabling mDNS Global Snooping



mDNS

Global Configuration

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

Master Services Database

Select Service None
Query Status □

Service Name	Service String	Query Status
AirPrint	_ipp._tcp.local.	☑
AppleTV	_airplay._tcp.local.	□
HP_Photosmart_Printer_1	_universal._sub._ipp._tcp.local.	☑
HP_Photosmart_Printer_2	_cups._sub._ipp._tcp.local.	☑
Printer	_printer._tcp.local.	☑
Scanner	_scanner._tcp.local.	□

The corresponding Cisco WLC CLI for globally enabling mDNS snooping is shown in Example 25-1.

Example 25-1 Enabling mDNS Global Snooping

```
General command/specific example:
(Cisco Controller) >config mdns snooping enable
! Globally enables mDNS snooping
```

The mDNS snooping query interval can be tuned with the command shown in Example 25-2 (again the range is 10 to 120 minutes). Example 25-2 shows both the general version of this command and the specific syntax to set the mDNS query interval to 10 minutes.

Example 25-2 Tuning the mDNS Query Interval

```
General command:
(Cisco Controller) >config mdns query interval minutes

Specific example:
(Cisco Controller) >config mdns query interval 10
```

```
! Sets the mDNS query interval to 10 minutes
```

These mDNS configuration commands can be verified by the **show network summary** command output, as illustrated in Example 25-3.

Example 25-3 Verifying mDNS Global Snooping and Query Interval—show network summary

```
(Cisco Controller) >show network summary

RF-Network Name............................. byod
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Disable
Secure Web Mode RC4 Cipher Preference....... Disable
OCSP........................................ Disabled
OCSP responder URL..........................
Secure Shell (ssh).......................... Enable
Telnet...................................... Enable
Ethernet Multicast Forwarding............... Disable
Ethernet Broadcast Forwarding............... Disable
IPv4 AP Multicast/Broadcast Mode............ Unicast
IGMP snooping............................... Disabled
IGMP timeout................................ 60 seconds
IGMP Query Interval......................... 20 seconds
MLD snooping................................ Disabled
MLD timeout................................. 60 seconds
MLD query interval.......................... 20 seconds
User Idle Timeout........................... 300 seconds
ARP Idle Timeout............................ 300 seconds
Cisco AP Default Master..................... Disable
AP Join Priority............................ Disable
Mgmt Via Wireless Interface................. Enable
Mgmt Via Dynamic Interface.................. Disable
Bridge MAC filter Config.................... Enable
Bridge Security Mode........................ EAP
Mesh Full Sector DFS........................ Enable
AP Fallback ................................ Enable
Web Auth CMCC Support ...................... Disabled
Web Auth Redirect Ports .................... 80
Web Auth Proxy Redirect  ................... Disable
Web Auth Captive-Bypass   .................. Enable
Web Auth Secure Web  ....................... Enable
Fast SSID Change ........................... Enabled
AP Discovery - NAT IP Only ................. Enabled
IP/MAC Addr Binding Check .................. Enabled
CCX-lite status ............................ Disable
oeap-600 dual-rlan-ports ................... Disable
oeap-600 local-network ..................... Enable
oeap-600 Split Tunneling (Printers)......... Disable
WebPortal Online Client .................... 0
mDNS snooping............................... Enabled
mDNS Query Interval......................... 10 minutes
<snip>
```

Step 2—Editing the Default mDNS Profile

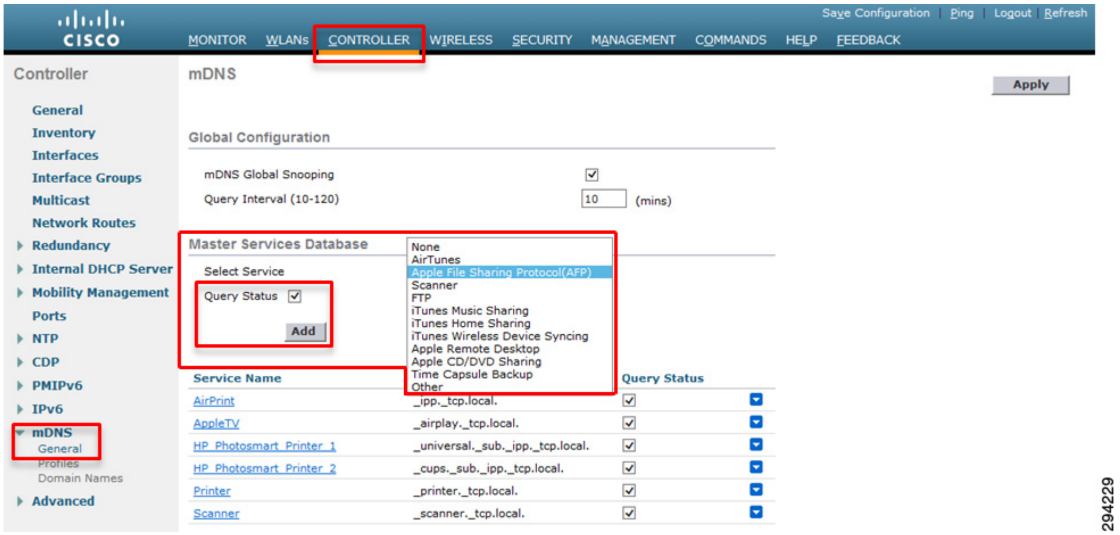
Additional Bonjour services may be added to the default mDNS profile (or even removed from it). To add additional Bonjour services, perform the following:

1. Select the Bonjour Service to be added from the **Master Services Database** drop-down list.

2. Enable the **Query Status Checkbox** for the service.
3. Click the **Add** button.
4. The added service will subsequently appear under the Service Name bar (in alphabetical order).

Figure 25-13 shows the Apple File Sharing Protocol (AFP) service being added to the default mDNS profile.

Figure 25-13 Use-Case 1—Step 2—Adding Bonjour Services to the Default mDNS Profile



mDNS

Global Configuration

mDNS Global Snooping ☑

Query Interval (10-120) 10 (mins)

Master Services Database

Select Service Apple File Sharing Protocol(AFP)

Query Status ☑

Service Name		Query Status
AirPrint	_ipp._tcp.local.	☑
AppleTV	_airplay._tcp.local.	☑
HP_Photosmart_Printer_1	_universal._sub._ipp._tcp.local.	☑
HP_Photosmart_Printer_2	_cups._sub._ipp._tcp.local.	☑
Printer	_printer._tcp.local.	☑
Scanner	_scanner._tcp.local.	☑

Bonjour services can be added to the default (or non-default) profiles with the command shown in Example 25-4. The Profile Name of the default mDNS profile is "**default-mdns-profile**".

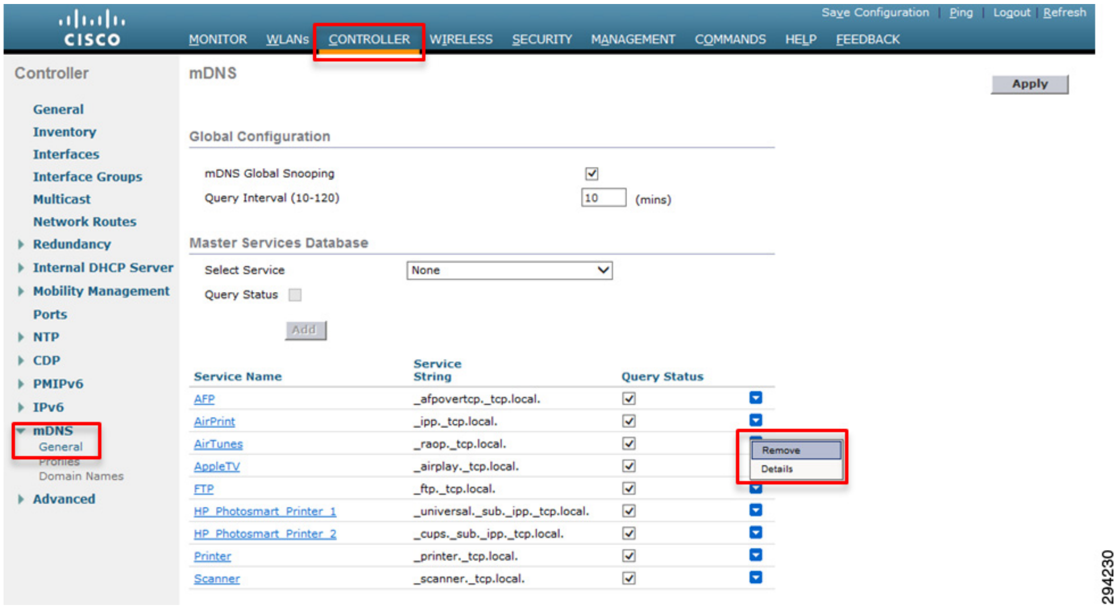
Example 25-4 Adding Bonjour Services to a mDNS Profile

```
General Command:
(Cisco Controller) >config mdns profile service add mdns-profile-name mdns-service-name

Specific example:
(Cisco Controller) >config mdns profile service add default-mdns-profile AirPrint
! Adds the Apple AirPrint service to the default mDNS profile
```

Conversely, services can be removed from the default mDNS profile by clicking the blue-box at the end of the row for the service and then selecting **Remove**.

This is shown in Figure 25-14 where the AirPlay service (the service that allows for iTunes music to be streamed to a remote Apple Airport Express device, which in turn can supply an audio signal of the music to speakers) is removed from the default mDNS profile.

Figure 25-14 Use Case 1—Step 2b—Removing Bonjour Services from the Default mDNS Profile



mDNS

Global Configuration

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

Master Services Database

Select Service None
Query Status □

Service Name	Service String	Query Status
AFP	_afpovertcp._tcp.local.	☑
AirPrint	_ipp._tcp.local.	☑
AirTunes	_raop._tcp.local.	☑
AppleTV	_airplay._tcp.local.	☑
FTP	_ftp._tcp.local.	☑
HP_Photosmart_Printer_1	_universal._sub._ipp._tcp.local.	☑
HP_Photosmart_Printer_2	_cups._sub._ipp._tcp.local.	☑
Printer	_printer._tcp.local.	☑
Scanner	_scanner._tcp.local.	☑

Bonjour services can also be removed from the default (or non-default) profiles with the command shown in Example 25-5.

Example 25-5 Removing Bonjour Services from a mDNS Profile

```
General Command:
(Cisco Controller) >config mdns profile service delete mdns-profile-name mdns-service-name

Specific example:
(Cisco Controller) >config mdns profile service delete default-mdns-profile AirTunes
! Deletes the Apple AirTunes service from the default mDNS profile
```

The addition/removal of services to a mDNS profile can be verified by the **show mdns profile** command, which can either show a summary of configured profiles or a detailed view of a specific profile, as shown in Example 25-6 and Example 25-7, respectively.

Example 25-6 Verifying mDNS Profiles—show mdns profile summary

```
(Cisco Controller) >show mdns profile summary
Number of Profiles.............................. 1

ProfileName                       No. Of Services
--------------------------------  ---------------
default-mdns-profile                   6

(Cisco Controller) >
```

Example 25-7 Verifying mDNS Profiles—show mdns profile detailed Profile-Name

```
(Cisco Controller) >show mdns profile detailed default-mdns-profile

Profile Name.................................... default-mdns-profile
Profile Id...................................... 2
No of Services.................................. 6
```

```
Services......................................... AirPrint
                                                  AppleTV
                                                  HP_Photosmart_Printer_1
                                                  HP_Photosmart_Printer_2
                                                  Printer
                                                  Scanner

No. Interfaces Attached.......................... 1
Interfaces....................................... dynamic

No. Interface Groups Attached.................... 0
No. Wlans Attached............................... 4
Wlan Ids......................................... 1
                                                  3
                                                  4
                                                  5

(Cisco Controller) >
```

Step 3—Apply the Default mDNS Profile an Interface (or Interface-Group)

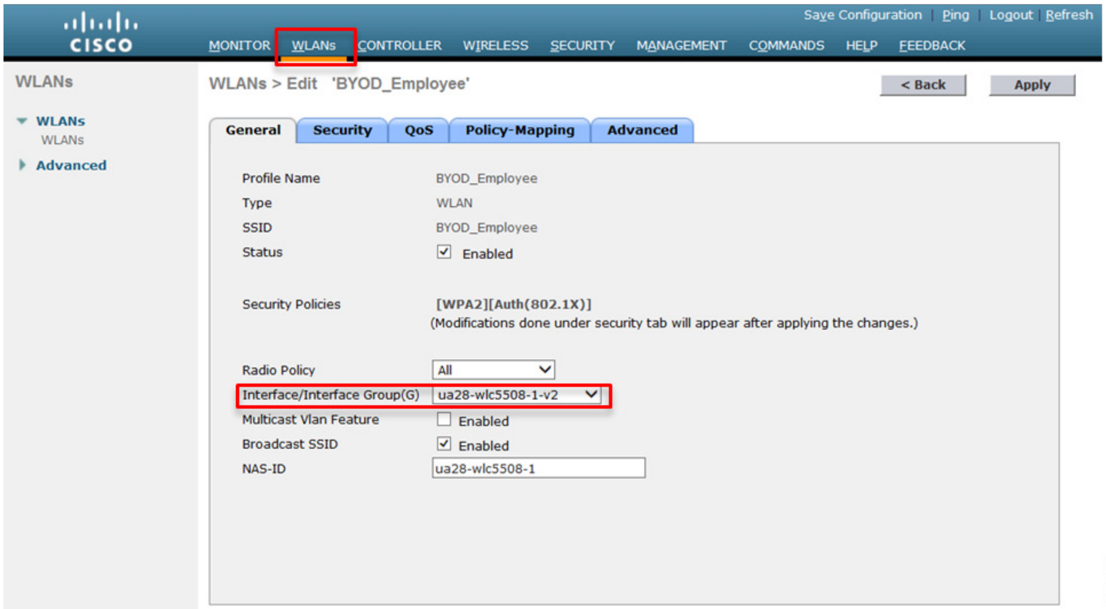
Bonjour service policies may be applied to interfaces, VLANs, or WLANs. In this example the Bonjour policies (as represented in the Default mDNS Profile) are attached to an interface.

There are five types of interfaces are available on the Cisco WLC controller. Four of these are static and are configured at setup time and the fifth type is dynamic and user-defined:

- Management interface (static and configured at setup time; mandatory)
- AP-manager interface (static and configured at setup time; mandatory)
- Virtual interface (static and configured at setup time; mandatory)
- Service-port interface (static and configured at setup time; optional)
- Dynamic interface (user-defined)

In this case, it is assumed that the ua28-wlc5508-1-v2 interface is applied to the BYOD_Employee WLAN (in line with the recommendations in Chapter 9, “BYOD Wireless Infrastructure Design”), as shown in Figure 25-15. If this is not the case, then the policies should be applied to whatever (static or dynamic) interface is associated with the WLAN. This association is verified by selecting the **WLANs** heading bar and then selecting the WLAN number that corresponds to the BYOD_Employee WLAN.

Figure 25-15 Use Case 1—Verifying WLAN/Interface Association



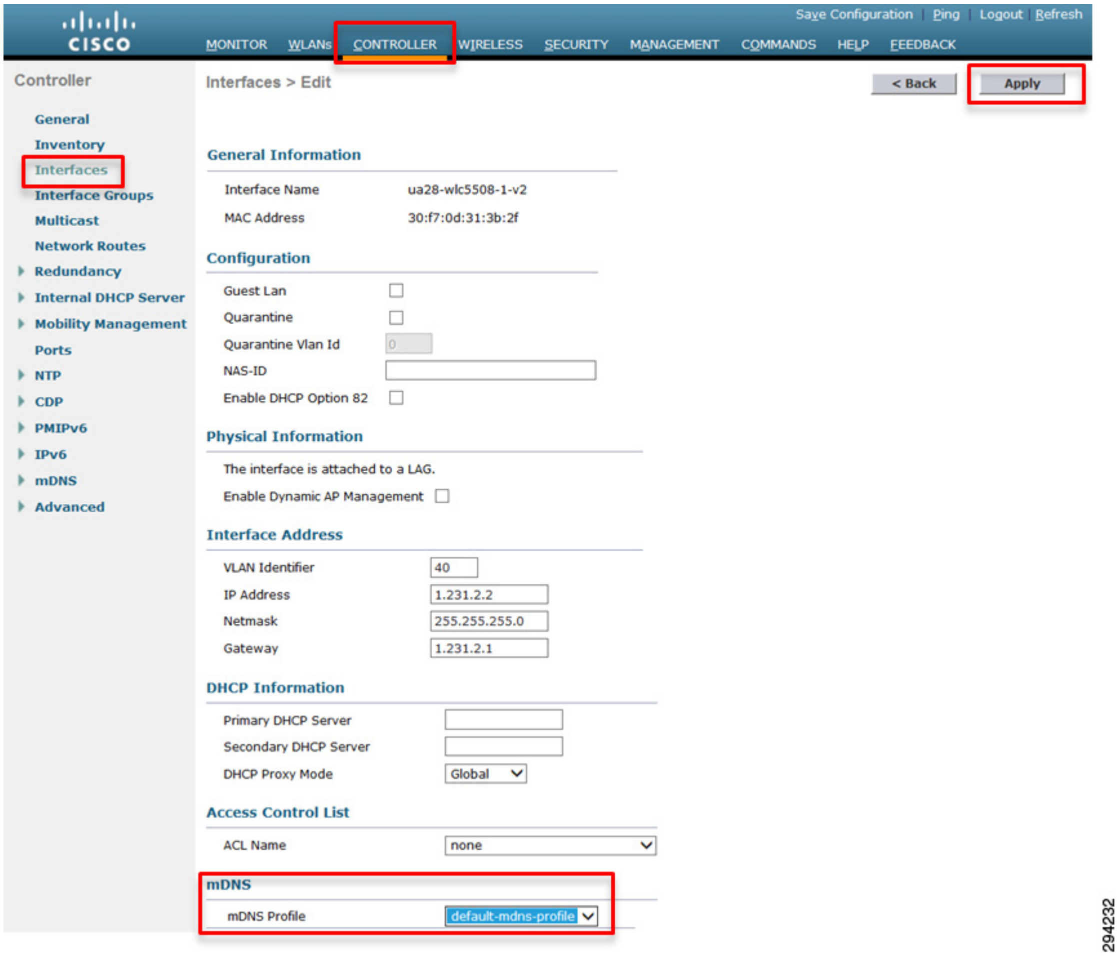
WLANs > Edit 'BYOD_Employee'

Profile Name	BYOD_Employee
Type	WLAN
SSID	BYOD_Employee
Status	☑ Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	ua28-wlc5508-1-v2
Multicast Vlan Feature	□ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	ua28-wlc5508-1

To apply the Default mDNS policies to an interface, perform the following:

1. Click the **CONTROLLER** heading-bar and then the **Interfaces** (or **Interface Group**) link on the left.
2. Select the interface that corresponds to the VLAN/WLAN to which the Bonjour service policies are to be applied.
3. At the bottom of the **Interface > Edit** page, select the **default-mdns-profile** from the **mDNS Profile** drop-down list.
4. Click the **Apply** button at the top-right of the page.

Figure 25-16 Use Case 1—Step 3—Applying the Default mDNS Profile to an Interface



Interfaces > Edit

General Information

Interface Name	ua28-wlc5508-1-v2
MAC Address	30:f7:0d:31:3b:2f

Configuration

Guest Lan	□
Quarantine	□
Quarantine Vlan Id	0
NAS-ID	
Enable DHCP Option 82	□

Physical Information

The interface is attached to a LAG.

Enable Dynamic AP Management □

Interface Address

VLAN Identifier	40
IP Address	1.231.2.2
Netmask	255.255.255.0
Gateway	1.231.2.1

DHCP Information

Primary DHCP Server	
Secondary DHCP Server	
DHCP Proxy Mode	Global

Access Control List

ACL Name	none

mDNS

mDNS Profile	default-mdns-profile

As Figure 25-16 shows (in this case) the ua28-wlc5508-1-v2 interface corresponds to VLAN 40, which is where the wired AirPrint printer(s) reside. Bonjour service advertisements from these printers will now be shared with other WLANs/VLANs.

The Default mDNS profile can be added to the interface associated with the WLAN with the commands shown in Example 25-8.

Example 25-8 Adding a mDNS Profile to an Interface

```
General command:
(Cisco Controller) >config interface mdns-profile {interface-name | all} mdns-profile-name

Specific example:
(Cisco Controller) >config interface mdns-profile ua28-wlc5508-1-v2 default-mdns-profile
! Adds the default mDNS profile to the “ua28-wlc5508-1-v2” interface
```

The mDNS profile attached to an interface can be verified by the command **show interface detailed** *interface-name*, as shown in Example 25-9. Alternatively, if the mDNS profile is attached to an interface-group, then the show command would be **show interface group detailed** *interface-group-name*.

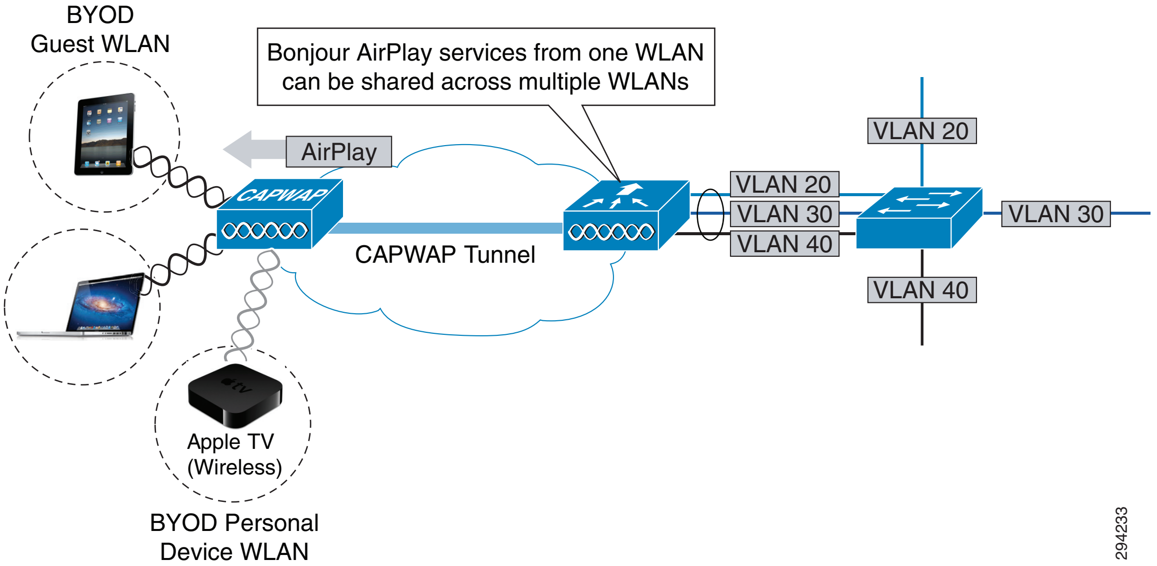
Example 25-9 Verifying Interface mDNS Profiles—show interface detailed interface-name

```
(Cisco Controller) >show interface detailed ua28-wlc5508-1-v2

Interface Name.................................. ua28-wlc5508-1-v2
MAC Address..................................... 30:f7:0d:31:3b:2f
IP Address...................................... 10.225.43.2
IP Netmask...................................... 255.255.255.0
IP Gateway...................................... 10.225.43.1
External NAT IP State........................... Disabled
External NAT IP Address......................... 0.0.0.0
VLAN............................................ 40
Quarantine-vlan................................. 0
Active Physical Port............................ LAG (13)
Primary Physical Port........................... LAG (13)
Backup Physical Port............................ Unconfigured
DHCP Proxy Mode................................. Global
Primary DHCP Server............................. 10.230.1.61
Secondary DHCP Server........................... Unconfigured
DHCP Option 82.................................. Disabled
IPv4 ACL........................................ Unconfigured
IPv6 ACL........................................ Unconfigured
mDNS Profile Name............................... default-mdns-profile
<snip>
```

Use Case 2—Wireless-to-Wireless Bonjour Gateway Service Policy—BYOD Guest AirPlay Example

In this secondary Bonjour Gateway use case, wireless guest devices are permitted to access Apple TV devices (using AirPlay) so that guests may share presentations, video, or other content with employees. Incidentally, Apple TVs, like some AirPrint printers, may be connected via wired or wireless connections; this design supports both options. However in this case, assume the Apple TV is residing in the BYOD Personal Devices WLAN, as shown in Figure 25-17.

Figure 25-17 Use Case 2—Cisco WLC Bonjour Gateway Wireless-to-Wireless Design Example



To highlight design and deployment options, in this example Bonjour service policies are configured by:

- Step 1—Creating a new mDNS profile.
- Step 2—Adding Bonjour services to the new mDNS profile.
- Step 3—Enabling mDNS snooping and the new mDNS profile directly on the WLAN.

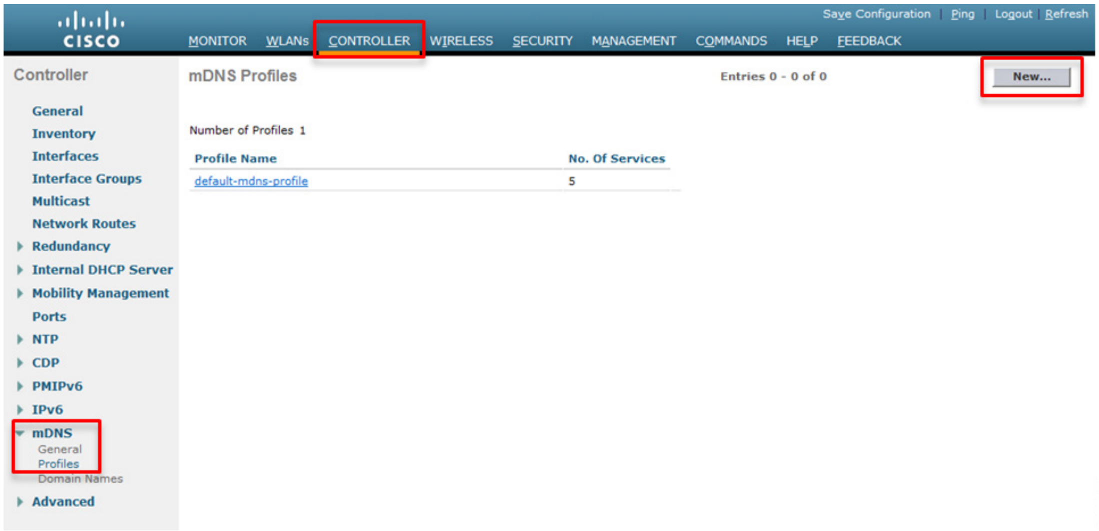
Each of these steps is detailed in turn.

Step 1—Creating a New mDNS Profile

The first step in this example is to create a new mDNS profile, which can be done by performing the following:

1. Click the **CONTROLLER** heading-bar and expand the mDNS link on the lower left and click **Profiles**.
2. Click the **New** button at the top-right, as shown in Figure 25-18.

Figure 25-18 Use Case 2—Step 1a—Creating a New mDNS Profile



mDNS Profiles

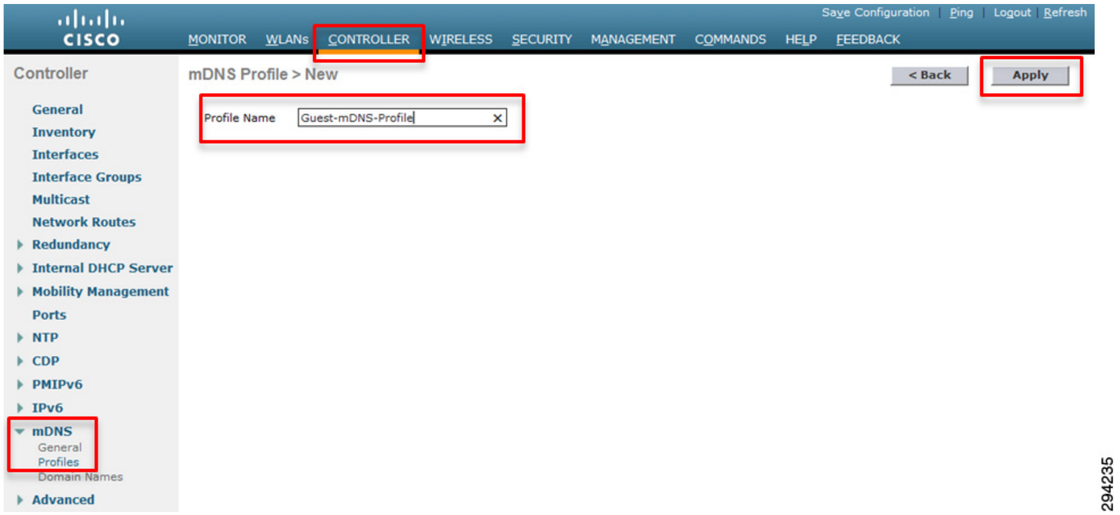
Entries 0 - 0 of 0

Number of Profiles 1

Profile Name	No. Of Services
default-mdns-profile	5

3. Give the new profile a name and click the **Apply** button, as shown in Figure 25-19.

Figure 25-19 Use Case 2—Step 1b—Naming the New mDNS Profile



mDNS Profile > New

Profile Name: Guest-mDNS-Profile

The corresponding Cisco WLC CLI for creating a new mDNS profile is shown in Example 25-10, which creates a new mDNS profile named “**Guest-mDNS-Profile**”.

Example 25-10 Creating a New mDNS Profile

```
General command:
(Cisco Controller) >config mdns profile create mdns-profile-name

Specific example:
(Cisco Controller) >config mdns profile create Guest-mDNS-Profile
! Creates a new mDNS profile named "Guest-mDNS-Profile"
```

Newly created mDNS profiles will be displayed by the **show mdns profile summary verification** command, as shown in Example 25-11.

Example 25-11 Verifying mDNS Profiles—show mdns profile summary

```
(Cisco Controller) >show mdns profile summary
Number of Profiles................................ 2

ProfileName                        No. Of Services
--------------------------------  ---------------
Guest-mDNS-Profile                      0
default-mdns-profile                    6

(Cisco Controller) >
```

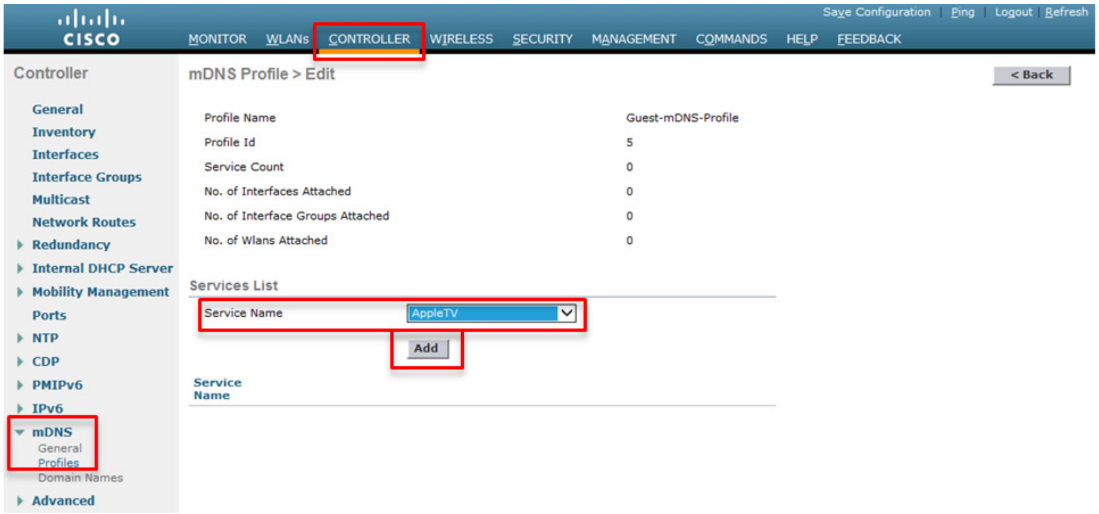
Step 2—Adding Bonjour Services to the New mDNS Profile

In this particular use case, only the AirPlay service will be offered to BYOD guest devices. Therefore the Bonjour AirPlay service needs to be added to the new mDNS Profile, which is done by performing the following:

1. Select and click the new mDNS profile.
2. Select the desired Bonjour service(s) from the **Services List** drop-down list and click the **Add** button, as shown in Figure 25-20.

3. The added service will subsequently appear under the **Service Name** bar.

Figure 25-20 Use Case 2—Step 2—Adding Bonjour Services to the New mDNS Profile



mDNS Profile > Edit

Profile Name Guest-mDNS-Profile
Profile Id 5
Service Count 0
No. of Interfaces Attached 0
No. of Interface Groups Attached 0
No. of Wlans Attached 0

Services List

Service Name AppleTV

Service Name

The corresponding Cisco WLC CLI for adding Bonjour services to a profile is shown in Example 25-12.

Example 25-12 Adding Bonjour Services to a mDNS Profile

```
General command:
(Cisco Controller) >config mdns profile service add mdns-profile-name mdns-service-name

Specific example:
(Cisco Controller) >config mdns profile service add Guest-mDNS-Profile AppleTV
! Adds the AppleTV service to the “Guest-mDNS-Profile” profile
```

Services within a mDNS profile can be verified by the **show mdns profile detailed** command, as presented in Example 25-13.

Example 25-13 Verifying mDNS Profiles—show mdns profile detailed Profile-Name

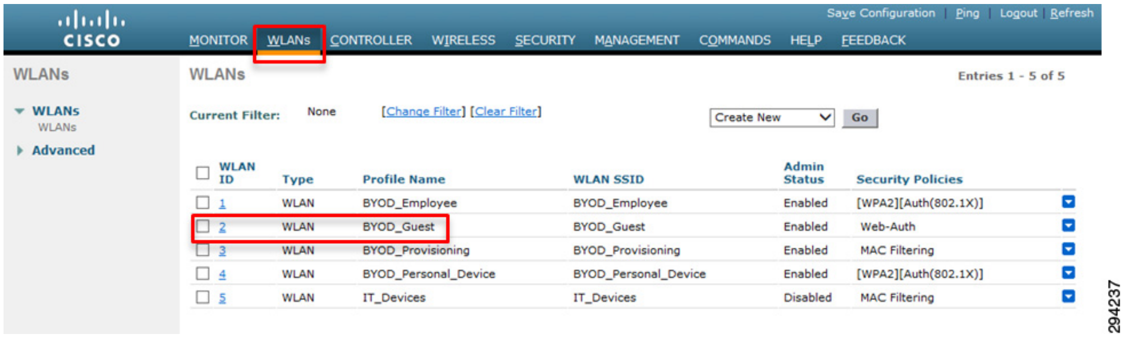
```
(Cisco Controller) >show mdns profile detailed Guest-mDNS-Profile

Profile Name................................... Guest-mDNS-Profile
Profile Id..................................... 1
No of Services................................. 1
Services....................................... AppleTV

No. Interfaces Attached........................ 0
No. Interface Groups Attached.................. 0
No. Wlans & Guest-LANs Attached................ 0

(Cisco Controller) >
```

Step 3—Enable mDNS Snooping and the New mDNS Profile on the WLAN

Once all the Bonjour services have been added to the new profile, it can be added to the desired WLAN (in this case, the BYOD_Guest WLAN) by performing the following:

1. Click the **WLANs** heading-bar and select the desired WLAN (in this case, the BYOD_Guest WLAN, as shown in Figure 25-21).

Figure 25-21 Use Case 2—Step 3a—Selecting the WLAN to which the New mDNS Profile Will Be Applied



WLANs

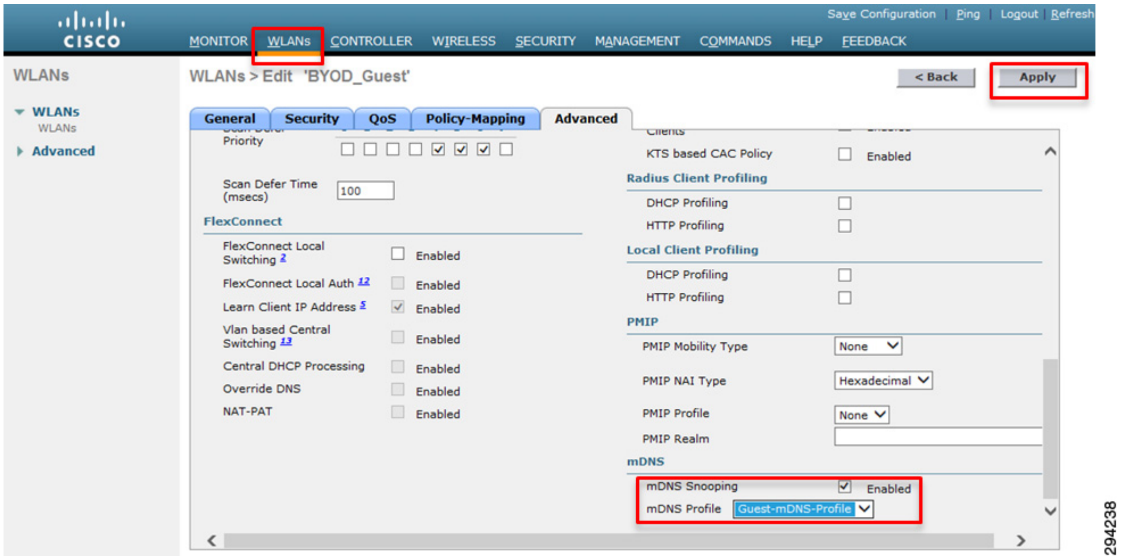
Entries 1 - 5 of 5

Current Filter: None [Change Filter] [Clear Filter]

□ WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
□ 1	WLAN	BYOD_Employee	BYOD_Employee	Enabled	[WPA2][Auth(802.1X)]
□ 2	WLAN	BYOD_Guest	BYOD_Guest	Enabled	Web-Auth
□ 3	WLAN	BYOD_Provisioning	BYOD_Provisioning	Enabled	MAC Filtering
□ 4	WLAN	BYOD_Personal_Device	BYOD_Personal_Device	Enabled	[WPA2][Auth(802.1X)]
□ 5	WLAN	IT_Devices	IT_Devices	Disabled	MAC Filtering

2. Click the **Advanced** tab and scroll to the bottom.
3. Ensure that the **mDNS Snooping** checkbox is selected.
4. Select the **mDNS Profile** from the drop-down list.
5. Click the **Apply** button at the top-left.

Figure 25-22 Use Case 2—Step 3b—Enabling mDNS Snooping on the WLAN and Applying the New mDNS Profile



WLANs > Edit 'BYOD_Guest'

Priority □ □ □ □ ☑ ☑ ☑ □

Scan Defer Time (msecs) 100

FlexConnect

FlexConnect Local Switching 2 □ Enabled
FlexConnect Local Auth 12 □ Enabled
Learn Client IP Address 5 ☑ Enabled
Vlan based Central Switching 13 □ Enabled
Central DHCP Processing □ Enabled
Override DNS □ Enabled
NAT-PAT □ Enabled

Clients

KTS based CAC Policy □ Enabled

Radius Client Profiling

DHCP Profiling □
HTTP Profiling □

Local Client Profiling

DHCP Profiling □
HTTP Profiling □

PMIP

PMIP Mobility Type None
PMIP NAI Type Hexadecimal
PMIP Profile None
PMIP Realm

mDNS

mDNS Snooping ☑ Enabled
mDNS Profile Guest-mDNS-Profile

The corresponding Cisco WLC CLI for these steps of enabling mDNS snooping and a specific mDNS profile on a WLAN is shown in Example 25-14 and Example 25-15, respectively.

Example 25-14 Enabling mDNS Snooping on a WLAN

```
General command/specific example:
(Cisco Controller) > config wlan mdns enable
```

Example 25-15 Adding a mDNS Profile to a WLAN

```
General command:
(Cisco Controller) >config wlan mdns profile {wlan-id | all } mdns-profile-name

Specific example:
(Cisco Controller) >config wlan mdns profile 2 Guest-mDNS-Profile
! Adds the "Guest-mDNS-Profile" to WLAN 2 (the BYOD_Guest WLAN, as shown in Figure 21)
```

The mDNS settings of a WLAN can be verified by the **show wlan** *wlan-id* verification command, as shown in Example 25-16.

Example 25-16 Verifying WLAN mDNS Settings—show wlan

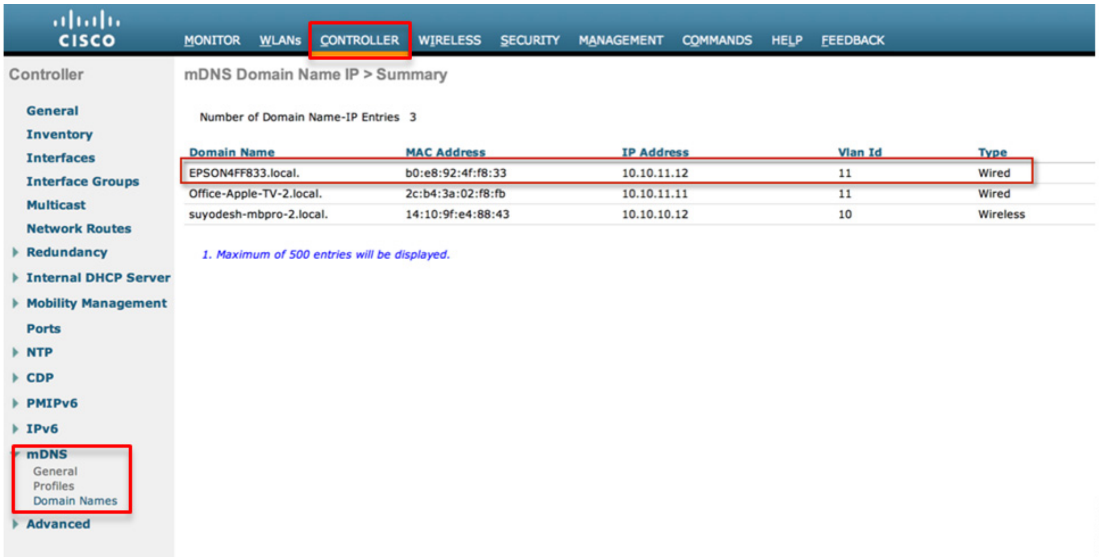
```
(Cisco Controller) >show wlan 2


WLAN Identifier.................................. 2
Profile Name..................................... BYOD_Guest
Network Name (SSID).............................. BYOD_Guest
Status........................................... Enabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Enabled
Network Admission Control
Client Profiling Status
    Radius Profiling ............................ Disabled
     DHCP ....................................... Disabled
     HTTP ....................................... Disabled
    Local Profiling ............................. Disabled
     DHCP ....................................... Disabled
     HTTP ....................................... Disabled
  Radius-NAC State............................... Disabled
  SNMP-NAC State................................. Disabled
  Quarantine VLAN................................ 0
Maximum number of Associated Clients............. 0
Maximum number of Clients per AP Radio........... 200
Number of Active Clients......................... 0
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. 1800 seconds
User Idle Timeout................................ Disabled
Sleep Client..................................... disable
Sleep Client Timeout............................. 12 hours
User Idle Threshold.............................. 0 Bytes
NAS-identifier................................... ua28-wlc5508-1
CHD per WLAN..................................... Enabled
Webauth DHCP exclusion........................... Disabled
Interface........................................ ua27-5508-2-guest
Multicast Interface.............................. Not Configured
WLAN IPv4 ACL.................................... unconfigured
WLAN IPv6 ACL.................................... unconfigured
WLAN Layer2 ACL.................................. unconfigured
mDNS Status...................................... Enabled
mDNS Profile Name................................ Guest-mDNS-Profile
<snip>
```

Verifying Bonjour Gateway Operation

In addition to the GUI and CLI configuration-verification screenshots and commands that have been highlighted in the previous sections, Cisco WLC software has some additional options for verifying Bonjour Gateway operation, which we now discuss.

For instance, a summary of all mDNS records can be shown by clicking the **CONTROLLER** heading-bar, expanding the **mDNS** link on the lower left, and then clicking **Domain Names**, as shown in Figure 25-23.

Figure 25-23 Verifying mDNS Domain Names



mDNS Domain Name IP > Summary

Number of Domain Name-IP Entries 3

Domain Name	MAC Address	IP Address	Vlan Id	Type
EPSON4FF833.local.	b0:e8:92:4f:f8:33	10.10.11.12	11	Wired
Office-Apple-TV-2.local.	2c:b4:3a:02:f8:fb	10.10.11.11	11	Wired
suyodesh-mbpro-2.local.	14:10:9f:e4:88:43	10.10.10.12	10	Wireless

1. Maximum of 500 entries will be displayed.

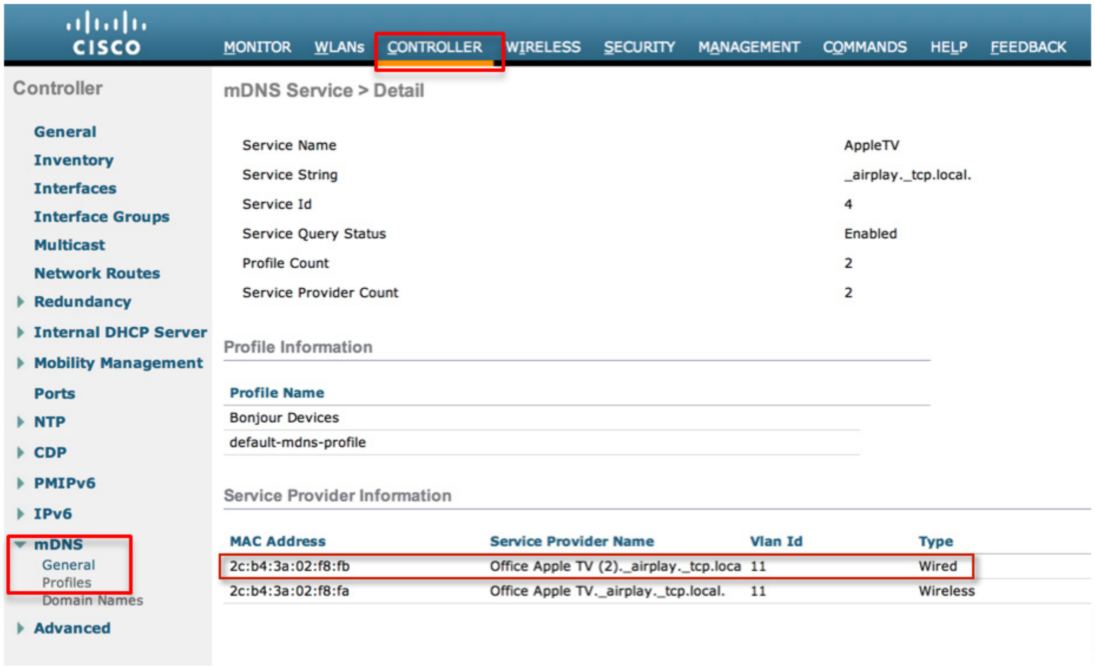
A summary of mDNS records can also be provided via the CLI with the command **show mdns domain-name-ip summary**, as shown in Example 25-17.

Example 25-17 Verifying mDNS Records—show mdns domain-name-ip summary

```
(Cisco Controller) >show mdns domain-name-ip summary

Number of Domain Name-IP Entries................. 3

DomainName                MAC Address        IP Address    Vlan Id  Type      TTL   Time left
                                                                              (sec)  (sec)
--------------------     ----------------   -----------   ------- ------     ----- -----

EPSON4FF833.local.        b0:e8:92:4f:f8:33  10.10.10.12   11      Wired     4725  4354
Office-Apple-TV.local.    2c:b4:3a:02:f8:fb  10.10.11.11   11      Wired     4725  4712
suyodesh-mbpro-2.local.   14:10:9f:e4:88:43  10.10.10.12   10      Wireless  4725  3753

(Cisco Controller) >
```

Also, clicking on any service listed within an mDNS profile will display a **mDNS Service>Detail** screen that will display device-level details—including MAC address, VLAN, and network-type (wired or wireless) for any and all devices providing that Bonjour service. For example, Figure 25-24 shows that the Apple TV service is available both via the wired and wireless networks.

Figure 25-24 Verifying mDNS Service Details



mDNS Service > Detail

Service Name	AppleTV
Service String	_airplay._tcp.local.
Service Id	4
Service Query Status	Enabled
Profile Count	2
Service Provider Count	2

Profile Information

Profile Name
Bonjour Devices
default-mdns-profile

Service Provider Information

MAC Address	Service Provider Name	Vlan Id	Type
2c:b4:3a:02:f8:fb	Office Apple TV (2)._airplay._tcp.loca	11	Wired
2c:b4:3a:02:f8:fa	Office Apple TV._airplay._tcp.local.	11	Wireless

Device-level mDNS service detail is also available via the CLI using the command **show mdns service detailed** *mdns-service-name*, as demonstrated in Example 25-18.

Example 25-18 Verifying mDNS Service Details—show mdns service detailed

```
(Cisco Controller) >show mdns service detailed AppleTV

Service Name.................................... AppleTV
Service Id...................................... 4
Service query status............................ Enabled
Service LSS status.............................. Disabled
Service learn origin............................ Wireless and Wired
Number of Profiles.............................. 2
Profile......................................... Guest-mDNS-Profile
                                                 default-mdns-profile

Number of Service Providers ..................... 1
Number of priority MAC addresses ................ 0
ServiceProvider                               MAC Address       AP Radio MAC
Vlan Id     Type        TTL     Time left

(sec)      (sec)
--------------------                         ----------------   ----------------
-------    ------     -----   ---------

Office Apple TV._airplay._tcp.local.         2c:b4:3a:02:f8:fa  04:da:d2:b2:47:10
11      Wireless      4500      4460
```

Additionally, the CLI allows for a summary of mDNS services to be displayed via the **show mdns service summary** command, as shown in Example 25-19.

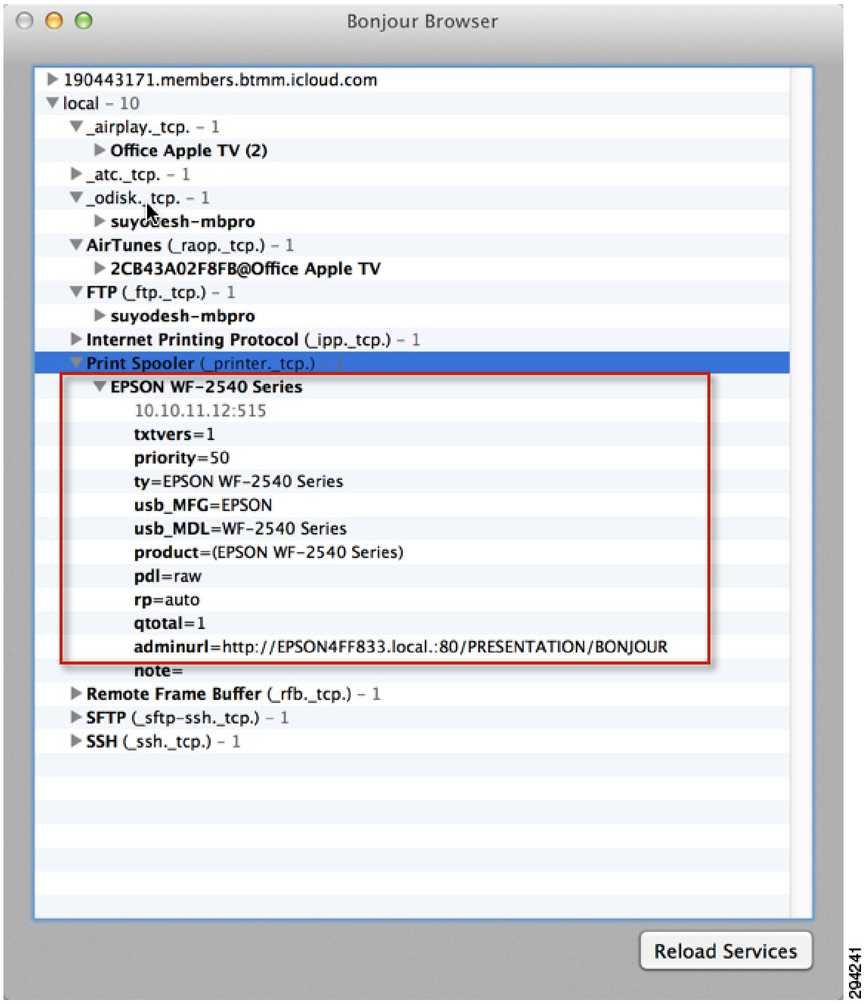
Example 25-19 Verifying mDNS Service Summary—show mdns service summary

```
(Cisco Controller) >show mdns service summary
```

```
Number of Services............................... 11

Service-Name                      LSS   Origin     No SP    Service-string
-------------------------------- ----  ----------  -----   ---------------
AFP                              No    All           0   _afpovertcp._tcp.local.
AirPrint                         No    All           1   _ipp._tcp.local.
AirTunes                         No    All           1   _raop._tcp.local.
AppleTV                          No    All           1   _airplay._tcp.local.
FTP                              No    All           1   _ftp._tcp.local.
HP_Photosmart_Printer_1          No    All           1   _universal._sub._ipp._tcp.local.
HP_Photosmart_Printer_2          No    All           0   _cups._sub._ipp._tcp.local.
Printer                          No    All           1   _printer._tcp.local.
Scanner                          No    All           1   _scanner._tcp.local.
TimeCapsuleBackup                No    All           0   _adisk._tcp.local.
iTuneHomeSharing                 No    All           0   _home-sharing._tcp.local.

(Cisco Controller) >
```

Finally, it bears mentioning that third-party tools are also available to verify mDNS operations. For example, Figure 25-25 shows Tildesoft's "Bonjour Browser" displaying mDNS details for the Epson wired AirPrint printer.

Figure 25-25 Verifying Bonjour Gateway Operation via Third-Party Tools—Tildesoft Bonjour Browser Example



```
▶ 190443171.members.btmm.icloud.com
▼ local – 10
  ▼ _airplay._tcp. – 1
    ▶ Office Apple TV (2)
  ▶ _atc._tcp. – 1
  ▼ _odisk._tcp. – 1
    ▶ suyodesh-mbpro
  ▼ AirTunes (_raop._tcp.) – 1
    ▶ 2CB43A02F8FB@Office Apple TV
  ▼ FTP (_ftp._tcp.) – 1
    ▶ suyodesh-mbpro
  ▶ Internet Printing Protocol (_ipp._tcp.) – 1
  ▼ Print Spooler (_printer._tcp.) – 1
    ▼ EPSON WF-2540 Series
        10.10.11.12:515
        txtvers=1
        priority=50
        ty=EPSON WF-2540 Series
        usb_MFG=EPSON
        usb_MDL=WF-2540 Series
        product=(EPSON WF-2540 Series)
        pdl=raw
        rp=auto
        qtotal=1
        adminurl=http://EPSON4FF833.local.:80/PRESENTATION/BONJOUR
        note=
  ▶ Remote Frame Buffer (_rfb._tcp.) – 1
  ▶ SFTP (_sftp-ssh._tcp.) – 1
  ▶ SSH (_ssh._tcp.) – 1
```

Advanced Bonjour Gateway Scenario Operation

This section will briefly overview Bonjour Gateway operation in three additional scenarios:

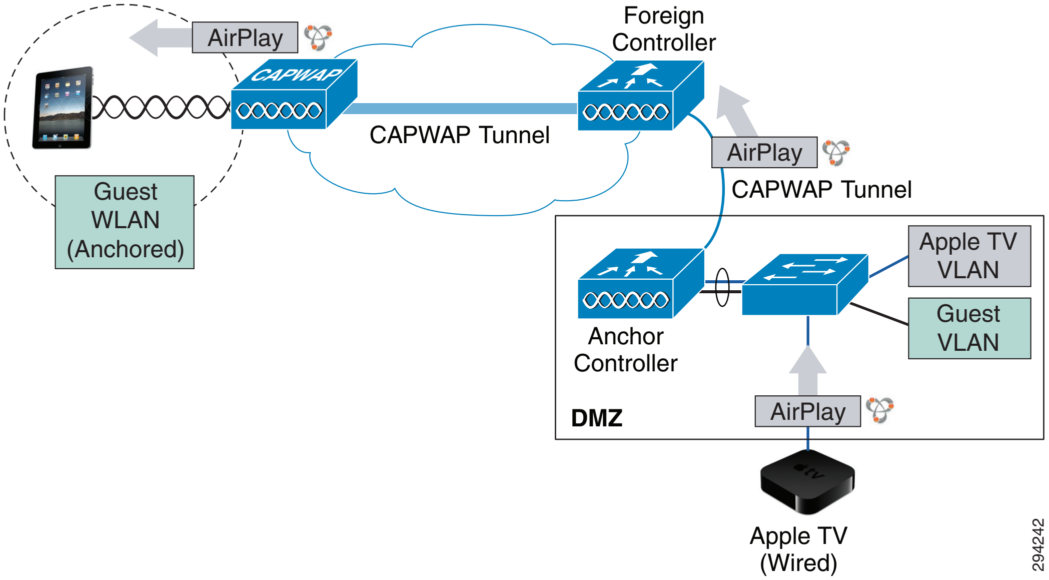
- Guest Anchoring
- Layer 3 Roaming
- FlexConnect

While the configuration and verification of the Bonjour Gateway feature remains the same for these scenarios, it may be helpful for network administrators to understand how this feature operates in these contexts.

Guest Anchoring

In guest anchoring scenarios, the guest WLAN is able to see Bonjour services advertised to the anchor controller. This is because the Bonjour queries and advertisements are sent inside the Control and Provisioning of Wireless Access Points (CAPWAP) tunnel, as shown in Figure 25-26.

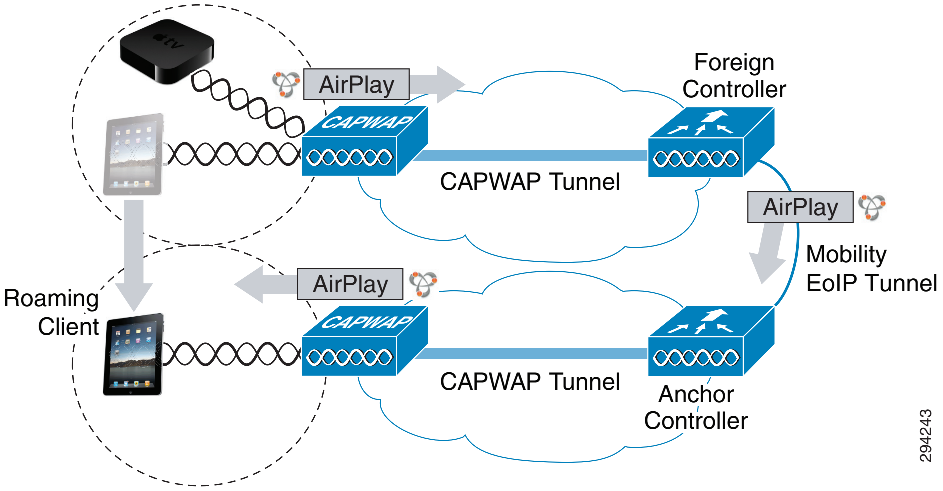
Figure 25-26 Bonjour Gateway Operation in Guest Anchoring Scenarios



Layer 3 Roaming

Bonjour Gateway with Layer 3 roaming works across Ethernet over IP (EoIP) tunnels to ensure that users moving among access points (APs) on different controllers continue to see the devices they saw on the original controller. The Bonjour services on the anchor controller are displayed to the client, including both wired and wireless devices, as shown in Figure 25-27.

Figure 25-27 Bonjour Gateway Operation in Layer 3 Roaming Scenarios



FlexConnect

For centrally-switched WLANs, the behavior for Bonjour is the same as if the AP was in local mode. In this case, Bonjour queries from the client are sent to the controller and Bonjour responses from the controller are sent back to the AP in the unicast CAPWAP tunnel. This means FlexConnect APs will not require “Multicast-Unicast” mode to support Bonjour.

For locally switched WLANs, the behavior for Bonjour will continue to work for a single subnet only.

Summary

This paper overviewed Apple’s Bonjour protocol—a zero-configuration protocol for advertising, discovering, and connecting to network services—and how it can be effectively managed within a BYOD enterprise context.

The design limitation of Bonjour’s use of link-local multicasting was discussed, showing how it limited the usefulness of the protocol to only a single Layer 2 domain. To enable the use of Bonjour in (multi-WLAN/VLAN) BYOD enterprise networks, the Cisco WLC Bonjour Gateway was introduced. Next, an overview of the operation of the Bonjour Gateway feature was provided, showing how it can be used to snoop, cache, and proxy-respond to Bonjour service requests. Additionally, it was shown how these responses could be selectively enabled and disabled, allowing for administrative policy-based control of Bonjour services.

Following this, deployment details of this feature were presented by considering two main use-case scenarios:

- Printing from wireless devices to wired printers.
- Sharing Bonjour services between wireless devices in different WLANs.

Step-by-step configuration guidance was presented for each scenario, using slightly different approaches to highlight the various configuration options available. Each step was presented for not only the Cisco WLC GUI configuration and verification, but also for the Cisco WLC CLI.

Additional verification options were also highlighted, as well as how the Bonjour Gateway operates in various advanced scenarios, including guest anchoring, Layer 3 roaming, and FlexConnect deployments.

References

- Cisco Wireless LAN Controller Configuration Guide, Release 7.4
  http://www.cisco.com/en/US/docs/wireless/controller/7.4/configuration/guides/consolidated/b_cg74_CONSOLIDATED.html
- Cisco Wireless LAN Controller Configuration Guide, Release 7.4—Configuring Multicast Domain Name System
  http://www.cisco.com/en/US/docs/wireless/controller/7.4/configuration/guides/consolidated/b_cg74_CONSOLIDATED_chapter_01011.html#d75540e531a1635
- Cisco WLC Bonjour Gateway Deployment Guide
  http://www.cisco.com/en/US/docs/wireless/technology/bonjour/Bonjour_Deployment.html