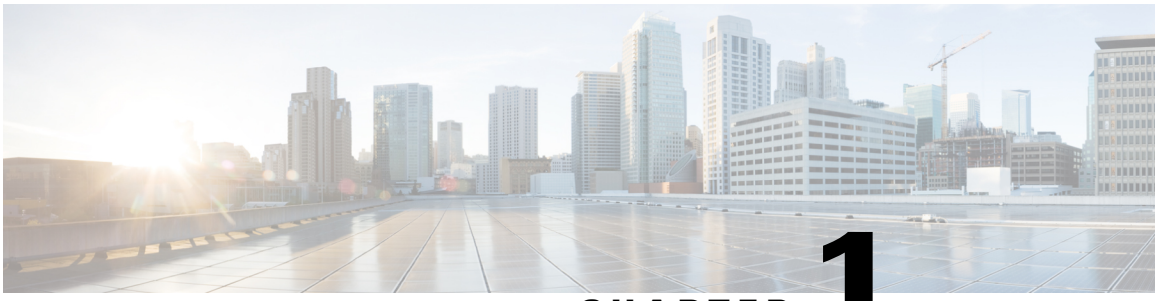
Apple Bonjour Services on the Cisco mDNS Enabled Controllers

Last Modified: December 24, 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

Overview

Bonjour is Apple's version of Zeroconf - it is mDNS with DNS-SD. Apple devices will advertise their services via IPv4 and IPv6 simultaneously (IPv6 link local and Globally Unique).

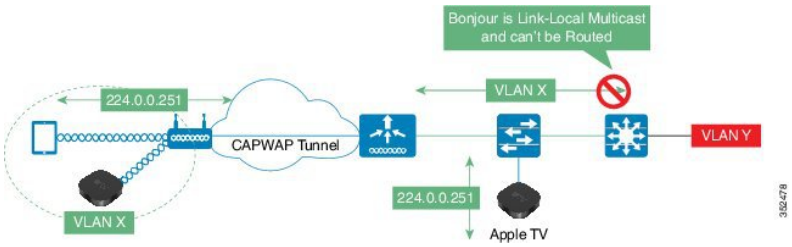
The Bonjour protocol operates on service announcements and service queries which allow devices to ask and advertise specific applications such as:

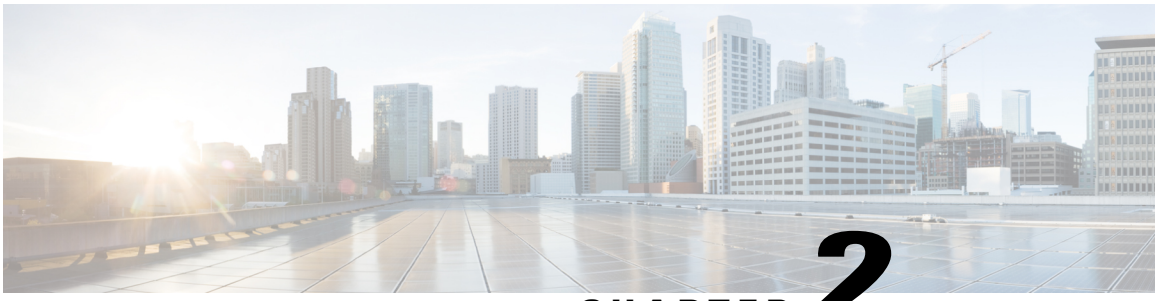
- Printing Services
- File Sharing Services
- Remote Desktop Services
- iTunes Wireless iDevice Syncing (in Apple iOS v5.0 - v7.0)
- AirPlay offering the following streaming services:
    - Music broadcasting in iOS v4.2 – v7.0
    - Video broadcasting in iOS v4.3 – v7.0
    - Full screen mirroring in iOS v5.0 – v7.0 (iPad2, iPhone4S or later)

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

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

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


Bonjour is Link-Local Multicast and can't be Routed
224.0.0.251
CAPWAP Tunnel
VLAN X
VLAN Y
224.0.0.251
VLAN X
Apple TV
352478



CHAPTER 2

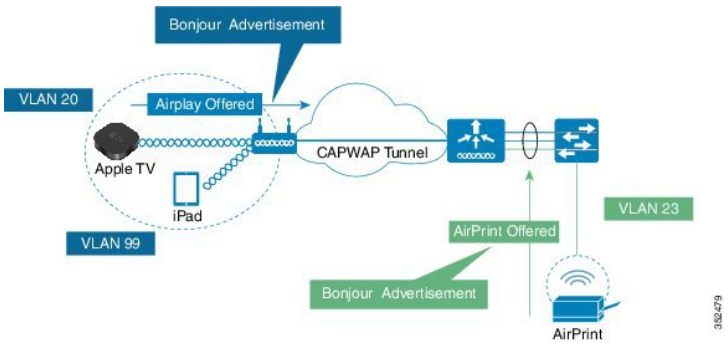
Cisco Bonjour Gateway Solution

From 7.4 release WLC supports Bonjour gateway functionality on WLC itself for which you need not even enable multicast on the controller. The WLC will snoop all Bonjour discovery packets and will not forward the same on AIR or Infra network.

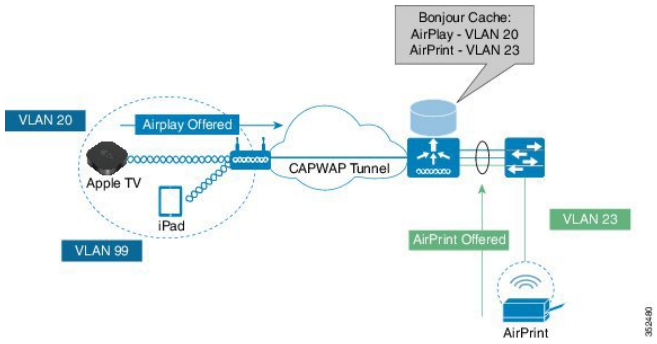
Bonjour is Apple's version of Zeroconf - it is mDNS with DNS-SD. Apple devices will advertise their services via IPv4 and IPv6 simultaneously (IPv6 link local and Globally Unique).

To address this issue Cisco WLC acts as a Bonjour Gateway. The WLC listens for Bonjour services and by caching those Bonjour advertisements (AirPlay, AirPrint etc.) from the source/host e.g. AppleTV and responding back to Bonjour clients when they ask/request for a service. The following illustrates this process.

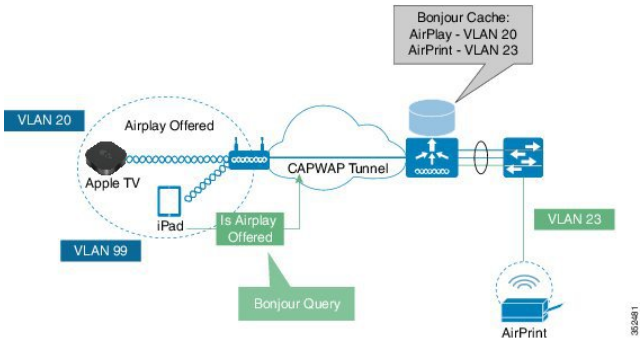
Step 1 The Controller listens for the Bonjour services.



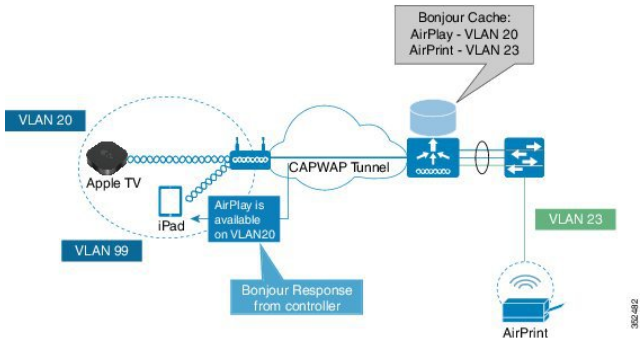
Step 2 The WLC then cache those Bonjour services.

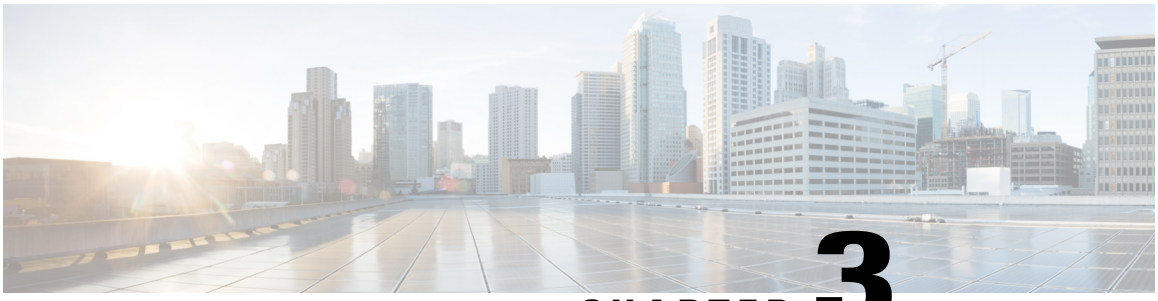


Step 3 Listens for the client queries for services.



Step 4 The WLC sends a unicast response to the client queries for Bonjour services.





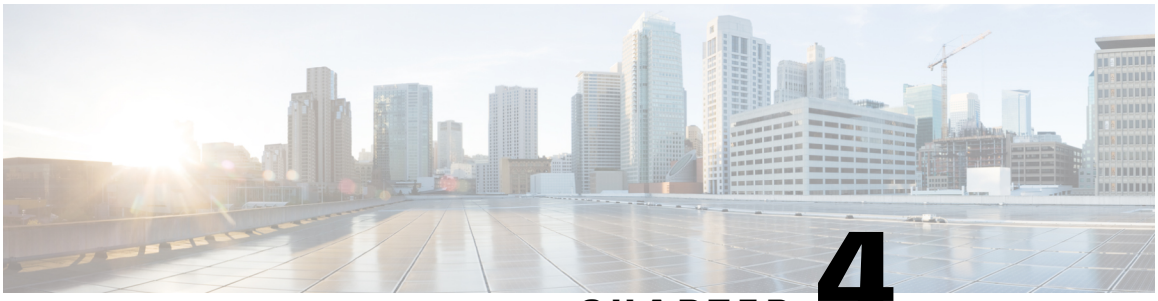
CHAPTER 3

Bonjour Deployment using mDNS Gateway

From 7.4 release WLC supports Bonjour gateway functionality on WLC itself. WLC will snoop all Bonjour discovery packets and will not forward the same on AIR or Infra network thus minimizing the traffic flow and increasing overall network performance on both wired and wireless or over the air networks.

In addition to creating the mDNS Gateway that supports a total of the 6400 services and up to 16000 services on the high end controllers, network admin can create Bonjour Policy Profiles to manage the services and their access. Bonjour Policy Profile is a list of allowed network applications such as AirPlay or Printing and can be enforced on the WLAN, VLAN or on the Interface Group. Also the Bonjour service profile provides filtering to allow only certain WLANs, Interfaces or Interface Groups to access specific service types.

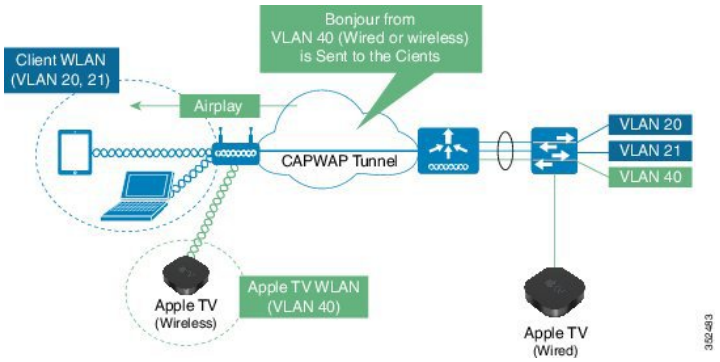
Only one mDNS profile can be applied to one WLAN.



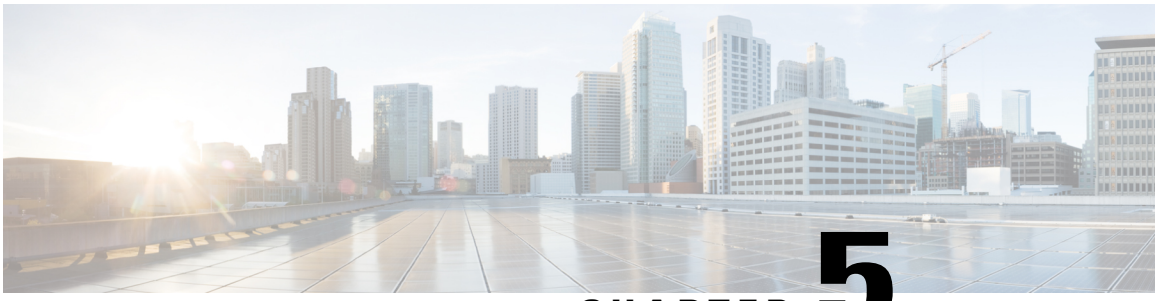
CHAPTER 4

mDNS services with Wired Bonjour Devices

mDNS Gateway as illustrated below supports both wireless and wired Bonjour Devices.



In most scenarios, some Bonjour devices may be directly connected to the switch or device. Bonjour services can be accessed even when the Bonjour device is connected via an Ethernet cable on a network.



CHAPTER 5

LSS (Location Specific Services) and mDNS AP

In release 7.5 additional Bonjour enhancements were added on the WLC. One of them is processing of mDNS service advertisements to support LSS. Basically all valid mDNS service advertisements received at the WLC will be tagged with the MAC address of the AP associated with the service advertisement from the Service Provider device, so in essence only clients connected to the same AP as the SP will have access to that service. LSS only applies to wireless SP-DB entries. There is no location awareness for wired SP devices.

To summarize,

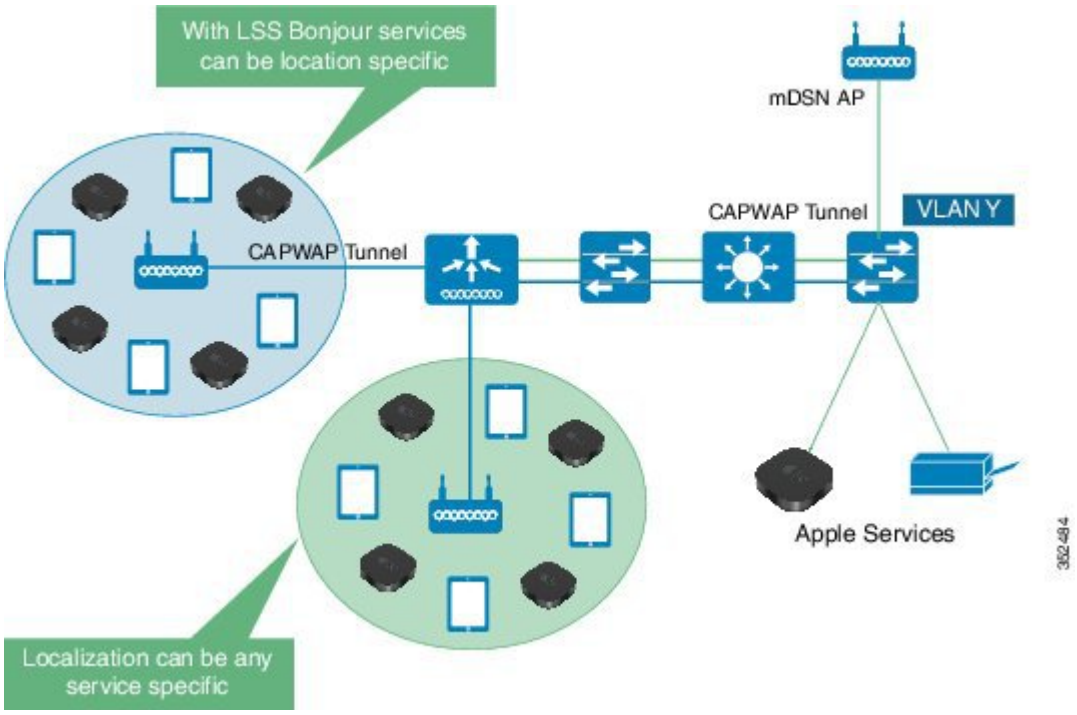
- LSS filtering applies only to wireless SP-DB entries.
- Wireless SP-DB entries are filtered based on the AP-NEIGHBOR-LIST if LSS is enabled for the service.
- Only client in the same “RF neighborhood” as the service provider will be granted permission to use that service

The location of clients and service providers is established by the MAC address of their associated AP's. The RRM DB provides the list of neighboring AP for any given AP and this information will be acted upon while filtering the SP-DB wireless entries in response to mDNS queries originating from wireless clients.

For Wired clients / service providers there is no sense of location that could be applied similarly and so the wired SP-DB entries cannot be filtered similarly.

Below is the network diagram of LSS enabled Bonjour gateway.

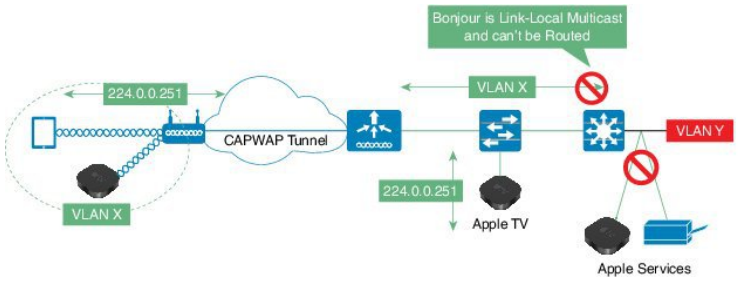
When the client query for the service the WLC using the client AP MAC address look up the RRM DB for the neighbor AP-list and filter the SP-DB for the service with the service provider's associate with the AP-list while responding to the query.



• mDNS AP, page 10

mDNS AP

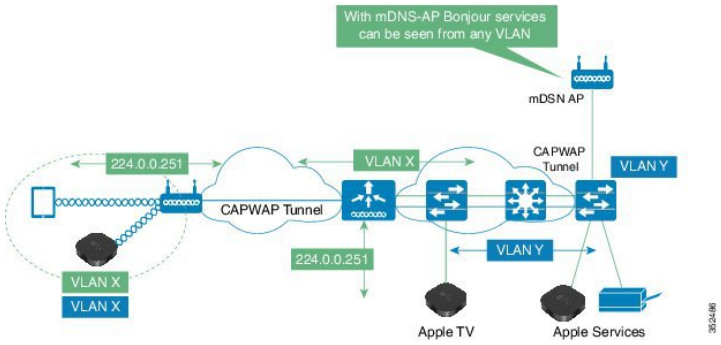
Bonjour mDNS as mentioned earlier, is a link local multicast and thus forwarded on Local L2 domain. Therefore mDNS services behind the Router or not L2 adjacent will not be seen by WLC in release 7.4 as illustrated below.

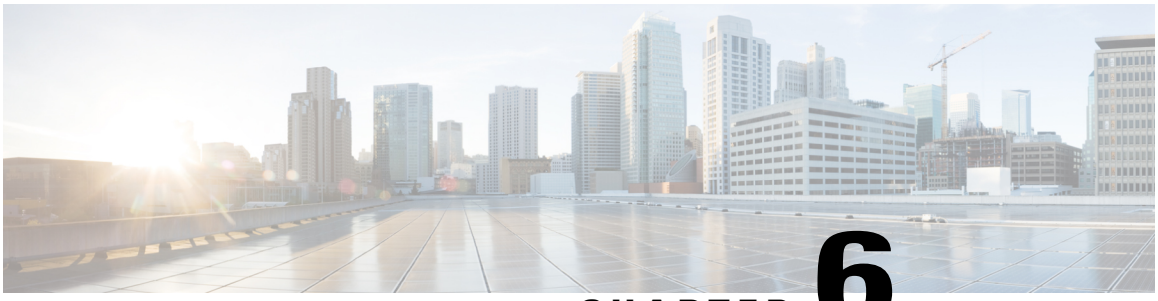


In release 7.5 the mDNS AP was added as enhancement and to correct the mDNS L2 limitations. mDNS AP has the ability to snoop wired Services on VLANs invisible to WLC

- This enhancement allows the controller to have the visibility of wired service providers, which are on VLANs that are not visible to the controller.
- VLAN visibility at the WLC is achieved by APs forwarding the mDNS advertisements to the controller.
- The maximum number of VLANs that AP can snoop is 10.

- This feature is supported on local and monitor mode AP.





CHAPTER 6

Bonjour mDNS enhancements in Phase III rel 8.0

Introduction to Bonjour Policies

Starting 8.0 release; the following new capabilities will be added to the Bonjour Services Directory functionality:

- Ability to apply granular access policies per unique service instance
- Ability to apply granular access policies based upon user-groups so two users can have differentiated access even though they are connected to the same SSID and get and IP address from the same VLAN
- Ability to define granular location per wired as well as wireless Bonjour Service(per Access Point or AP Group)

In release 8.0 the IT administrators can define how the service instance is shared, which is articulated as "service instance is shared with whom" i.e. user-id, "service instance is shared with which role/s" i.e. client-role and "what is the location allowed to access the service instance" i.e. client location. This configuration can be applied to wired and wireless service instances and the response to any query will solely be based on the policy configured for each service instance. This allows selective sharing of service instances based on the location, user-id or role.

Several customers have expressed preference to connect their Apple TV via the wired ethernet connection due to 802.1x capabilities. The 8.0 release allows filtering of wired services at par with wireless service instances. While mDNS profile associated with the client checks for service type being queried before responding to the query, the access policy further allows filtering of specific service instances based on querying client location and role or user-id. With Bonjour access policy there will now be two levels of filtering client queries, one (1) at the service type level by using the mDNS profile and then (2) at the service instance level using the access policy associated with the service each instance.

A service instance or a set of service instances discovered and cached by the WLC could be associated with an access policy filter which acts like a lens that determines which clients and what kind of client context [role or user-id] can see and access the service instance. Bonjour access policy filters can be configured for specific service instances identified by the MAC address of the devices publishing the services.

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

Currently we support a maximum of 5 service groups for a single MAC address.

Client Context Attributes

Any client initiating an mDNS query can be associated with a set of attributes that describe the context of the client and attributes like "location" can change dynamically when clients move to a different location. The user can formulate a rule by combining attributes with logical **OR** operations and attach the rule to the policy. A policy is composed of one **single rule**, even though we could provision for multiple rules.

mDNS Profile Attached to Local Policies

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

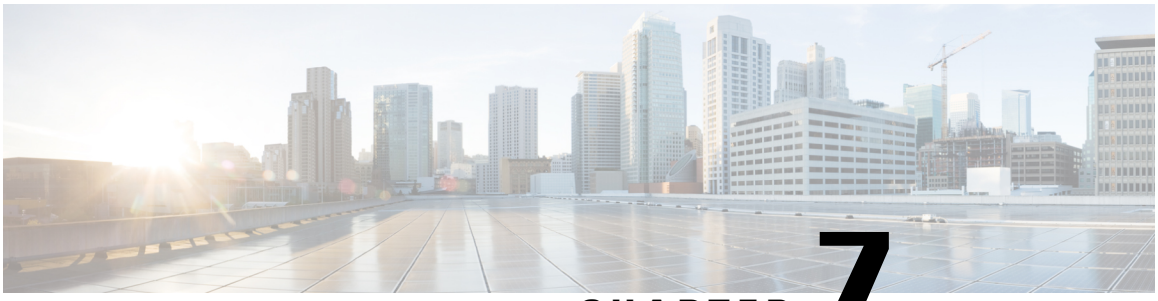
- Local policy just decides/controls if the service type is allowed or not
- Bonjour access policy for the specific service instance will eventually decide if the client can use the service.

Summary:

As shown in the examples above Teacher will have access to certain Apple TVs such as : Apple TV 1 and Apple TV 2 in specific location .

Student based on the policy designed will have only access to the Apple TV2 in specific location.

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

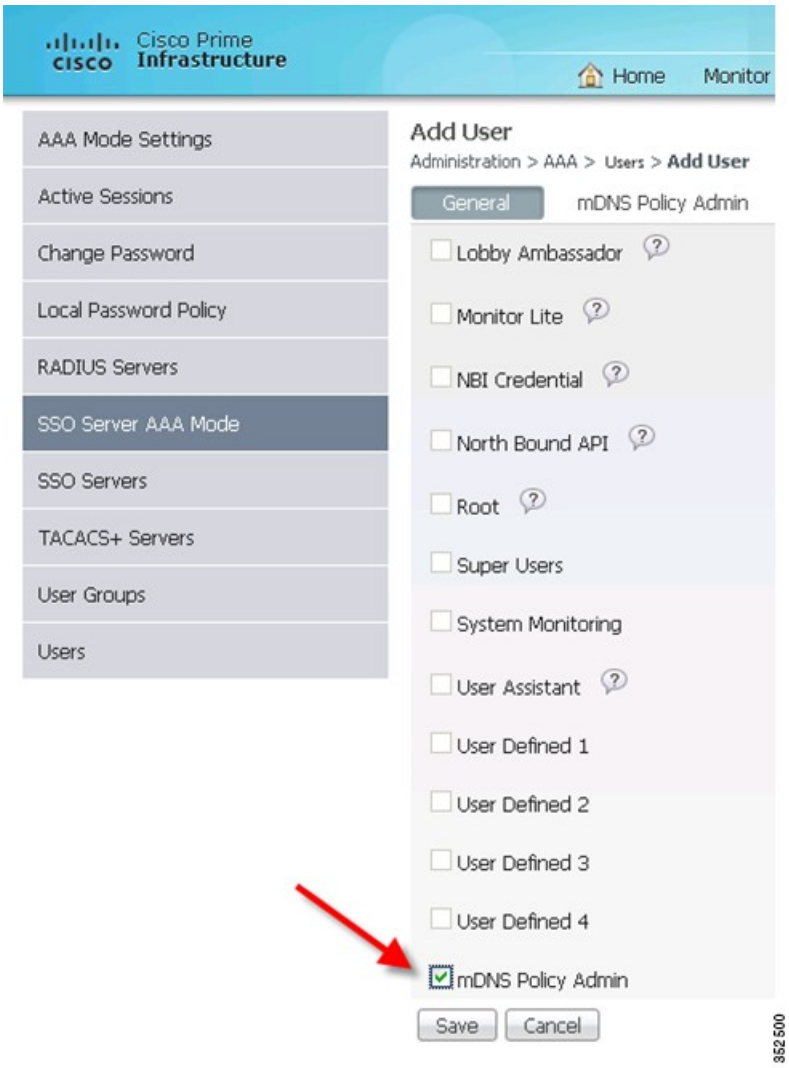


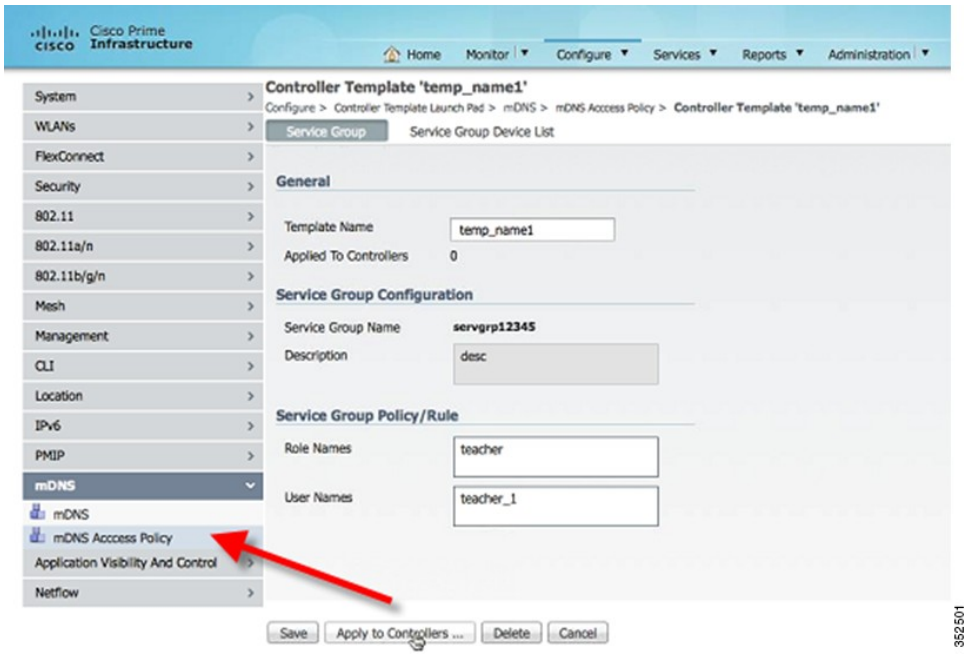
CHAPTER 7

(Optional) Cisco Prime Infrastructure Portal for Modifying User Access privileges per Service Instance

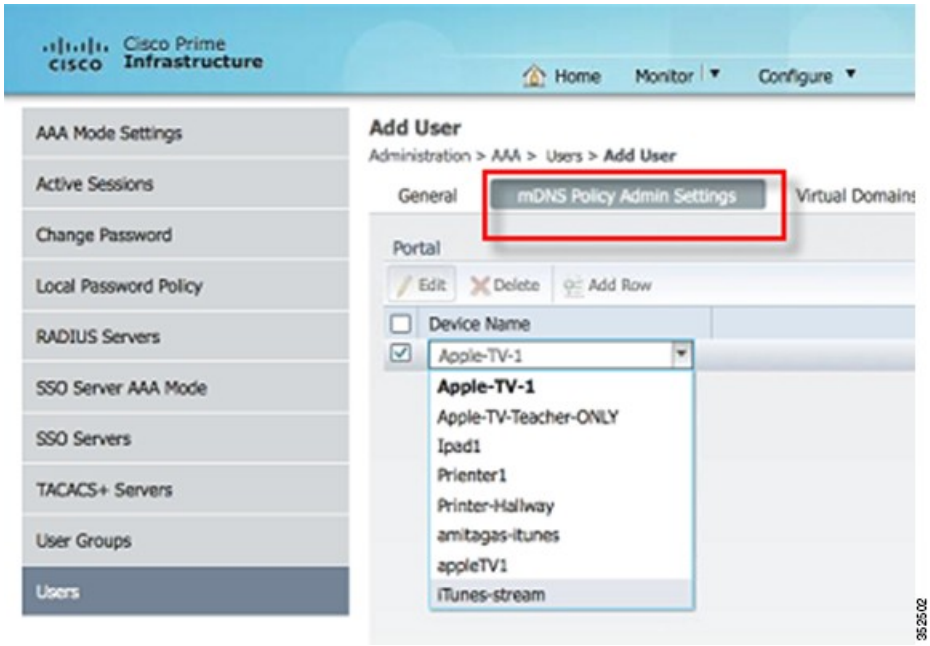
Another enhancement added in PI 2.2 is the capability of the Administrator or another pre-provisioned user to manage access privilege per service instance via the Cisco Prime Infrastructure portal.

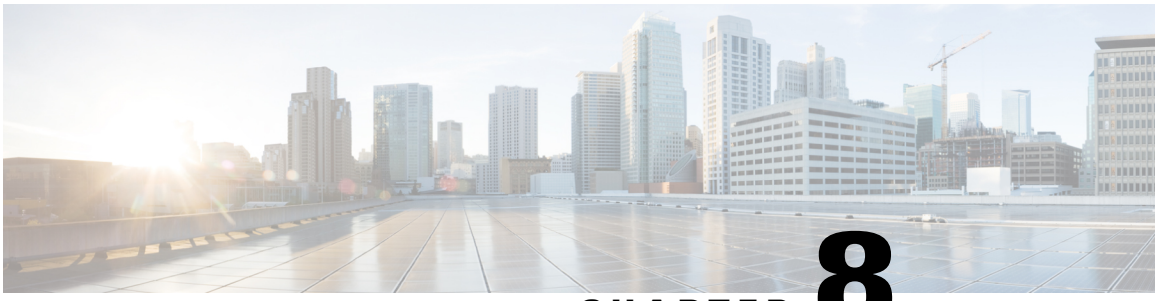
Imagine if the IT Administrator of a school allows each teacher privileges to access the Apple TVs in each classroom. Now in a particular class if a teacher wants to allow a student access to the Apple TV in that classroom; he/she can do so using the mDNS Policy Admin portal within PI. i.e. Student gets access to one specific Service Instance as oppose to all services the teacher has via the new PI Portal. This grant can be time specific and applied to multiple controllers.


Cisco Prime
Infrastructure
Home
Monitor
AAA Mode Settings
Active Sessions
Change Password
Local Password Policy
RADIUS Servers
SSO Server AAA Mode
SSO Servers
TACACS+ Servers
User Groups
Users
Add User
Administration > AAA > Users > Add User
General
mDNS Policy Admin
Lobby Ambassador
Monitor Lite
NBI Credential
North Bound API
Root
Super Users
System Monitoring
User Assistant
User Defined 1
User Defined 2
User Defined 3
User Defined 4
mDNS Policy Admin
Save
Cancel
352500



The policies can be very specific down to a specific service that the user can use.





CHAPTER 8

Summary of Features by Release

	WLC 7.4	WLC 7.5	WLC 8.0	WLC 8.0 + ISE 1.2	WLC 8.0 + Pi 2.1
Bonjour Gateway	Available	Available	Available		
Limit mDNS Over Air	Available	Available	Available		
Manage Bonjour Services on VLAN or WLAN	Available	Available	Available		
Manage Bonjour Services in Profiles	Available	Available	Available		
Manage Wireless Bonjour Services by Location		Available	Available		
Manage Bonjour SP with mDNS AP		Available	Available		
Manage Bonjour Wired and Wireless Services by Location			Available		
Manage Bonjour Services by Rule			Available	Available	
Manage Bonjour Services by Name				Available	
Manage Bonjour Services by Device			Available	Available	
User Assigned Bonjour Services					Available