·I|III|II CISCO

Cisco Wireless LAN Controller Bonjour Phase IV Deployment Guide, Release 8.1

Last Updated: June, 2015

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

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

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

http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-0/WLAN-Bonjour-DG.html

Overview

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

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

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

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

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

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



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

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

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

Table 1 on page 3 lists the services that are offered in phases 1, 2, 3, and 4.

Bonjour - 7.4 (Phase 1)	Bonjour - 7.5 (Phase 2)	Bonjour - 8.0 (Phase 3)	Bonjour - 8.1 (Phase 4)
 Bonjour service with mDNS gateway for wired and wireless services Bonjour service policy applied per interface or per WLAN 	 Support of mDNS services across L3 domains Introduction of mDNS AP for Bonjour service snooping on 10 wired VLANs 	 Bonjour GW with access policy controlled service discovery Device service mapping to access policy 	Number of supported services is scaled
 mDNS services cached on the controller 	 LSS - Location Specific Services 	 Bonjour group and single access policy management 	
 Bonjour services available on all controller seen L2 domains 	 Priority MAC of Bonjour service Origin based service diagonal 	 Bonjour profile control by local policy Introduction of Ponjour 	
 Bonjour services supported on the Anchor controller 	 6400 services and service providers per service type 	administrator to manage specific Bonjour services from	
 Bonjour services supported with L2 and L3 roaming 	Service type	Cisco Prime	
 100 services and 64 service providers per service type 			
 mDNS is not supported on access points in FlexConnect mode in a locally switched WLAN and mesh access points 			

Table 1Summary of Services in Phase 1, 2, 3, and 4

Introduction to Bonjour Policies and New Requirements

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

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



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

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

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

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

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



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

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

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

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

Bonjour Service Groups

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

In release 8.0, service limit: 6400 on 2500, 5508, WiSM2 and vWLC and 16000 services on 7510 and 8510 UC Controllers.

In release 8.1, the service limit has changed to be more reflective of number of the AP licenses and clients supported and will change accordingly on 5508 and WiSM-2 controllers.

	Bonjour Cache @ Full Scale	Bonjour Cache @ 80% Scale
5508 in 8.0 release	6400	6400
5508 in 8.1 release	1000	2400
WiSM2 in 8.0 release	6400	6400
WiSM2 in 8.1 release	2000	4800
5520, 7500, 8500, vWLC	16,000	16,000
2504 in 8.0 release	6400	6400
2500 in 8.1 release	Not supported	Not supported

As shown in the table, in release 8.1, 5508 controller is scaled down to support only 1000 services at full scale (500 APs and 7000 clients). With 80% scale (400 APs and 5400 users), the same 5508 controller supports 2400 services. Similarly, WiSM-2 supports 2000 services at full scale (1000 APs and 15000) and 4800 services at 80% scale. Number of Bonjour services remains unchanged on the 7500 and vWLC controllers. 5520 and 8500 series controllers support 16,000 services in release 8.1.

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

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

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

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

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

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

Table 2 on page 7 depicts a possible policy configuration with the service group named AppleTV-teachers.

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

 Table 2
 Example for Policy Configuration with the Service Group Name

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

Device Access Policy Constructs and Rules

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

Client Context Attributes in an mDNS Policy

Any client initiating an mDNS query can be associated with a set of attributes that describe the context of the client. The attributes, for example location, can change dynamically when the clients move to a different location. Only these enumerated attributes will be used to articulate a Bonjour access policy rule. The list of attributes and how they are fetched are detailed in Table 3 on page 8. The user can formulate a rule by combining these attributes with logical OR operations and attach the rule to the policy. A policy is composed of a single rule, even though multiple rules can be provisioned.

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

Table 3Attributes and Their Usage

Service Instance	List	
MAC ADDRESS		
NAME	Add	
LOCATION TYPE	AP Group	
LOCATION	AP Group AP Name	4
(Location value 'Any	AP Location (means no poncy check on location attribute will be performed.)	35329

Access Policy Rules

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

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

RULE is defined as,

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

Policy/Rule	(Policy is enforced if any of the below condition	is is met)
Role Names	student	
User Names	ma	

Configuring mDNS Bonjour Policies

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

- 1. On the Controller tab, in the left pane, click mDNS > General.
- 2. In the right pane, in the Global Configuration area, check the mDNS Global Snooping and mDNS Policy check boxes.

cisco	MONITOR WLA		WIRELESS S	ECURITY M		INT CO	OMMANDS	HE	:LP
Controller	mDNS								
General Inventory	Global Configur	ation							
Interface Groups	mDNS Global Sr	ooping				-			
Multicast	mDNS Policy				-	-			
Network Routes	Query Interval (10-120)		10	(min:	5)			
Redundancy									
Internal DHCP Server	Master Service	s Database							
Mobility Management	Select Service	[None	6					
Ports	Query Status	1							
• NTP	LSS Status	1							
CDP	Origin	LL ~							
PMIPv6		and the second							
F IPv6		Add							
mDNS	Service Name		Service String		Query Status	LSS Status	Origin		
Profiles	AirTunes		_raoptcp.local.		2		ALL	~	E
Domain Names mDNS Browser	Airplay		_airplaytcp.local.		V		ALL	¥	2
mDNS Policies	HP Photosmart P	ninter 1	_universalsubip	ptcp.local.	V		ALL	~	-

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

WIc > config mdns policy enable

```
(Cisco Controller) >config mdns policy ?
disable Enable / Disable mDNS access policy.
enable Enable / Disable mDNS access policy.
service-group Configures mDNS service-group.
(Cisco Controller) >config mdns policy enable
```

- 3. To configure the mDNS Service group, do the following:
 - a. On the Controller tab, in the left pane, click mDNS > mDNS policies.
 - b. In the right pane, click Add Group.
 - c. In the Add New mDNS Service Group area, enter the group name and description for the mDNS service group.
 - d. Click Add.

 cisco	MONITOR WLA		WIRELESS	SECURITY	MENAGEMENT	Sign Co COMMANDS	nfiguration Eng HELP EEEDBAC	Logout Befresh X
Controller General Inventory	mDNS Service	Groups Service Group			Ð	atries 1 - 3 of 3	-	Add Group
Interfaces Interface Groups Multicast > Network Routes > Redundancy > Internal DHCP Server > Mobility Management	mDNS Service G Description Number of mDNS Number of Admir mDNS Service G	Policies Created Policies roup Name	Cancel 3 3 Description		Origin			
Ports	ATV-student		Apple TV for s	tudent use	WLC			
h NTD	ATV-teather		Apple TV for t	eacher use	WLC			
E COD	default-mdns-polis	a.	Default Acces	s Policy created	f by WL: WLC			
PMIPv6 PMIPv6 mDNS General Profiles Domain Names mDNS Browser mDNS Proviser								

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

WIc> config mdns service-group create

(Cisco Controller	>config mdns policy service-group create ?	
(service-group-na	me> Enter a mDNS service-group name. 🔶 👘	
(Cisco Controller	>config mdns policy service-group create	53299

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

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



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



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

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

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

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

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

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

ւվուի։ cisco	MONITOR WLAN	s <u>c</u> ontroller	WIRELESS	<u>s</u> ecurity	MANAGEMENT	СОММА
Controller General Inventory Interfaces Interface Groups	mDNS Service (mDNS Service Gr Service Instance	Groups > Edit roup Name ^{A'} 9 List	TV-teacher			
Multicast Network Routes Redundancy Internal DHCP Server Mobility Management Ports	MAC ADDRESS NAME LOCATION TYPE LOCATION (Location value 'A MAC ADDRESS	10:40:f3:ef:06:f9 Apple TV 2 AP Group Other ny' means no policy NAME	Add Any check on location	n attribute will	I be performed.)	
▶ NTP	00:1d:e0:08:18:b7	Reflector	AP Grou	ip A	ny	
▶ CDP	10:40:f3:e5:d1:b6	Apple TV1	AP Grou	ip A	ny	
PMIPv6	10:40:f3:ef:06:f9	Apple TV 2	AP Grou	ip A	iny	
▶ IPv6	b0:e8:92:58:75:a3	Printer	AP Grou	ip A	ny	
 mDNS General Profiles Domain Names mDNS Browser mDNS Policies Advanced 	Policy/Rule (P Role Names ta User Names	olicy is enforced if a	any of the below o	conditions is m	net)	

The mDNS service groups are listed after being created.

 cısco		N WIRELESS SECURITY MAN	AGEMENT C <u>O</u> MMA	NDS
Controller	mDNS Service Groups			
General Inventory	mDNS Service Group Name	Description	Origin	
Interfaces	ATV-student1	Apple services for Student1	WLC	
Interface Groups	ATV-teacher	Apple TV services for teachers	WLC	
Multicast	Guest Serice	Services for Guests	WLC	
Natuork Poutos	default-mdns-policy	Default Access Policy created by W	L WLC	
 Mobility Management Ports NTP CDP PMIPv6 				
h IBu6				
mDNS General Profiles Domain Names mDNS Browcer mDNS Prolicies				

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

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

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

cisco Identity Services Engine	Home Operations Policy Administration	
System Identity Management Identities Groups External Identity So	Network Resources Neb Portal Management De Feed Service urces Identity Source Sequences Settings	
Identities	Vetwork Access Osers ✓ Edk + Add Change Status + @elmport @ Expert + XDelete + P_Duplicate	Une Marillo Car
Users Endpoints	Status Name Description Hist Name Last Name Email Address Status Address Status Address Status Address Status Address	User Identity Gro
Latest Manual Network Scan Results	Benabled 1 Student1 Enabled 1 Teacher1	Teachers

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

cisco Identity Services Engine		ation 🔻
🔆 System 🏾 🖉 Identity Management	Network Resources 🛛 🔠 Web Portal Management 🛛 🗔	Feed Service
Identities Groups External Identity Sources	Identity Source Sequences Settings	
Identity Groups	User Identity Groups	
	/ Edit - Add XDelete - @ Import @ Export	•
	Name	Description
Ser Identity Groups	ActivatedGuest	Users can bypass the Guest portal and access the ner
Endpoint Identity Groups	Employee	Default Employee User Group
	🗆 😤 Guest	Users must first sign into the network using the Gues
	SponsorAllAccount	Default Sponsor All Accounts
	SponsorGroupAccounts	Default Sponsor Group Accounts
	SponsorOwnAccounts	Default Sponsor Own Accounts
	Students	
	Teachers	212
		25,200

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

ditulto	ISEIS-MA admn Logaut Feedback	
Authentication Authorization Conditions Results	Administration Policy Administration Profiling Posture Gent Provisioning Security Group Access Policy Elements	Setup Assistant * P
Results	Authorization Profile Authorization Profile Name borjour-student Description * Access Type Access Accept Service Template DAL Name VLAN	
 Clent ProvisionIng Security Group Access 	Voice Domain Permission Web Redirection (CWA, DRW, MDM, NSP, CPP) Auto Smart Port Fitter-ID Advanced Attributes Settings Ciscoccisco-av-pair role=student	

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

student.

	-			
Cisco.cisco-ar-pai		lide-student	v	- 20
		_		
r Attributes Details		1		

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

	E R	ports	ig the	ont Protection S	enice Tracke	shoot							
Miscori	figured t	luppikan	6 ^{(j}		Miconilg	ured Network Devi 0	Cert (F)		RADBUS Drops 1	x.		Clerit Sto	oped Responding (7) 0
Show Live Sessons	Adder	Femore (Columns *	Refresh									Refresh Every 5 sec
me .	Status	Details	Repeat	Identity	Endpoint 3D	Endpoint Profile	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Server	Event
813-10-31 08:53:59.30	0		0	mine-student	F8:27-93:14:06:14						Not4pplicable	ISE12-MA	Session State is Authentica
013-10-31 08:53:59.30		ġ.		mke-student	F8.27.93.14.06.14		wit		bonjour-studient	User Identity Group.	NotApplicable	ISE12-MA	Authentication succeeded
013-10-31 08:50 14:90		.0		mile student	F8:27.92.14:06:14		we					19E12-MA	
013-10-31 08:45:00.715	5	a		mie-student	F8:27:93:14:06:14		wic		PermitAccess	User Identity Group.	NotApplicable	ISE12-MA	Authentication succeeded
013-10-31 08:44 17:30		.0		student	F8:27:93:14:06:14		wt					ISE12-MA	Authentication failed
013-10-31 08:42:24.15	0	.0			FB:27/9214:06:14		wic					ISE12-MA	RADBUS Request chopped

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

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

ululu cisco	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMEN	NT.
Controller General Inventory	MDNS Pr	rofiles Profiles 2					
Interfaces	Profile Na	me			N	. Of Services	
Interface Groups	default-md	ins-profile			0		1.1
Multicast Network Routes	sudent-Bo	njour	-		0		•
▶ Redundancy							
▶ Internal DHCP Server							

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

Authentication 💿 Authorization 📿 Pr Dictionaries Conditions Results	ofling 😨 Posture 🧕 Clent Provisioning 🚍 Security Group Access
Results	
	Advanced Attributes Settings Cisco:cisco-av-pair O = role=student O Attributes Detais Access Type = ACCESS_ACCEPT forces.user = mCMES_profile page attrifact Boolean

The figure below shows the ACS server configuration.

ababa	User Setup		
CISCO		1	Halp
User Setup			Account Disabled Delating a Visemann Supplementary line Tele
Greup Satup	Cisco IOS/PIX 6.x RADIUS Attributes		Password Authentication Group to which the user is assigned
Shared Profile Components	☑[009\001] cisco-av-pair		Ginot I Address Assignment Advanced Settings
Network Configuration	role=student		Network Access Restrictions Max Sestions Unact Double
Configuration			Account Disable Downloadable Atla Advanced TACACS+ Settings
Configuration	4		TACACS+ Enable Control TACACS+ Enable Reserved TACACS+ Conduct Reserved
Distances			IACASS Shell command Authorization Command Authorization Command Authorization for Network Device Management Applications
Portuse Validation	IETF RADIUS Attributes		Interface Section Service Interface Section Service RAD105 Vendor-Specific Attributes
Profiles	E[006] Service-Type		Time Bound Alternate Group
Reports and Activity	Authenticate only		Account Disabled Status
Call Coller	[007] Framed-Protocol		Select the Account Disabled check box to disable this account; clear the check box to enable the account.
Cars coordination	E [009] Framed-IP-Netmask		[Back to Top]
	0.0.0.0		Deleting a Username
	E[010] Framed-Routing		The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click Delete . When asked to confirm your action, click DK .
	Submit Delete Cancel		[Back to Top]

mDNS Profile Attached to Local Policies

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

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

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

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

CISCO	MONITOR WLANS CONTROLL	ER WIRELESS	ECURITY MAN	GEMENT CO	AMANDS HELP	P EEEDBACH
Security	Policy > Edit					
 AAA General RADIUS Authentication Accounting Fallback DNS Dewnloaded AVP TACACS+ LDAP 	Policy Name Policy Id Match Criteria Match Role String Match EAP Type	teacher EAP-FAST 👻		Staff 2		
Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	Device List Device Type	Apple-IPhone		•	add 1	
Local EAP Advanced EAP	Action				100	
Priority Order Certificate	IPv4 ACL	none •				
Access Control Lists	VLAN ID	0				
Wireless Protection	Qos Policy	none	•			
Policies	Session Timeout (seconds)	1800				
Web Auth	Sleeping Client Timeout (min)	720				
TrustSec SXP	Flexconnect ACL	none ·				
Advanced	AVC Profile	none 💌				
Harmeed	mDNS Profile	Teacher Class Pol				
	Active Hours					
	Day Start Time End Time	Mon Mours Hours	Mins Mins			

Use Cases for mDNS Bonjour Policies Deployments

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

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

Table 4Use Cases

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

USE Case #1 Deployment

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

Table 5Use Case #1

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

As mentioned in the Configuring mDNS Bonjour Policies, page 9 section, do the following to deploy the use case:

- 1. On the Controller tab, in the left pane, click mDNS > General.
- In the right pane, in the Global Configuration area, check the mDNS Global Snooping and mDNS Policy check boxes to enable the mDNS gateway services on the controller. This enables the Bonjour policies on the controller. Also, under services, ensure to enable desired Apple services for the controller to snoop.

cisco	MONITOR WLANS	CONTROLLER	WIRELESS SECUR	RITY MAN	AGEMEN	п со	MMANDS	HELP	EEEDBAC
Controller	mDNS	ų	1						
General Inventory	Global Configuration	on							
Interfaces Interface Groups Multicast Network Routes	mDNS Global Snoos mDNS Policy Ouery Interval (10-	ing 120)		V 15	(mins)				
Redundancy Internal DHCP Server	Master Services D	atabase							
 Mobility Management Ports NTP 	Select Service Query Status 🗌 LSS Status 🗌	1	lone	~					
CDP PMIPv6 IPv6	Origin ALL				1.000				
# mDNS General	Service Name	5	ervice String		Status	Status	Origin		
Profiles	AirTunes		raoptcp.local.	[2 [ALL		
mONS Browser	Airplay		_airplaytcp.local.	[2 (ALL	× 🖸	
mDNS Policies	HP Photosmart Printe	r 1 .	universal_sub_ipp_top	p.local.	2 [ALL	×	
Advanced	HP Photosmart Printe	r. 2	cupssubipptcp.loc	al. [2 [ALL	× 🖬	
	Printer-IPP		ipptcp.local.	[2 [ALL	× 🖬	
	Printer-IPPS		ippstcp.local.	(2 (ALL	× 🖬	
	Printer-LPD	1	printertop.local.	[2 (3	ALL	× 🖬	
	Brights PACHET		adi-datactroases too los	al la	21		ALL	~	

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

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

cisco		ER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Controller General Inventory Interfaces Interface Groups Multicast Network Routes Redundancy Internal DHCP Server	mDNS Profile > Edit Profile Name Profile Id Service Count No. of Interfaces Attached No. of Interface Groups Attached No. of Wlans Attached Services List					default 1 8 2 0 3	t-mdns-profil
Mobility Management Ports NTP CD0	Service Name	AirTunes	×			E.	
P COP	Service Name						
F PMIPVO	AirTunes						
F IPVD	Airplay						
w mDNS	HP_Photosmart_Printer_1						
Profiles	HP_Photosmart_Printer_2						
Domain Names	Printer-IPP						
mDNS Browser mDNS Policies	Printer-IPPS						
b. Advanced	Printer-LPD						
P Advanced	Printer-SOCKET						

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

cisco		INTROLLER WIRELESS	SECURITY	MANAGEMENT COM	MANDS HELP EEEDBAC	к
Controller	Interfaces					
General	Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Managemen	ŧ
Interfaces	ave vian	72	10.72.0.20	Dynamic	Disabled	
Interface Groups	bohiour client vian	73	10.73.0.20	Dynamic	Disabled	
Multicast	boniour vlan	71	10.71.0.20	Dynamic	Disabled	
Network Routes	management	70	10.70.0.62	Static	Enabled	
Redundancy	redundancy-management	70	0.0.0.0	Static	Not Supported	
Keudidancy	redundancy-port	untagged	0.0.0.0	Static	Not Supported	
Internal DHCP Server	service-port	N/A	10.10.10.10	Static	Disabled	
Ports	virtual	N/A	1.1.1.1	Static	Not Supported	

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

cisco	MONITOR WLANS CON	TROLLER WIRELESS SECURIT	y Management Commany	OS HELP EEEDBACK		Sage Contiguration Eng	Logout Eebresh
Controller General Inventory	mDNS Domain Name I	P > Summary P Entries 7					
Interfaces	Domain Name	MAC Address	IP Address	vian Id	Type	TTL (seconds)	Time Left (seconds)
Interface Groups	Apple-TV-2-room2.local.	10:40:f3:ef:06:f9	10.71.0.79	71	Wireless	4725	4086
Multicast	Apple-TV4-room4.local.	28:e7:df:d9:56:2d	10.71.0.80	71	Wireless	4725	4066
Network Routes	Dell-M2300-MA2.local.	00:1c:23:36:3e:d0	10.70.0.59	70	Wired	4725	4086
Redundancy	Dell-M2300-MA3.local.	00:1d:e0:08:18:b7	10.71.0.82	71	Wireless	4725	3166
Internal DHCP Server	EPSON5875A3.local.	b0:e8:92:58:75:a3	10.71.0.81	71	Wireless	4725	4086
Mobility Management	Office-Apple-TV-1.local.	10:40:f3:e5:d1:b6	10.70.0.167	70	Wired	4725	4086
Daste	Office-Apple-TV-3.local.	70:56:81:db:cd:a0	10.70.0.209	70	Wired	4725	4056
NTP COP PMIPv6 PMIPv6 IPv6 mDNS General Consis Names mONS Proteins mONS Proteins	I. Neximum of 500 entries	will de G epleyed.					

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

WLANs	WLANs						
WLANS WLANS	Current Filt	er: None	[Change Filter] [C	llear Filter]	Cr	reate New 🥑 🔽 Go	
Advanced	WLAN II	О Туре	Profile Name	WLAN SSID	Admin Status	Security Policies	
		WLAN	Bonjour-demo	Bonjour-demo	Enabled	[WPA][Auth(802.1X)]	
	2	WLAN	Bonjour services	bonjour-service	Enabled	[WPA][Auth(PSK)]	
	2	WLAN	Bonjour Client	bonjour-client	Enabled	802.1X	

7. Enable the AAA server.

ululu cisco	MONITOR WLANS	<u>C</u> ONTROLLER WIRELESS SE	CURITY MANAGI	EMENT COMMANDS
WLANs	WLANs > Edit Bo	njour Client'		
WLANS	General Securit	ty QoS Policy-Mapping	Advanced	
Advanced	Layer 2 Laye	r 3 AAA Servers		
	Select AAA server Radius Servers Radius Server Ov	s below to override use of defau rerwrite interface □Enabled	It servers on this	WLAN
	Authentication Ser	vers Accounting Servers		EAP Parameters
	Server 1	Enabled IP:10.91.104.107, Port:1812	Enabled	Enable
	Server 2	None	V None V	

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

VLANs	WLANs > Edit 'Bonjour	Client'	URITY MENAGEMENT	COMMANDS HELP EEEDBACK
WLANS WLANS	General Security	QoS Policy-Mapping	Advanced	
Advanced	Allow AAA Override	Enabled		DHCP
	Coverage Hole Detection	Enabled		DHCP Server
	Enable Session Timeout	1800		
	Aironet IE	Session Timeout (secs)		DHCP Addr. Assignment 🗹 Required
	Diagnostic Channel	Enabled		OEAP
	Override Interface ACL	IPv4 None M	IPv6 None 😒	Split Tunnel (Printers) Enabled
	Layer2 Ad	None 💌		Management Frame Protection (MFP)
	P2P Blocking Action	Disabled 💌		
	Client Exclusion ¹	Enabled 60 Timeout Value	(secs)	MFP Client Protection # Optional M
			mDNS	-
			mDN: Snoo	S ping 🗹 Enabled

- **9.** After general configurations for the mDNS are complete, configure Bonjour policy so that the following occurs upon users authentication:
 - a. Teacher authenticates and gets access to Reflector, Apple TV1, and Apple TV2 in any location.
 - b. Student authenticates and gets access to only Apple TV1 in any location.
 - c. Guest authenticates and gets no access to any Bonjour service.
- 10. Create mDNS service groups under Controller > mDNS Policies.

ahaha	_					Sa <u>v</u> e Cor	nfiguration <u>P</u> ir	ng Logout <u>R</u> efres
CISCO	MONITOR	WLANS		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP EEEDBAC
Controller		mDNS \$	Service Group	S				Add Group
General		mDNS S	ervice Group Na	me D	escription		Origin	
Interfaces	-	ATV-stud	ent1	1	Apple services	for Student1	WLC	
Interface C	roune 🐋	ATV-teac	her	,	Apple TV servic	es for teachers	WLC	
Multicact	roups	Guest Se	rice	5	Services for Gu	ests	WLC	
Network Ro	outes /	default-m	ndns-policy	C	Default Access	Policy created by V	VL WLC	

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

alludia				Sage Co	nfiguration
cisco	MONITOR WLANS CON	ROLLER WIRELESS SECUR	TY MANAGEMENT COMMAND	S HELP EEEDBACK	
Controller	mDNS Domain Name IF	> Summary			
General Inventory	Number of Domain Name-1	Entries 4			
Interfaces	Domain Name	MAC Address	IP Address	Vian 1d	Type
Interface Groups	Dell-M2300-MA2.local.	00:1c:23:36:3e:d3	10.70.0.59	0	Wired
Multicast	EPSON5875A3.local.	1c:df:0f:c6:a1:a4	10.71.0.50	71	Wired
Network Routes	Office-Apple-TV-1.local.	10:40:f3:e5:d1:b6	10.70.0.102	0	Wired
Redundancy	Office-Apple-TV-3.local.	70:56:81:db:cd:a0	10.70.0.117	0	Wired
 Mobility Management Parts NTP CDP PMIPv6 IPv6 mDNS General Profiles Domain Names mDNS Profices 	1. Maximum of 500 entries	will be displayed.			

cisco		Ns <u>C</u> ONTROLLER	WIRELESS SECURIT	Y MANAGEMENT	C <u>O</u> MM
Controller General Inventory Interfaces	mDNS Service mDNS Service	Groups > Edit Group Name A ce List	TV-teacher		
Multicast Network Routes Redundancy Internal DHCP Server Mobility Management Ports	MAC ADDRESS NAME LOCATION TYPE LOCATION (Location value	AP Group V Other V Any' means no policy	Add Any check on location attribute	will be performed.)	
▶ NTP	00:1d:e0:08:18:b	7 Reflector	AP Group	Any	
▶ CDP	10:40:f3:e5:d1:b	6 Apple TV1	AP Group	Any	
▶ PMIPv6	10:40:f3:ef:06:f9	Apple TV 2	AP Group	Any	
▶ IPv6	b0:e8:92:58:75:a	3 Printer	AP Group	Any	
 mDNS General Profiles Domain Names mDNS Browser mDNS Policies 	Policy/Rule Role Names User Names	(Policy is enforced if a	any of the below conditions	is met)	

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

cisco	MONITOR WL	ANS <u>C</u> ONTROLLE	R WIRELESS	SECURITY N	IANAGEMENT	CQN
Controller	mDNS Servic	e Groups > Edit				
General Inventory Interfaces	mDNS Service Service Instar	e Group Name nce List	ATV-student1			
Multicast Network Routes Redundancy Internal DHCP Server Mobility Management	MAC ADDRESS NAME LOCATION TYP LOCATION (Location value	S AP Group V Other e 'Any' means no polici	Add Any cy check on locatio	n attribute will b	e performed.)	
▶ NTP	MAC ADDRESS	NAME	LOCAT	ION-TYPE LOO	ATION	-
CDR	00:1d:e0:08:18:	:b7 wireless refle	ctor AP Gro	up Any	r	
F CDP	b0:e8:92:58:75:	a3 Apple TV 1	AP Gro	up Any	1	1
PMIPV6	Policy/Rule	(Policy is enforced it	any of the below	conditions is met	t)	-
 mDNS General Profiles Domain Names mDNS Browser mDNS Policies 	Role Names User Names	student				

	cisco	_	MONITOR	<u>W</u> LANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK	54	<u>ye</u> Configuration	Eus III	(Juego	Befresh
M	onitor												Entries 1 - 3 of	э		
* *	Summary Access Points Cisco CleanAir		None	L	Change Filter) (Cir	uar Filter)	AN Profile	WI AN SET	Em	or Mande	P	rotocol	Status	Auth	Bort	Slat Id
	Statistics	-	IP Addres		AF Name	WL	AS Prome	WLAN SSIL		er manne		010001	status	Auth	Furt	SIGCIO
			10.71.0.56		APd0d0.fd45.3	3526 Bor	your-test	Bonjour-test	st st	udent	80	12.110	Associated	Tes	1	0
*	CDP		10.71.0.50		APd0d0.fd45.3	b26 Bor	jour-test	Bonjour-test	te	acher	80	2.11a	Associated	Yes	1	1
۶	Rogues	-	10.71.0.58		APd0d0.fd45.3	b26 Bor	ujour-test	Bonjour-test	te te	acher	80	2.118	Associated	Yes	1	1
	Clients	_			1		e nor concerne		-				the second s	4	1	

Summary

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

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

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



Use Case #2 Deployment

Table 6Use Case #2

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

To configure the policy, perform the following steps:

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

Controller	mDNS Service Groups	> Edit	
General Inventory Interfaces Interface Groups	mDNS Service Group Na	ME ATV-teacher	
Multicast Network Routes	MAC ADDRESS 70:56: NAME Apple 1	81:db:cd:a0 ┥ FV2 🔶 Add	
 Redundancy Internal DHCP Server 	LOCATION TYPE AP Name	ne V AP2600-8aba	-
 Mobility Management Ports 	(Location value 'Any' mean:	no policy check on location attrib	bute will be performed.)
NTPCDP	10:40:f3:e5:d1:b6 Appl	e TV1 AP Name	AP2600-8aba
PMIPv6	Policy/Rule (Policy is en	forced if any of the below condition	ons is met)
▶ IPv6	Role Names teacher		
 mDNS General Profiles Domain Names 	User Names		

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

Controller	mDNS Domain Name IP	> Summary			
General Inventory	Number of Domain Name-IP	Entries 4			
Interfaces	Domain Name	MAC Address	IP Address	Vlan Id	Туре
Interface Groups	Dell-M2300-MA2.local.	00:1c:23:36:3e:d3	10.70.0.59	70	Wired
Multicast	EPSON5875A3.local.	b0:e8:92:58:75:a3	10.70.0.178	70	Wired
Network Routes	Office-Apple-TV-1.local.	10:40:f3:e5:d1:b6	10.70.0.167	70	Wired
Redundancy	Office-Apple-TV-2.local.	70:56:81:db:cd:a0	10.70.0.209	70	Wired

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

Wireless	S	All APs			
Acces	s Points	Current Filter	None	e [Chano	<u>ae Filter] [Clear Filter]</u>
* Radio: 80	s)2.11a/n/ac	Number of APs	5		
80 Du Globa	J2.11b/g/n ual-Band Radios I Configuration				
Advar	nced	AP Name	IP Address	AP Model	AP MAC
Mesh		AP6c20.560e.1a26	10.70.0.150	AIR-CAP1602E-A-K9	6c:20:56:0e:1a:26
DE De	ofiles	AP0022.90e3.3752	10.70.0.151	AIR-LAP1142N-A-K9	00:22:90:e3:37:52
RF PT	ones	APd0d0.fd45.3b26	10.70.0.153	AIR-LAP1042N-A-K9	d0:d0:fd:45:3b:26
FlexC	onnect Groups	AP2600-891d	10.70.0.154	AIR-CAP2602E-A-K9	44:2b:03:9a:89:1d
▶ 802.1	lla/n/ac	AP2600-8aba	10.70.0.155	AIR-CAP2602I-A-K9	44:2b:03:9a:8a:ba

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

С	ontroller	mDNS Service	Groups > Edit			
	General Inventory Interfaces Interface Groups Multicast Network Routes Redundancy Internal DHCP Server	MDNS Service	Group Name ATV	-student1 Add Any heck on location attribute	will be performed.)	
1	Ports					
•	NTP	10:40:f3:e5:d1:b	6 Apple TV1	AP Name	AP2600-8aba	
•	CDP					17
Þ	PMIPv6	Policy/Rule	(Policy is enforced if any	of the below conditions i	is met)	
Þ	IPv6	Role Names	student			
•	mDNS General Profiles Domain Names mDNS Browser mDNS Policies	User Names				
	Controllor	mDNS Sor	uiae Creune > Edit			
	Controller	1110142 261	nce Groups > Ealt			

Conoral					
Inventory	mDNS Service	Gro	oup Name ATV-t	eacher	
Interfaces	Service Insta	nce	List		
Multicast	MAC ADDRESS	6			
Network Routes	NAME			Add	
Redundancy	LOCATION TYP	E	AP Group 💌		
Internal DHCP Server	LOCATION		Other 💌	Any	
Mobility Management	(Location value	An	y' means no policy che	ck on location attrib	ute will be performed.
Ports	MAC ADDRESS	_	NAME	LOCATION-T	PE LOCATION
▶ NTP	10:40:f3:e5:d1:	b6	Apple TV1	AP Name	AP2600-8aba
▶ CDP	70:56:81:db:cd	a0	Apple TV2	AP Name	AP2600-8aba
 PMIPv6 IPv6 	Policy/Rule	(Po	licy is enforced if any o	of the below conditio	ons is met)
▼ mDNS	Role Names	tea	acher		
General Profiles Domain Names mDNS Browser mDNS Policies	User Names				

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

Debugging Bonjour



Summary

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

Debugging Bonjour

Following are the commands to debug Bonjour:

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

The above debugs are enhanced for the new features also.

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

Bonjour browser

- Bonjour browser is a cache of all the service advertisements seen at the WLC and not discovered because configuration did not allow learning.
- Service advertisements across all VLANs and ORIGIN types that are not learnt are displayed.
- Bonjour browser is a cache of top 500 entries.
- The user can add services by picking them from the Bonjour browser instead of typing the string.

Debugging Bonjour

		DELTE	- 1100 £00			
umber of S	ervices.					
Origin	VLAN	TTL (sec)	TTL left (sec)	Client MAC	AP-MAC	Service-string
ireless	11	4500	4377	9c:20:7b:fl:fd:cb	64:d9:89:42:34:70	device-info. tcp.local.
DNS AP	105	4500	777	28:e7:cf:ec:e9:51		_device-infotcp.local.

Bonjour SSO

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

Show Commands on WLC

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

Clear commands

To clear the mDNS database learned dynamically per service:

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

Show commands on AP CLI

AP3600# show capwap mcast mdns

Debugging Bonjour