**Enterprise**



**Solution Requirements Document**

**mDNS/SSDP (UPnP-DLNA) support across L3 Network**

**Author(s): Sindhu Mohandas**

**Revision: 7**

**Date: 26 May, 2016**

**Copyright © 1995-2016**

**ALE USA, Incorporated**

**ALL RIGHTS RESERVED WORLDWIDE**

**ALE USA, Inc.**

**26801 West Agoura Road, Calabasas, CA 91301**

**(818) 880-3500**

This specification contains information of a confidential and/or proprietary nature. Neither this specification nor any of the information contained herein may be reproduced, used or disclosed to or for the benefit of any other person or entity without the express written consent of ALE USA, Incorporated.

**TABLE OF CONTENTS**

[TABLE OF CONTENTS 2](#_Toc450297224)

[1 REVISION HISTORY 3](#_Toc450297225)

[2 Overview 5](#_Toc450297226)

[3 Use Cases 6](#_Toc450297227)

[4 SMB Solution REQUIREMENTS & ANALYSIs 7](#_Toc450297228)

[4.1 Requirements 7](#_Toc450297229)

[4.2 Analysis 7](#_Toc450297230)

[4.2.1 OTPION1 7](#_Toc450297231)

[4.3 Derived Requirements 9](#_Toc450297232)

[4.3.1 Configuration Requirement 10](#_Toc450297233)

[4.3.2 CONFIGURATION REQUIREMENT on AP 11](#_Toc450297234)

[5 MLB 12](#_Toc450297235)

[5.1 REQUIREMENTS 12](#_Toc450297236)

[5.2 ANALYSIS 12](#_Toc450297237)

[5.3 Workflow for service discovery and client mapping 14](#_Toc450297238)

[5.4 Derived Requirements 15](#_Toc450297239)

[5.4.1 CONFIGURATION WORKFLOW FOR OV 16](#_Toc450297240)

[6 AppENDIX 21](#_Toc450297241)

[6.1 BONJOUR 21](#_Toc450297242)

[6.2 UPnP/DLNA 21](#_Toc450297243)

[7 OTHER REFERENCES 23](#_Toc450297244)

# REVISION HISTORY

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Rev.** | **Date** | **Agile Revision** | **Update By** | **Revision Description** | **Status** |
| HAN AP Release | | | | | |
| 1 | 03/22/2016 |  | Sindhu  Mohandas | Initial Draft |  |
| 2 | 04/04/2016 |  | “ | Internal Review – Fred/Anish |  |
| 3 | 04/14/2016 |  | “ | Internal Review – Fred/Anish/Jean-Luc, Larry,Deepak,Sindhu |  |
| 4 | 04/22/2016 |  | “ | Review update |  |
| 5 | 04/28/2016 |  | “ | Configuration flow update |  |
| 6 | 05/04/2016 | A | “ | Updated with UPNP Architecture reference |  |
| 7 | 05/26/2016 | B | “ | Review update |  |

# Overview

Zero configuration networking is a set of protocols that can be used to assign IP addresses, resolve names and discover services.

Apple device use mDNS (multicast DNS) as the underlying protocol for Bonjour exchanges. Bonjour is used by Apple devices to discover Services over a network. These services include AppleTV or Print services. Bonjour, also known as zero-configuration networking, enables automatic discovery of computers, devices, and services on IP networks. Bonjour uses industry standard IP protocols to allow devices to automatically discover each other without the need to enter IP addresses or configure DNS servers. Specifically, Bonjour enables automatic IP address assignment without a DHCP server, name to address translation without a DNS server, and service discovery without a directory server.

Bonjour, using IP-based services, supports three fundamental operations, each of which is a necessary part of zero-configuration network services:

● Publication (advertising a service)

● Discovery (browsing for available services)

● Resolution (translating service instance names to addresses and port numbers for use)

Apple clients (iPhones, iPads, MacBooks) use bonjour/mDNS to resolve the IP address for the services. At the same time the servers (AppleTV, Printers) also advertize their services by broadcasting mDNS packets.

Apple's Bonjour protocol is built on multicast DNS, which is a Layer 2 non-routable protocol. This means that only clients on the same subnet as the AirPrint and AirPlay enabled devices can see those services. On a network that has multiple subnets, the multicast DNS advertisements will not reach users on different subnets. Enterprises, schools, universities and many other environments are typically built with multiple subnets, which means that although Apple services may be available to users, they will not be visible to them.

Similarly DLNA (Digital Living Network Alliance) is a standard that is derived from UPnP (Universal Plug and Play). DLNA uses SSDP (Simple Service Discovery Protocol) for service discovery on the network. It provides the ability to share digital media services for Android/Windows devices. The SSDP protocol also has the same limitation of local subnet scope. Hence the solution developed for extending mDNS across L3 is applicable to DLNA. The same solution should be implemented for both.

The ALE/HAN “mDNS/UPnP” solution shall provide the following functionality:

1. Allow mDNS/UPnP-DLNA compatible devices to discover network services across IP subnet boundaries
2. Allow selective sharing of services based on sharing rules. Service sharing rules shall be defined based on vlan, access role profile(UNP), username and location.
3. Provide the solution that is unified across wired/wireless network.
4. Provide multicast optimization over the wireless network.

# Use Cases

The solution is applicable to networks that have multiple subnets and have apple devices and services.

In large universities and enterprise networks, it is common for Bonjour-capable devices to connect to the network across VLANs. If a router floods all the mDNS traffic then that leads to lot of unnecessary traffic that consumes valuable air resources. The requirement is to prevent excessive multicast traffic over the WLAN. Multicast algorithms have to be implemented such that only the APs that have the Bonjour clients or services receive the traffic. It is also required to send traffic to targeted users based on policies defined in the system. The set of policies should be applied to determine which service device the clients can connect to. Using registration information from the services, the solution should create a grouping of related clients and services automatically.

This solution should be unified across wired and wireless Bonjour-capable devices and services.

There are two use cases that should be supported:

1. Small and Medium Business (SMB),
   1. The solution should work independent of OV/HAM.
   2. This use case is for networks with a few (<10) vlans and ~ 512 clients.
   3. Full policy based client to service mapping is not required for this use case. Vlan based enforcement to prevent forwarding multicast traffic across too many vlans may be supported.
   4. Multicast optimization should be implemented at the APs to conserve air bandwidth usage.
2. Medium to Large(MLB)
   1. This solution should work with OV/HAM
   2. The solution should use the OV/HAM for mDNS/UPnP feature management and control plane function to cache service publication, match the service to client mapping and push this to the edge switches and APs where the mDNS/UPnP snooping is enabled
   3. The solution should work even if the OV goes down, ie the edge switches and APs should continue to respond to client requests and cache service advertisements. Only new service to client policy mapping should be affected.
   4. The mDNS responder function should be distributed among the switches and APs.
   5. This solution should be able to enforce policy based mapping of clients to services. The policies could be as listed below and should be pushed to the edge switches and APs for enforcement.
      1. User group based
      2. Vlan based
      3. Location based
   6. Multicast optimization should be implemented at the APs to conserve air bandwidth usage.

# SMB Solution REQUIREMENTS & ANALYSIs

## Requirements

Following are the list of requirements of the solution:

1. Solution shall support discovery of Bonjour-mDNS/UPnP-DLNA services across IP subnets.
2. Solution shall be independent of OmniVista
3. Solution shall scale to a small number of vlans (<10) and ~512 clients
4. Solution shall support vlan based rules to allow or disallow services from being shared.
5. Solution shall implement multicast optimization in the APs.

## Analysis

In this solution the stitching of vlans to facilitate relay of mDNS/UPnP protocol message across IP subnet boundaries is implemented in one of the switches in the network. This switch should be manually configured to be the mDNS/UPnP relay agent.

. In this solution there is no access to a central authentication/byod/guest management component . The only rules to restrict client’s visibility to services shall be vlan based.

### OTPION1

This solution does not use any L2 tunneling technology. A router in the network that has interfaces in all the vlans in the network should be manually identified as the mDNS/UPnP relay agent of the network. . mDNS/UPnP relay agent will have all the vlan interfaces hence will have visibility to all the mDNS /UPnP activity on the network. In order to restrict the replication of mDNS/UPnP multicast across L3 boundaries vlan based policies may be defined for example “multicast {upnp | mdns} relay vlan-list{1, 2,3, 4-10}”.

#### ANALYSIS:

The mDNS/UPnP relay switch should have all the vlans on which mDNS services and mDNS clients are expected to be present on the network. In SMB network this should be a small number of vlans. The network requiring the mDNS/UPnP relay service should have vlans configured along all the networking elements along the way between the edge switches /APs and the mDNS relay agent switch which is ideally the router in the network.

This will not scale for large deployments with lot of vlans. This is only suitable for SMB with about < 512 users and few vlans (<10)vlans ( example : employee , guest, voice, management, employee byod vlan).

The mDNS/UPnP packets are snooped on the mDNS/UPnP relay device and forwarded to all the other vlans. The default behavior is to forward the packets to all the other vlans on the router. The only rule that can be supported is vlan based. For example one can specify a set of vlans like vlan x,y,z as part of the mDNS and/or UPnP relay group and the mDNS/UPnP frames are only forwarded across these vlans..



Figure 1: gateway

#### Workflow

Assumption is that all the vlans in which the mDNS /UPnP clients and servers are expected to be assigned on a particular switch/AP is accessible from the edge switches and APs to the switch running the mDNS/UPnP relay agent..



Figure 2: Workflow for SMB with gateway solution

## Derived Requirements

1. In this use case there is no OV. The configuration of the feature will happen at the switch through CLI or WebView and at the AP through HANLET.
2. A router in the network which has interfaces in all the vlans of the network should have mDNS /SSDP (protocol used by UPnP-DLNA) relay enabled.
3. The role of edge switches/APs is to forward all mDNS/SSDP (UPnP-DLNA) to the router in the vlan it comes in andforward all traffic from the router in the vlans..
4. In the ALE/Aruba use case
   1. when mDNS/SSDP relay is enabled a tunnel is created from the switches and APs to the controller
5. In the ALE/HAN use case when mDNS/SSDP relay is enabled there is no tunnel required. But there are different functions to be done based on the role of the switch in the network
   1. In gateway mode, the device is required to have vlan interfaces in all the vlans of the network and any mDNS/SSDP multicast packet is snooped and forwarded to all other vlans known to the gateway device
   2. In edge mode, the device just forwards the mDNS/SSDP multicast packets in the vlan.

# MLB

## REQUIREMENTS

Following are the list of requirements of the MLB solution:

1. Solution shall support Bonjour(mDNS)/UPnP services across IP subnets.
2. Solution shall include OmniVista/HAM .
3. Solution shall provide selective sharing to the services based on service sharing rules. The service sharing rules shall be defined based on vlan, access role profile, location and username.
4. Solution shall scale to ~5000 clients.
5. Solution shall work even if OV goes down for services that have already been discovered and for which policies have already been pushed to the edge switches and APs. Only the new service advertisement will be impacted.
6. Multicast optimization shall be implemented at the APs.

## ANALYSIS

The wireless solution for MLB use case shall consist of OmniVista as the central management and Authentication manager platform. But the solution is controller-less.There is no data plane at the OV/HAM. The solution shall use OV/HAM platform for management, mDNS/UPnP service cache, configuration of service sharing rules for clients to access the services, push the service sharing rules to the edge switches and APs where the mDNS/UPnP enforcement happens.

By default,when mDNS/UPnP relay is not enabled, all the mDNS/UPnP packets coming into the wired switches or wireless APs are forwarded in the L2 scope. There is no special processing required.

If mDNS/UPnP relay is enabled, by default,

* The edge switches and APs shall continue to forward the mDNS/UPnP in the L2 domain.
* The edge switches and APs will cache service discovery information pushed down from OV.
* The switches / APs shall respond to any client requesting for a service that is not in the same L2 domain as the client without any other restriction.

If mDNS/UPnP relay is enabled with enforcement based on service sharing rules,then

* The edge switches and APs shall stop even the L2 forwarding of the mDNS/UPnp packets.
* The edge switches and APs shall cache service discovery information and the service sharing rules pushed down from OV.
* The edge switches and APs shall process the packets. Then based on the service advertisement cache and service sharing rules pushed down from OV, they will selectively respond to the mDNS/UPnP queries.

The HAN Wireless solution is distributed i.e there is no central controller that does the control plane and forwarding plane functions. All control and forwarding plane is in the Access points and switches.

When the apple device publishes its service, a multicast frame (L2 scope) is sent out. It is received by an AP or a switch. If mDNS/UPnP relay is enabled, then the switch/AP should process the mDNS multicast packet in software and send the service information to the central entity that is reachable by all the APs and switches. This central entity shall be OV.

OV should maintain the service record and provide the service sharing rules configuredfor the service to all the discovered swithes and APs on which mDNS/UPnP relay is enabled..

Following diagram shows the components of the solution. The green lines represent the communication to share the service information from the AP/switches to OV. This shall be via SNMP Traps. The Red lines represent the communication from OV to the AP/Switches to push the service sharing rules. This shall be pushed via SNMP mibs for switches and via WMA towards the APs.



Figure 3: MLB solution with OV

NOTE: With this approach the switches and APs have to implement the proxy function where it is required to understand the protocol working instead of blindly tunneling the packet off to a relay agent by just determining it is an mDNS or ssdp packet. This will be software development effort and both the AP/Switch teams should work together to leverage the implementation of the core protocol exchange instead of duplicating the effort.

## Workflow for service discovery and client mapping

The following diagram shows mDNS workflow how AP and switches along with OmniVista mDNS/UPnP application and HAM facilitate clients to see the services advertised by the server across L3 boundaries.

The workflow should be applicable between wired service/wired client, wired service /wireless client or wireless service/wireless client. It should be applicable mDNS or DLNA-UPnP devices.

## 



Figure 4: Workflow with OV

## Derived Requirements

Based on the above workflow following requirements can be derived:

1. **OV REQUIREMENT**: The mDNS/UPnP relay application should be added to OV. The configuration interface of this application should work both in ARUBA mDNS/UPnP-DLNA relay configurationmode and in the HAN solution mode. Details of the configuration interface is in section 5.4.1.
2. **OV REQUIREMENT**: This mDNS/UPnP application on OV should be responsible for the following
   * 1. to receive mDNS/UPnP published records from APs (via WMA) or switches via TRAP,
     2. store the records,
     3. age out records based on the record’s TTL
     4. Get the mDNS/UPnP Service sharing rules configured in HAM during device registration by the OV administrator or the end-user.
     5. Send service sharing rule configuration to all the edge devices so that the edge devices can respond to client queries based on the rules.
     6. Push the service cache to all the switches/APs (via WMA) that are coming on to the network that have mDNS/UPnP relay enabled.
3. **OV/SWITCH/AP REQUIREMENT**: The switches shall send the service advertisement information to OV via SNMP TRAP. APs shall send syslogs to WMA which in turn is translated to a TRAP message to OV. The TRAP should contain all the necessary information required for switches/APs to respond to a client query for the service.
4. **OV REQUIREMENT:** OV shall perform polling every 5 minutes to get the service advertisement records from the switches and APs.
5. **OV REQUIREMENT**: The mDNS/UPnP relay feature should be enabled on the edge devices (switches and APs) by OV.The IP address of the OV where the TRAP needs to be sent is should be configured on the switches.
6. **SWITCH / AP REQUIREMENT:** When mDNS/UPnP relay is enabled on the switch or AP
   1. All the mDNS/UPnP multicast packets are copied to CPU while being forwarded in the L2 domain
   2. The service information is sent as a TRAP to OV.
   3. OV TRAP manager should share this information with mDNS/UPnP application. This application shall cache the service information, , the vlan, the MAC Address, the IP address/port of the service, the role (access role profile) of the server publishing the service.
   4. Similarly the mDNS/UPnP client traffic is copied to CPU while being forwarded in the L2 domain and the switch/AP shall respond to the query like a proxy if a service record exists on the switch.
   5. If mDNS/UPnP service sharing rule enforcement is enabled, then the mDNS/UPnP multicast packets should not be forwarded at L2. The switch/AP shall respond to queries based on the service sharing rule associated with the requested service that has been pushed from OV.
7. **OV REQUIREMENT:**
   1. OV is responsible for pushing the service and service sharing rules to the switches coming on to the network which have mDNS/UPnP relay enabled and to switches that reboots and comes back up.
   2. The service information and the service sharing rules are kept at the edge switch/AP.
8. **OV REQUIREMENT**: OV shall provide an interface to configure mDNS/UPnP relay and its associated service sharing rules. This is defined in section 5.4.1
9. **OV REQUIREMENT**: The OV(mDNS/UPnp application) shall interact with application/HAM to get a list of access role profiles, vlan, username, location (known to HAM either by configuration or via registration/authentication) from which the administrator/end-user can create service sharing rules..
10. **OV REQUIREMENT**: The number of clients to be supported is 5000 and number of services is 1000.
11. **SWITCH/AP REQUIREMENT**: The switches and APs should understand the mDNS/DLNA-UPnP protocol for service publishing /discovery and resolution in order to act as a responder. This is entirely a software based solution.

### CONFIGURATION WORKFLOW FOR OV <- applicable to MLB use case

Assumption:

1. In the MLB network, there is a possibility that some portions of the network may still have ARUBA and others HAN, hence OV should support configuration of mDNS/UPnP-DLNA feature for both vendors.
2. It is a requirement that the same switch would be supporting both the ARUBA and HAN products. Hence the CLI configuration framework should support this requirement.
3. In the presence of both HAN APs and ARUBA APs connected to the same AOS switch, the assumption is
   1. The ALE switches will continue to tunnel all mDNS/SSDP packets to the Aruba controller via L2 GRE tunnel .
   2. The HAN AP shall also implement the same L2 GRE tunnel to the Aruba controller in tunnel mode. This way the defining service caching (AirGroup) rules , enforcement and forwarding functionality is contained in the Aruba controller.
   3. The ALE-switch and HAN APs are just required to forward all mDNS /SSDP multicast packets to the Aruba controller and forward the packets coming from the Aruba controller in the vlan associated with the traffic.
4. In the use case with OV assumption there are two cases that needs to be supported
   1. Use case without HAM
   2. Use case with HAM

OmniVista mDNS Application configuration requirements:

OV mDNS application should provide the ability for the administrator to select ARUBA solution or HAN solution. Based on the selection, different workflows need to be presented to the administrator.

When the user selects HAN workflow, the GUI Menu for HAN mDNS/SSDP configuration should be presented. Following GUI illustrations are sample only:

#### mDNS/SSDP (UPnP-DLNA) configuration



Figure 5: The mDNS/UPnP-DLNA configuration

1. Select the list of switches/AP or AP Groups to apply this configuration
2. Ability to enable/disable the mDNS/SSDP ( protocol used by UPnP-DLNA)
3. Specify the IP address of OV for the switch/AP to notify the service publication. Switch will use TRAP/ AP will communicate to WMA which inturn will raise a trap to OV.
4. Specify if service sharing rule enforcement is to be enabled or not
5. Specify the list of shared device rules (not sure if it should be here). Figure 8 is the interface that should be shown when Add shared device is selected by the administrator.
   1. Solution with HAM - Two types of users should be able to configure the service and service sharing rules. The end-user and the OV administrator.
      1. The end-user should provide the login credentials before they can register device/service and service sharing rules. The end-user shall be able to register during the first login / registration process or later. HAM should have the end-user information in its database.
      2. The OV administrators should provide the administrator login and if the login has RBAC rules that allow them to use the mDNS application and allow them to register and configure services/service sharing rules then they will be redirected to the appropriate configuration pages.
   2. Solution without HAM – Two types of users should be able to configure the service and service sharing rules. The end-user and the OV administrator
      1. The end-users have to be created in OV as OV Admins with very minimal privilege, just to just register the device mac address/service and rules. So the OV network administrator should have created these users before.

#### mDNS/UPnP-DLNA shared device/service registration

The shared device registration workflow portal should be available to the end-user and to the administrator. It is independent of the presence of BYOD registration application (HAM). There are two types of administrators that can register service devices, the network administrator and an end user type of administrator. The user with network administrator privileges can add/remove/modify all the registered devices. The end-user with user level privileges can only add/remove/modify only the devices he or she added.

For endusers, a portal should be available, which the user can access. In the presence of HAM the end-users are known to HAM in its database. In the absence of HAM the end-users should have a login created in OV to configure the mDNS/SSDP services and sharing rules.

1. The First Page should first prompt the user
   1. Toenter the username / password
   2. Then select ok/cancel



Figure 6: end-user login page to register shared device

1. Once the end-user is authenticated ( in the presence of HAM they are authenticated against the HAM database and in the absence of HAM a local database maintained by OV) the following information should be requested
   1. Device name being shared
   2. Device mac address being shared
   3. List of mac address to share this device with
   4. Then specify the list of switches /APs this has to be pushed to



Figure 7: Configuration of the shared device

1. For OV administrator the following information should be requested.



Figure 8: OV Administrator shared device registration

In the presence of BYOD application (HAM), the employee device registration page should allow similar sharing rules to the end-user. The end-user when registering their BYOD device for the first time should be prompted “Do you want to share a service” and be redirected to the “service sharing rules page as shown in Figure 7.

The number of devices a particular end-user or employee is able to share should be limited. The number could be limited to 4 devices per user.

#### mDNS/UPnP-DLNA services

The following services should be supported by default in Phase 1.

1. AirPrint
2. AirPlay
3. iShare
4. DLNA-Print
5. Chromecast
6. DLNA-media

The rest of the services like iTunes,iChat and remote mgmt can be supported in Phase 2.

Generic Service Sharing Rules can be created per service instead of per device per service.

Example: AirPrint service is allowed by user/user-role/vlan /location/SSID/



### CLI /Web Configuration SMB/MLB use cases

#### Configuration Requirement on Switch

##### Global configuration if the network has either HAN products and ALE or ARUBA and ALE supported by the switch.

ALE switches already have configuration to support mDNS/SSDP(for UPnP/DLNA)

1. mdns-relay {enable | disable} mode { tunnel | gateway | proxy | L2-forward}
   * 1. tunnel: is for ALE/ARUBA on edge switches
     2. gateway : is for ALE/HAN on the router that is forwarding mDNS across L3 boundary
     3. proxy : this is the mode in the MLB use case in the presence of OV for ALE/HAN Solution (for distributed mDNS/SSDP proxy function). The edge switches/APs shall cache the service information and respond to client requests if from a different vlan. If there is a notification-server IP address configured then in this mode a TRAP should be sent to that IP address of OV.
     4. L2-forward: This is the basic mode where the mDNS/UPnp multicast frames are forwarded normally on the L2 vlan.
     5. Since the mode was not part of the existing software release in order to be compatible we should leave the default as tunnel if no mode is specified.
2. ssdp-relay {enable | disable} mode { tunnel | gateway | proxy| L2-forward}
   * 1. tunnel: is for ALE/ARUBA on edge switches
     2. gateway: is for ALE/HAN on the router that is forwarding SSDP across L3 boundary
     3. proxy: this is the mode in the MLB use case in the presence of OV i for ALE/HAN Solution. The edge switches/APs shall cache the service information and respond to client requests coming from a different vlan. If there is a notification-server IP address configured then in this mode a TRAP should be sent to that IP address of OV .
     4. L2-forward: This is the basic mode where the mDNS frames are forwarded normally on the L2 vlan.
3. mdns-relay { tunnel *ip-interface-name* } 🡨 this exists today and doesn’t change. This is applicable only when the mode is tunnel
4. mdns-relay { gateway vlan-list *vlan[-vlan]* } <- default is forward to ‘all’ vlans if vlan-list is not provided. Vlan list can be comma separated vlans or vlan range
5. ssdp-relay { gateway vlan-list *vlan[-vlan]*} <- default is forward to ‘all’ vlans if vlan-list is not provided. Vlan list can be comma separated vlans or vlan range.
6. show {mdns-relay | ssdp-relay} config
7. show {mdns-relay | ssdp-relay} service-cache <- applicable on ly in proxy mode
8. mdns-relay notification-server address {*IP address*} mask {*mask*} <- applicable in proxy mode with OV
9. ssdp-relay notification-server address { *IP address*} mask {*mask*}<- applicable in proxy mode with OV

##### Configuration per port to support the use case where a switch has to support ARUBA APs and HAN AP hence switch needs to support both tunnel mode and other modes. But a single port on the switch will support only one mode.

##### Global configuration if the network has either HAN products and ALE or ARUBA and ALE supported by the switch.

ALE switches need to add per port configuration to support mDNS/SSDP(for UPnP/DLNA)

1. mdns-relay port { chassis/slot/port[-portn ]} {enable | disable} mode { tunnel | gateway | proxy | L2-forward}
   * 1. tunnel: is for ALE/ARUBA on edge switches
     2. gateway : is for ALE/HAN on the router that is forwarding mDNS across L3 boundary
     3. proxy : this is the mode in the MLB use case in the presence of OV for ALE/HAN Solution. The edge switches/APs shall cache the service information and respond to client requests if from a different vlan. If there is a notification-server IP address configured then in this mode a TRAP should be sent to that IP address of OV. <-applicable to MLB usecase -edge switches where the devices (service publishers and clients) are connected
     4. L2-forward: This is the basic mode where the mDNS/UPnp multicast frames are forwarded normally on the L2 vlan. <- this is applicable to SMB use case on the edge switches.
     5. Since the mode was not part of the existing software release in order to be compatible we should leave the default as tunnel if no mode is specified.
2. ssdp-relay port { chassis/slot/port[-portn ]} {enable | disable} mode { tunnel | gateway | proxy| L2-forward}
   * 1. tunnel: is for ALE/ARUBA on edge switches
     2. gateway: is for ALE/HAN on the router that is forwarding SSDP across L3 boundary <- applicable to router in SMB
     3. proxy: this is the mode in the MLB use case in the presence of OV i for ALE/HAN Solution. The edge switches/APs shall cache the service information and respond to client requests coming from a different vlan. If there is a notification-server IP address configured then in this mode a TRAP should be sent to that IP address of OV <-applicable to MLB use case- edge switches where the devices (service publishers and clients) are connected.
     4. L2-forward: This is the basic mode where the mDNS frames are forwarded normally on the L2 vlan <- this is applicable to SMB use case on the edge switches.
3. mdns-relay { tunnel *ip-interface-name* } 🡨 this exists today and doesn’t change. This is applicable only when the mode is tunnel. This configuration is not required per port because there is only one tunnel per switch.
4. mdns-relay { gateway vlan-list *vlan[-vlan]* } <- default is forward to ‘all’ vlans if vlan-list is not provided. Vlan list can be comma separated vlans or vlan range. This configuration is not required per port because there is only one vlan-list per switch in the gateway mode.
5. ssdp-relay { gateway vlan-list *vlan[-vlan]*} <- default is forward to ‘all’ vlans if vlan-list is not provided. Vlan list can be comma separated vlans or vlan range. This configuration is not required per port because there is only one vlan-list per switch in the gateway mode
6. show port {chassis/slot/port[-portn]} {mdns-relay | ssdp-relay} config
7. show {mdns-relay | ssdp-relay} service-cache <- applicable on ly in proxy mode
8. mdns-relay notification-server address {*IP address*} mask {*mask*} <- applicable in proxy mode with OV
9. ssdp-relay notification-server address { *IP address*} mask {*mask*}<- applicable in proxy mode with OV

#### CONFIGURATION REQUIREMENT on AP

1. Ability to enable/disable the mDNS/SSDP (protocol used by UPnP/DLNA for service discovery and publication)
2. Ability to specify the mode. For AP shall support the following modes
   1. L2-forward mode - where the mDNS/SSDP frames are forwarded in the L2 vlan
   2. proxy mode - where the mDNS/SSDP frames are terminated on the AP and forwarded across the L3 based on rules configured on the AP and a service cache is maintained on AP and service notification is made to WMA via syslog which is translated to TRAP from WMA to OV.
   3. Tunnel mode – where the HAP has to operate in a network with ARUBA and ALE switches. In this mode a L2 GRE (that interoperates with Aruba controller) has to be created from HAN AP. All mDNS packerts are forwarded to Aruba controller. Aruba controller matches the service rules and forwards traffic back to the tunnels. The HAP shall process packets from tunnel and forward it in the vlan in which the packet was tagged with in the tunnel.
3. Ability enable/disable proxy function at the AP to prevent flooding of client requests in the network if there is a cache for the requested service on the AP
4. Ability to show the configuration

Ability to show the service-cache <-in proxy mode

# AppENDIX

## BONJOUR

More details on the mDNS protocol used for zero configuration networking is described here in the following articles:

<https://developer.apple.com/bonjour/>

<https://developer.apple.com/library/mac/documentation/Cocoa/Conceptual/NetServices/Articles/NetServicesArchitecture.html>

<http://files.multicastdns.org/draft-cheshire-dnsext-multicastdns.txt>

<http://hes-standards.org/doc/SC25_WG1_N1164.pdf>

<https://tools.ietf.org/html/rfc6762>

<https://developer.apple.com/library/mac/documentation/Networking/Conceptual/dns_discovery_api/Articles/registering.html>

<http://opensource.apple.com//source/mDNSResponder/mDNSResponder-107/README.txt>

## UPnP/DLNA

<http://upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.1.pdf>

DLNA is suite of standards that uses UPnP for its discovery of network devices (which is a long list of manufacturers producing device and is also supported by all major operating systems). SSDP is a UPnP protocol that uses HTTP notification announcements that give service-type URI and unique service name.

1. **Service publication** 
   1. The DLNA/UPnP – SSDP packet containing the service record is received at the switch and trapped to the CPU.
      1. The DLNA/UPnP multicast Ethernet frame is a multicast UDP packet
         * With destination UDP port number 1900
         * Destination Multicast MAC of 01:00:5e:7f:ff:fa
         * And the following multicast IP address based on Ipv4 or Ipv6:
           1. 239.255.255.250 (IPv4 site-local address)
           2. [FF02::C] (IPv6 [link-local](http://en.wikipedia.org/wiki/Link-local_address))
           3. [FF05::C] (IPv6 site-local)
           4. [FF08::C] (IPv6 organization-local)
           5. [FF0E::C] (IPv6 global)
      2. The packet is identified by the multicast IP address and MAC address in the packet and the UDP port number.
2. Service Discovery and service resolution
3. The DLNA/UPnP wireless/wired clients first sends a service discovery to discover all the devices which provide that service.
4. Service discovery makes use of the SSDP multicast frames using MSEARCH HTTP method.
5. The client then sends the service resolution message to determine the end device from which it wants the service.
6. Service discovery typically takes place only once in a while—for example, when a user first selects a printer.
7. After Discovery
   1. Once the DLNA client and DLNA server are mapped the traffic between them flows normally

# OTHER REFERENCES

<http://www.win.tue.nl/~johanl/educ/IoT-Course/mDNS-SD%20Tutorial.pdf>

<http://agnat.github.io/node_mdns/user_guide.html>

<https://developer.apple.com/library/mac/documentation/Cocoa/Conceptual/NetServices/Articles/about.html>