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.

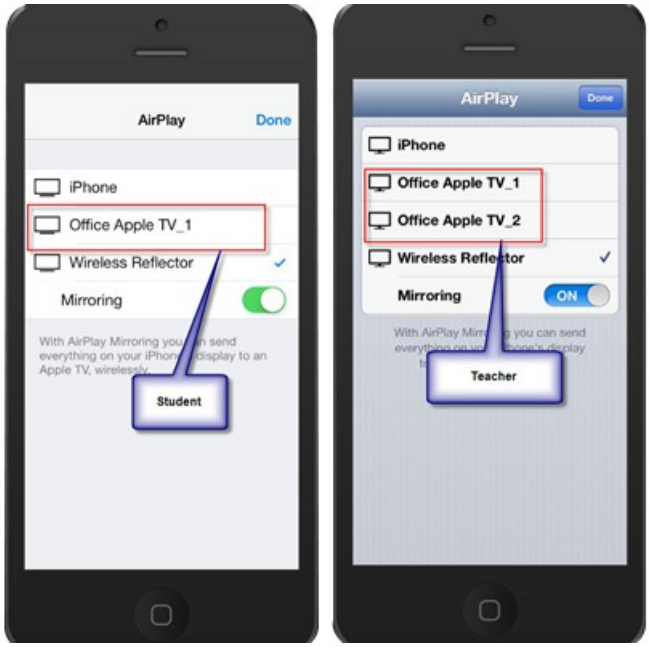
Client Context Attributes

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.