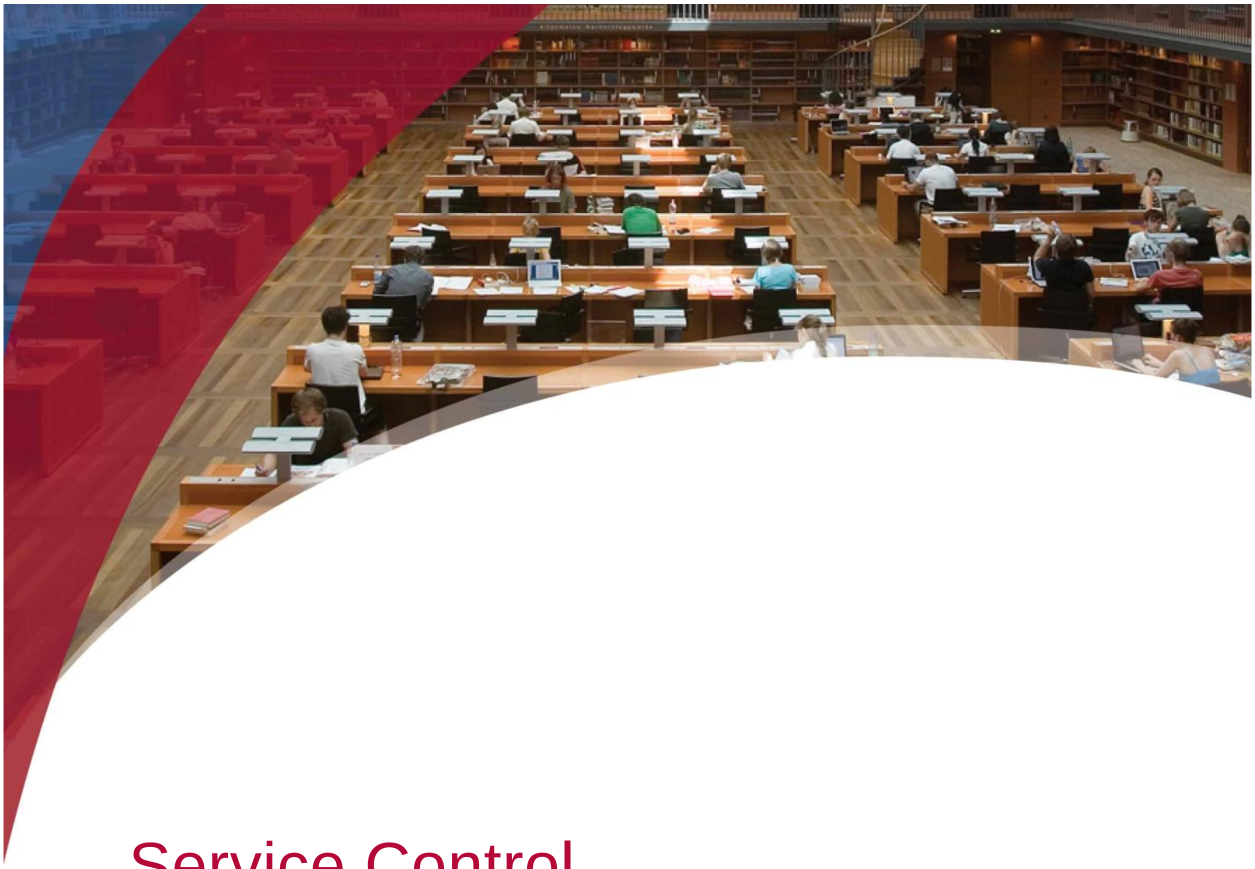
Meru NETWORKS®
Powering the All-Wireless Enterprise™



Service Control Deployment Guide

August 2013

Contents

Introduction

Zero Configuration networking (ZeroConf) is a group of technologies that include service discovery, address assignment, and name resolution without manual intervention or configuration. Bonjour is Apple's implementation of ZeroConf. Bonjour locates devices such as printers, external displays, other computers, and the services those devices offer on a local network, using multicast Domain Name System (mDNS) service records.

The Bonjour protocol was originally designed for the home network and not for larger networks, such as enterprise or campus networks. Bonjour's service advertisements are limited to a single subnet and hence services advertised are not seen by devices on different subnets. Bonjour also does not provide any inherent means to manage the visibility of these services.

This guide is based on Meru System Director Release 6.0 and discusses how to use Service Control to manage Bonjour services in a network.

Service Control Overview

Service Control is Meru's implementation for managing Zero Configuration network protocols in System Director. Service Control offers the ability to manage the discovery and advertisement of Bonjour services on a wireless network, solving the most common issues faced in campus deployments.

Most campus networks use multiple VLANs, and it is common for a user with an iPad to attempt to connect to an Apple TV on a different VLAN, which is not possible unless the Apple TV services are advertised in the VLAN to which the iPad user is connected.

Making all services available across subnets leads to a flood of mDNS traffic over the air, which can affect overall network performance. The additional traffic leads to a flood of services being discovered by user devices, which can cause confusion for users. For example, if Apple TV services are propagated on all VLANs, an iPad user might see hundreds of Apple TV devices in a large campus, which makes selecting the correct device more difficult.

Service Control allows you to manage Bonjour services by controlling service discovery and advertisement, using flexible policies based on service type, location, and user groups.

The main features include:

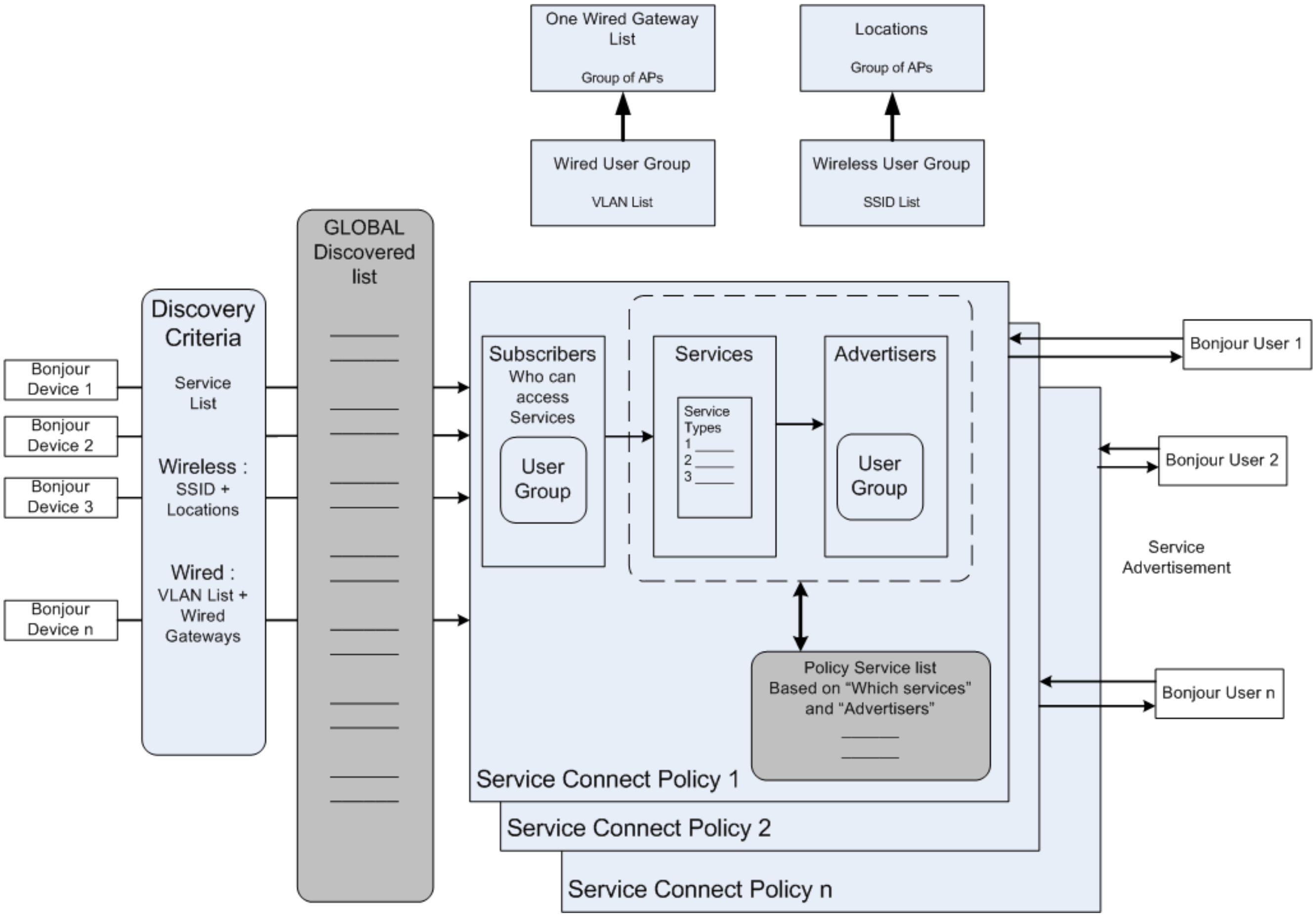
- Discovery and advertisement of Bonjour services
- Support for Bonjour services across subnets and VLANs
- Support for Bonjour in wired and wireless deployments
- Support for managing service advertisements by service type, location, and user group
- Reduction of multicast traffic over the air by filtering services, as well as limiting the service advertisements to designated VLANs

Figure 1 provides an overview of the Service Control architecture. There are five key components that form the functional aspect Service Control:

- Locations
- Wired gateway list
- User groups
- Global discovered list
- Service Control policies

These components are the key definitions based on which the propagation of Bonjour traffic occurs and entity access control can be managed.

Figure 1: Architecture Overview



Locations

A location is a logical entity that groups a configurable list of APs for Bonjour discovery and advertisement on the wireless domain. You can create multiple locations on the controller and group different APs for each of these locations, based on where they are deployed. Locations are used in Service Control policies to bridge user locations and service locations. For example, a location named "Liberal Arts" can include all APs that are deployed in the Liberal Arts building.

Wired Gateway List

The wired gateway list allows an administrator to select a list of APs from the network, which acts as Bonjour gateways for discovery and advertisement on wired VLANs. The controller can also be included in this list.

Due to the multicast nature of Bonjour packets, you need to add only one or two APs for each VLAN in which Bonjour packet control is required. System Director always uses the wired gateway list as discovery criteria and in policies in which the administrator has added this VLAN as part of the configuration.

User Groups

A user group is a collection of users for whom the same access control and policies apply. When creating user groups, SSIDs are used to map wireless users, and VLAN IDs are used to map wired users. You can create multiple user groups on the controller, and each group can be mapped to different policies, allowing them to access different Bonjour-capable devices, or limiting them to a subset of the Bonjour devices.

A typical example of a user group is an SSID. User groups can be used when creating Service Control policies. For example, user groups named "Staff" and "Students" can be created to segregate the user population, which allows you to create a Service Control policy for each user group.

Global Discovered List

The global discovered list is the list of all Bonjour services that are discovered by System Director. By default, System Director discovers Bonjour services in wireless and wired domains for a predefined set of service types (such as AirPrint and AirPlay). The wireless domain includes all SSIDs at all locations. The wired domain includes all configured VLANs and Ethernet interfaces at all locations. You can change the default global service discovery list to meet your requirements. We recommend that you have no more than one or two APs per SSID or VLAN as part of the global discovered list. In other words, no more than one or two APs per SSID or VLAN should be configured as part of the global service discovery criteria.

Service Control Policies

You can configure access control over the services discovered by System Director by creating Service Control policies. A policy defines who (subscribers in terms of *user groups@locations*) can access which services (in terms of service types) advertised by which users and devices (advertisers in terms of user *groups@locations*).

The following provides an example of students in the Liberal Arts building who need to access print services advertised by printers located only in the Liberal Arts building:

- Subscriber: Students@Liberal Arts
- Service type: AirPrint
- Advertiser: Printers@Liberal Arts

In the previous example, "Students" is the SSID mapped to the relevant user group. "Liberal Arts" is the location defined as a group of APs deployed in that building. "AirPrint" is the Bonjour service type. "Printers" is the advertising user group mapped to the relevant SSID for print services, which is mapped to a VLAN (for example, VLAN10) on the wire. If there is a wired printer on VLAN10 and a wireless printer associated to the relevant advertiser SSID, then both printers are available to the Students user group in the Liberal Arts building.

A Service Control policy consists of the following:

- Policy name

  Name of the policy.

- Subscriber user group

  Group of users who seek Bonjour services to which the policy is applied.

- Service types

  Only services listed in a policy are available to the subscriber user group specified in the policy. In the previous example, AirPrint is specified as the service type. If AirPlay is included in the policy, then the same access control applies to the Students group, except now they also have access to any AppleTV devices in the Liberal Arts building.

- Advertisers user group

  Refers to the service origin point mapped to an advertising user group. Only services advertised in the SSIDs or VLANs of these user groups are accessible by the subscribers. In the previous example, "Printers" is defined as the advertiser user group.

The service type and advertiser user group define which services are available to the subscribers of a Service Control policy. System Director applies this filtering to the global discovered list to determine the services to be advertised for that policy. Only one subscriber user group and one advertiser user group can be selected when creating a Service Control policy.

Functional Characteristics

As of System Director Release 6.0, only IPv4 services are supported.

By default, Service Control is disabled, and Bonjour traffic is not propagated. In this scenario, to enable multiple Bonjour devices on the same subnet to see each other, you must enable the multicast flag in the ESSID configuration.

After Service Control is enabled, Active Discovery is initiated (based on the global service discovery criteria), and the global discovered list is populated. When Service Control is enabled, enabling or disabling the multicast flag in the ESSID configuration has no effect on Bonjour traffic.

If multiple entities (APs) discover the same advertiser, a single entry is maintained for that advertiser, along with a listing of all reporting entities. If an AP goes offline, the service discovered by it is removed from the global discovered list (if this is the only AP that discovered the service). If multiple APs discovered the same service, the service continues to appear, while the AP list reporting this service gets pruned by the removal of the now-offline AP.

Discovery of Bonjour services is enabled across all APs in the global service discovery criteria list and on the primary and secondary wired interfaces of the APs. Bonjour devices connected by Ethernet to the secondary interfaces of the APs are discovered only if these interfaces are enabled by applying wired port profiles to them. As part of the global service discovery criteria, discovery can be limited to controllers, APs, or both.

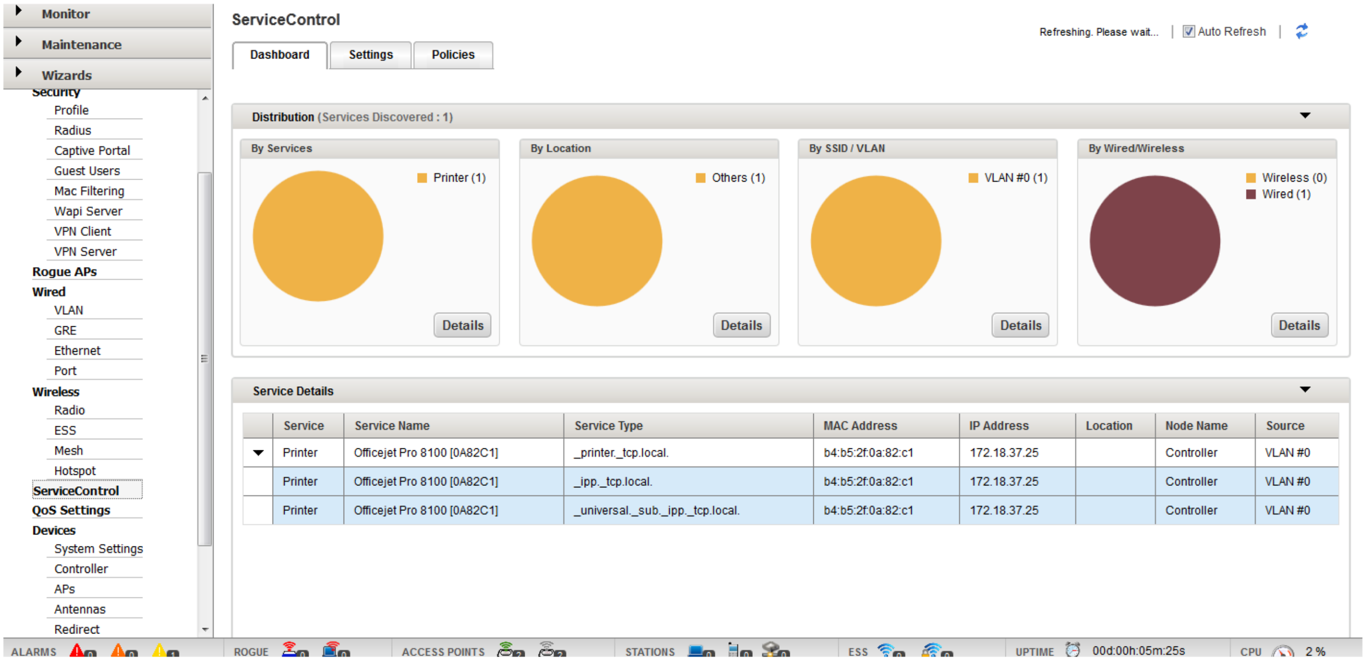
Services in the global discovered list are dynamically updated by passive discovery. (Passive discovery refers to interval-based advertisements sent out by advertisers.) If a wireless advertiser roams from one AP to another, the relevant AP ID is updated in the global discovered list as the discovery origin point for that service. If a wireless advertiser disconnects from the network, its entry is removed from the global discovered list.

There is a list of well-known service types/services (see Deployment Considerations) maintained on the controller. You can edit the list to include or exclude services. A single service type can be associated with multiple services. For example, the service type "_airplay._tcp.local." can be associated with services named “AppleTV1” and “AppleTV2.” System Director does not perform service name conflict resolution across subnets. Make sure that Bonjour devices have unique service names.

Configuring Service Control

To access the Service Control dashboard: In the Web UI, select **Configuration > Service Control**. The Service Control dashboard appears, as shown in Figure 2. The dashboard shows Bonjour services discovered by the controller, along with information about where the services are hosted (location), the SSIDs/VLANs that the services are associated with, and whether the service is wired or wireless.

Figure 2: Service Control Dashboard



	Service	Service Name	Service Type	MAC Address	IP Address	Location	Node Name	Source
▼	Printer	Officejet Pro 8100 [0A82C1]	_printer._tcp.local.	b4:b5:2f:0a:82:c1	172.18.37.25		Controller	VLAN #0
	Printer	Officejet Pro 8100 [0A82C1]	_ipp._tcp.local.	b4:b5:2f:0a:82:c1	172.18.37.25		Controller	VLAN #0
	Printer	Officejet Pro 8100 [0A82C1]	_universal._sub._ipp._tcp.local.	b4:b5:2f:0a:82:c1	172.18.37.25		Controller	VLAN #0

For information about managing Service Control, see the *Meru System Director Configuration Guide*.

Configuring Service Control Settings

From the Service Control dashboard, click the **Settings** tab to configure Service Control parameters.

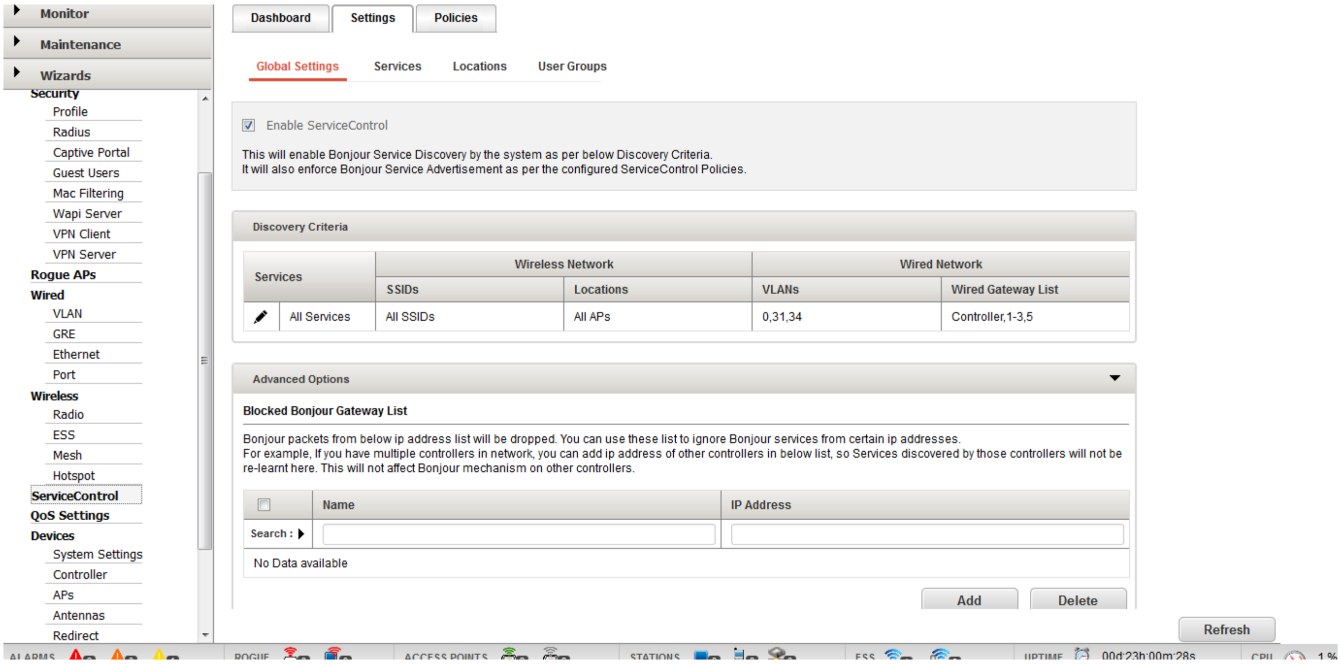
Use the Settings tab to perform the following tasks:

- Configuring Global Settings
- Configuring Locations
- Configuring User Groups

Configuring Global Settings

On the **Settings** tab, click **Global Settings** to configure global settings, as shown in Figure 3. You can enable or disable Service Control, as well as manage discovery criteria and the blocked Bonjour gateway list.

Figure 3: Configuring Global Settings



☑ Enable ServiceControl

This will enable Bonjour Service Discovery by the system as per below Discovery Criteria.
It will also enforce Bonjour Service Advertisement as per the configured ServiceControl Policies.

Discovery Criteria

	Services	Wireless Network		Wired Network	
		SSIDs	Locations	VLANs	Wired Gateway List
✎	All Services	All SSIDs	All APs	0,31,34	Controller,1-3,5

Advanced Options

Blocked Bonjour Gateway List

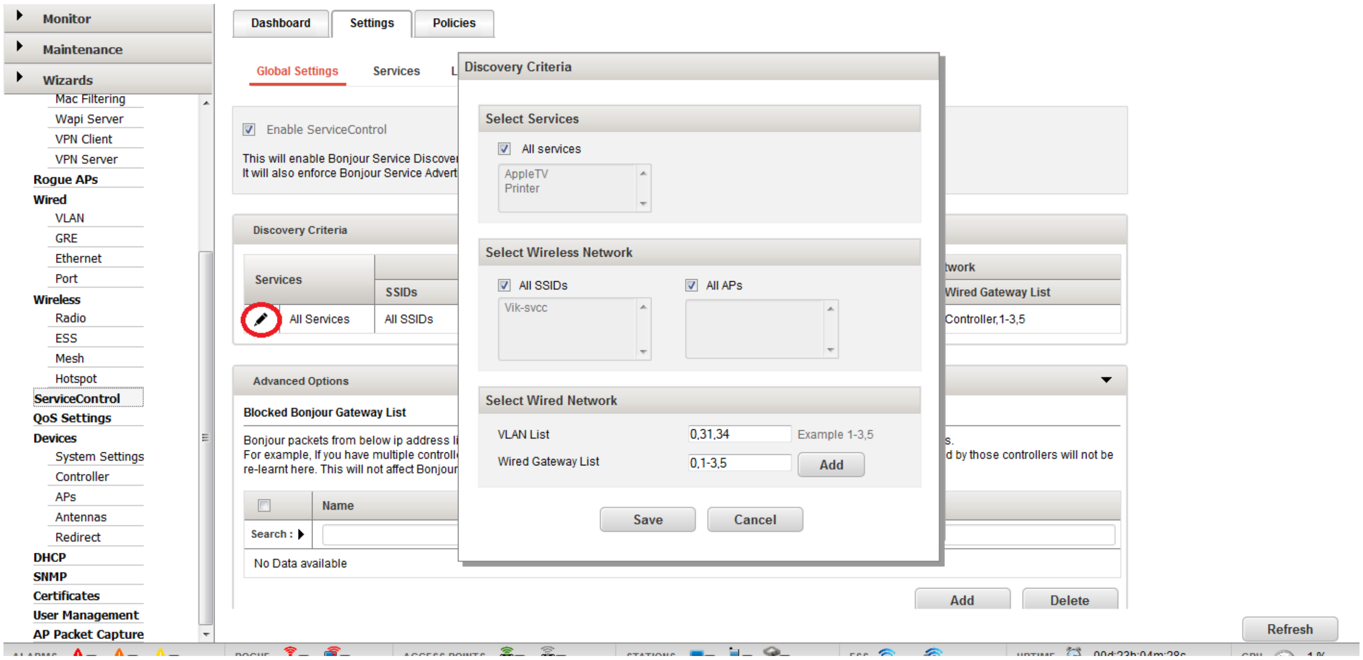
Bonjour packets from below ip address list will be dropped. You can use these list to ignore Bonjour services from certain ip addresses.
For example, If you have multiple controllers in network, you can add ip address of other controllers in below list, so Services discovered by those controllers will not be re-learnt here. This will not affect Bonjour mechanism on other controllers.

□	Name	IP Address
Search : ▸		
No Data available		

Editing Discovery Criteria

To edit discovery criteria, on the Global Settings page, click the **Edit** icon in the Discovery Criteria section. (See Figure 4.) You can configure the wired gateway list, along with SSIDs, VLANs, and APs for which discovery occurs.

Figure 4: Editing Discovery Criteria



Discovery Criteria

Select Services

☑ All services

AppleTV
Printer

Select Wireless Network

☑ All SSIDs ☑ All APs

Vik-svcc

Select Wired Network

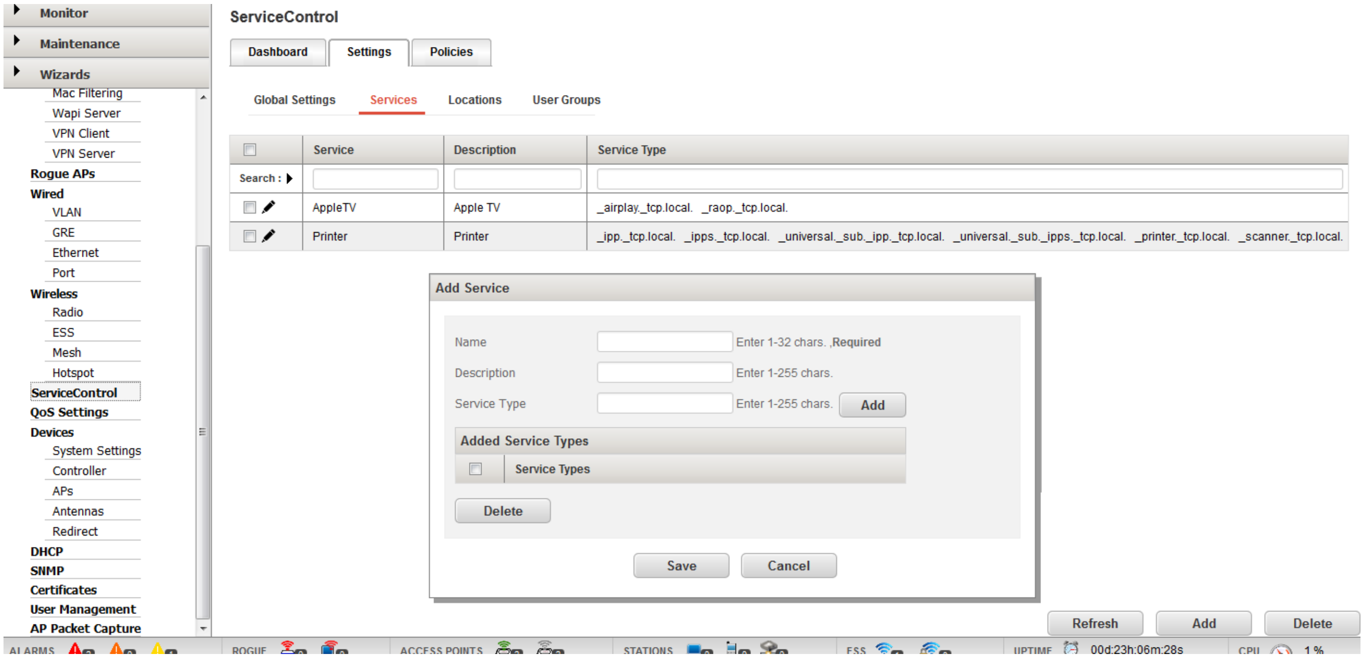
VLAN List: 0,31,34 Example 1-3,5

Wired Gateway List: 0,1-3,5

Managing Service Control Services

To access the Services page, on the **Settings** tab, click **Services**. You can review the list of configured service types and manage them. To add services, click **Add**. (See Figure 5.)

Figure 5: Adding Services



□	Service	Description	Service Type
□	AppleTV	Apple TV	_airplay._tcp.local. _raop._tcp.local.
□	Printer	Printer	_ipp._tcp.local. _ipps._tcp.local. _universal._sub._ipp._tcp.local. _universal._sub._ipps._tcp.local. _printer._tcp.local. _scanner._tcp.local.

Name Enter 1-32 chars. ,**Required**

Description Enter 1-255 chars.

Service Type Enter 1-255 chars.

Added Service Types

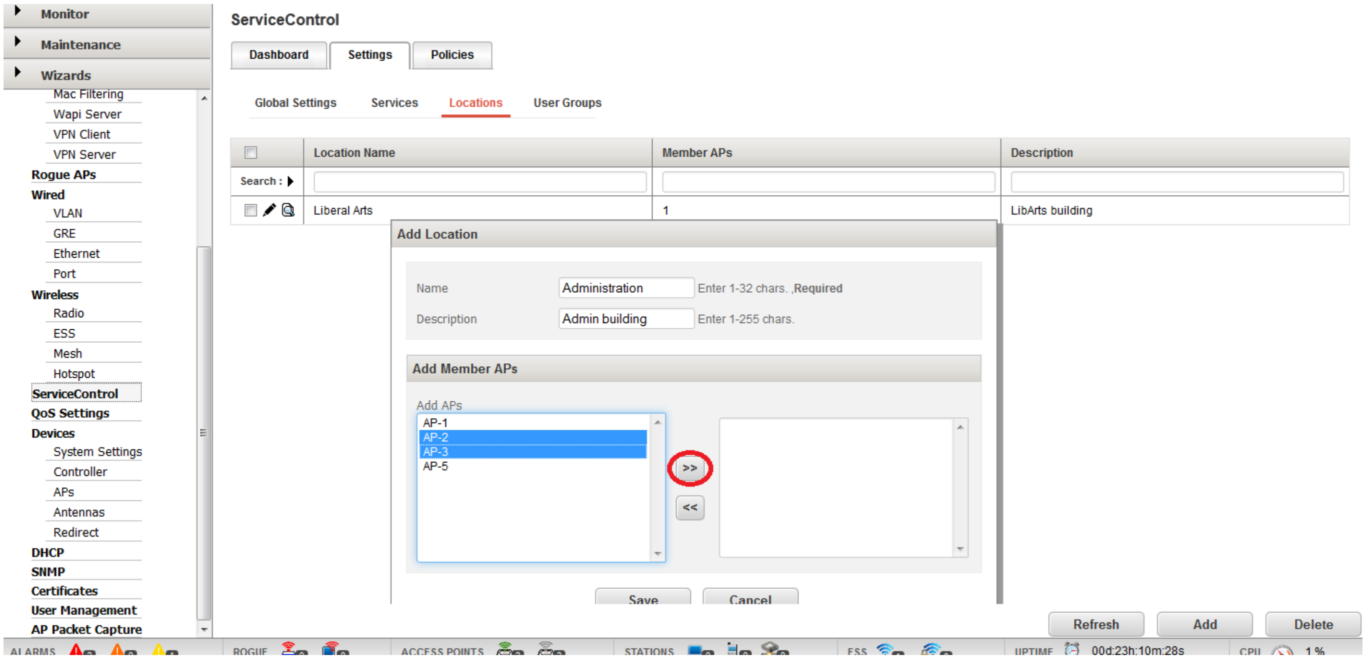
□ Service Types

Configuring Locations

To access the Locations page, on the **Settings** tab, click **Locations**. You can review a list of configured locations and manage them. To create a location, click **Add**. (See Figure 6.) When adding a location, select the APs that are present in that location.

After creating a location, which specifies the APs that are present at that location, you can specify the location as part of creating a user group, which are one of the building blocks for creating Service Control policies.

Figure 6: Creating Locations



□	Location Name	Member APs	Description
□	Liberal Arts	1	LibArts building

Add Location

Name: Administration — Enter 1-32 chars. ,Required

Description: Admin building — Enter 1-255 chars.

Add Member APs

Add APs:
AP-1
AP-2
AP-3
AP-5

>>
<<

Save   Cancel

UPTIME 00d:23h:10m:28s   CPU 1 %

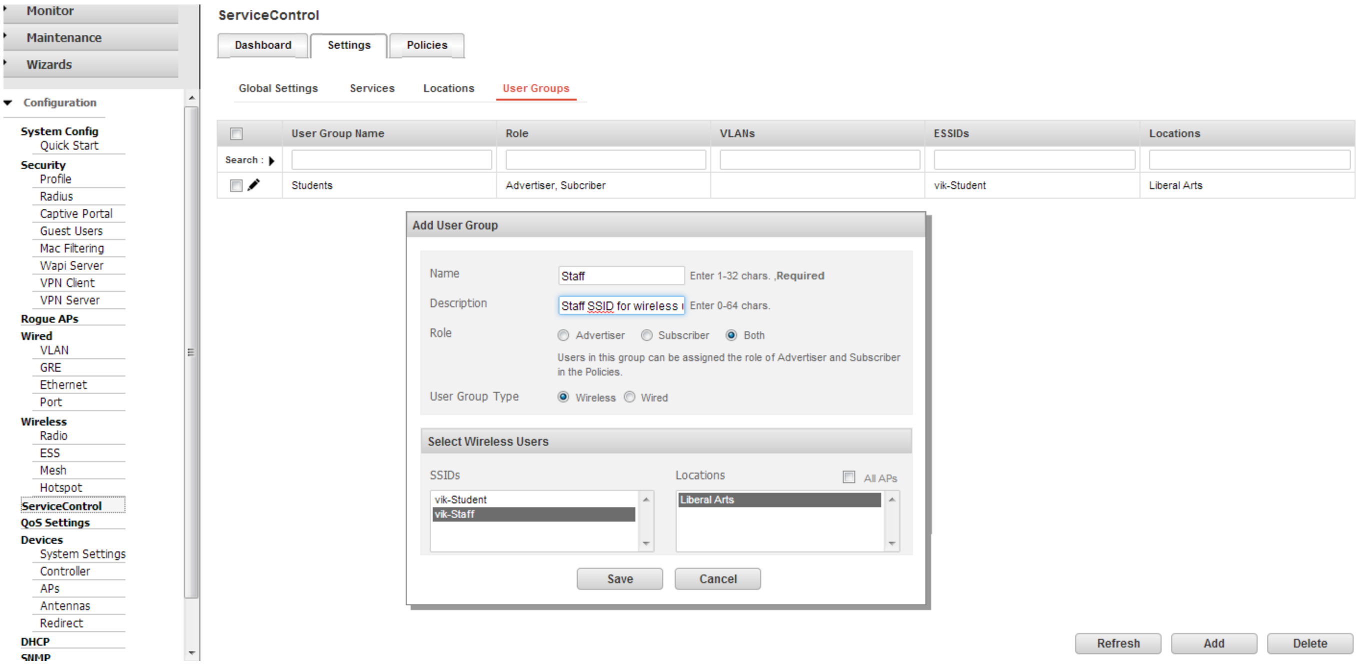
Configuring User Groups

To access the User Groups page, on the **Settings** tab, click **User Groups**. You can review a list of configured user groups and manage them. To create a user group, click **Add**. (See Figure 7.) Make sure to use a consistent naming convention when creating user groups. (For example, for wired users, you can use VLAN IDs as user group names. For wireless users, you can use the target SSID and location, which consists of a group of APs, as the user group name.)

Select one of the Role settings to define whether the clients that are part of this user group are allowed only as subscribers, only as publishers, or are allowed as subscribers and publishers.

You can then use the user group as a building block to create a Service Control policy. For information about creating Service Control policies, see Configuring Service Control Policies.

Figure 7: Creating User Groups



□	User Group Name	Role	VLANs	ESSIDs	Locations
Search :					
□	Students	Advertiser, Subcriber		vik-Student	Liberal Arts

Add User Group

Name	Staff	Enter 1-32 chars. ,Required
Description	Staff SSID for wireless	Enter 0-64 chars.
Role	○ Advertiser ○ Subscriber ● Both	
	Users in this group can be assigned the role of Advertiser and Subscriber in the Policies.	
User Group Type	● Wireless ○ Wired	

Select Wireless Users

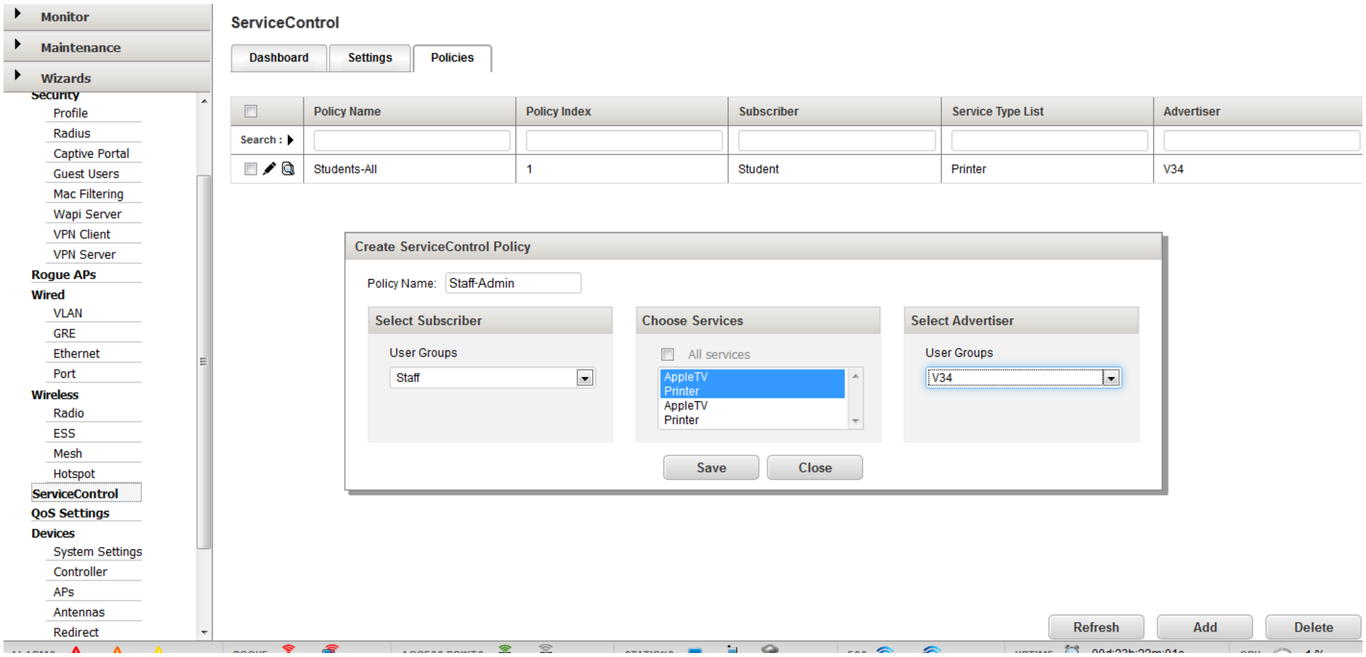
SSIDs: vik-Student, vik-Staff (selected)

Locations: □ All APs; Liberal Arts (selected)

Configuring Service Control Policies

From the Service Control dashboard, click the **Policies** tab. You can review configured policies, as well as create new policies by clicking **Add**, as shown in Figure 8.

Figure 8: Creating Service Control Policies



□	Policy Name	Policy Index	Subscriber	Service Type List	Advertiser
Search :					
□	Students-All	1	Student	Printer	V34

Create ServiceControl Policy

Policy Name: Staff-Admin

Select Subscriber	Choose Services	Select Advertiser
User Groups: Staff	□ All services AppleTV (selected) Printer (selected) AppleTV Printer	User Groups: V34

Deployment Examples

A common Bonjour deployment is at a university. There are typically two types of users: students and staff. Each user group has its own SSID, which is broadcast by all APs across the campus. Each building has its own network or VLAN. There are multiple Bonjour-capable devices on the university network. Depending on the location/network, services are accessible only from the building/network in which they are located because protocols such as ZeroConf do not support sending advertisements outside the subnet from which they are originated.

Using Service Control, you can address the following challenges:

- Using a Bonjour device/service, regardless of source and destination location/network
- Controlling access to Bonjour devices/services, based on user group and location

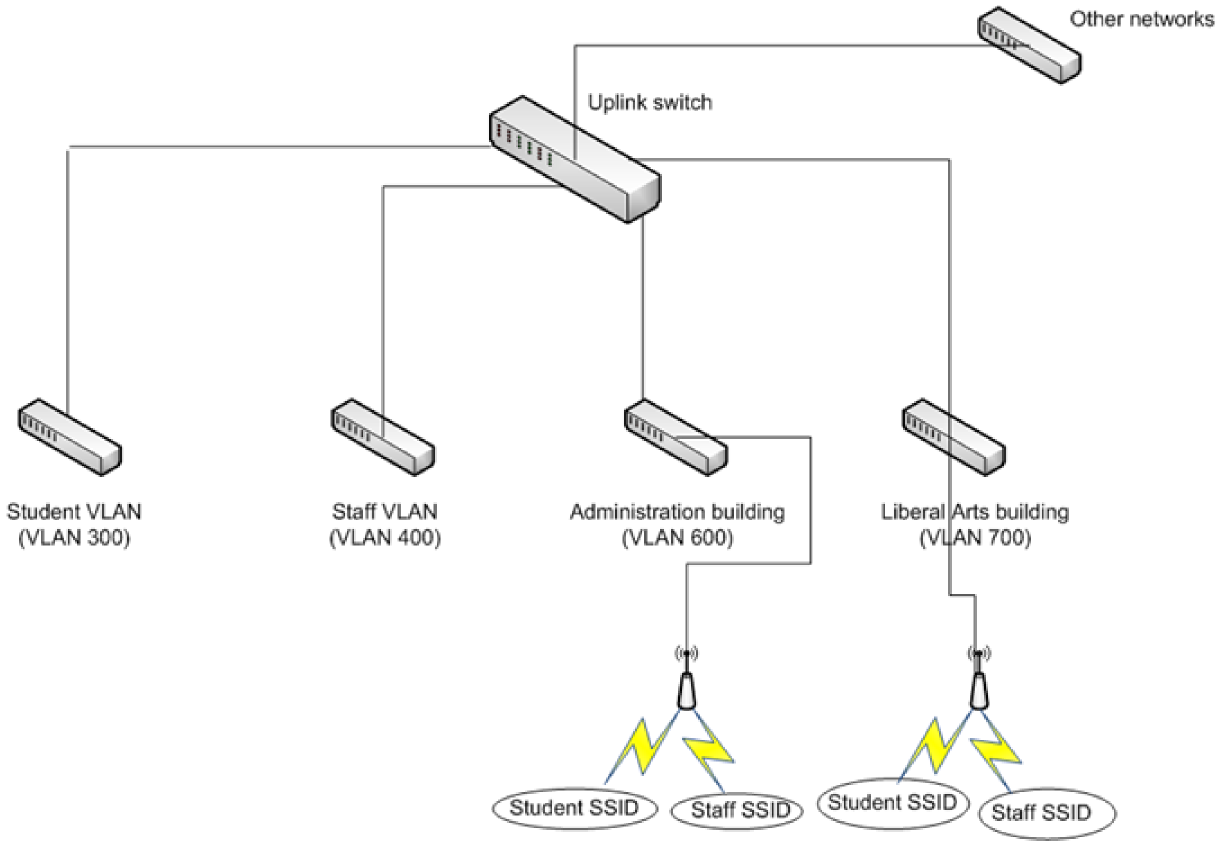
The following use cases illustrate how you can use Service Control for deployment of Bonjour services in a university, using various combinations of wired and wireless advertisers and subscribers:

- Use Case 1: Wired Advertisers and Wireless Subscribers
- Use Case 2: Wireless Advertisers and Wired Subscribers
- Use Case 3: Wired Advertisers and Wired Subscribers
- Use Case 4: Wireless Advertisers and Wireless Subscribers

All of the use cases share the following network configuration, as shown in Figure 9:

- There are four VLANs configured on the wired network: Student (300), Staff (400), Administration (600), and Liberal Arts (700).
- The Student and Staff VLANs are mapped to the relevant SSIDs that are broadcast by the APs. All APs in the Administration building are connected to VLAN 600, and all APs in the Liberal Arts building are connected to VLAN 700.
- The Administration VLAN refers to the wired network segregation, specific to the Administration building.
- The Liberal Arts VLAN refers to the wired network segregation, specific to the Liberal Arts building.
- Service Control is enabled.

Figure 9: Common Network Configuration for Use Cases



Use Case 1: Wired Advertisers and Wireless Subscribers

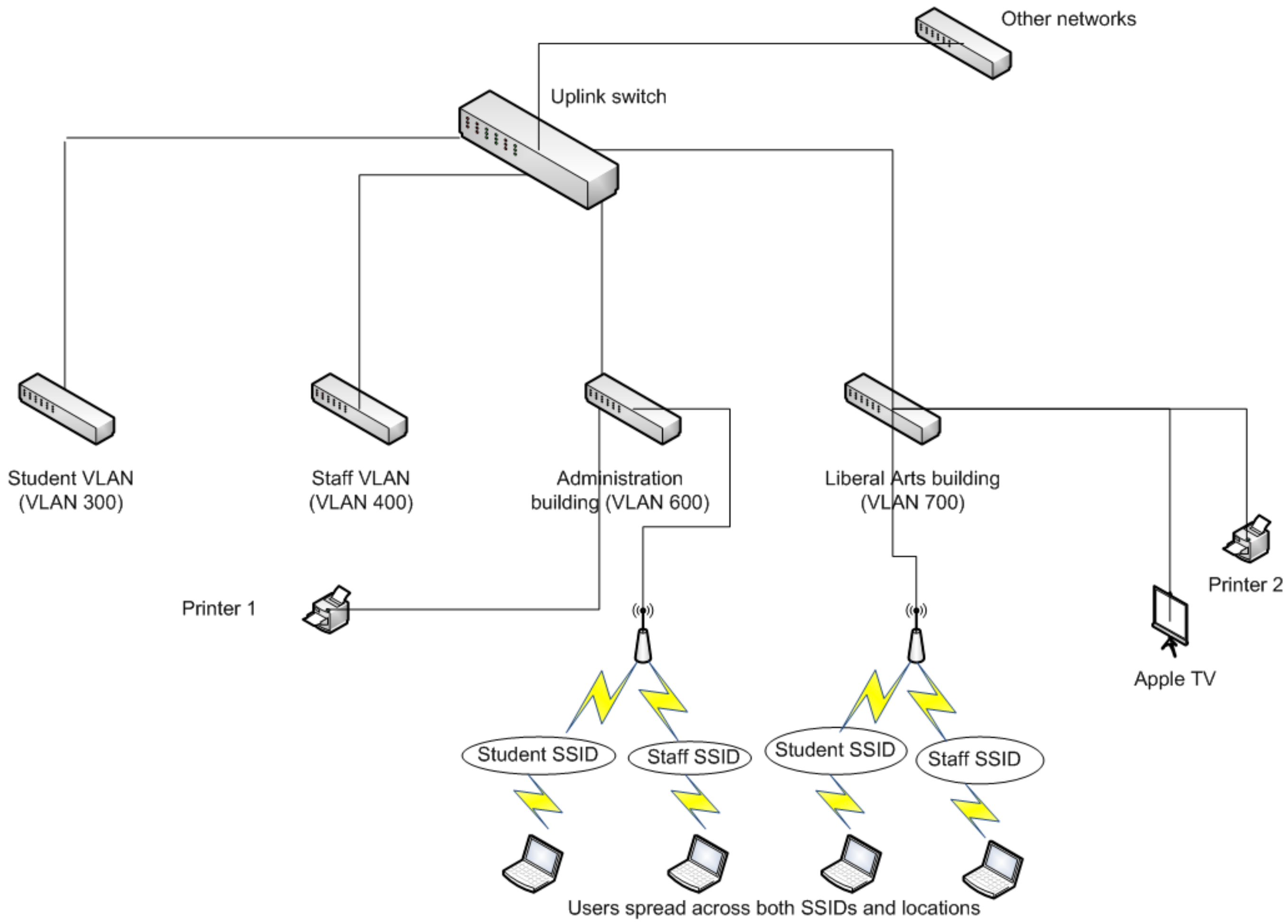
In this use case, printing services are required for staff and students in the Administration and Liberal Arts buildings. Staff members also require access to Apple TV. The printers and Apple TV device are connected to the wired network (wired advertisers), and staff and students are using wireless devices (wireless subscribers).

Figure 10 shows a network diagram of configured VLANs and advertiser locations for this use case. One printer (Printer 1) is connected by Ethernet in the Administration building. An Apple TV device and a printer (Printer 2) are connected by Ethernet in the Liberal Arts building.

Requirements

- Printer 1 is available only to staff when they are in the Administration building. Students never have access to this printer.
- Printer 2 is available to all users and available only when users are in the Liberal Arts building.
- Apple TV is available only to staff, regardless of user location (users can be in either of the two buildings). Students never have access to it. Additionally, this device needs to be available regardless of the user location (user can be in either of the two buildings).

Figure 10: Use Case 1 Network Diagram



Creating User Groups

To implement the use case requirements, you need to create user groups on the controller. When user groups are created, they require the mapping (or grouping) of SSIDs or VLANs to a subset of APs, which allows for location-based control of Bonjour packet flow. This mapping is relevant only for Service Control and is not associated with the ESS-AP mappings for ESSID configuration.

Create the following user groups:

- Student-LibArts: Maps the “Student” SSID to the APs in the Liberal Arts building.
- Staff-LibArts: Maps the “Staff” SSID to the APs in the Liberal Arts building.
- Staff-Admin: Maps the “Staff” SSID to the APs in the Administration building.
- V600: Specifies a wired VLAN (VLAN 600).
- V700: Specifies a wired VLAN (VLAN 700).

Creating Service Control Policies

After creating user groups, you need to create Service Control policies. In general, a subscriber user group is allowed to discover particular service types associated with an advertiser user group.

Create the following Service Control policies:

- Students-All: Any user that connects to the “Student” SSID in the Liberal Arts building has access to print services that are hosted on VLAN 700.
- Staff-LA: Any user that connects to the “Staff” SSID in the Liberal Arts building has access to print and AppleTV services that are hosted on VLAN 700.
- Staff-AD-Print: Any user that connects to the “Staff” SSID in the Administration building has access to print services on VLAN 600.
- Staff-AD-Tv: Any user that connects to the “Staff” SSID in the Administration building has access to AppleTV services that are hosted on VLAN 700. This policy is required because staff in the Administration building must have access to AppleTV services hosted in a different building/location/VLAN.

After Service Control is enabled, the default behavior is to drop all Bonjour packets, unless a policy exists that specifies that a specific service is available to a specific user group. Therefore, you do not need to create a policy for preventing students from accessing Printer 1 or AppleTV.

Table 1 lists the configuration parameters for the Service Control policies.

Table 1: Use Case 1 Service Control Policies

Policy Name	Subscriber User Group	Service Type	Advertiser User Group
Students-All	Student-LibArts	Printer	V700
Staff-LA	Staff-LibArts	Printer, AppleTV	V700
Staff-AD-Print	Staff-Admin	Printer	V600
Staff-AD-Tv	Staff-Admin	AppleTV	V700

Use Case 2: Wireless Advertisers and Wired Subscribers

In this use case, printing services are required for staff and students in the Administration and Liberal Arts buildings. Staff members also require access to Apple TV. The printers and Apple TV device are connected to the wireless network (wireless advertisers), and staff and students are using wired devices (wired subscribers).

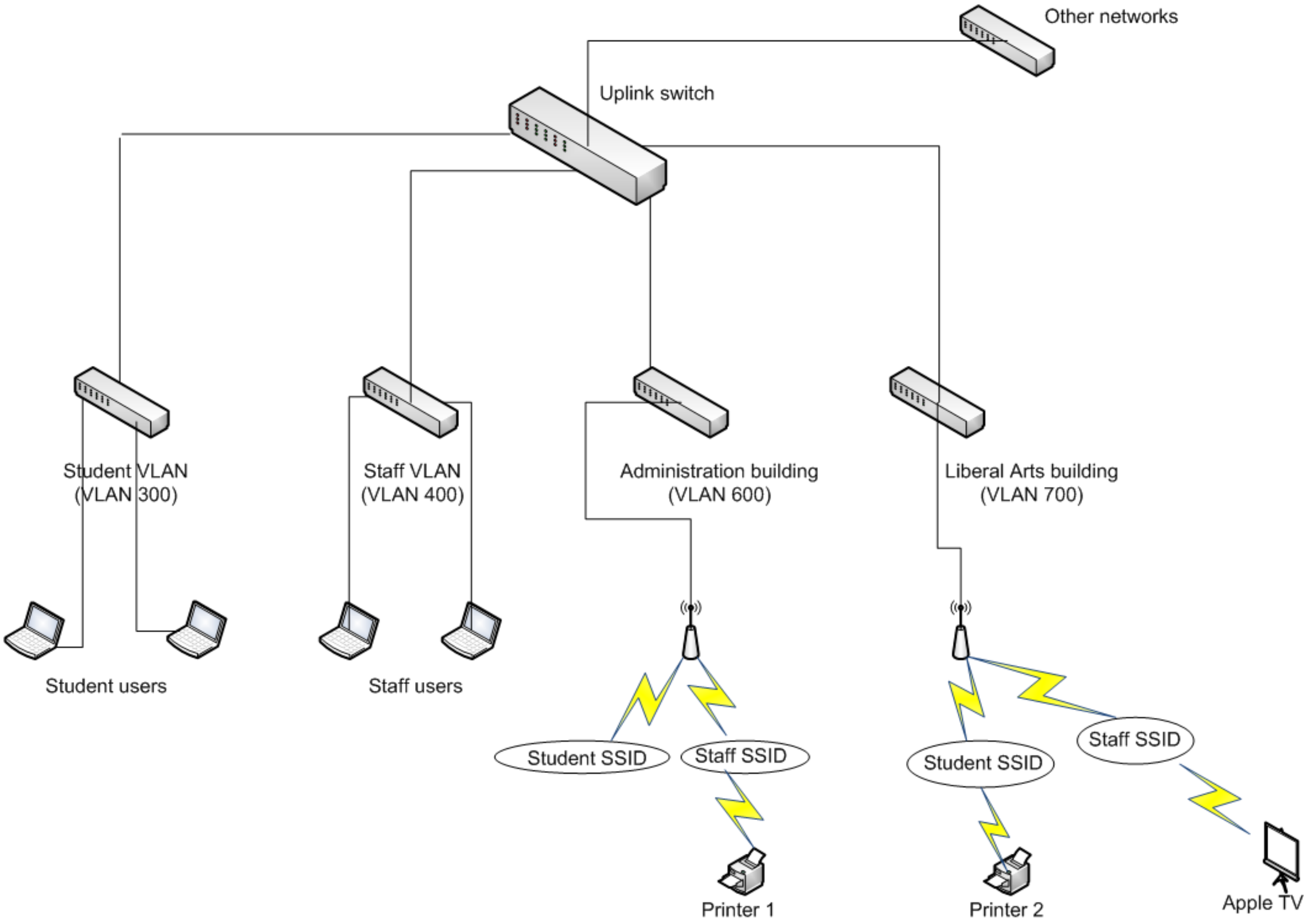
Figure 11 shows a network diagram of configured VLANs and advertiser locations for this use case:

- Printer 1 is connected wirelessly to the "Staff" SSID in the Administration building.
- Printer 2 is connected wirelessly to the "Student" SSID in the Liberal Arts building.
- An Apple TV is connected wirelessly to the "Staff" SSID in the Liberal Arts building.
- Student and Staff users are connected by Ethernet to their respective VLANs.

Requirements

- Printer 1 is available only to staff. Students never have access to this printer.
- Printer 2 is available to all users.
- Apple TV is available only to staff. Students never have access to this device.

Figure 11: Use Case 2 Network Diagram



Creating User Groups

To implement the use case requirements, you need to create user groups on the controller. When user groups are created, they require the mapping (or grouping) of SSIDs or VLANs to a subset of APs, which allows for location-based control of Bonjour packet flow. This mapping is relevant only for Service Control and is not associated with the ESS-AP mappings for ESSID configuration.

Create the following user groups:

- Student-LibArts: Maps the “Student” SSID to the APs in the Liberal Arts building.
- Staff-LibArts: Maps the “Staff” SSID to the APs in the Liberal Arts building.
- Staff-Admin: Maps the “Staff” SSID to the APs in the Administration building.
- V300: Required to specify a wired VLAN (VLAN 300).
- V400: Required to specify a wired VLAN (VLAN 400).

Creating Service Control Policies

After creating user groups, you need to create Service Control policies. In general, a subscriber user group is allowed to discover particular service types associated with an advertiser user group.

Create the following Service Control policies:

- Students-All: Any user that connects to V300 (Student VLAN) with Ethernet has access to print services that are hosted on devices connected to the “Student” SSID in the Liberal Arts building (for example, Printer 2).
- Staff-LA-Print: Any user that connects to V400 (Staff VLAN) with Ethernet has access to print services that are hosted on devices connected to the “Student” SSID in the Liberal Arts building (for example, Printer 2).
- Staff-AD-Print: Any user that connects to V400 (Staff VLAN) with Ethernet has access to print services that are hosted on devices connected to the “Staff” SSID in the Liberal Arts building.
- Staff-Tv: Any user that connects to V400 (Staff VLAN) with Ethernet has access to Apple TV services that are hosted on devices connected to the “Staff” SSID in the Administration building (for example, Apple TV).

After Service Control is enabled, the default behavior is to drop all Bonjour packets, unless a policy exists that specifies that a specific service is available to a specific user group. Therefore, you do not need to create a policy for preventing students from accessing Printer 1 or AppleTV.

Table 2 lists the configuration parameters for the Service Control policies.

Table 2: Use Case 2 Service Control Policies

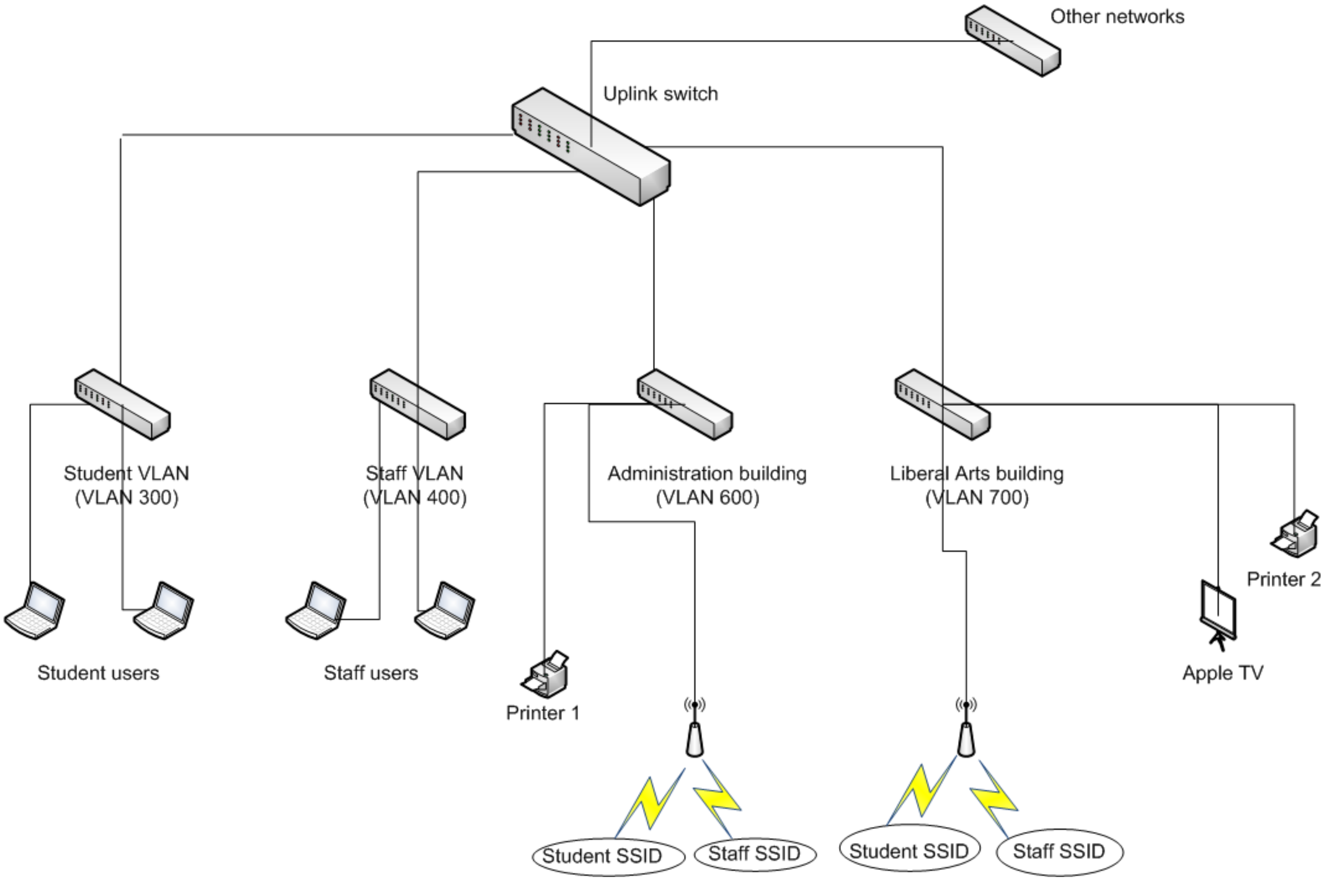
Policy Name	Subscriber User Group	Service Type	Advertiser User Group
Students-All	V300	Printer	Student-LibArts
Staff-LA-Print	V400	Printer	Student-LibArts
Staff-AD-Print	V400	Printer	Staff-Admin
Staff-Tv	V400	AppleTV	Staff-LibArts

Use Case 3: Wired Advertisers and Wired Subscribers

In this use case, printing services are required for staff and students in the Administration and Liberal Arts buildings. Staff members also require access to Apple TV. The printers and Apple TV device are connected to the wired network (wired advertisers), and staff and students are using wired devices (wired subscribers).

Figure 12 shows a network diagram of configured VLANs and advertiser locations for this use case. One printer (Printer 1) is connected by Ethernet in the Administration building. An Apple TV device and a printer (Printer 2) are connected by Ethernet in the Liberal Arts building. Student and staff are connected by Ethernet to their respective VLANs.

Figure 12: Use Case 3 Network Diagram



Requirements

- Printer 1 is available only to staff. Students never have access to this printer.
- Printer 2 is available to all users.
- Apple TV is available only to staff. Students never have access to this device.

Creating User Groups

To implement the use case requirements, you need to create user groups on the controller. When user groups are created, they require the mapping (or grouping) of SSIDs or VLANs to a subset of APs, which allows for location-based control of Bonjour packet flow. This mapping is relevant only for Service Control and is not associated with the ESS-AP mappings for ESSID configuration.

Create the following user groups:

- V300: Specifies a wired VLAN (VLAN 300).
- V400: Specifies a wired VLAN (VLAN 400).
- V600: Specifies a wired VLAN (VLAN 600).
- V700: Specifies a wired VLAN (VLAN 700).

Creating Service Control Policies

After creating user groups, you need to create Service Control policies. In general, a subscriber user group is allowed to discover particular service types associated with an advertiser user group.

Create the following Service Control policies:

- Students-All: Any user that connects to V300 (Student VLAN) with Ethernet has access to print services that are hosted on VLAN 700 (for example, Printer 2).
- Staff-AD-Print: Any user that connects to V400 (Staff VLAN) with Ethernet has access to print services that are hosted on VLAN 600 (for example, Printer 1).
- Staff-LA-PrintTv: Any user that connects to V400 (Staff VLAN) with Ethernet has access to print and AppleTV services that are hosted on VLAN 700 (for example, Printer 2 and AppleTV).

After Service Control is enabled, the default behavior is to drop all Bonjour packets, unless a policy exists that specifies that a specific service is available to a specific user group. Therefore, you do not need to create a policy for preventing students from accessing Printer 1 or AppleTV.

Table 3 lists the configuration parameters for the Service Control policies.

Table 3: Use Case 3 Service Control Policies

Policy Name	Subscriber User Group	Service Type	Advertiser User Group
Students-All	V300	Printer	V700
Staff-AD-Print	V400	Printer	V600
Staff-LA-PrintTv	V400	Printer, AppleTV	V700

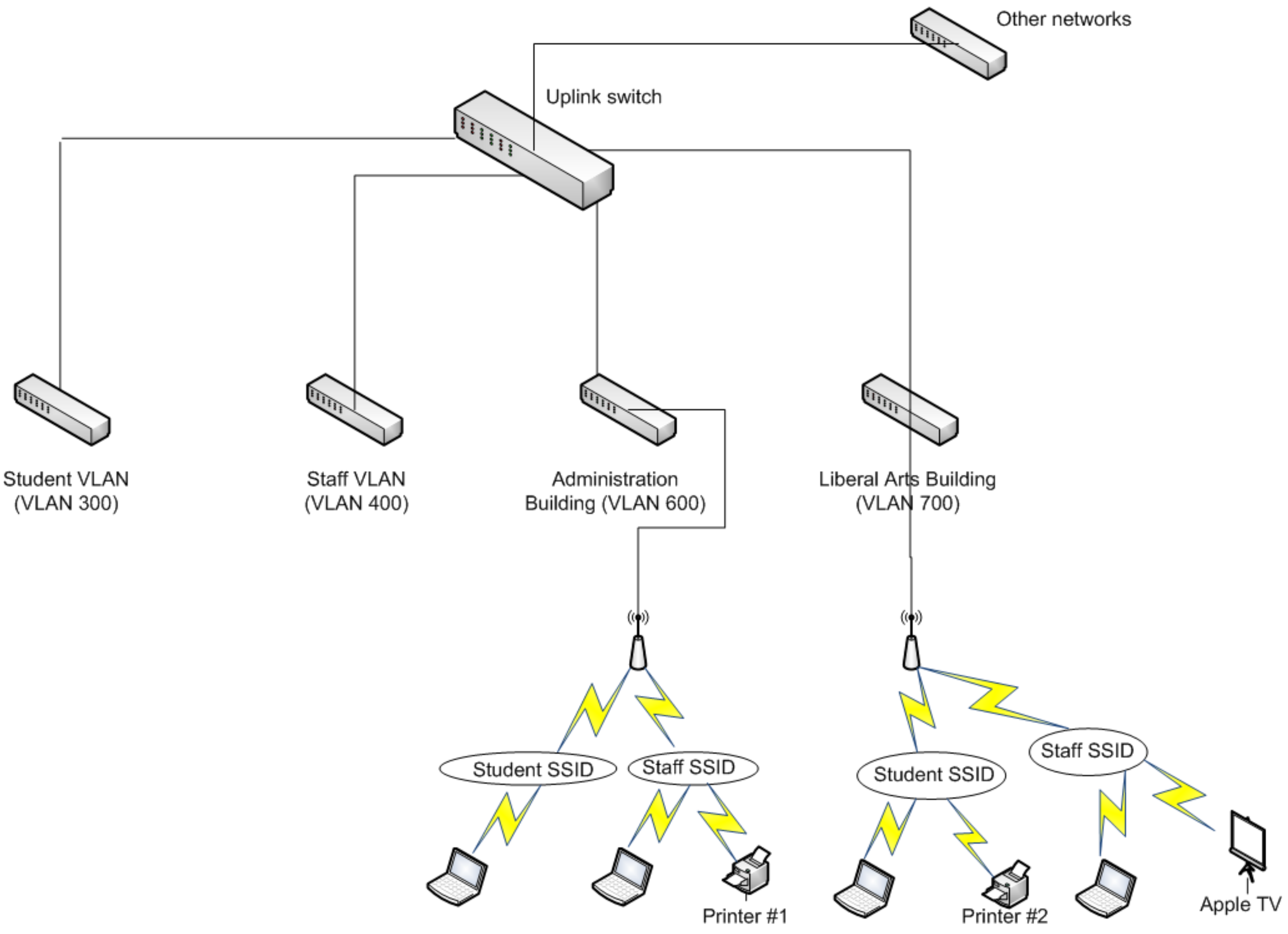
Use Case 4: Wireless Advertisers and Wireless Subscribers

In this use case, printing services are required for staff and students in the Administration and Liberal Arts buildings. Staff members also require access to Apple TV. The printers and Apple TV device are connected to the wireless network (wireless advertisers), and staff and students are using wired devices (wired subscribers).

Figure 13 shows a network diagram of configured VLANs and advertiser locations for this use case:

- Printer 1 is connected wirelessly to the "Staff" SSID in the Administration building.
- Printer 2 is connected wirelessly to the "Student" SSID in the Liberal Arts building.
- An Apple TV is connected wirelessly to the "Staff" SSID in the Liberal Arts building.
- Student and staff are connected wirelessly to their respective SSIDs.

Figure 13: Use Case 4 Network Diagram



Requirements

- Printer 1 is available only to staff when they are in the Administration building. Students never have access to this printer.
- Printer 2 is available to all users and is available only when they are in the Liberal Arts building.
- Apple TV is available only to staff, regardless of where they are located (in Administration and Liberal Arts buildings). Students never have access to this printer.

Creating User Groups

To implement the use case requirements, you need to create user groups on the controller. When user groups are created, they require the mapping (or grouping) of SSIDs or VLANs to a subset of APs, which allows for location-based control of Bonjour packet flow. This mapping is relevant only for Service Control and is not associated with the ESS-AP mappings for ESSID configuration.

Create the following user groups:

- Student-LibArts: Maps the “Student” SSID to the APs in the Liberal Arts building.
- Staff-LibArts: Maps the “Staff” SSID to the APs in the Liberal Arts building.
- Staff-Admin: Maps the “Staff” SSID to the APs in the Administration building.

Creating Service Control Policies

After creating user groups, you need to create Service Control policies. In general, a subscriber user group is allowed to discover particular service types associated with an advertiser user group.

Create the following Service Control policies:

- Students-All: Any user that connects to the “Student” SSID in the Liberal Arts building has access to print services that are wirelessly connected to the “Student” SSID in the Liberal Arts building (for example, Printer 2).
- Staff-LA-Print: Any user that connects to the “Staff” SSID in the Liberal Arts building has access to print services that are wirelessly connected to the “Student” SSID in the Liberal Arts building (for example, Printer 2).
- Staff-LA-Tv: Any user that connects to the “Staff” SSID in the Liberal Arts building has access to AppleTV services that are wirelessly connected to the “Staff” SSID in the Liberal Arts building.
- Staff-AD-Print: Any user that connects to the “Staff” SSID in the Administration building has access to print services that are wirelessly connected to the “Staff” SSID in the Administration building (for example, Printer 1).
- Staff-AD-Tv: Any user that connects to the “Staff” SSID in the Administration building has access to AppleTV services that are wirelessly connected to the “Staff” SSID in the Liberal Arts building. This policy is required because staff in the Administration building must have access to AppleTV services hosted in a different building/location/VLAN.

After Service Control is enabled, the default behavior is to drop all Bonjour packets, unless a policy exists that specifies that a specific service is available to a specific user group. Therefore, you do not need to create a policy for preventing students from accessing Printer 1 or AppleTV.

Table 4 lists the configuration parameters for the Service Control policies.

Table 4: Use Case 4 Service Control Policies

Policy Name	Subscriber User Group	Service Type	Advertiser User Group
Students-All	Student-LibArts	Printer	Student-LibArts
Staff-LA-Print	Staff-LibArts	Printer	Student-LibArts
Staff-LA-Tv	Staff-LibArts	AppleTV	Staff-LibArts
Staff-AD-Print	Staff-Admin	Printer	Staff-Admin
Staff-AD-Tv	Staff-Admin	AppleTV	Staff-LibArts

Using Printopia

Printopia is an application that can be used in networks in which AirPrint-capable printers are not deployed. After installing Printopia on a Mac, associate one printer in the network to Printopia. The Mac, which acts as an AirPrint gateway device, now advertises service names that allow iOS-based devices (such as iPads and iPhones) to discover and print to the specified printer.

For System Director 6.0, we recommend enabling Printopia only after Service Control has been enabled on the controller.

Some versions of Printopia provide access control functionality. Given the capabilities of Service Control, we recommend that you do not configure Printopia-based access control policies. We recommend that each printer in the network that does not support AirPrint has one Printopia profile associated with it. All policies configured in Service Control continue to take effect, as non-AirPrint-capable printers are now able to advertise AirPrint services.

Deployment Considerations

Table 5 lists the current Service Control-related configuration parameter limits.

Table 5: Configuration Parameter Limits

Configuration Parameter	Size Limit
Maximum number of VLANs in global discovery criteria	128
Maximum number of service types (default list prepopulated, as described in Table 6)	128
Maximum number of user groups	64
Maximum number of Service Control policies	128

Table 6 lists the predefined service types on the controller.

Table 6: Predefined Service Types

Service Name	Service Types
Apple TV	_airplay._tcp.local. _raop._tcp.local.
Printer	_ipp._tcp.local. _ipps._tcp.local. _universal._sub._ipp._tcp.local. _universal._sub._ipps._tcp.local. _printer._tcp.local. _scanner._tcp.local.

Table 7 lists controller model-specific information.

Table 7: Model-Specific Controller Information

Controller	Maximum APs	Maximum Number of Locations	Maximum Clients	Maximum Discovery List Entries
MC1500	30	8	500	1024
MC1550	50	16	1000	2048
MC5K-BLK1A4 (with Accelerator)	300	64	3000	4096
MC5K-BLK1C4 (without Accelerator – Copper Module)	200	64	2000	4096
MC5K-BLK1F2 (without Accelerator - Fiber Module)	200	64	2000	4096
MC3200	200	64	2000	4096
MC4200 with 1GbE Module	500	128	5000	8192
MC4200 with 10GbE Module	500	128	5000	8192
MC6K-BLC-6P	500	128	5000	8192
MC1500-VE	30	8	500	1024
MC1550-VE	50	16	1000	2048
MC3200-VE	200	64	2000	4096
MC4200-VE	500	128	5000	8192

Where to Find More Information

For information about configuring Service Control and other System Director features, see the *Meru System Director Configuration Guide*.