AIRPLAY AND AIRPRINT ON CAMPUS NETWORKS

AN ARUBA AIRGROUP SOLUTION GUIDE

ARUBA networks

Table of Contents

Warning and Disclaimer

This guide is designed to provide information about wireless networking, which includes Aruba Network products, While Aruba uses commercially reasonable efforts to ensure the accuracy of the specifications contained in this document, this Guide and information in it is provide on an *as is* basis. Aruba assumes no liability or responsibility for any errors or omissions.

ARUBA DISCLAIMS ANY AND ALL OTHER REPRESENTATIONS AND WARRANTIES, WEATHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NONINFRINGEMENT, ACCURACY AND QUET ENJOYMENT. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF ARUBA EXCEED THE AMOUNTS ACUTALLY PAID TO ARUBA UNDER ANY APPLICABLE WRITTEN AGREEMENT OR FOR ARUBA PRODUCTS OR SERVICES PURSHASED DIRECTLY FROM ARUBA, WHICHEVER IS LESS.

Aruba Networks reserves the right to change, modify, transfer, or otherwise revise this publication and the product specifications without notice.

Introduction

Apple AirPlay, AirPrint and other zero-configuration (zeroconf) services based on the Bonjour protocol are essential services in campus Wi-Fi networks.

Bonjour is a Layer 2 protocol that relies on multicast messages. In order to enable Bonjour services on campus networks, IT departments must perform customization to enjoy the following capabilities:

- Forward Bonjour across subnets and VLANs, especially as devices like Apple TVs and printers are often on a different subnet than user devices like laptops.
- Limit Bonjour traffic over the wireless LAN (WLAN) to prevent performance issues. Multicast traffic by default goes out on all Wi-Fi access points (APs) and often at the lowest rates, taking up valuable airtime.
- Limit Bonjour traffic by VLAN and service-type for security reasons. Network engineers often configure certain VLANs for administrative access and prefer to block user traffic like Bonjour on these VLANs. Similarly, Bonjour can be used for a variety of applications beyond AirPlay and AirPrint, some of which may need to be blocked per the organization's security policy.
- Limit Bonjour traffic by ownership and location to ensure a better user experience. Campus networks can have hundreds, if not thousands of Bonjour-capable devices. It is likely that not all these devices are for every individual.

  Additionally, seeing a list of all printers and Apple TVs in a campus is confusing to an individual who is looking for an Apple TV in the classroom or a printer in the closest library. The ability to restrict Bonjour traffic by ownership, personal or shared; and location of device addresses this very common issue.

AirGroup™ from Aruba Networks® is an integrated capability in Aruba WLANs that enables Bonjour services like AirPlay and AirPrint on campus networks. The name AirGroup refers to a number of individual networking features that extend Bonjour across subnets, as well as limit unnecessary Bonjour traffic to improve Wi-Fi performance.

AirGroup also improves the end-user experience by leveraging device location and ownership information to limit the Printers and Apple TVs each individual can see on their device.

Capabilities within AirGroup are available through software updates on Aruba WLANs that are managed by Mobility Controllers as well as Aruba Instant™, which utilizes Virtual Controller technology.

Some AirGroup features can be enabled on non-Aruba WLANs by adding an overlay Mobility Controller. Location and ownership-based access control requires the Aruba ClearPass Access Management System™.

What is Zero Configuration Networking (zeroconf)?

Zeroconf is a set of protocols that enable service discovery, address assignment and name resolution for desktop computers, mobile devices and network services. It is designed for flat, single-subnet IP networks such as wireless networking at home.

Bonjour, Apple's trade name for its zeroconf implementation, is the most common example. It is supported by most of the Apple product line including the Mac OS X operating system, iPhone, iPod Touch, iPad, Apple TV and AirPort Express.

Bonjour can be installed on computers running Microsoft Windows and is supported by most new network-capable printers. Bonjour is also included within popular software programs such as Apple iTunes, Safari and iPhoto.

Bonjour uses multicast DNS (mDNS) to locate devices and the services that those devices offer. Since the addresses used by the protocol are link-local multicast addresses, each query or advertisement can only be forwarded on its respective VLAN, but not across different VLANs.

Bonjour can be extended across subnets by using custom router configurations that forward mDNS traffic between VLANs. Another approach uses a dedicated Bonjour gateway like an Aruba Mobility Controller with AirGroup features.

Aruba WLANs with ArubaOS™ 6.1.5 or later have native mDNS proxy capabilities so that no external gateway or custom router configuration is required.

WLANs and Bonjour

In large universities and enterprise networks, it is common for Bonjour-capable devices to connect to the network across VLANs. As a result, user devices such as an iPad on VLAN 30 will not be able to discover the Apple TV that resides on another VLAN.

When a router is enabled to propagate all the mDNS traffic between VLANs across wired and wireless networks, the network is flooded with mDNS traffic that consumes valuable wireless airtime.

Network administrators are faced with a difficult choice between propagating mDNS traffic across VLANs – and risking a significant reduction in wireless performance – or blocking mDNS traffic to prevent connectivity for Bonjour-capable devices and services.

As mentioned before, Aruba AirGroup adds mDNS proxy capabilities to campus WLANs so that Bonjour messages can be forwarded across subnets or VLANs. To prevent excessive multicast traffic over the WLAN, AirGroup includes multicast optimization algorithms that forward Bonjour messages to *targeted* user devices, instead of all devices on all APs.

IT can additionally specify which Bonjour services are not allowed on specific VLANs and what Bonjour services are allowed on others.

AirGroup also enables location- and ownership-based access control of Bonjour traffic. With Aruba ClearPass, users and IT can self-register personal and shared devices, respectively.

Using registration information, Aruba ClearPass automatically creates an *AirGroup* that associates individuals to their personal devices and user groups to their shared devices.

These ownership and location associations are then available to Aruba WLANs and Aruba Mobility Controllers acting as Bonjour gateways to make Bonjour forwarding and blocking decisions.

As a result, IT departments can deliver a personal network experience where only the teacher in a classroom can have access to the classroom Apple TV and a person on the second floor of a building can only see the printer on the same floor.

How does Aruba AirGroup work?

AirGroup integrated in a Mobility Controller. Full AirGroup capabilities are available as a feature of Aruba Wi-Fi solution where Wi-Fi data is centralized with a Mobility Controller (ArubaOS 6.1.5). Aruba ClearPass adds ownership and location based traffic control. This option is ideal for campus networks.

AirGroup integrated in Aruba Instant. Like the integrated Mobility Controller option, full AirGroup capabilities are available as a feature in Aruba WLANs where Wi-Fi data is distributed among Aruba Instant APs.

Aruba ClearPass adds ownership- and location-based traffic control. This option is ideal for K-12 networks and does not require a Mobility Controller. AirGroup in Aruba Instant is available in an upcoming version in 2012.

Overlay AirGroup Mobility Controller on an Aruba WLAN. A number of AirGroup capabilities are available by overlaying any Mobility Controller (ArubaOS 6.1.5) on older Aruba WLANs. Adding Aruba ClearPass adds traffic control based on device ownership. This option is ideal for existing Aruba customers who do not want to change their existing Aruba WLAN setup.

Overlay AirGroup Mobility Controller on a third-party WLAN. A number of AirGroup capabilities are available by overlaying any Mobility Controller (ArubaOS 6.1.5) on third-party WLANs. Aruba ClearPass adds traffic control based on device ownership. This option is ideal for instances where existing WLAN cannot be replaced.

The table below lists the different capabilities available with each deployment mode.

	AirGroup in a controller-based WLAN	AirGroup in Aruba Instant	Overlay AirGroup controller on an Aruba WLAN	Overlay AirGroup controller on a third-party WLAN
Forward Bonjour across subnets and VLANs	✓	✓	✓	✓
Limit multicast over Wi-Fi	✓	✓	✓*	✓*
Limit Bonjour by service and VLAN	✓	✓	✓	✓
Limit Bonjour by user role	✓	✓	✗	✗
Limit Bonjour by device owner	✓ with ClearPass	✓ with ClearPass	✓ with ClearPass	✗
Limit Bonjour by device location	✓ with ClearPass	✓ with ClearPass	✗	✗

** Does not work when user device and shared device (Apple TV, printer) are on the same VLAN.*

Once it is set up, AirGroup in an Aruba WLAN with Aruba ClearPass works as follows:

1. An end user is authorized by the network administrator to register a service – such as AirPlay to Apple TV – using the Aruba ClearPass device registration interface.

   The end user logs into ClearPass using corporate network credentials and gets access to a web registration portal.

   After registration, this restricts the use of this service to mobile devices logged onto the network under that user's identity.

2. Aruba Mobility Controllers or Aruba Instant Virtual Controllers continuously maintain state information for all mDNS services by running service discovery in Layer 2. Aruba Mobility Controllers or Aruba Instant Virtual Controllers query Aruba ClearPass to map access privileges of a particular mobile device to available services.

3. Aruba Mobility or Virtual Controllers respond back to the query listing made by a mobile device based on contextual data – user role, device type and location.

Discovering services with Aruba Mobility Access Switches

If a shared wired service, such as a printer, is connected to an Aruba S2500 or S3500 Mobility Access Switch, a centralized Aruba Mobility Controller automatically correlates the APs connected to that switch with shared mDNS services. In this case, there is no need to make the service VLANs visible to the Mobility Controller in Layer 2.

When a Mobility Access Switch is managed by an Aruba Mobility Controller, it collects discovery information for all downstream devices. This allows a Mobility Controller to discover devices on VLANs that appear at the switch but not at the Mobility Controller.

Furthermore, Aruba Mobility Controllers can estimate the physical location of mobile devices associated with an AP under its control. The Mobility Access Switch also offers estimated locations of wired devices directly connected to it. This eliminates the need for an administrator to place the wired device delivering the services, such as an Apple TV, on a floor plan.

When a Mobility Access Switch is deployed standalone and not managed by an Aruba Mobility Controller, it will then perform the Aruba Group service discovery tasks.

Example: WLANs in higher education

The example below shows a higher education environment with shared, local and personal services that are available to mobile devices. With Aruba AirGroup, context-based policies determine which services are visible to end user mobile devices.

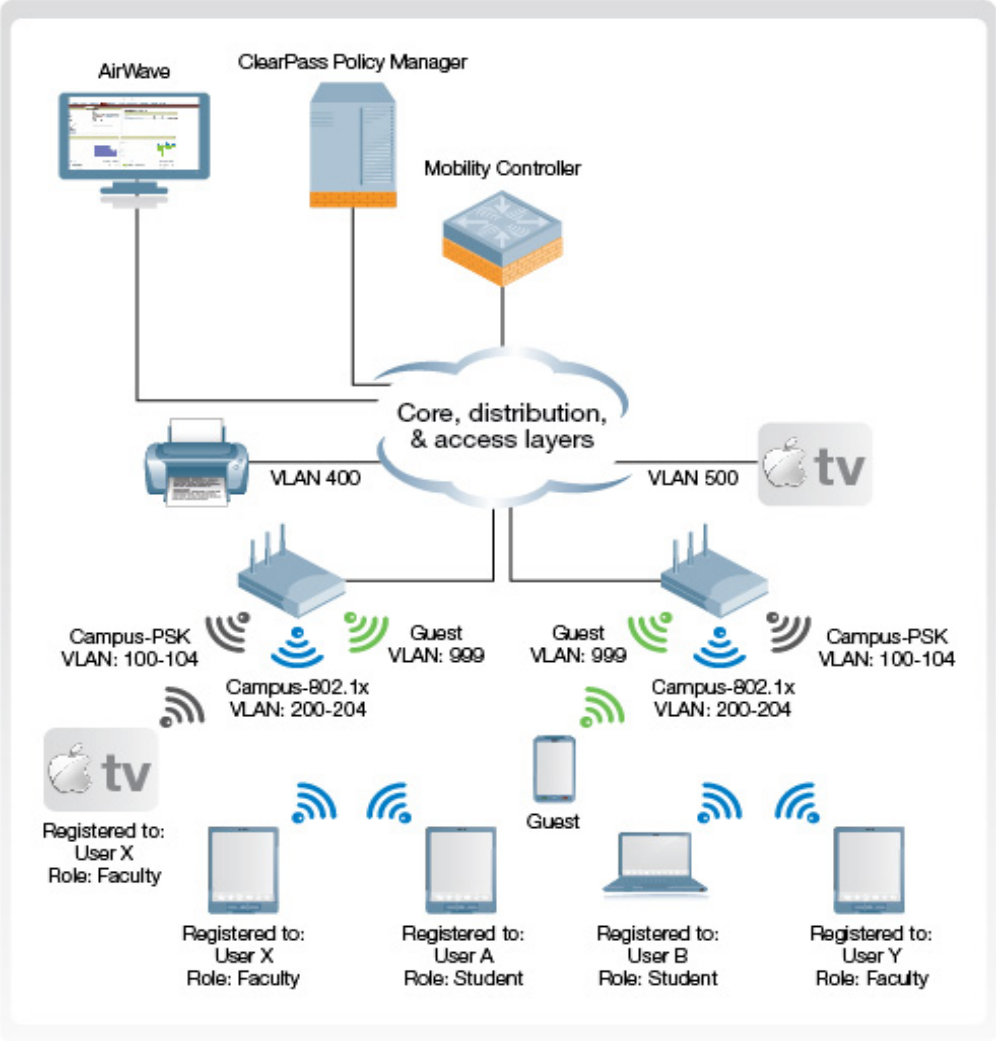

Figure 1: Aruba AirGroup in a higher-education environment.

	Faculty	Student	Visitor
mDNS services	User X's iPad	User B's MacBook	Windows Laptop
Apple TV in the lab, registered to user role *Faculty*	✓	✗	✗
Apple TV in the dorm room, registered to User B	✗	✓	✗
Apple TV in a lecture hall accessible to faculty	✓	✗	✗
Printer located in a lab accessible to faculty and students	✓	✓	✗

Table 1: Sample policies for Aruba AirGroup in a higher education environment.

Deploying Aruba AirGroup

Aruba AirGroup can be deployed with Aruba ClearPass (recommended for large WLANs) or optionally without ClearPass in smaller networks. The network administrator and end user experience in each case is outlined below.

1. **Small network deployment**

   a. < five user VLANs
   b. Dozens of mDNS-capable devices
   c. Hundreds of Bonjour-capable clients
   d. Aruba Mobility Controller

   Network administrator experience

   - Deploy ArubaOS with Aruba AirGroup feature.
   - Administrator defines network access policies and user roles.

   End user experience

   - User connects to the WLAN. User is automatically assigned a role based on authentication credentials.
   - Bonjour-capable devices and services allowed for that role are accessible by the user.

2. **Large university or enterprise network**

   a. Dozens of user VLANs
   b. Hundreds of mDNS-capable devices
   c. Thousands of Bonjour-capable clients
   d. Aruba Mobility Controller
   e. Aruba ClearPass Policy Manager
   f. Aruba S2500 or S3500 Mobility Access Switch (optional)

   Network administrator experience

- Deploy ArubaOS with Aruba AirGroup feature.
- Administrator defines network access policies and user roles.
- Administrator can use the ClearPass registration page to identify shared services and map them to physical locations based on the AP name or AP group name.

End user experience

- User connects to the WLAN using a mobile device. User is automatically assigned an administrator-defined role based on authentication credentials.
- Users, such as students in dorm rooms, are asked to register personal devices like Apple TVs and gaming consoles.

Why Aruba AirGroup?

Aruba WLANs with AirGroup technology enable context-aware access to Apple Bonjour and other zeroconf-enabled devices without constraining WLAN performance. Only AirGroup delivers:

1. Context-aware access control using Aruba Mobility Controllers. A user's role in an organization (e.g. marketing), the user's devices (e.g. iPad) and the user's location (e.g. conference room) are taken into account before zeroconf services are made available.
2. Self-registration of services using the Aruba ClearPass Policy Manager. Users and IT administrators can register devices that support zeroconf while policies define user- and location-based access privileges.
3. Zero-touch installation of services. AirGroup requires no wired or wireless network configuration changes. No additional SSIDs, VLANs, IP subnets, IP routing and configuration MAC filters are required.

Aruba Networks
1344 Crossman Avenue
Sunnyvale, CA 94089-1113
Phone: +1 408-227-4500
Fax: +1 408-227-4550
Email: info@arubanetworks.com
Get Directions »