
SOLUTION GUIDE

DLNA, AIRPLAY AND AIRPRINT ON CAMPUS NETWORKS

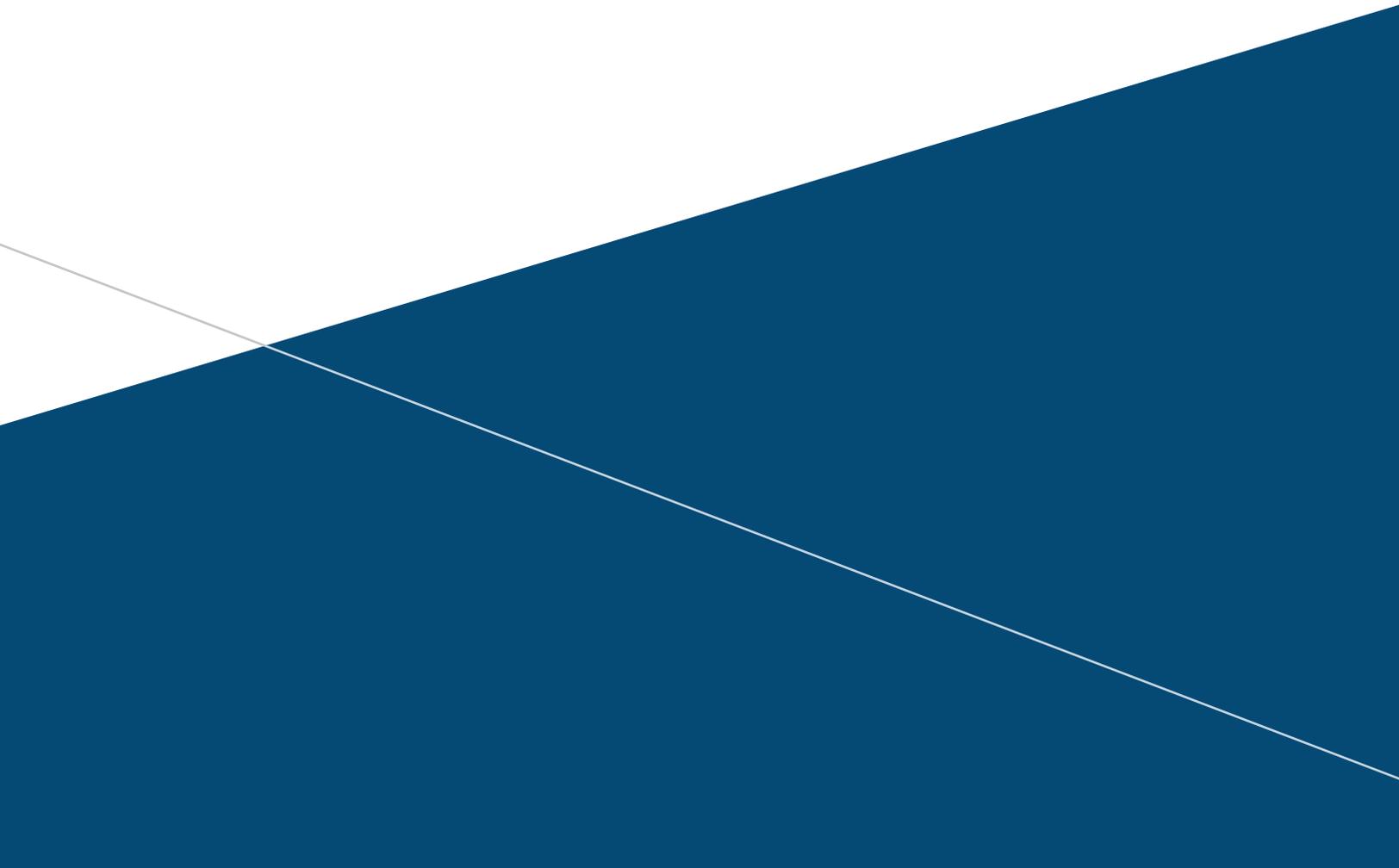


TABLE OF CONTENTS

WARNING AND DISCLAIMER	3
INTRODUCTION	3
WHAT IS ZERO CONFIGURATION NETWORKING (ZEROCONF)?	3
WHAT IS DLNA?	4
MAKING DLNA AND BONJOUR WORK OVER WLANS	4
HOW DOES ARUBA AIRGROUP WORK?	4
DISCOVERING SERVICES WITH ARUBA MOBILITY ACCESS SWITCHES	5
EXAMPLE: WLANS IN HIGHER EDUCATION	6
DEPLOYING ARUBA AIRGROUP	7
WHY ARUBA AIRGROUP?	7
ABOUT ARUBA NETWORKS, INC.	8

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 provided 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, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, ACCURACY AND QUIET ENJOYMENT. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF ARUBA EXCEED THE AMOUNTS ACTUALLY PAID TO ARUBA UNDER ANY APPLICABLE WRITTEN AGREEMENT OR FOR ARUBA PRODUCTS OR SERVICES PURCHASED 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

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

DLNA and Bonjour rely on Layer 2 protocols that use multicast messages. In order to enable Bonjour and DLNA services on campus networks, IT departments must perform customization to enjoy the following capabilities:

- Forward DLNA and 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 DLNA and 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 DLNA and 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, DLNA Bonjour can be used for a variety of applications beyond screen-sharing and printing, some of which may need to be blocked per the organization's security policy.
- Limit DLNA and Bonjour traffic by ownership and location to ensure a better user experience. Campus networks can have hundreds, if not thousands of shared devices. It is likely that not all these devices are for every individual.

Additionally, seeing a list of all printers and projectors and shared media appliances 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 DLNA and 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 DLNA and Bonjour services like screen-sharing, media-streaming and printing on campus networks. The name AirGroup refers to a number of individual networking features that extend DLNA and Bonjour across subnets, as well as limit unnecessary DLNA and 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, projectors, Google Chromecasts 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 and controllerless Aruba Instant™ APs.

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™ have native mDNS proxy capabilities so that no external gateway or custom router configuration is required.

WHAT IS DLNA?

DLNA is a trade organization that establishes interoperability guidelines for multimedia devices. It certifies communication between devices, allowing them to find and recognize each other, and share digital content. As of February 2013, there are over 18,000 device models that are DLNA-certified.

DLNA leverages Universal Plug-and-Play (UPnP) to allow devices to discover each other on the network and then communicate and share media. UPnP relies on standards-based networking technologies for addressing, discovery, and control. It uses the Simple Services Discovery Protocol (SSDP) to discover services on a Layer 2 network, just as Bonjour uses mDNS for the same.

MAKING DLNA AND BONJOUR WORK OVER WLANS

In large universities and enterprise networks, it is common for DLNA- and Bonjour-capable devices to connect to the network across VLANs. As a result, user devices such as an Samsung tablet on VLAN 30 will not be able to discover the LCD television 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 DLNA- and Bonjour-capable devices and services.

As mentioned before, Aruba AirGroup adds mDNS proxy capabilities to campus WLANs so that DLNA and 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 DNLA and Bonjour services are not allowed on specific VLANs and what services are allowed on others.

AirGroup also enables location, time-of-day and ownership based access control of DLNA and 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 DLNA and Bonjour gateways to make 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 LCD television 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. Aruba ClearPass adds ownership, time-of-day, 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, time-of-day, and location based traffic control. This option is ideal for K-12 networks and does not require a Mobility Controller.

AirGroup Domains. AirGroup domains allow two devices, such as an iPad and an Apple TV, to discover each other, even when they terminate on different Mobility Controllers or Instant AP clusters.

Mobility Controllers can be configured as members of an AirGroup domain so that information about Apple TVs and Chromecasts can be shared between Mobility Controllers. Similarly, two or more Aruba Instant clusters can be configured as members of an AirGroup domain so users on one Instant cluster can discover services on another Instant cluster.

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 or DLNA to Google Chromecast – 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 and Aruba Instant continuously maintain state information for all mDNS services by running service discovery in Layer 2. Aruba Mobility Controllers and Aruba Instant query Aruba ClearPass to map access privileges of a particular mobile device to available services.
3. Aruba Mobility Controllers and Aruba Instant 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 S1500, 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.

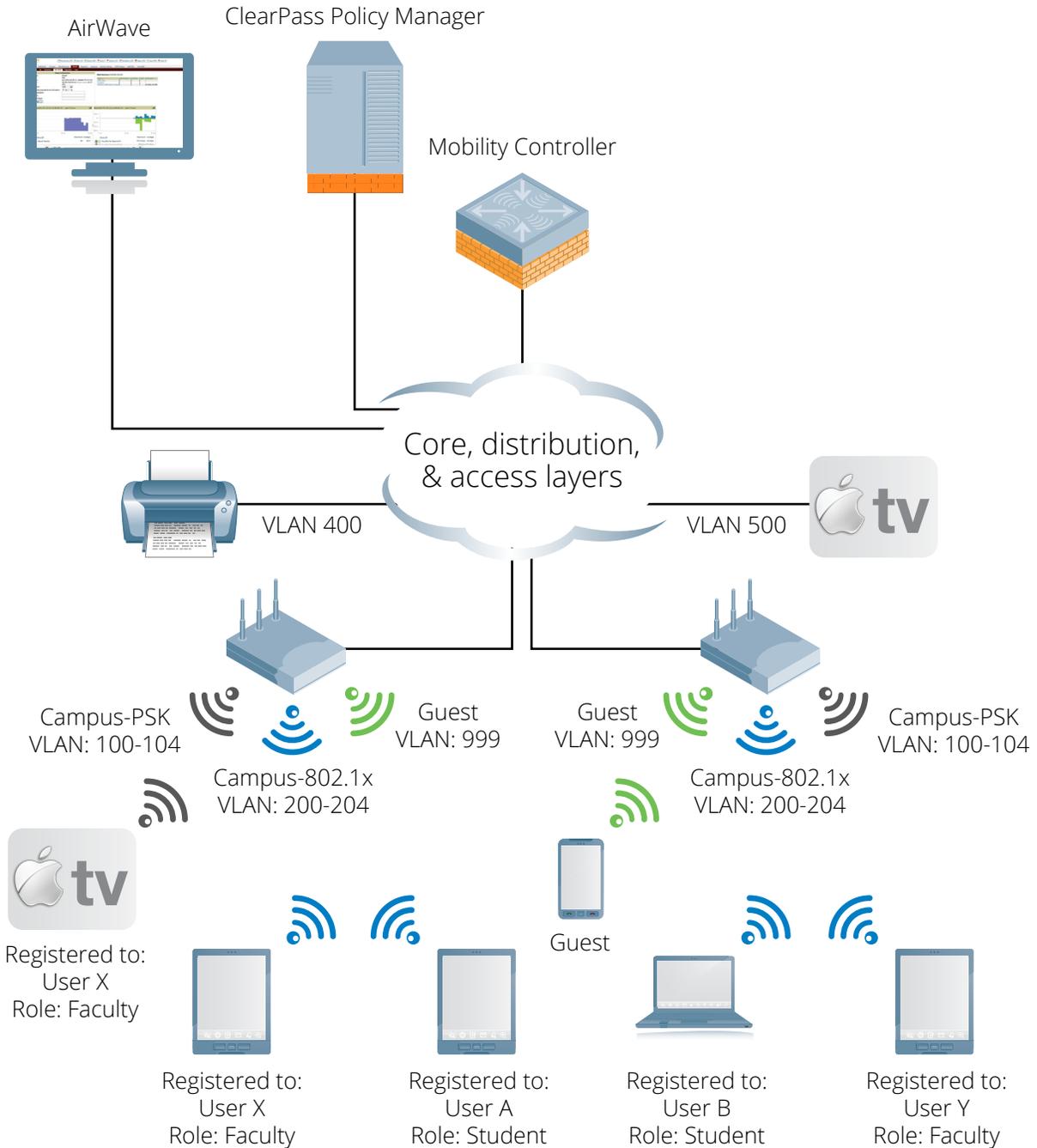


Figure 1

SAMPLE POLICIES FOR 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	✓	✓	✗

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 DLNA- and 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.
- DLNA- and 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 DLNA- and Bonjour-capable clients
- D. Aruba Mobility Controller
- E. Aruba ClearPass Policy Manager
- F. Aruba S1500, 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 DLNA, Apple Bonjour and other shared 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. Samsung Galaxy tablet), time-of-day (e.g. 5:30 p.m. on Tuesday) and the user's location (e.g. conference room) are taken into account before shared services are made available.
2. Self-registration of services using the Aruba ClearPass Policy Manager. Users and IT administrators can register devices that support media-sharing 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.

ABOUT ARUBA NETWORKS, INC.

Aruba Networks is a leading provider of next-generation network access solutions for the mobile enterprise. The company designs and delivers Mobility-Defined Networks that empower IT departments and #GenMobile, a new generation of tech-savvy users who rely on their mobile devices for every aspect of work and personal communication. To create a mobility experience that #GenMobile and IT can rely upon, Aruba Mobility-Defined Networks™ automate infrastructure-wide performance optimization and trigger security actions that used to require manual IT intervention. The results are dramatically improved productivity and lower operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, Africa and Asia Pacific regions. To learn more, visit Aruba at www.arubanetworks.com. For real-time news updates follow Aruba on [Twitter](#) and [Facebook](#), and for the latest technical discussions on mobility and Aruba products visit Airheads Social at <http://community.arubanetworks.com>.



1344 CROSSMAN AVE | SUNNYVALE, CA 94089

1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com

©2014 Aruba Networks, Inc. Aruba Networks®, Aruba The Mobile Edge Company® (stylized), Aruba Mobility Management System®, People Move. Networks Must Follow®, Mobile Edge Architecture®, RFProtect®, Green Island®, ETIPS®, ClientMatch®, Bluescanner™ and The All Wireless Workspace Is Open For Business™ are all Marks of Aruba Networks, Inc. in the United States and certain other countries. The preceding list may not necessarily be complete and the absence of any mark from this list does not mean that it is not an Aruba Networks, Inc. mark. All rights reserved. Aruba Networks, Inc. reserves the right to change, modify, transfer, or otherwise revise this publication and the product specifications without notice. While Aruba Networks, Inc. uses commercially reasonable efforts to ensure the accuracy of the specifications contained in this document, Aruba Networks, Inc. will assume no responsibility for any errors or omissions. SG_AirGroup_041414