aruba
a Hewlett Packard Enterprise company

TECH BRIEF

AIRGROUP

Chromecast and Bonjour Services on Wi-Fi Networks

INTRODUCTION

Digital Living Network Alliance (DLNA), Apple AirPlay, AirPrint, Google Chromecast and other zero-configuration (zeroconf) services based on the Bonjour and Chromcast protocols are essential services in Wi-Fi networks. They rely on Layer 2 protocols that use multicast messages. In order to enable Bonjour and Google services on campus networks, IT departments must customize their deployment and:

- **Forward Chromecast 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 Chromecast 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 Chromecast 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 Chromecast 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 Chromecast and Bonjour traffic by ownership (personal or shared) and location of device addresses this very common issue.

KEY BENEFITS

- Context-aware access to shared services like Chromecast and Bonjour
- User role, device, time-of-day, and location-based rules
- Self-registration of services used in conjunction with Aruba ClearPass Policy Manager
- Zero-touch installation of services, with no wired or wireless network configuration changes required.
- No additional SSIDs, VLANs, IP subnets, IP routing, and configuration MAC filters are required
- Flexible deployment with cloud and on-premises management options for AP only and AP and gateway deployments

ARUBA AIRGROUP

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.

ArubaOS and InstantOS provide AirGroup capabilities to controller-based and AP-only environements. Location and secure network access control requires an Aruba ClearPass license.

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

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 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.

Google Chromecast works with DLNA to leverage 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 and 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 Conductor

Full AirGroup capabilities are available as a feature of Aruba Wi-Fi solution where Wi-Fi data is centralized with a Mobility Conductor. Aruba ClearPass adds ownership, time-of-day, and location-based traffic control. This option is ideal for campus networks.

AirGroup integrated in Aruba Instant or ArubaOS 10 and managed by Aruba Central

Like the integrated Mobility Conductor option, full AirGroup capabilities are available as a feature in Aruba WLANs where Wi-Fi data is distributed among Aruba APs. Aruba Central serves as a cloud-based management plane to orchestrate multiple networks. Aruba ClearPass adds ownership, time-of-day, and location-based traffic control. This option is ideal for many commercial/mid-size networks and does not require a Mobility Conductor.

AirGroup islands

AirGroup Islands allow for areas of AirGroup management across regions. Each Island is configured by a profile and applied to a group in the hierarchy. Note that discovery and roaming servers are limited to the designated Island.

Step by step

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

- 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.
- Aruba Mobility Conductors (in AOS 8) or Aruba APs (in AOS 10 or InstantOS) continuously maintain state information for all mDNS services by running service discovery in Layer 2. Aruba Mobility Conductors and Aruba APs query Aruba ClearPass to map access privileges of a particular mobile device to available services.
- Aruba Mobility Conductors or Aruba APs 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 SWITCHES

If a shared wired service, such as a printer, is connected to an Aruba Switch, a centralized Aruba Mobility Conductor 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 Conductor in Layer 2.

EXAMPLE: WLANS IN HIGHER EDUCATION

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

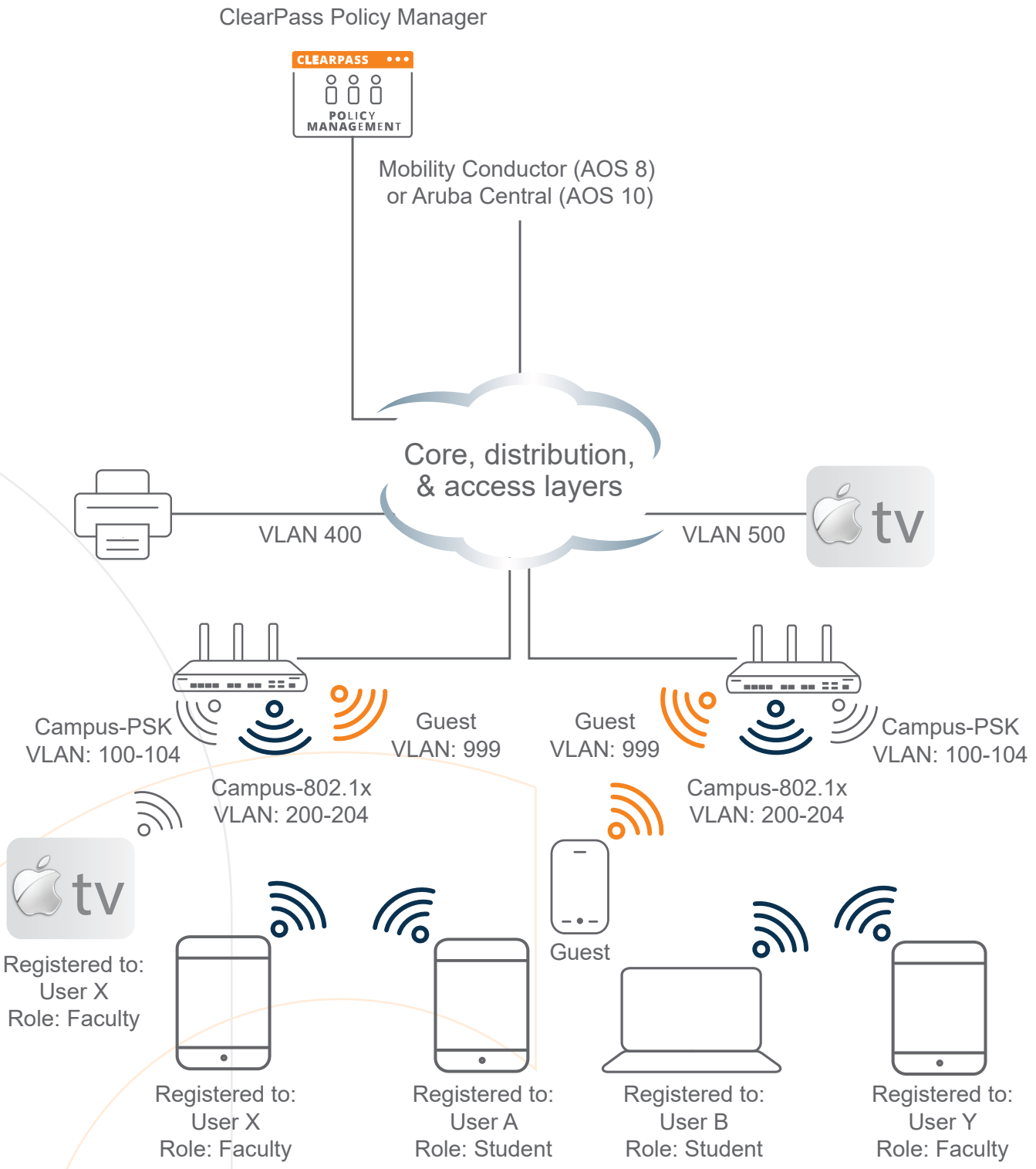

Figure 1. WLAN networks in higher education

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	√	X	X
Apple TV in the dorm room, registered to user B	X	√	X
Apple TV in a lecture hall accessible to faculty	√	X	X
Printer located in a lab accessible to faculty and students	√	√	X

DEPLOYING ARUBA AIRGROUP

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**
   - Fewer than 5 user VLANs
   - Dozens of mDNS-capable devices
   - Hundreds of DLNA- and Bonjour-capable clients
   - Airgroup service runs in Aruba Central or on Instant APs
- **Network administrator experience**
  - 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**
   - Dozens of user VLANs
   - Hundreds of mDNS-capable devices
   - Thousands of DLNA- and Bonjour-capable clients
   - Aruba Mobility Conductor
   - Aruba ClearPass Policy Manager
   - Aruba CX or AOS-S 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.

LEARN MORE

Explore Aruba's Wi-Fi solution and connect with the Airheads community.

TB_Airgroup_RVK_070721 a00116174enw