aruba
a Hewlett Packard Enterprise company

Aruba Instant

Version 2.0.1

Authors:
Vishal Mann
Roopesh Pavithran
Andrew Tanguay

Contributors:
Sathya Narayana Gopal
Yan Liu

Validated Reference Design

Copyright Information

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

www.arubanetworks.com

3333 Scott Blvd

Santa Clara, CA 95054

Phone: 1-800-WIFI-LAN (+800-943-4526)

Fax 408.227.455

Contents

Revision History

The following table lists the revisions of this document:

Revision	Date	Change Description
2.2.0	12/4/2018	Chapter 3 Published
2.1.0	8/9/2017	Chapter 2 published
2.0.1	7/1/2018	Minor edits post publication
2.0.0	6/21/2018	Initial Publication

Table 0-1 *Revision History*

About This Guide

Overview

The Aruba Validated Reference Design (VRD) series is a collection of documentation specifically designed to enable customers so that they can achieve optimal results utilizing Aruba products. Aruba VRDs are intended to not only serve as deployment guides but also to provide descriptions of Aruba technology, recommendations for product selections, network design decisions, configuration procedures, and best practices for deployment. Together these guides comprise a reference model for understanding Aruba technology and designs for common customer deployment scenarios. Each Aruba VRD network design has been constructed in a lab environment and vigorously tested by Aruba engineers. Our customers rely on these proven designs to rapidly deploy Aruba solutions in their production environments with the assurance that they will perform and scale as expected.

This VRD describes Aruba Instant which is the most efficient way to deploy enterprise-grade Wi-Fi in practically any environment. Aruba Instant provides a best in class Wi-Fi solution with a distributed design that does not require the deployment of a physical controller. The solution requires minimal time and expertise to set up, contains robust feature set, and comes fully-equipped with all of the security and management functionality required to accelerate your business in a highly cost-effective manner. In addition to providing an overview of the Aruba Instant solution, this guide describes the different use cases and deployments, as well as provides configurations and recommendations that will empower anyone deploying instant to achieve the best possible outcome for their production environment.

Intended Audience and Scope

This guide is intended for administrators who are responsible for deploying and configuring Aruba Instant devices in customer premises. Readers should have at least a basic understanding of WLAN concepts. This is a base design guide for Aruba Instant, and it is assumed that readers have at least a working understanding of fundamental wireless concepts and Aruba technology.

Related Documents

In addition to this document, the IAP product documentation includes the following:

- Aruba Instant User Guide
- Aruba Instant CLI Reference Guide
- Access Point Product Line
- End of Life Information

Conventions

Typographical Conventions

The following conventions are used throughout this manual to emphasize important concepts:

Style Type	Description
Italics	Italics are used to emphasize important terms and to mark the titles of books.
Bolded>words	Bolded words indicate an option that should be selected in the Graphical User Interface (GUI). The angled brackets indicate that the choices are part of a path in the GUI.
`Command Text`	Command text in this font will appear inside of a box and indicates commands that can be entered into the Command Line Interface (CLI).
<Arguments>	In the command examples, italicized text within single angle brackets represents items that should be replaced with information appropriate to your specific situation. For example: `# send <text message>` In this example, you would type “send” at the system prompt exactly as shown, followed by the text of the message you wish to send. Do not type the angle brackets.
`[Optional]`	Command examples enclosed in brackets are optional. Do not type the brackets.
`{Item A | Item B}`	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

Table 0-2 *Typographical Conventions*

Informational Icons

The following informational icons are used throughout this guide:

Indicates helpful suggestions, pertinent information, and important things to remember.

Indicates a risk of damage to your hardware or loss of data.

Indicates a risk of personal injury or death.

Graphical Icons

Figure 0-1 *Icon Set*

Aruba Instant Overview

Introduction

During the early days of Wi-Fi, wireless networks were designed almost exclusively for user convenience and were not considered mission-critical. It was very common even for a large organization to deploy only a handful of access points (APs) in select common areas such as lobbies, cafes, and CTO offices. Network administrators would build wireless networks using what we now refer to as fat APs (also known as autonomous APs) because performance, quality of service (QoS), mobility, scalability, and manageability were not critical factors. However, as wireless technology began to proliferate and as organizations began to realize the advantages of wireless networks, the scale of wireless deployment grew. As deployment sizes grew, scalability and manageability became major issues with the fat AP technology. This demand led to the evolution of controller-based WLANs with thin APs.

In controller-based WLAN technology with thin APs, the management and control plane functions are centralized at the controller and the data plane is either centralized or switched locally at the APs, depending on the mode of operation. Controller-based WLANs allow networks to scale up to thousands of APs while providing a single point of management and configuration. The development of controller-based WLAN technology led to a rapid increase in the adoption of wireless networks due to the ease of management and scalability they offered. The controller-based solution could be easily deployed as a network overlay without any alterations to the existing wired infrastructure.

Aruba's controller-based architecture consists of the Aruba Operating System (interchangeably referred to as ArubaOS™ or AOS), Mobility Masters, Mobility Controllers (MCs), and APs. In the past few years, advancements in AP hardware technology such as chipsets and memory have opened up the possibility of realistically deploying and relying on distributed WLAN system technology. Modern APs allow wireless vendors to distribute the management, control, and data paths among APs without the need for a physical controller while still retaining most of the same management functionality. This architecture is suitable not only for small and medium-sized WLAN deployments but also for distributed enterprises which require feature-rich, enterprise-grade solution that can be managed from a single interface. Aruba's approach to the controllerless architecture such customers are seeking is Aruba InstantOS™ and Aruba Instant™ APs (IAPs).

Access Point Types

Fat (Autonomous) APs

A Fat AP (also sometimes referred to as an “autonomous” AP) is a term used to refer to a category of access point such as those described in the introduction of this document. These were the only types of APs available during the time when enterprise Wi-Fi deployments were in their infancy and Wi-Fi was considered a luxury or nice to have rather than being seen as mission-critical as it is by the vast majority of enterprises and users today. These fat APs would typically be located in common areas where providing a large amount of user wired network access would be unpractical or could pose a security risk such as cafes, lobbies, or CTO offices. IT staff personnel were required to individually configure every AP that was deployed one by one in a process that was both labor intensive as well as time consuming. An architectural diagram of a typical Wi-Fi deployment from the time when fat APs were almost exclusively the only type of wireless access device in production can be seen below:

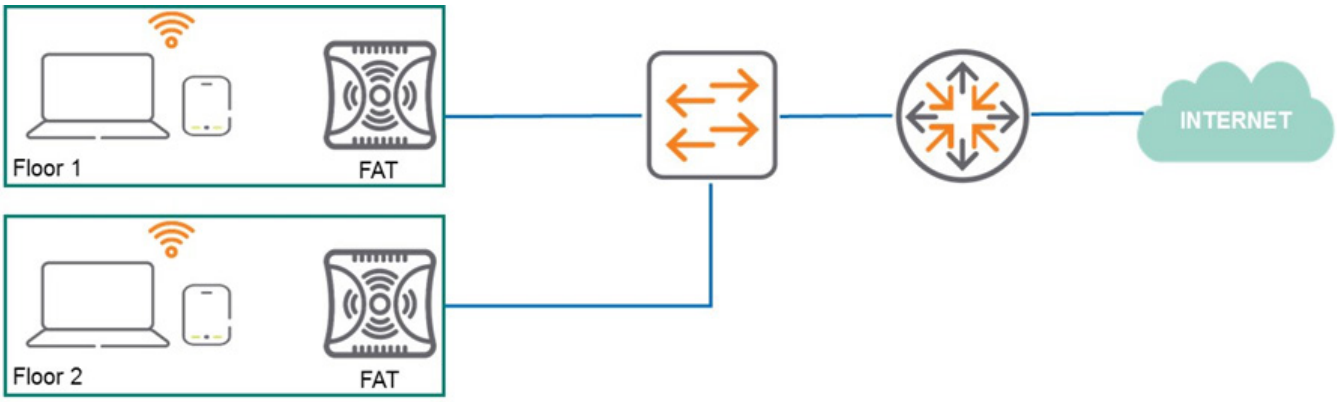


Figure 1-1 *Typical Fat AP Deployment Architecture*

While this design was acceptable back when the demand for Wi-Fi availability was relatively low it did have some significant drawbacks including the fact that each AP needed to be individually managed and configured. As Wi-Fi technology progressed and client device capabilities increased organizations began to realize the advantages of Wi-Fi networks for both guest access as well as for employee productivity. It didn’t take long before Wi-Fi went from a novelty to becoming the de facto access standard expected by every user on the network. Unfortunately the fact that fat APs needed to be individually managed imposed significant limitations to enterprises attempting to scale and grow their Wi-Fi deployments. Organizations needed a significantly more efficient method to centrally manage devices which were growing rapidly more complex and experiencing increased demand from users. This increase in demand led to the development of controller based WLAN solutions to enable administrators to gain control they needed to manage their rapidly growing and evolving networks.

Controller-Managed APs

In wireless LAN controller-based deployments the management plane and control planes are centralized at the controller while the data plane can either be centralized or switched locally at APs, depending on the requirements of the deployment scenario. Adding controllers to Wi-Fi deployments allowed organizations to scale their network up to thousands of APs in order to keep up with demand while simultaneously introducing the management functionality they needed. Administrators now had single point of management and configuration for the entire network and eliminated the cumbersome requirement of having to individually manage and manually configure every AP. An example of how the network architecture evolved to accommodate the arrival of wireless LAN controller can be seen below:

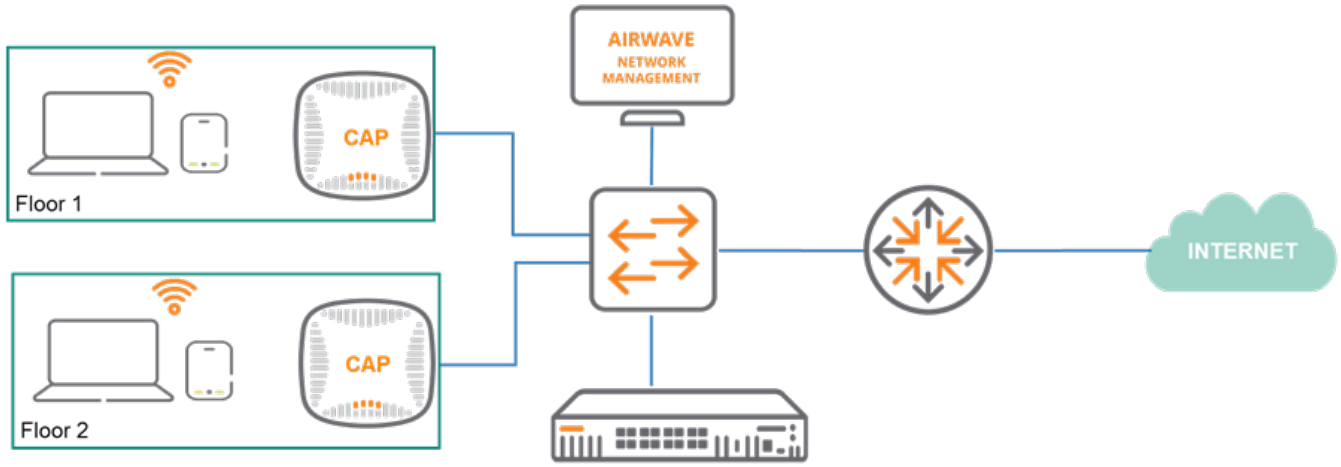


Figure 1-2 Typical *Controller-based Deployment*

Adding controllers and network management systems to wireless deployments introduced added functionality which made it dramatically easier for administrators to control their networks. However, enabling a single point of management for Wi-Fi deployments required significant investment and resources as well. The cost of deploying controllers and management functionality at the time was so high that typically only large enterprises had the ability to allocate the resources required for such solutions.

Some examples of controller-based WLAN networks include:

- Organizations that require centralized encryption and decryption of wireless data e.g. government, financial, and other security conscious organizations
- Large campuses that require thousands of APs at a single location e.g. universities, large enterprises, etc.
- Organizations with large layer 2 domain that do not want to conduct a major overhaul to their deployment such as adding or deleting VLANs to their edge network

Distributed APs

While networking solutions had evolved to provide new and innovative techniques for managing Wi-Fi access at campus deployments, providing wireless connectivity at remote locations was still a major challenge for distributed organizations such as retail chains and K-12 schools. These organizations needed an enterprise-grade WLAN solution that was not only cost effective but also provided mobility, security, and centralized management. In addition, distributed enterprises such as restaurants, hotels, retail chains and hospitals needed to comply with data privacy regulations such as Payment Card Industry (PCI) and Data Security Standard (DSS) in the financial industry and Health Insurance Portability and Accountability Act (HIPAA) for healthcare.

Due to significant advancements in AP hardware technology it is now possible to use APs in a distributed environment where the management, control, and data planes can be separated without the need of a physical controller. Aruba's solution for this scenario is called Aruba Instant. Instant provides enterprise-grade WLAN performance, security, and scalability that is user-friendly and simple to deploy. Enabling this degree of functionality at remote sites without requiring the usage of controller provides organizations with the control they require without excessively impacting their budgets.

Instant allows administrators to automate their entire deployment with features such as zero-touch provisioning (ZTP), firmware upgrades, and inventory management. Aruba recognizes that as enterprises grow in size they might eventually need to move to a controller based architecture for management purposes. It is for that reason that IAPs were developed with the ability to be converted into controller-based APs thereby providing seamless scalability, investment protection, and future-proofing the network.

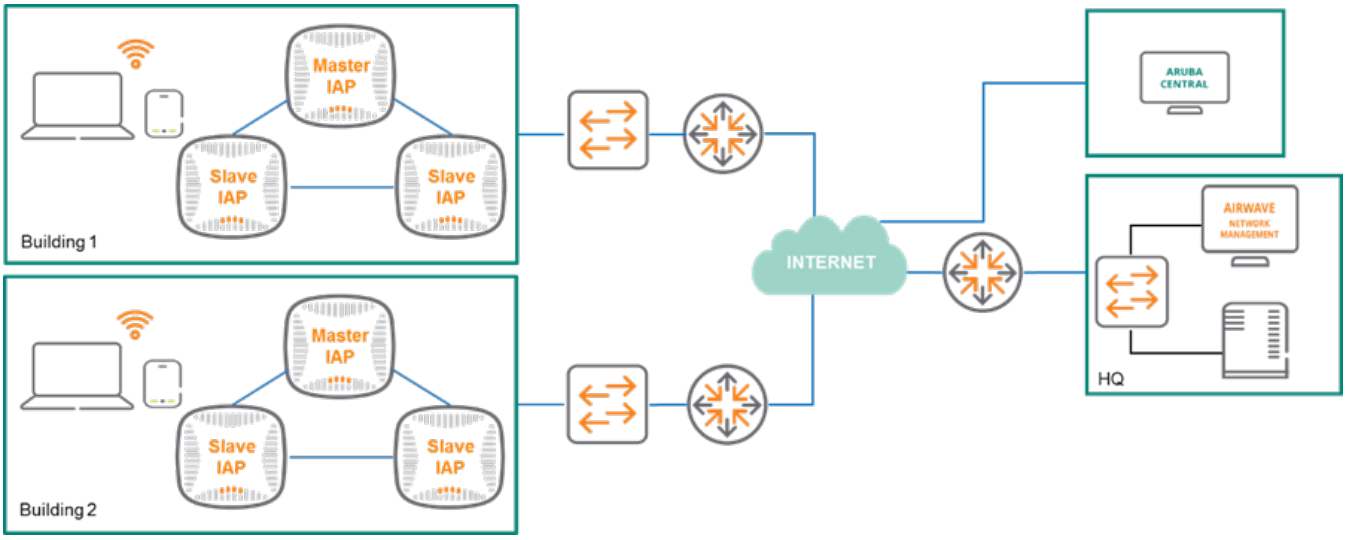


Figure 1-3 *Typical Distributed AP Architecture*

Verticals

Providing reliable wireless connectivity at remote sites has always been a challenge for organizations with distributed locations. These deployments require the same robust WLAN functionality as a large campus including voice and video optimization, high reliability, and strong security. In addition, the high cost and difficulty of deployment renders the implementation of physical controllers at every site nearly impossible. These organizations need a solution that is both affordable and simple to operate in a highly distributed environment. The solution must be able to be centrally configured and managed while ensuring that the network remains secure. For a solution to be viable for such customer it must consist of an enterprise-grade WLAN that can be deployed rapidly at geographically-dispersed locations that often have limited or no on-site IT resources.

The Aruba Instant solution was purpose-built to address these unique challenges faced by customers with distributed deployments. Instant combines enterprise-grade WLAN performance, security, and scalability with industry-leading ease-of-use and affordability. With Aruba Instant, the entire deployment process is automated, including zero-touch provisioning, firmware upgrades, and inventory management. Administrative personnel can cost effectively deploy thousands of Aruba IAPs anywhere in the world with unprecedented speed and simplicity. Below is a collection of some of the verticals which have seen tremendous benefits from deploying Instant. However, an ideal candidate for Instant is any organization with distributed sites looking for a solution that is capable of addressing all wireless connectivity needs, simple to manage, secure, and scales effortlessly.

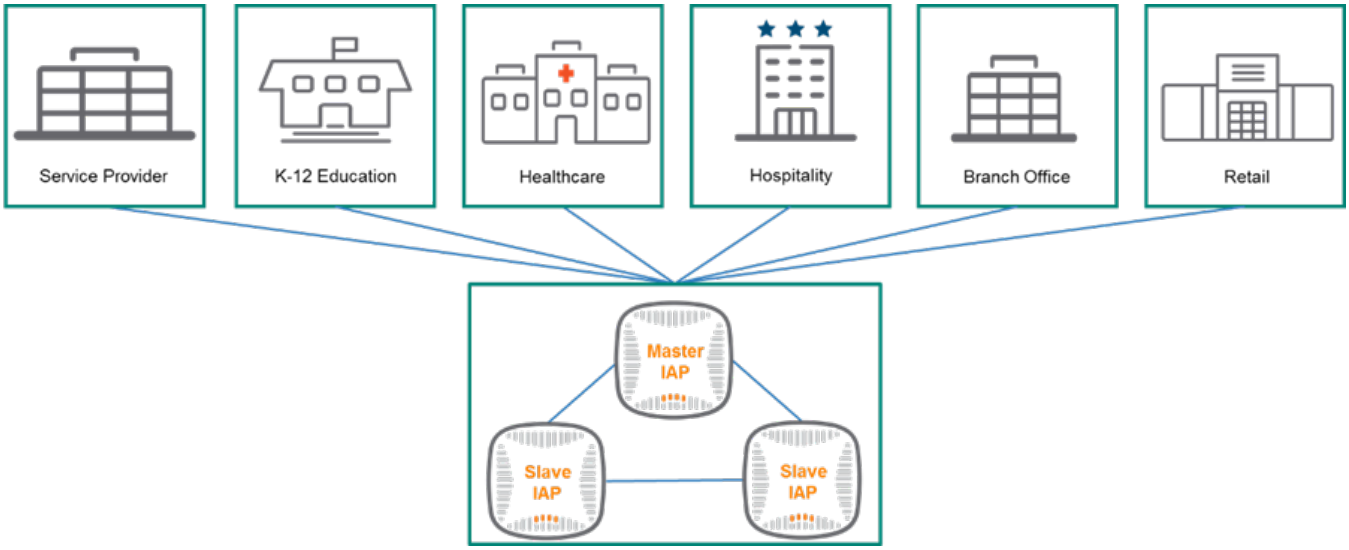


Figure 1-4 *Sample Aruba Instant Verticals*

Deployment Modes

Aruba Instant consists of a family of high-performance Instant Access Points (IAPs) which run the Aruba InstantOS and provide a completely distributed WLAN system without requiring a physical controller.

IAPs in same layer 2 domain form a group also known as a cluster. A cluster consists of a single Master IAP which is elected according a predefined election protocol and multiple constituent Slave IAPs. Clusters also have a management function Aruba refers to as the Virtual Controller or VC. The VC can be thought of as the combined intelligence for the cluster which provides functionality similar to a physical controller with the key difference that it operates a distributed basis to make decisions for the cluster. The virtual controller UI is hosted on the Master IAP for the cluster.

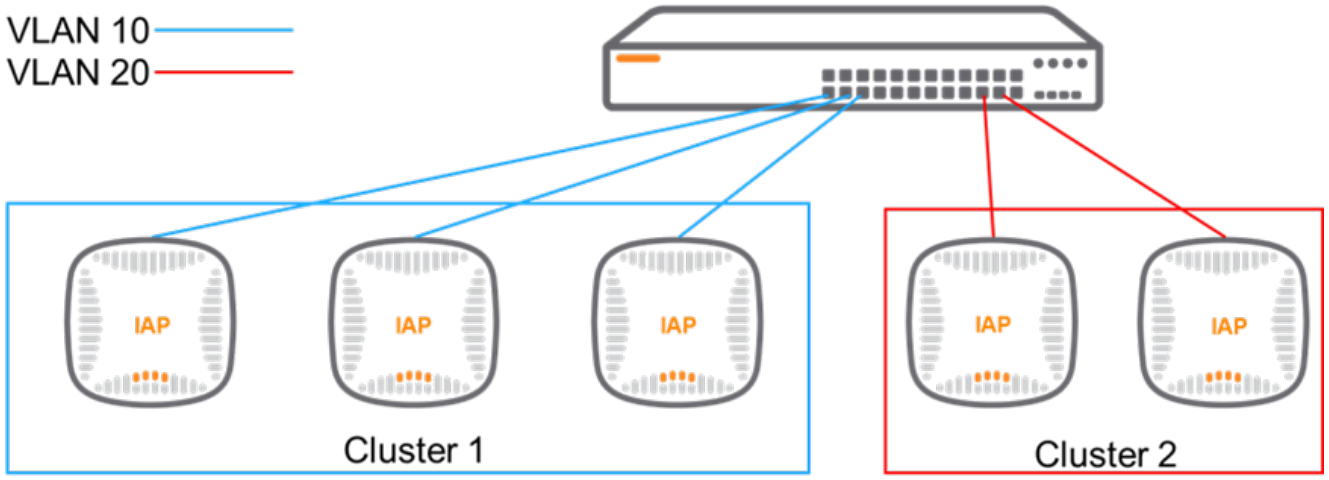


Figure 1-5 *Instant Cluster Mode*

Management functions such as image sync, cluster monitoring, and image management, are coordinated by the Master IAP for the cluster through a centralized management plane.

IAP Operations

Master Election Process

IAPs are capable of operation in one of 4 possible states:

- Initial
- Slave
- Potential Master
- Master

Every cluster holds an election based on the same Master Election Protocol to determine which IAP will serve as the Master for the cluster. Every IAP in a cluster will run through the steps depicted in the figure below as part of the Master IAP election process:

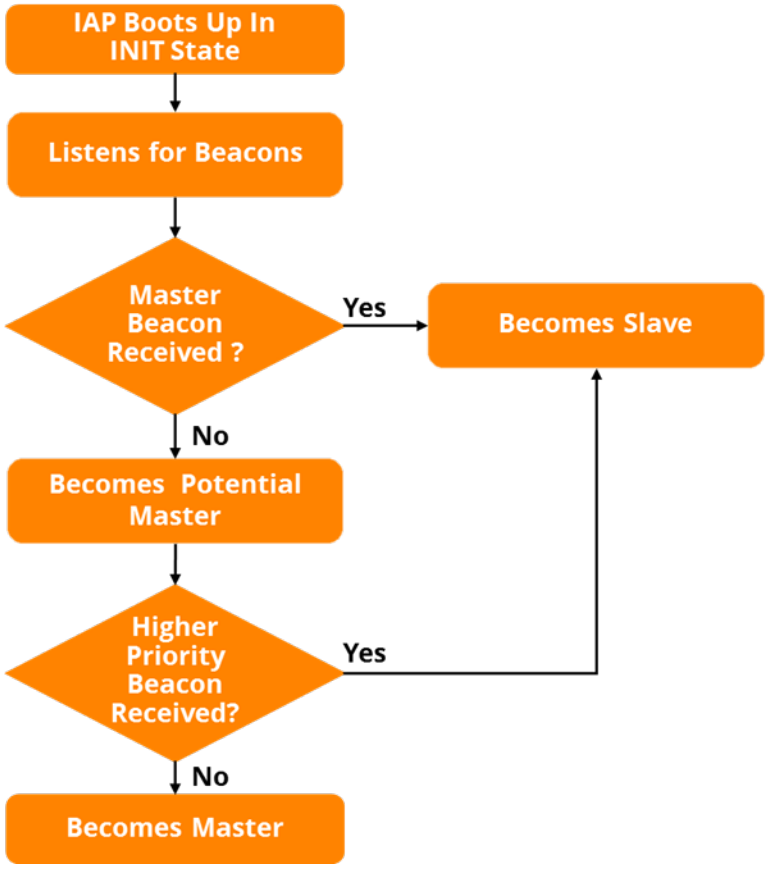


Figure 1-6 *Master IAP Election Process*

When an IAP first boots up it will begin in the Initial state and listen for beacons from an existing Master for a random period of time. If it does not receive a master beacon it will transition into the Potential Master state. In the Potential Master state, the IAP waits again and listens for a master

beacon for a random back off period of anywhere between 10 and 30 seconds. If the IAP receives a beacon from a Master with a valid IP address during the back off period it will then transition to the Slave state. If the IAP fails to receive a master beacon in the specified timeframe it will assume the role of the Master and commence broadcasting master beacons once every second. While acting as the Master the IAP may receive a beacon from new members which have been added to the cluster and are operating in the Potential Master state. If the acting Master receives a beacon with a higher priority it will abdicate its role and transition into the Slave state. If the beacon contains a lower priority the incumbent Master IAP will ignore it and remain in its role.

By default, the IAP that will win the election is randomized and any IAP within the cluster may become the Master. However, there is a possibility that multiple IAPs may enter a Master or Potential Master state even after this randomization. This scenario is common in a large layer 2 domain. In that case the Master Election Resolution Algorithm will determine the Master IAP for the cluster. The criteria for which IAP will be selected as Master are listed below in order of significance. If two IAPs tie then the next criterion in the list will be examined and so on until a discrepancy is found and the winner is determined:

1. **Preferred Master:** An IAP configured as Preferred Master will be selected as the master for the cluster
2. **IP Scope:** An IAP with a non-default IP address (non-169.x.x.x)
3. **USB Modem:** An IAP with a 3g/4g dongle
4. **Uptime:** IAP with the longer uptime receives a higher priority
5. **Media Access Control (MAC):** If two IAPs tie in categories 1-4 then the IAP with the higher MAC address prevails

An IAP with a USB modem will ignore master beacon messages in the first 5 minutes after it boots up after which it will become the cluster Master. The previous Master will reboot and join the cluster as a Slave.

An IAP with a USB modem will become the Master if it attempts to join a cluster and that cluster does not have a designated Preferred Master. If there are no designated preferred masters or IAPs with USB modems then the IAP with the longest uptime will win the election and become the Master.

Master Failover

Once the election has concluded and an IAP is selected as Master it will begin broadcasting master beacons one a second to every slave in the cluster. These beacons are used as the primary failure detection mechanism since the Slaves will become aware that the Master IAP has failed if they cease to receive master beacons. If such an event occurs the Slaves in the cluster will continue to listen for a random interval of between 10 and 40 seconds. If they fail to receive a master beacon during the random interval then each slave will transition into the Potential Master state and will

begin sending unicast beacon request messages to failed Master. If a the Slave does not receive a master beacon within 8 seconds after it begins unicasting the failed Master it will transition and assume to role of Master for the cluster.

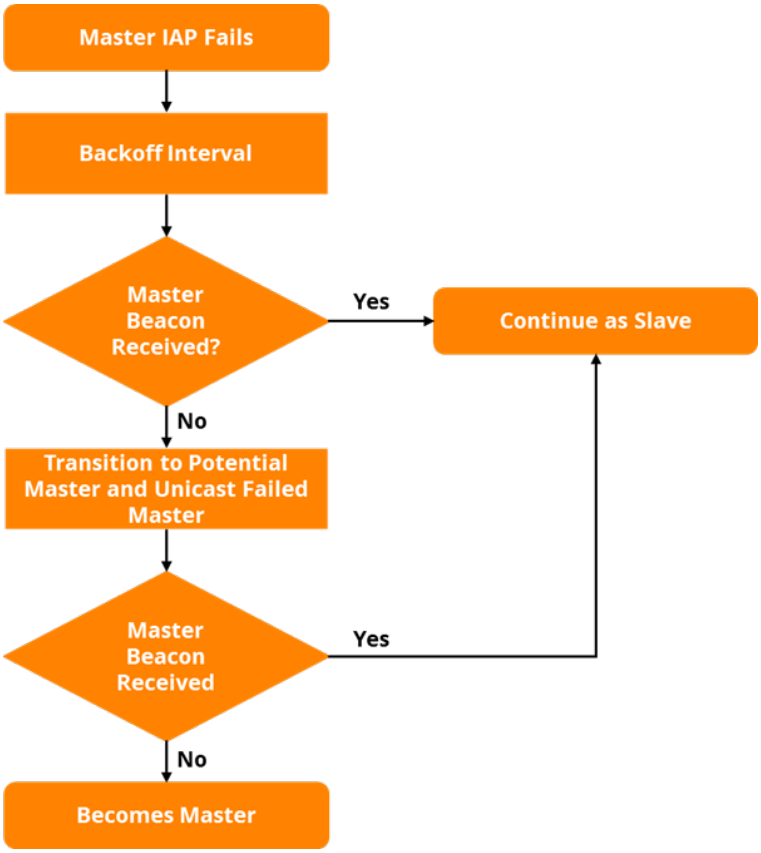


Figure 1-7 *Master IAP Failover*

When a Master IAP fails the clients that were associated to it will need to re-associate to a new IAP. The clients connected to the rest of the Slave IAPs will remain unaffected by a Master failure. A Master IAP failure event will have the following impact on its associated clients:

1. Clients which were authenticated to the failed Master IAP will need to re-associate to a new IAP
2. Clients using Magic Guest VLAN will need to wait till new Master is elected since Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT) are both coordinated by the Master IAP
3. If Dynamic Remote Authentication Dial In User Service (RADIUS) Proxy (DRP) has been enabled and new clients attempt to associate to an IAP during the re-election process they will be required to wait until a Master has been elected
4. If the Master IAP is acting as a Virtual Private Network (VPN) client and is forwarding client traffic to the datacenter that flow will be disrupted until a new Master is elected
5. After the failure it will take approximately 30-70 seconds until the VC IP becomes reachable

Preferred Master

In most cases, the master election process will automatically select the best IAP for the role of cluster Master. Once designated as Master, the IAP will then apply its image and configuration to all other Instant APs in its cluster.

However, as a best practice Aruba recommends designating an IAP as a Preferred Master. Doing so will ensure that the desired IAP will become master even if another IAP with a longer uptime attempts to join the cluster. According to the election process criteria, the preferred master status is always the first metric checked and will supersede all other factors. If an IAP is more convenient than others for troubleshooting and console access purposes then it should be designated as the Preferred Master. Another key advantage to designating a preferred master is for configuration preservation. A “golden” IAP with an ideal configuration can be designated as the preferred master ensuring that it will always push out its configuration to other cluster members and preventing the loss of a desirable configuration for the cluster.

InstantOS allows an IAP to be configured as the Preferred Master via the local cluster GUI. The figure below demonstrates the 4 step process of what would occur in the event of a Preferred Master Failure:

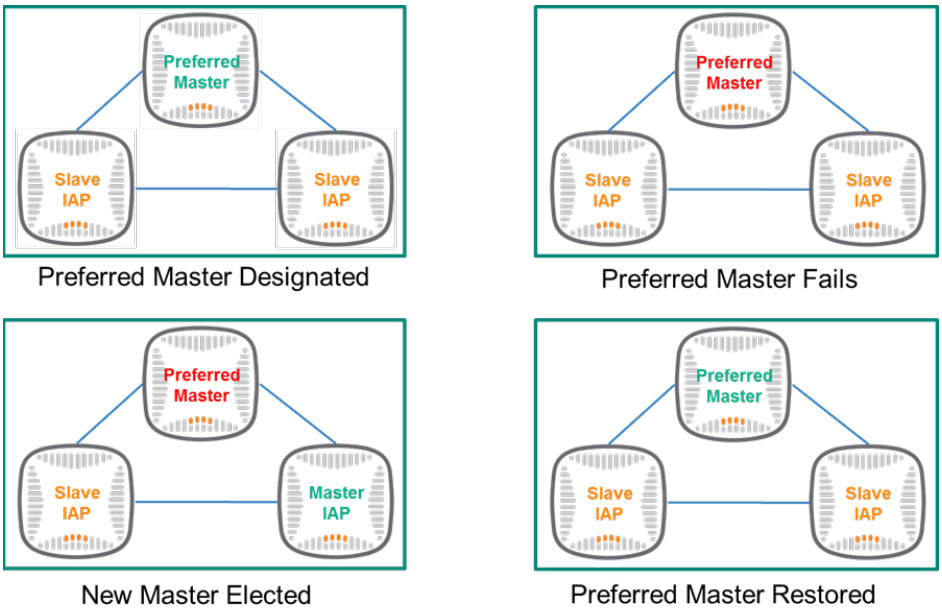


Figure 1-8 *Preferred Master Failure Process*

1. IAP is designated Preferred Master via CLI or local GUI
2. Preferred Master IAP failure triggers re-election algorithm
3. Once the election algorithm completes a new IAP from the cluster becomes Master
4. When the Preferred Master comes online it will resume its role as the cluster Master once more. The IAP that was the Master prior to the re-election will automatically reboot and join the cluster as a Slave

Multiple Preferred Masters

An IAP configured as a Preferred Master will never become a slave of another Master unless it has a factory default configuration. If a new IAP is designated as a Preferred Master and is introduced into a cluster with a pre-existing Master then the new IAP will abandon its attempt to join that cluster and form a new cluster by itself.

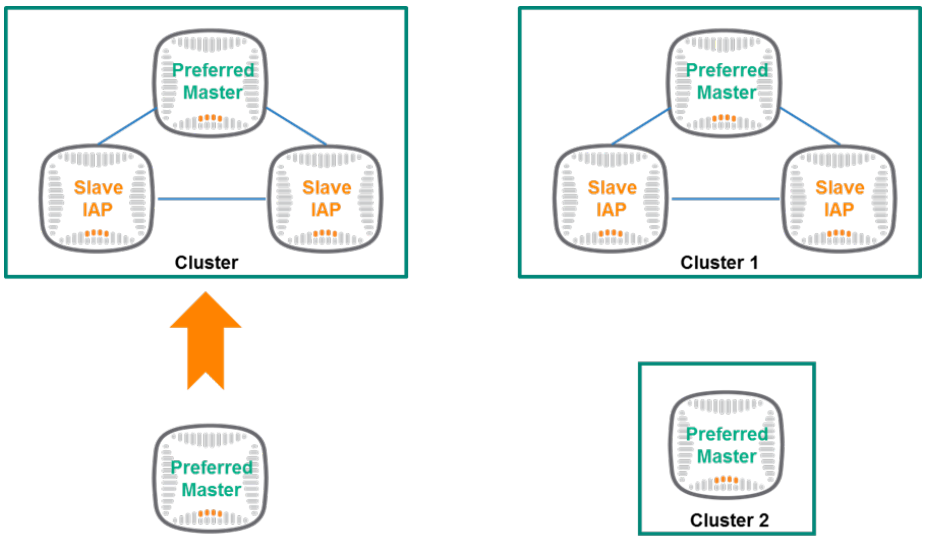


Figure 1-9 *Cluster with Multiple Preferred Masters*

CAUTION

Aruba strongly discourages customers from configuring multiple preferred masters in the same cluster.

Multi-model AP Cluster

IAPs of different models in the same layer 2 domain are capable of forming a cluster together. The determining factor to whether or not IAPs will be able to successfully form a cluster is the Instant image on the devices. In the figure below, we'll assume that the three IAPs in a cluster have an Instant image of version 6.5.4.3 and an administrator wants to add new instant IAP with code version 6.5.4.0 to the same layer 2 domain:

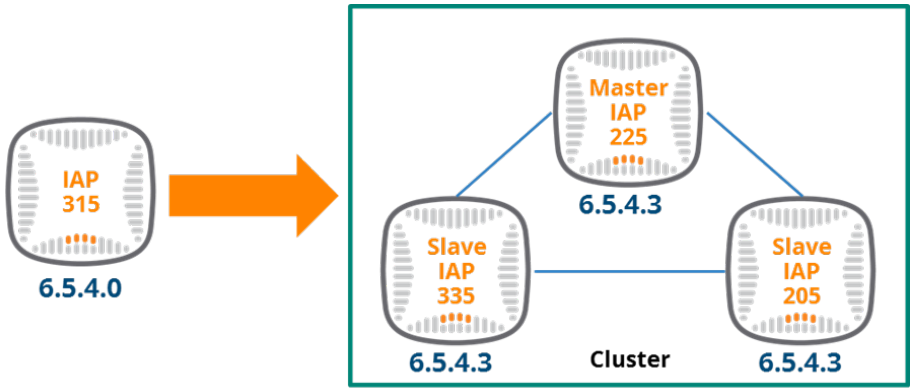


Figure 1-10 *IAP with Different Image Joining Cluster*

The new IAP will begin receiving Master beacons and will transition to a Slave state regardless of its model. Next it will try to reach device.arubanetworks.com and pull down the same image version as that of the Master IAP which in this case is 6.5.4.3. Once it has finished upgrading the new IAP joins the cluster and all IAPs in that cluster will have same Instant image of 6.5.4.3.

Each AP has a minimum required Instant software version specific to its particular model. When a new IAP is added into the cluster, it can join the cluster as long as the APs in that cluster are running the minimum required version for that IAP model. If the existing cluster is running a version which predates the minimum required version of new IAP, the IAP will not join the cluster and may reboot with the reason “image sync failed” provided. If the Cluster is managed by AirWave and the server has the image for the Master IAP in it, then new IAP will receive its new image from AirWave server.

If the new IAP cannot reach device.arubanetworks.com and fails to download the same image as the Master IAP it will not join the cluster.

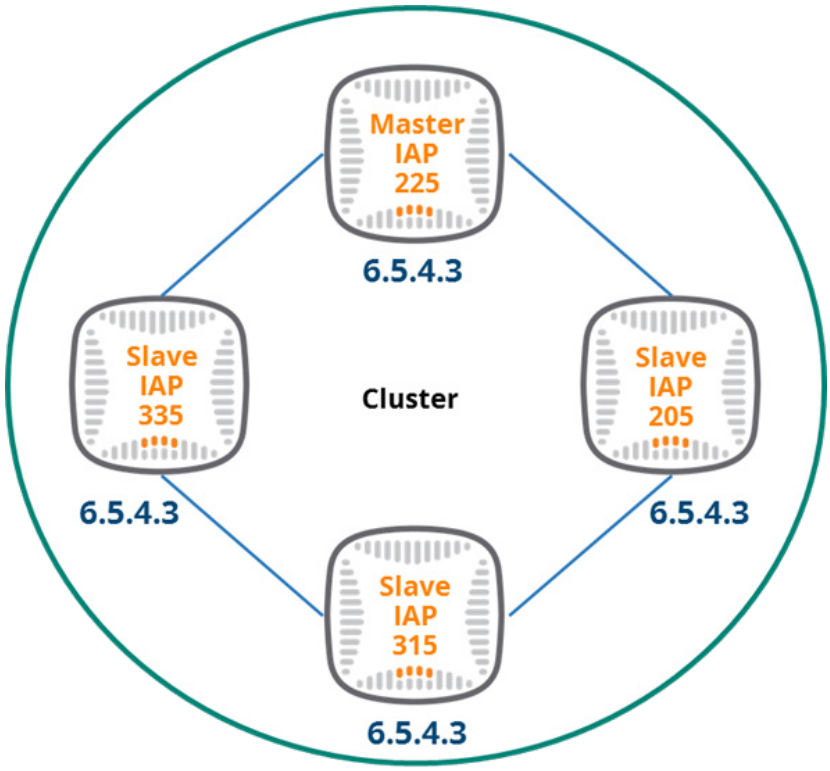


Figure 1-11 IAP has Joined the Cluster

Instant AP Platform	Minimum Required Instant Software Version
AP-203H	Instant 6.5.3.0 or later
AP-203R/AP-203RP, AP-303H, AP-365/AP-367	Instant 6.5.2.0 or later
IAP-207, IAP-304/IAP-305	Instant 6.5.1.0-4.3.1.0 or later
IAP-314/IAP-315 IAP-334/IAP-335	Instant 6.5.0.0-4.3.0.0 or later
IAP-324/IAP-325	Instant 6.4.4.3-4.2.2.0 or later
IAP-205H IAP-228 IAP-277	Instant 6.4.3.1-4.2.0.0 or later
IAP-204/IAP-205 IAP-214/IAP-215	Instant 6.4.2.0-4.1.1.0 or later
IAP-103	Instant 6.4.0.2-4.1.0.0 or later
IAP-274/IAP-275	Instant 6.3.1.1-4.0.0.0 or later
IAP-114/IAP-115 IAP-224/IAP-225	Instant 6.2.1.0-3.3.0.0 or later
RAP-155/RAP-155P	Instant 6.2.0.0-3.2.0.0 or later

Table 1-1 *Supported Instant AP Platforms*

Additional information for Aruba products can be accessed through the Related Documents section.

Cluster Architecture

Just like any other device in a network the functions of an IAP are best understood when thought of as three operational planes:

- Management Plane
- Control Plane
- Data Plane

Out of these planes only the management plane is centralized in Instant. The control and data planes are distributed. The determination of how a function is mapped to a plane and whether or not is centralized, is determined by the function's relationship to Cluster Master. If a function requires traffic to be sent to the Cluster Master for normal operation then it is considered centralized. Each plane and the functions associated with them in an Aruba Instant architecture will be discussed in the following sections.

Management Plane

The figure below illustrates the functions which are part of the centralized management plane in Aruba Instant for IAPs in Cluster Mode:

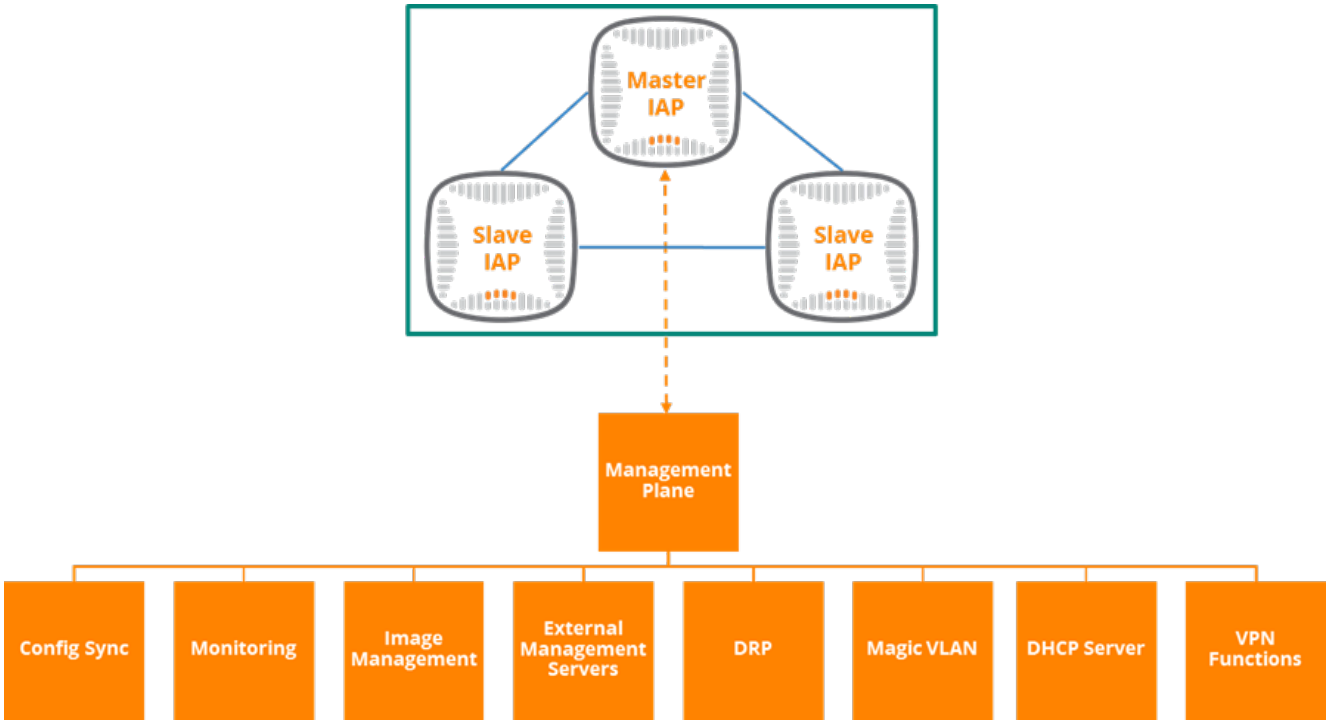


Figure 1-12 *Management Plane Functions*

- **Cluster Configuration Sync** - Once the Master IAP is configured, the slave in that cluster will download its configuration from the Master IAP. Any changes pushed from the local GUI will be synchronized to all the IAPs in that cluster
- **Cluster Monitoring** - All the IAPs in a cluster will periodically provide status updates to the Master IAP. This data is presented on the cluster's local GUI
- **Firmware Upgrade Orchestration** - Images for the entire cluster can be pushed through the local GUI. This can be done automatically by clicking on the "Check for newer option" button or manually by downloading the image and pointing it via "Browse" option or providing a URL to a server containing the image.
- **Communication with Management Platforms** - Management platforms such as AirWave and Central communicate with the Master IAP. The configuration changes made through these platforms are sent to the Master IAP.
- **Dynamic RADIUS Proxy (DRP)** - The IAP acts as an authenticator when 802.1x security has been configured for client authentication. This means that each IAP must be individually added as a NAS client into the RADIUS server. However, in an environment where adding of each IAP as a NAS client is not feasible DRP can be used. When DRP is enabled, all IAPs in a cluster send RADIUS messages to the Master IAP which acts as a RADIUS proxy.

- **DHCP server for client VLANs** - Another common VLAN deployment is configuring a DHCP server on the Master IAP of the Aruba Instant cluster. The types of VLANs which can be configured in such a scenario include:
  - Local mode
  - Centralized Layer 2 mode
  - Distributed Layer 2 mode
  - Centralized Layer 3 mode
  - Distributed Layer 3 mode

  If an Aruba Instant SSID is mapped to a VLAN in a cluster with a Master configured to perform DHCP then the client traffic on that SSID is tagged accordingly and will flow through the Master. The VLAN ID that is used in the DHCP configuration for these VLANs must be supported on the uplink switch that connects to the IAPs.
- **Magic VLAN** - An SSID with VC-assigned IP address option is referred to as the Magic VLAN. The Magic VLAN was created to simplify guest traffic on the network without any requiring modification to the underlying wired infrastructure. Magic VLAN clients receive the IP address directly from the DHCP scope created on the Master IAP. Traffic coming from clients is forwarded to the Master IAP via AP VLAN which then source NATs it to the VC IP address. Broadcast and multicast packets are not allowed in the Magic VLAN.
- **VPN** - An IAP network does not require a physical controller to provide configured WLAN services. When VPN is configured, the Master IAP for the cluster creates a VPN tunnel to a mobility controller in the corporate office. The controller acts as a VPN endpoint and does not supply the Instant AP with any configuration information. Third-party VPN concentrators are also supported by Aruba Instant.

CAUTION

Aruba strongly recommends the network-assigned IP addressing option for client IP assignment for security purposes. Do not use the VC-assigned IP option in an environment in which a VLAN-based segregation is required between the guest VLAN and the AP VLAN.

NOTE

Aruba recommends using a dedicated uplink VLAN on IAP trunk links for guest access. Magic VLANs should only be utilized if there is no alternative option.

Control Plane

The figure below illustrates the functions which are part of the distributed control plane in Aruba Instant:

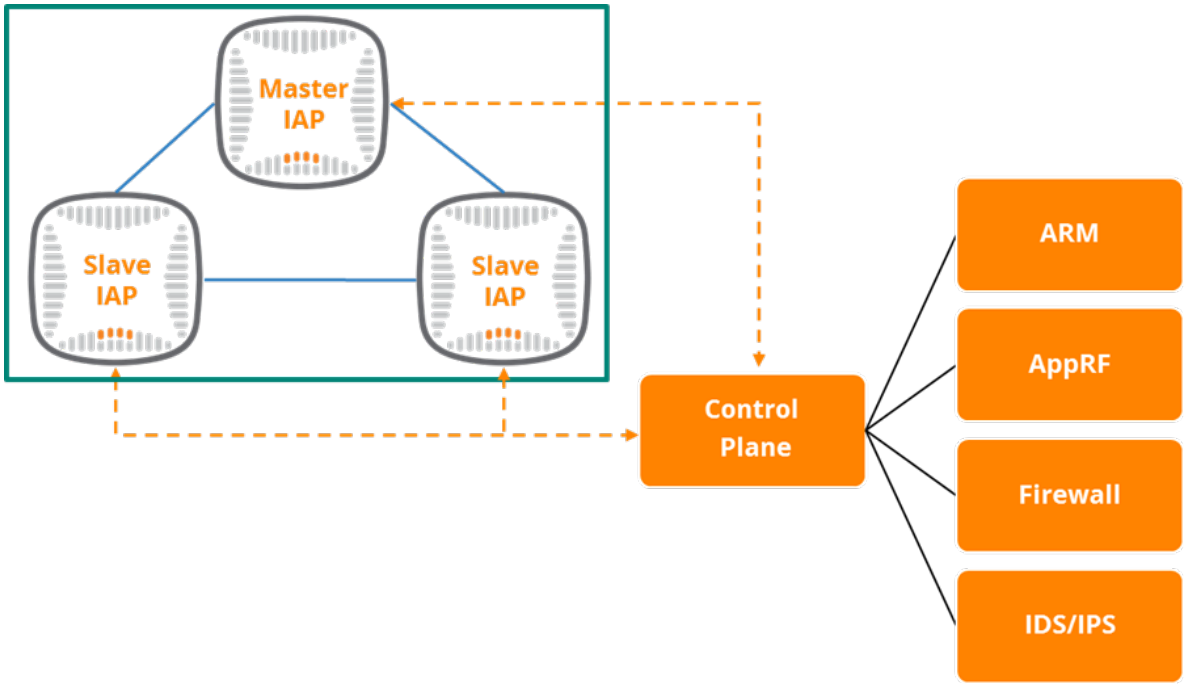


Figure 1-13 *Instant Control Plane Functions*

Adaptive Radio Management

As networks have evolved and mobile devices have become the de facto standard access method, RF interference has become pervasive. Unfortunately, any radio in a device capable of RF communication is susceptible to interference and IAPs are no exception. Wireless devices, walls, cubes, office doors, microwave ovens, and even human bodies can all have an adverse impact on the performance an RF environment. Due to constantly evolving needs of clients on the network the utilization of static channel and power plans is not practical and can often lead to poor network performance. APs must have the ability to dynamically adjust power and transmit settings order to properly function in an RF environment with any degree of density. Aruba developed our innovative Adaptive Radio Management (ARM) technology specifically to address the challenges posed to network performance in high-density RF environments. ARM has several constituent components which all collaborate to deliver this functionality:

- **Auto Channel** – Monitors the RF spectrum for both 802.11-based and non-Wi-Fi sources of interference. Depending on the conditions in the environment ARM will utilize these data points to dynamically adjust the AP channel if necessary in the event that the previous channel the AP was using becomes unacceptably congested
- **Auto Power** – Also commonly known as coverage hole detection, if an AP goes down, ARM automatically fills in the RF hole and increases power on surrounding APs to compensate until the original AP is restored. Once the failed AP comes back online ARM resets the network to a new optimal setting.

NOTE

IAP transmit power can be configured between 9 and 127 dBm. Aruba's best practice recommendations for signal strength are provided in the table below.

Open Office*	Walled Office/Classroom*
5Ghz: Min 12/Max 15	**5 GHz:** Min 15/Max 18
2.4Ghz: Min 6/Max 9	**2.4 GHz:** Min 6 /Max 9

*Signal strengths listed in dBm

Table 1-2 *Best Practice Transmit Power Settings*

- **Client-aware Scanning** – When ARM is enabled, APs will not change the channel that clients currently connected clients are using. This results in a much more stable environment for clients. The only exception to this behavior are triggers from high priority events such as radar or excessive noise. It is recommended to enable client-aware scanning for most deployments
- **Band steering** – ARM will automatically steer clients that support both 2.4 GHz and 5GHZ bands to the 5GHz band as it is less congested. This in turn frees up valuable space in the 2.4GHz band for clients that are not 5GHz-capable. Band steering works in coordination with Aruba's airtime fairness feature which ensures that legacy clients will never be bandwidth-starved
- **Client Match** - ARM continuously monitors the RF environment and dynamically load balances clients at the time of association. Evenly distributing clients in this manner allows sticky clients to roam to IAPs with high signal strength, prevents APs from becoming overburdened, and dramatically improves the user experience. ClientMatch will not trigger AP changes for clients that are actively transmitting data

ARM Best Practices

The following table outlines Aruba's best practice recommendations for ARM settings based on extensive internal testing. While these recommendations will be appropriate for the majority of customers, all factors should be considered pertaining to each individual deployment when determining settings for ARM:

Feature	Default Setting	Sparse AP with Data Only	Dense AP with Data Only	Recommended Settings for Voice and Video	High Interference Environment
Scanning	Enabled	Enabled	Enabled	Enabled	Enabled
Client Aware Scanning	Enabled	Enabled	Enabled	Enabled	Disabled
Background Spectrum Monitoring	Disabled	Disabled	Disabled	Disabled	Enabled
Client Match	Disabled	Enabled	Enabled	Enabled	Enabled
Band Steering	Prefer 5Ghz	Prefer 5Ghz	Prefer 5Ghz	Prefer 5Ghz	Prefer 5Ghz
Airtime Fairness	Default Access	Fair Access	Fair Access	Fair Access	Fair Access
Min Transmit Power	18	18	9	18	12
Broadcast Filtering	Disabled	All	ARP	ARP (Disabled if running Multicast)	ARP
Multicast Optimization	Disabled	Enabled	Enabled	Enabled	Enabled
Dynamic Multicast Optimization	Disabled	Disabled	Disabled	Enabled	Disabled
Interference Immunity Level	2	2	2	2	2*
Beacon Interval	100ms	100ms	100ms	100ms	100ms
Wide Channel Band	5GHz	5GHz	5GHz	5GHz	5GHz
Local Prob Req Threshold (db)	0	0	25	25	25
Dynamic CPU Management	Automatic	Automatic	Automatic	Automatic	Automatic

* Modify if directed by Aruba Support

Table 1-3 *ARM Best Practices*

AppRF

AppRF is Aruba's custom-built layer 7 firewall. It consists of integrated Deep Packet Inspection (DPI) functionality as well as a cloud-based Web Policy Enforcement (WPE) service. Each IAP has its own DPI engine which performs packet analysis and classification. They are also connected to Aruba's web-based URL database aruba.brightcloud.com for web category caching and verifying the reputation of URLs accessed by clients on the network. In conjunction with WPE, DPI provides the ability to analyze and identify applications, application categories, web categories, web reputation, and web URLs based on client data packets. Traffic shaping policies such as bandwidth control and per-application QoS can be defined for unique client roles. E.g. bandwidth-hungry applications may be blocked on a guest role within an enterprise. AppRF also enables compliance with privacy standards such as Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), and Children's Internet Protection Act (CIPA).

IDS/IPS

The Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) features detect unauthorized network devices and take appropriate action to prevent any security breaches on the network. IAPs provide a user-friendly wizard which assists administrators in configuring the setting that are most appropriate for their deployments.

The IDS and IPS functions are divided into following components:

- **Infrastructure** - For the network to function as intended, attacks on the infrastructure must be detected and mitigated accordingly. Aruba considers the infrastructure to consist of authorized IAPs, the wired network where IAPs are attached, and the RF medium itself. Any AP that is detected in the RF environment but is not connected to the wired network is considered to be interfering. Any unauthorized AP that is connected to the wired network is considered a Rogue AP
- **Client** - Clients that attach to a network should also be monitored. Any client that successfully authenticates, associates, and uses encryption is considered a valid station. Aruba Instant looks for specific attacks such as Hotspotter and TKIP replay which target clients attaching to the wireless network. The system also watches valid stations that are attempting to connect to rogue or neighboring APs.

All VLANs where a rogue AP could connect must be trunked to IAPs in order to enable rogue classification. Aruba recommends adjusting the detection and protection settings to "Low". Setting the detection to "Medium" or "High" might result in false positives or too many alerts.

Data Plane

The data plane of the IAP is completely distributed and is responsible for handling client as well as AP traffic. In a cluster there are two basic types of VLANs:

AP VLAN

The VLAN which all APs in a cluster have in common is referred to as the AP VLAN. AP-generated traffic such as RADIUS transactions, management traffic, SNMP, Syslog, and communication between IAPs are all forwarded through the AP VLAN. In most deployments it is the native VLAN of the trunk port the AP uses to connect. AP-generated traffic is left untagged and it is recommended to maintain that default setting. However, AP traffic can be tagged by changing the uplink management VLAN value in the WebUI if needed.

NOTE

Aruba recommends enabling DHCP on the AP VLAN for large deployments. Static IP addresses can also be assigned in smaller deployments if desired.

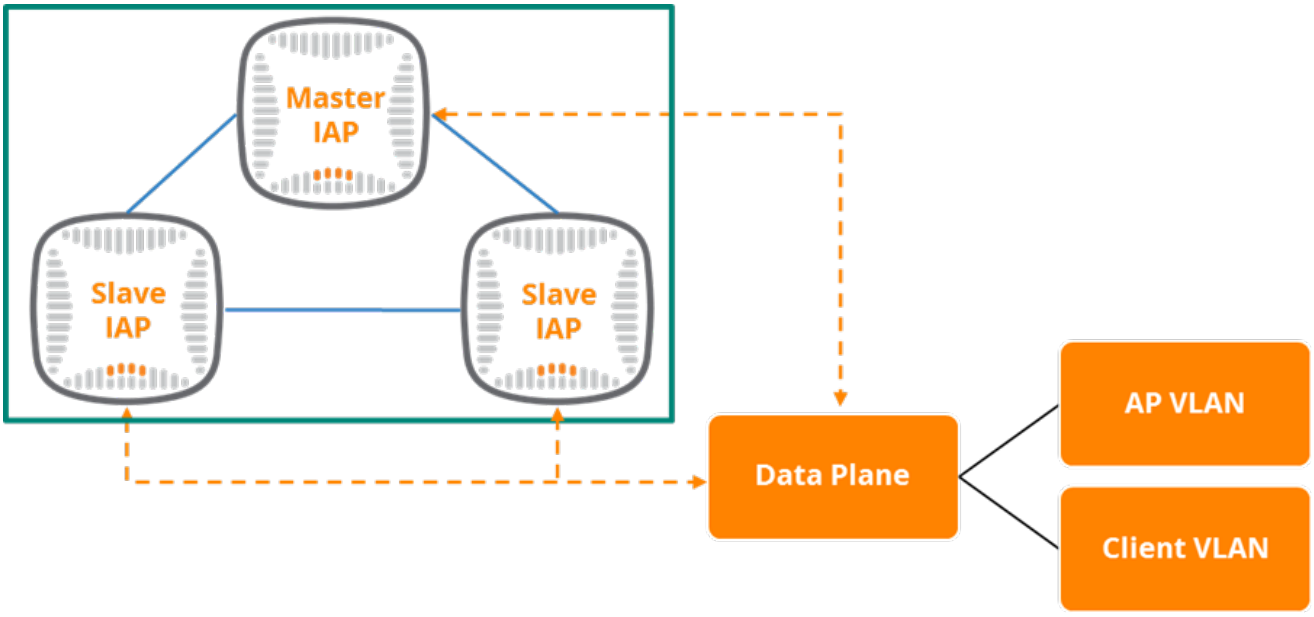


Figure 1-14 *Instant Data Plane Functions*

Client VLAN

The VLAN used to serve clients in an Instant cluster is referred to as the Client VLAN. The clients are assigned an IP address either by the DHCP server on the network or from the DHCP server on the IAP cluster.

NOTE

Aruba recommends configuring different VLANs for APs and Clients

VLANs managed by the uplink network are commonly deployed with Aruba Instant. For example, if VLAN 20 is managed by the uplink network and is mapped to the “Employee” SSID, the client traffic is examined by the firewall of the IAP where the client is connected and directly bridged to VLAN 20 without flowing through the Master IAP of the cluster.

Deploying Instant

Cluster Security

Datagram Transport Layer Security

Control plane messages between IAPs are exchanged using the Process Application Programming Interface (PAPI) protocol which operates on UDP port 8211. While PAPI functions well for its intended purpose of carrying control plane traffic these messages have the potential to be decoded by an expert hacker. Alternatively, Datagram Transport Layer Security (DTLS) operating on UDP port 4434 can be used to provide security for control plane messages between IAPs in a cluster. Advantages of using DTLS for cluster security are as follows:

- Mutual authentication between IAPs in a cluster using device certificates
- Peer MAC address validation against IAP whitelist
- Control plane messages are securely transmitted

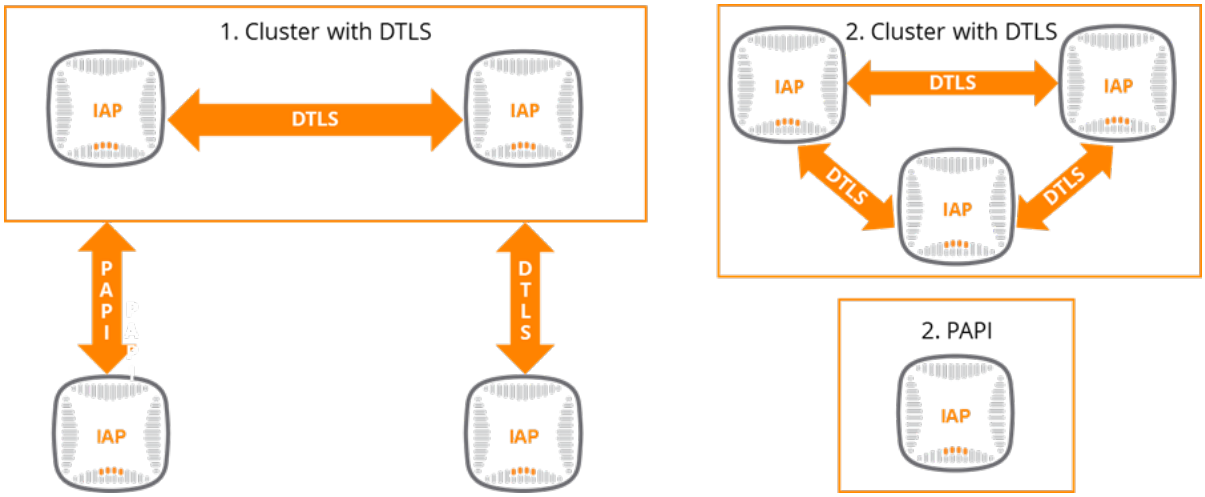


Figure 1-15 *IAPs Joining a DTLS Cluster*

A Slave IAP with a non-default configuration that has enabled DTLS will not be able to join a cluster where DTLS is disabled. An IAP in this scenario is considered to be in “Locked Mode”. In order for a DTLS-enabled IAP to join a non-DTLS cluster it must either be reset to its factory settings or DTLS must be disabled. Conversely, a non-DTLS enabled IAP cannot join a cluster that is currently using DTLS unless DTLS is disabled for the entire cluster.

Most Aruba devices contain a TPM chip which performs cryptographic operations and stores security keys. However, some devices do not have this chip and the keys are stored in flash which reduces the level of protection for these devices. Starting with Instant 6.5.3, device certificates are issued by a new PKI to non-TPM devices. The private key is encrypted using the Advanced Encryption Standard (AES), compressed, and stored in the certificate files in flash. These devices are called “low assurance devices”. Clusters which have DTLS enabled can be configured to either permit or deny low assurance devices from joining the cluster.

Auto-Join

When a new IAP is added to a layer 2 network with an existing IAP network, the new IAP will join the cluster via the Auto-Join feature. Auto-Join is enabled by default for purposes of IAP deployment simplification. Once the initial cluster deployment is complete, Aruba recommends disabling auto-join to prevent unauthorized IAPs from joining the cluster. Additional IAPs can be added manually by using MAC the address of the new IAP or by temporarily enabling auto-join.

Aruba recommends configuring clusters with DTLS enabled and the auto-join feature disabled.

Unified Access Points

Historically, all Aruba APs were manufactured as either Campus APs (CAPs) or Instant APs (IAPs). Campus APs were based on an AOS image and controller-managed whereas an IAP was a controllerless AP with an Instant image. Another key difference between the two was how they were assigned a country code. Campus APs did not have a country code assigned in their Stock Keeping Unit (SKU) as they obtained it from their controller. All IAPs had a country code in their SKU for regulatory purposes as they would not be managed by a controller and therefore could not receive a country code in the same manner as a CAP. Instant clusters must be homogenous with only one country code permitted at a time. If an AP started life as an IAP it could be converted to a CAP at any time, however APs which were manufactured as CAPs required a controller for operation and could not be converted to IAPs.

Effective as of unified release 6.5.2.0, Aruba has unified all new access point platforms so that a single AP can act as either a CAP or an IAP with a single SKU. These devices are collectively referred to as Unified APs (UAPs). Since administrators may freely convert a UAP back and forth between operation as a CAP or as an IAP, all UAPs are assigned a country code in their SKU to eliminate the possibility of being deployed as an IAP under an incorrect regulatory domain.

NOTE

Aruba recommends avoiding placing IAPs and controller-managed APs in the same VLAN.

The boot process which determines the operating mode for a UAP is outlined in the image and steps listed below:

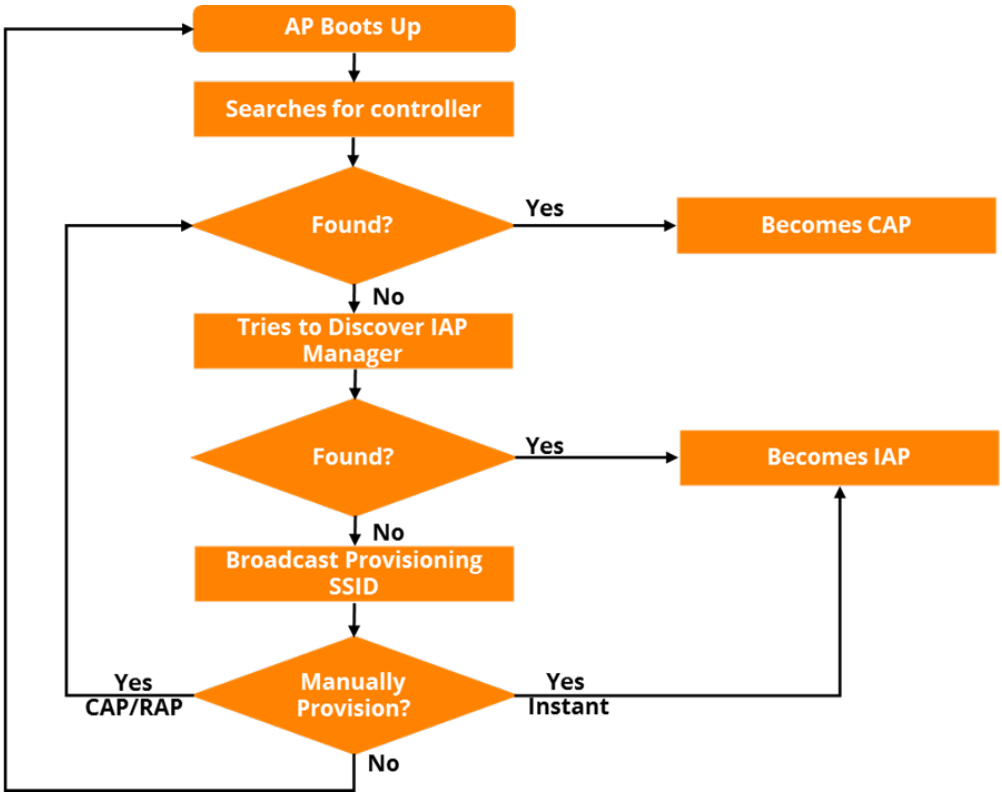


Figure 1-16 *IAP Boot Process*

NOTE

Aruba recommends avoiding placing IAPs and controller-managed APs in the same VLAN.

1. The UAP boots up.
2. UAP enters the controller discovery state and attempts to find a controller using static, DHCP, ADP, DNS-based controller discovery techniques.
3. If a controller is discovered, the UAP receives its IP address or domain assignment, connects to the controller, and downloads the image. The AP then reboots and will operate as a Campus AP.
4. If the AP cannot find a controller then it initiates the Instant discovery process and attempts to locate an existing cluster Master, Activate, AirWave, or Central.
5. If a VC is discovered, the UAP joins the existing cluster and downloads the Instant image from the Master. After the image is downloaded the AP reboots and will run as an IAP. If

the UAP fails to locate a VC it attempts to locate Activate, AirWave or Central, upgrade its image, and form a new IAP cluster.

6. If the UAP cannot locate Activate, AirWave, or Central then it will broadcast “SetMeUp” SSID so that it can be provisioned*.
7. The “SetMeUp” SSID can be used to manually convert the AP to an IAP if it has a manufacturing image, otherwise it will operate as an IAP by default. At this stage the UAP could also be manually provisioned as a CAP or RAP under the management of a controller.
8. If the AP is not upgraded to an ArubaOS or Instant image, it enters a 15 minute reboot period. If there is no keyboard input or configuration (manual upgrade) within 15 minutes then the AP reboots and repeats the process.

*The FIPS variant of a UAP will not broadcast the “SetMeUp” SSID.

Country Codes

Aruba IAPs and UAPs are available in the following variants:

1. United States (US)
2. Japan (JP)
3. Israel (IL)
4. Egypt
5. Rest of the World (RoW)

Improper country code assignments can disrupt wireless transmissions. Most countries impose penalties and sanctions on operators of wireless networks with devices set to improper country codes.

Management Options

Aruba Instant is a highly versatile platform with numerous management options that have been designed to suit the needs of a variety of use cases. While it is possible to manage all IAPs in a single cluster at a remote location using the local GUI, organizations with a large number of remote sites will typically find that approach to be challenging. Any configuration change would require an administrator to log on to the local GUI for each individual cluster. Aruba provides two management options to specifically address the challenges associated with managing, monitoring, and troubleshooting multiple clusters deployed in remote locations: AirWave and Central.

AirWave

Aruba AirWave is a powerful platform capable of managing Aruba's wireless and wired devices alike along with a wide range of third party devices. It can deployed as either a physical or a virtual appliance and provides real-time monitoring, reporting, troubleshooting, configuration, and firmware management. AirWave also offers a suite of tools which assist organization with demonstrating regulatory compliance, strengthening wireless security, and managing RF coverage.

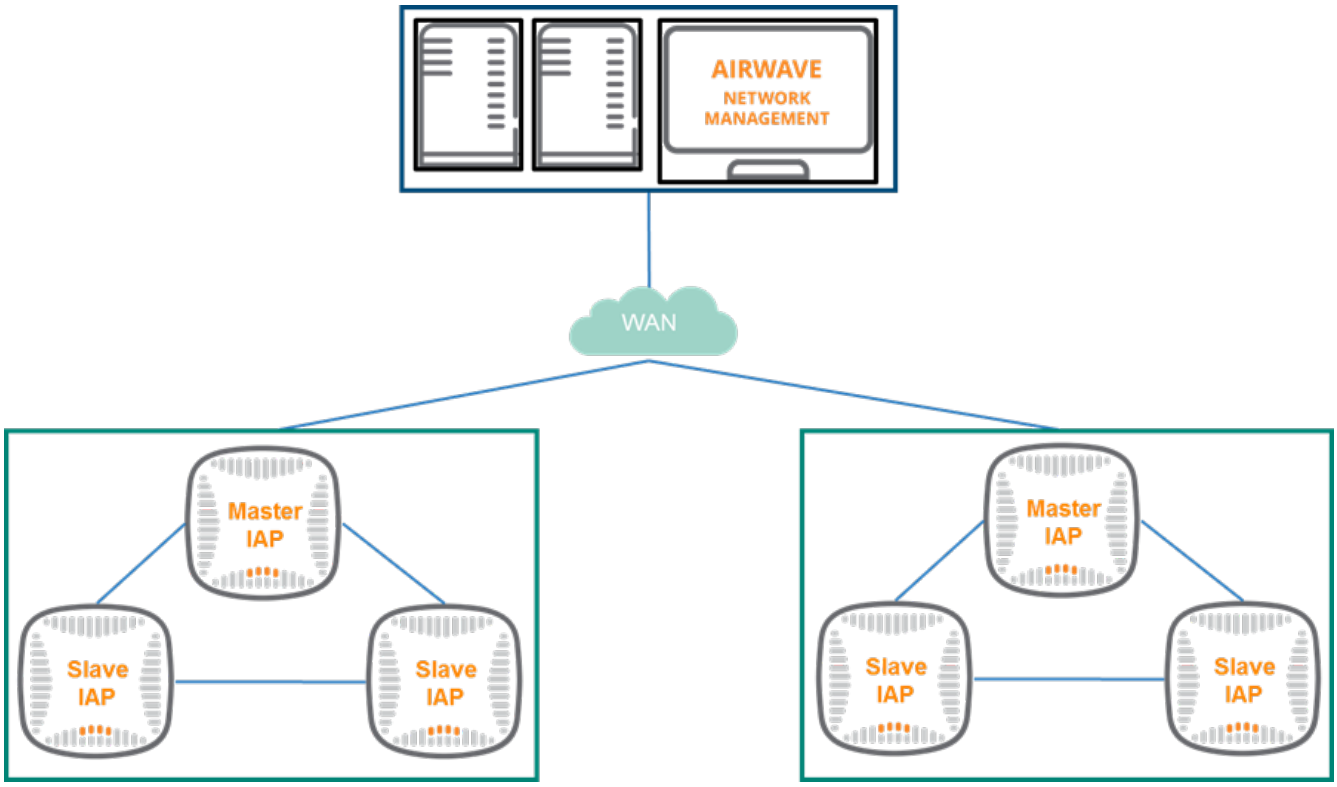


Figure 1-17 *Instant Clusters Managed by AirWave*

Central

Aruba Central is a public cloud based management platform that provides monitoring, configuration, firmware management and troubleshooting for IAPs and switches. Central uses a secure HTTPs or Websocket connection and provides a strong mutual authentication mechanism using certificates for all communication with Instant APs.

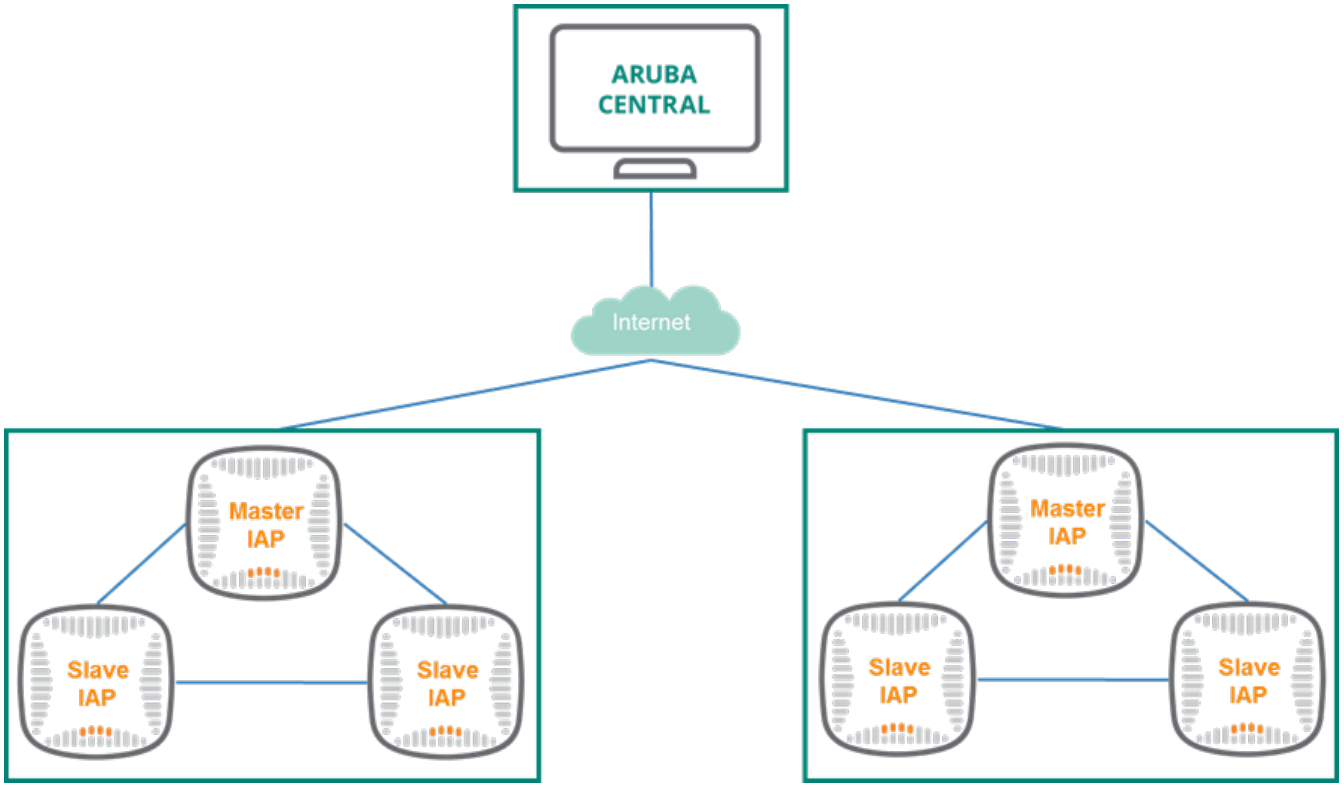


Figure 1-18 *Instant Clusters Managed by Central*

Provisioning

AirWave

IAPs can be provisioned for AirWave either manually or using any of the following Zero Touch Provisioning (ZTP) methods:

- Activate
- DHCP Options
- DNS

Activate

Aruba activate is a cloud-based inventory management and provisioning service which automatically deploys IAPs without the need for manual intervention. The service is offered to Aruba customers free of charge. Aruba refers to the provisioning process provided by Activate as Zero Touch Provisioning (ZTP).

When a customer purchases a device from Aruba, it is automatically added to the Activate server and an account is created on the customer's behalf. Activate allows customers to define specific rules which automatically point IAPs to the AirWave server. Once an IAP is connected to AirWave its configuration and firmware are updated automatically.

DHCP Options

IAPs can be provisioned with AirWave using DHCP options 43 and 60. The DHCP client on the IAPs sends out a DHCP request with option 60 and a string value of “ArubaInstantAP” to the DHCP server. When the DHCP server receives the request it checks to see if option 43 has been configured. If option 43 configuration is verified then a corresponding IP address for AirWave is returned.

DNS Based

IAPs can discover an AirWave server through the domain name option in situations where it is not possible to use DHCP options or perform ZTP with Activate. For example, if the domain “abc” is included in the DHCP configuration, the IAPs will search for the DNS server records for “aruba-AirWave.abc”. If no domain is specified then the IAP will search records for “aruba-AirWave”.

Manual Provisioning

IAPs may be manually added to Airwave by providing shared key and IP address of the Airwave server in the VC WebUI.

Aruba recommends using ZTP for IAP deployment whenever possible.

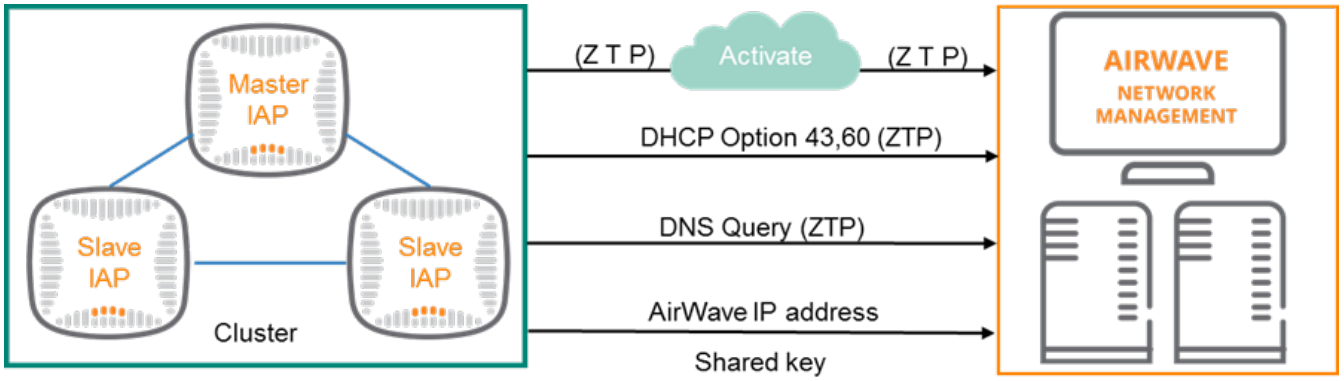


Figure 1-19 *AirWave Provisioning Options*

Central

IAPs can be provisioned for Central using any of the following methods:

- Subscription Key
- Cloud Activation key
- Activate Account
- MAC and Serial Number

Subscription Key/ZTP

Aruba Central has its own version of the ZTP process for provisioning. When IAPs are purchased they are automatically associated with a user account and the purchaser receives a subscription key. When the user inputs the subscription key Central import all devices that the customer purchased without the need for any additional steps.

Cloud Activation Key

Multiple IAPs can be provisioned at the same time by adding the cloud activation key and serial number of the master IAP to Aruba Central. The slave IAPs are automatically added as well.

Activate Account

IAPs are associated to an Activate user account upon purchase. Users can enter their Activate credentials in Central to import IAPs as well.

MAC and Serial Number

IAPs can be manually added by putting the MAC address and serial number combination into Aruba central. Up to 32 devices may be added to Central using the MAC and serial number method.

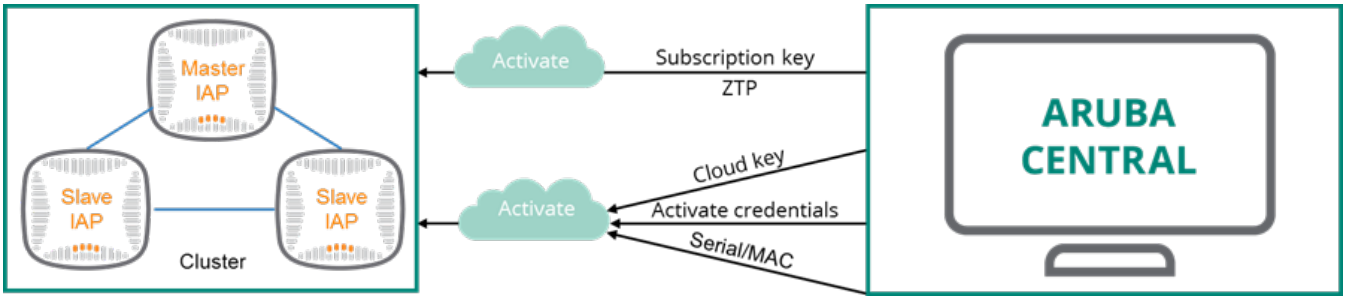


Figure 1-20 *Central Provisioning Options*

IAP Conversion

Instant APs can be converted to either Campus APs (CAPs) or Remote APs (RAPs) if there is a need to centralize the traffic, simplify vlans, or for remote locations that require site-to-site VPN to leverage datacenter services. IAPs are typically converted to CAPs when there is a need to simplify VLAN management and centralize traffic. This is generally done over private links such as LANs and Multiprotocol Label Switching (MPLS). The VC in the cluster initiates the process by sending the conversion command to all cluster members. All IAPs will then download the firmware and configuration from the controller where they will be terminated. This conversion can be coordinated via Local GUI, Activate, AirWave, or Central.

IAPs are converted to RAPs for the same reasons with the addition of the need to leverage datacenter services remotely. The conversion process is identical to that of converting an IAP to a CAP with the exception that RAPs will form IPSec VPN tunnels to the desired controller over the internet.

Only an AP that was originally an IAP is capable of reverting back to operating as an IAP after it has been converted to a CAP/RAP. APs that were originally manufactured as CAP/RAPs cannot be converted to IAPs unless they are UAPs. All UAPs are compatible with controllers and can be freely converted back and forth between any type of AP.

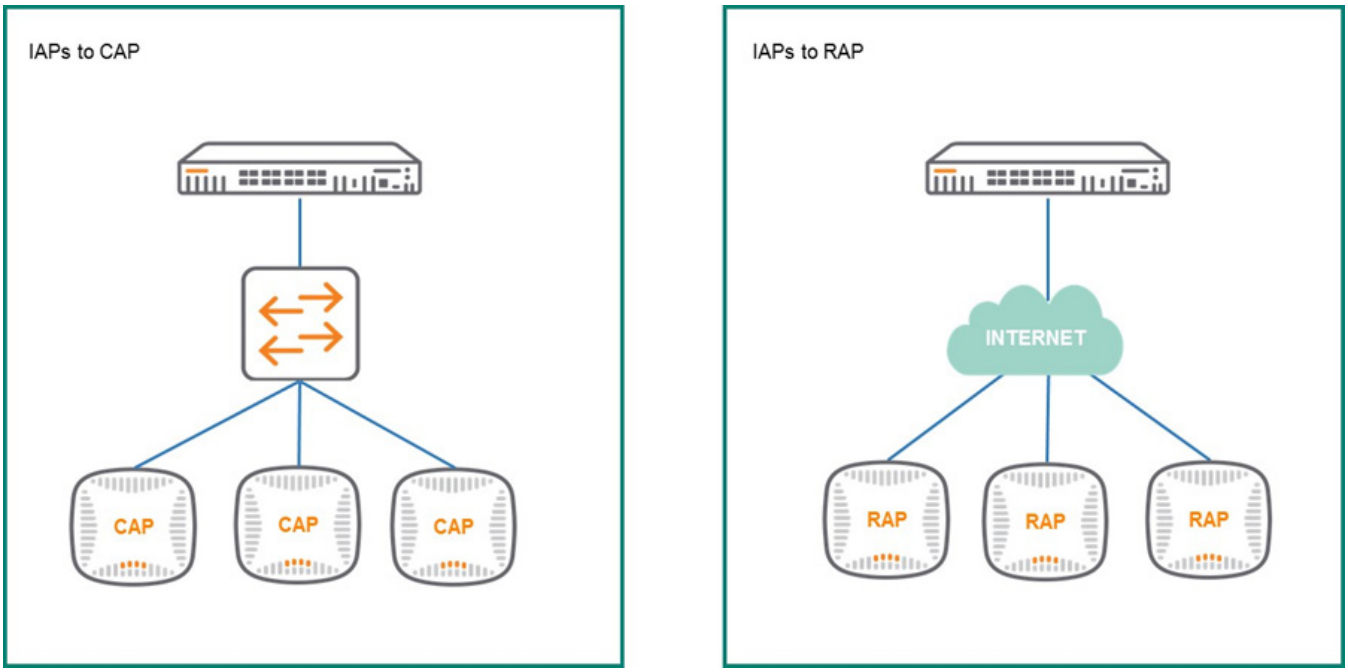


Figure 1-21 *IAP Conversion*

Security

Authentication

The following types of authentication are available with Aruba Instant:

- **Open System Authentication** – Open system means that there is no authentication. Any station can join the network freely without requiring a key. It can be combined with MAC authentication to provide low level security in certain situations
- **Wired Equivalent Privacy (WEP)** - The most common version of WEP is static WEP, where all stations share a single key for authentication and encryption. Other versions of WEP have different key lengths and dynamic key assignments. Aruba considers WEP to be vulnerable and strongly advises against using it in a production environment.

- **Pre-Shared Key (PSK)** - PSK is part of the WPA/WPA2 personal certifications. PSK authentication is the most common form of authentication for consumer grade Wi-Fi routers. Like WEP, the same key is used by all devices for authentication and encryption. PSK's primary benefit is that it is simple and easy to configure for a small number of devices. However, the key must usually be changed on devices manually which can quickly become cumbersome as the user count increases. In addition, if an attacker discovers the key they will gain access to the network and will be able to decrypt user traffic at will. Security best practices mandate that the key should be changed whenever someone with access to the key leaves the organization. The key should also be complex and rotated on a regular basis
- **Wireless Internet Service Provider roaming (WISPr)** - Allows WISPr-enabled clients to connect to the guest network
- **Captive Portal** - After a user accesses the network, they are presented with a landing page on their web browser which requires the user to register, supply login credentials, or acknowledge an acceptable use policy (AUP) before they are allowed to browse the web. After whatever registration steps that have been configured are completed the user is usually placed in a limited-access role that allows basic web browsing but denies access to any of the internal resources of the enterprise. Captive portal authentication can be used in conjunction with MAC authentication if deemed appropriate and is typically used for Guest SSIDs
- **Enterprise Authentication** - Includes 802.1X and Extensible Authentication Protocol (EAP), which is part of the Wi-Fi Protected Access (WPA) and WPA2 Enterprise certifications. Many different types of authentication can be used in the EAP framework, with Protected EAP (PEAP) or EAP Transport Layer Security (EAP-TLS) being the most popular choices. EAP-TLS uses server and client-side certificates while a TLS tunnel is created to send user credentials. When the authentication process is complete, the client and the IAP each have copies of the keys that are used to safeguard the integrity of the user session

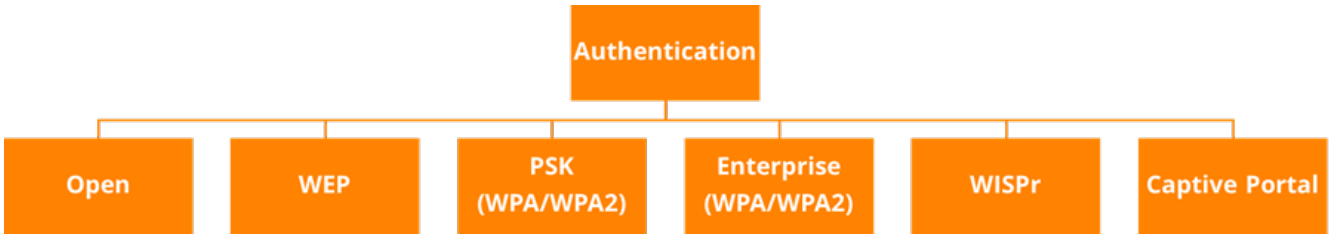


Figure 1-22 *Aruba Instant Authentication Options*

The following table outlines Aruba's best practice recommendations for authentication with Aruba Instant:

Authentication Type	Employee	Guest
Open	Not Recommended	Recommended with a higher-level authentication method
WEP	Not Recommended	Not Recommended
PSK	Recommended for devices that do not support stronger authentication	Can be used but the PSK key should be rotated in a regular basis
802.1X	Recommended	N/A
WISPr	N/A	Recommended in public places such as airports
Captive Portal	N/A	Recommended

Table 1-4 *Authentication Best Practices for Instant*

Encryption

The following types of encryption are available with Aruba Instant:

- **Open** – Open networks have no encryption and offer no protection from wireless packet captures. Most hot spot or guest networks are open networks and the end user is expected to use their own protection methods such as VPN or Secure Sockets Layer (SSL) to secure their transmissions.
- **Temporal Key Integrity Protocol (TKIP)** - TKIP is a part of the WPA certification and was created as a stopgap measure to secure wireless networks that previously used WEP encryption whose 802.11 adapters were not capable of supporting AES encryption. TKIP uses the same encryption algorithm as WEP, but TKIP is significantly more secure and has an additional message integrity check (MIC).
- **Advanced Encryption Standard (AES)** – AES is a part of the WPA2 certification and is now widely supported as the recommended encryption type for all wireless networks containing sensitive data. AES leverages 802.1X or PSK to generate unique keys for all devices. AES provides a high level of security, similar to what is used by IP Security (IPSec) clients.
- **WEP** - Though WEP is an authentication method, it is also used as an encryption algorithm where all users typically share the same key. However, WEP is easily broken with automated tools, and should be considered no more secure than an open network

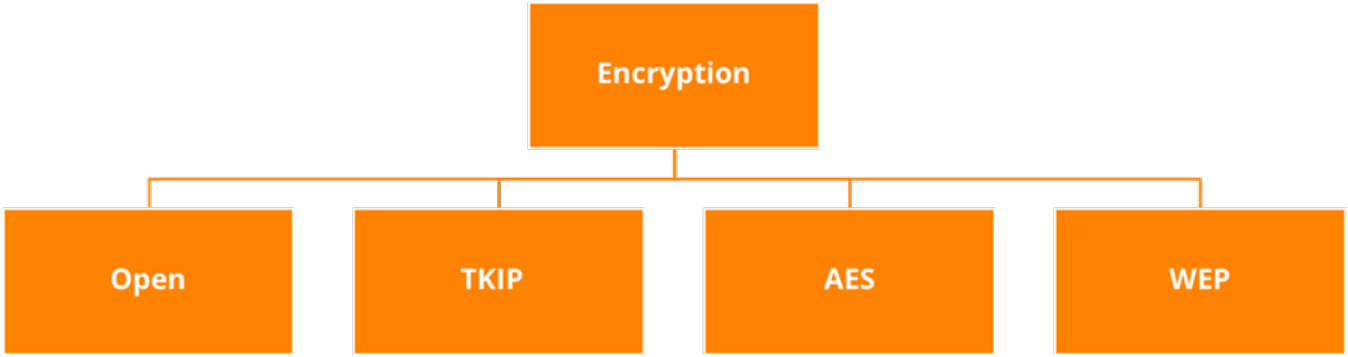


Figure 1-23 *Aruba Instant Encryption Options*

The following table outlines Aruba's best practice recommendations for encryption with Aruba Instant:

Encryption Type	Employee	Guest
Open	Not Recommended	Recommended
WEP	Not Recommended	Not Recommended
TKIP	Not Recommended	Not Recommended
AES	Recommended	Recommended when using PSK

Table 1-5 *Encryption Best Practices for Instant*

Access Rules

Role-Based

All IAPs support a role-based firewall that allows users to obtain network access based on their user role. These roles can be assigned based on various attributes e.g. Vendor Specific Attributes, MAC address, AP Name, etc. The users connected to the Service Set Identifier (SSID) are all on the same subnet however they have different rights customized for their needs. When a user joins an SSID they will be placed into a default role until an administrator assigned them a new one. A RADIUS server such as ClearPass Policy Manger (CPPM) can also dynamically assign roles for users.

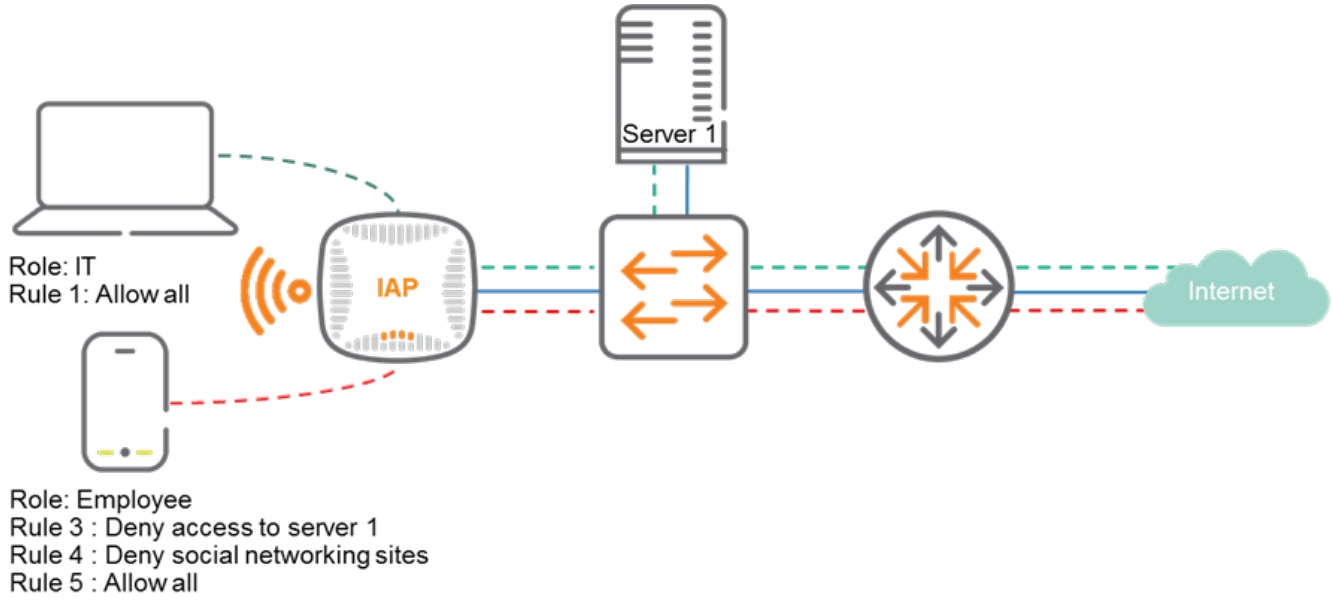


Figure 1-24 *Role-based Access*

Network-Based

Network-based access means that users connected to the same SSID will have common rules specified for a network. These rules can be based on an access control list, captive portal, VLAN assignment etc.

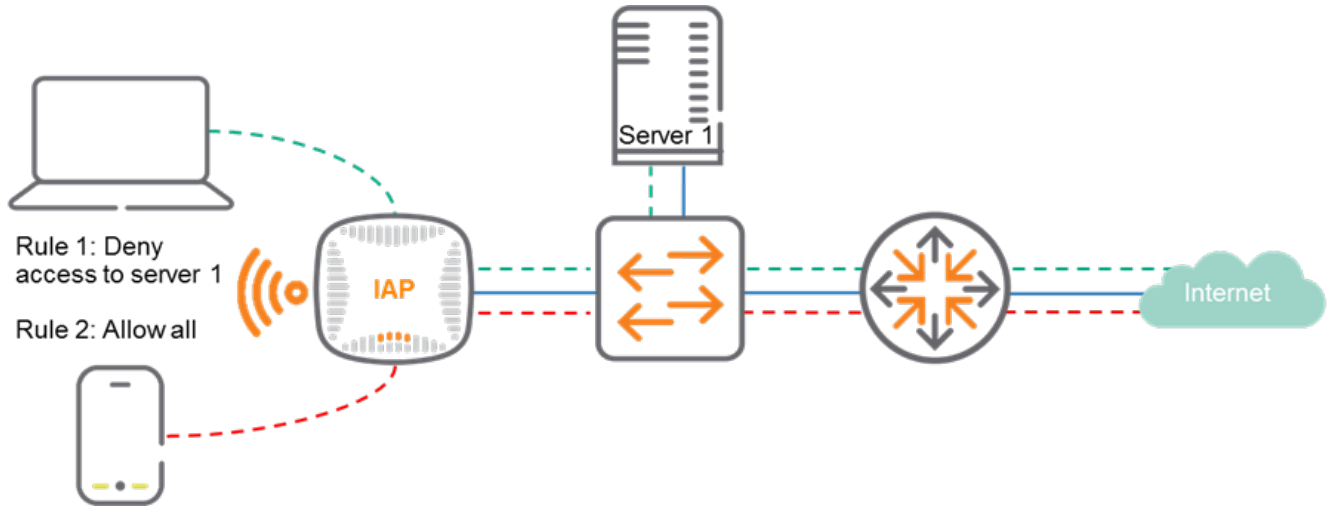


Figure 1-25 *Network-based Access*

Unrestricted

Unrestricted access allows users connected to the SSID to gain network access without any restriction on destinations or type of traffic.

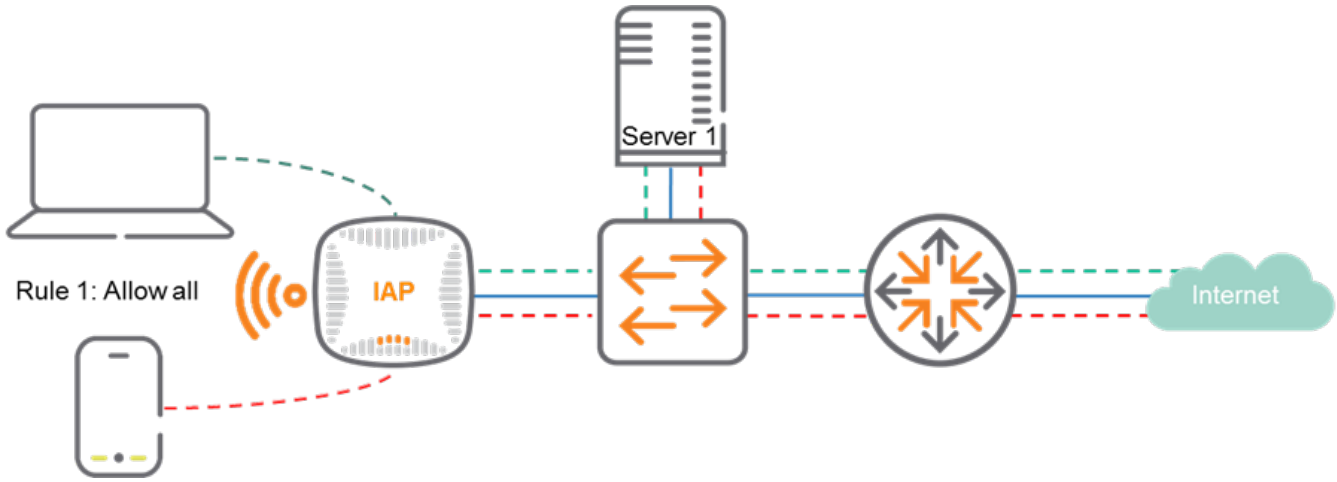


Figure 1-26 *Unrestricted Access*

NOTE

Aruba recommends using a RADIUS server to manage access rules rather than locally assigning them on the IAP. A RADIUS server will need to send the Aruba-User-Role attribute back to an IAP to change client's role.

Deployment Models

Cluster Mode

For the Instant Cluster Mode deployment model we'll use the example of a K-12 school district which requires enterprise-grade Wi-Fi infrastructure, security, and centralized management. Since each school is considered an individual site and the number of IAPs at each school is less than 128, cluster mode will be the best choice for a deployment model. Each school will contain an individual cluster with IAPs deployed based on site survey data. Once the desired IAPs are have been deployed, the auto-join feature is disabled and DTLS is enabled for cluster communications per Aruba's best practice recommendations.

The K-12 school in this scenario is managed by an IT team which prefers cloud-based management servers, therefore Aruba Central is the ideal choice for cluster management. Each school cluster will have its own VC with Aruba Central coordinating all monitoring, configuration, and reporting. Depending on the school's requirements, ClearPass could be used to provide 802.1x authentication for students, teachers, and district employees as well as provide a captive portal for guests trying to gain internet access.

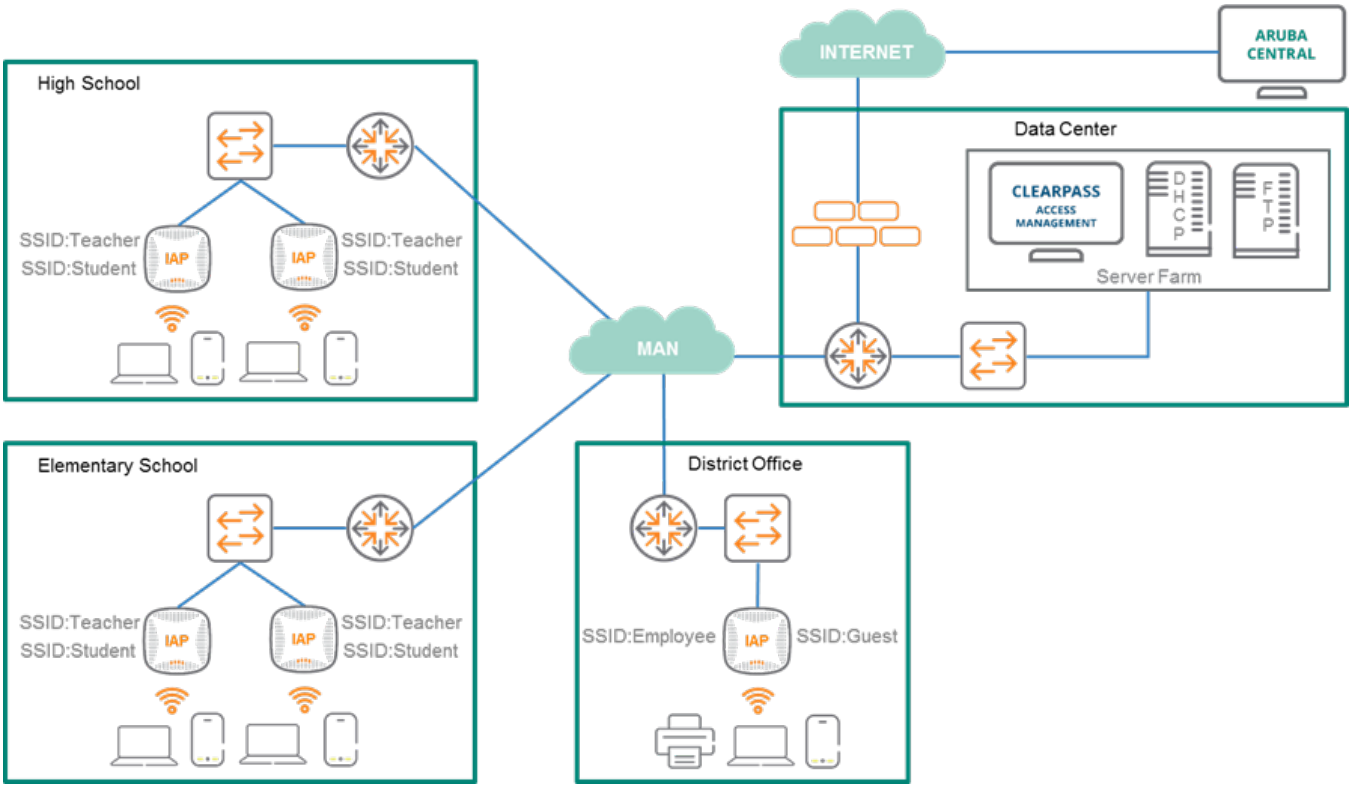


Figure 1-27 *Cluster Deployment Model*

Branch Connectivity

Distributed Network Design

A branch office is a location other than a main office where business is conducted however the term has different connotations depending on the type of organization deploying the branch. In the context of a retail chain the term *branch* represents stores that serve customers, whereas for a traditional enterprise organization a branch would be defined as an offsite location where employees and contractors congregate for their daily work. Regardless of the type of organization a branch serves the main objective of any branch office network is to provide the following functions:

- Secure employee access
- Guest Access
- Support applications such as voice and video
- Devices like printers, mobile, kiosks, security cameras
- Comply with regulations such as PCI, HIPPA, and CALEA
- Secure sensitive data
- Provide a highly-available network

Branch offices generally have a need for secure communication with the centralized corporate network. This connectivity is typically provided through of WAN connectivity options such as leased lines, MPLS, or forming a VPN over the public Internet. Connecting branch offices through leased lines can be extremely cost prohibitive compared to options such as MPLS or VPN over Internet. The decision of whether to use VPN or MPLS for branch connectivity is dependent on numerous factors which need to be weighed including cost, security policies, and service availability.

Aruba Instant is a powerful platform which is fully capable of providing wireless connectivity for a branch office network. The number of IAPs required in a network depends on factors such as number of users, the size of the branches, and the type of services required at each branch. The physical design options that are available with Aruba Instant for branch office networks as follows:

- Single IAP branch
- Multi-IAP branch

Single IAP Branch

Single-IAP deployments consist of branches that are supported by a single AP. These branch locations typically have no more than 30 wireless users and a handful of wired devices.

Examples of single-IAP branch deployments include locations such as:

- Home offices,
- Home-based call centers,
- Small retail stores (i.e. a coffee shop or restaurant chain)
- Mobile clinics
- Offsite offices of law firms
- Realty groups

In addition to wireless access, some single-IAP deployments require support for wired devices. IAP models with extra wired ports are ideal for these deployments because they simplify the network design and eliminate the need for additional switching equipment.

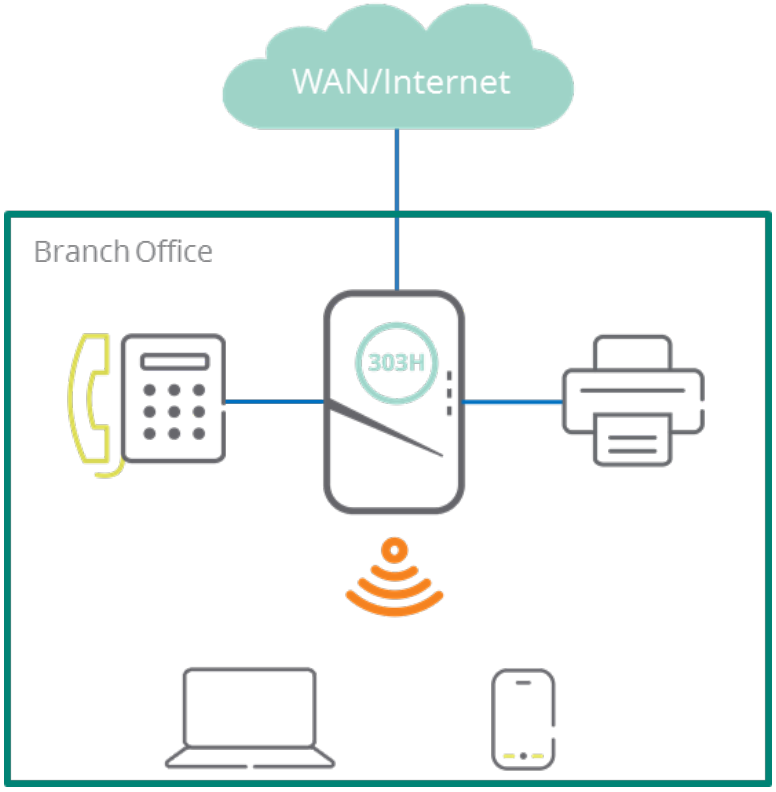


Figure 2-1 *Typical Single IAP Branch Deployment*

The uplink Ethernet port of the IAP is directly connected to the WAN uplink which eliminates the need for additional networking infrastructure at the branch. An IAP with a USB modem is also capable of acting as an uplink.

Multi-IAP Branch

The Multi-IAP Branch design consists of two options:

- Hierarchical Mode
- Flat Mode

Hierarchical Mode

In Hierarchical Mode one port of the multiport IAP acts as an uplink since it is connected to the WAN network. The remaining IAP ports are referred to as downlink ports and can be used to connect other multiport IAPs or wired devices. The IAP that is connected to the WAN through the uplink port is referred to as the *root IAP*. The root IAP provides DHCP services and well as a Layer 3 connection to the ISP WAN uplink through NAT. The root IAP will always win the Master election for the Aruba Instant cluster.

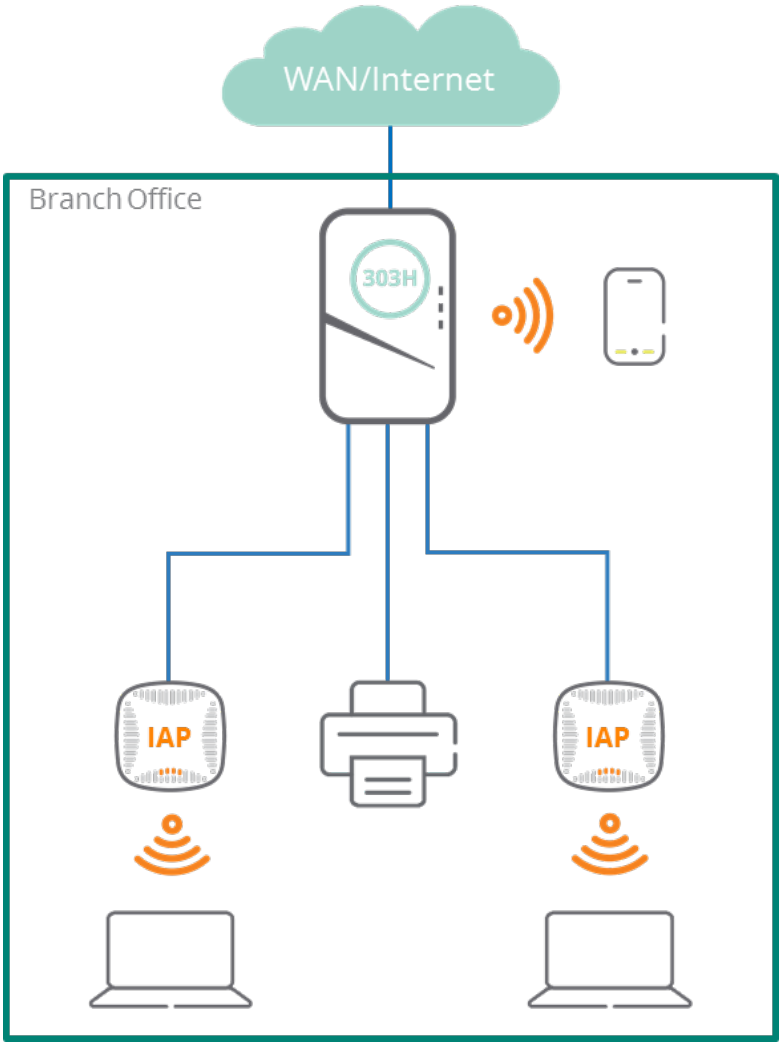


Figure 2-2 *Typical Multi-IAP Branch Hierarchical Mode Deployment*

Only the root IAP in the network uses its downlink port(s) to connect to the other IAPs. Other IAPs connected to the root IAP can only use their ports to connect unmanaged switches or end devices. Daisy chaining is not allowed.

NOTE

Aruba advises against using Hierarchical Mode if more than 5 IAPs are required in a network.

Flat Mode

The Flat Mode design is a default deployment model for a multi-IAP network and is recommended for all branch networks that require more than five IAPs. In Flat Mode, all of the IAPs deployed at the branch are connected to an uplink switch. If the Aruba Instant cluster is required to support multiple VLANs then the uplink switch must be a managed switch. In addition, the IAPs must be trunked to that uplink switch so that they may carry the appropriate VLAN tags.

E.g., if the AP VLAN, the employee VLAN, and the guest VLANs are VLANS 10, 20, and 30 respectively, then the IAPs should be trunked into the uplink switch with the native VLAN 10 and tagged VLANs of 20 and 30. The figure below represents what a typical Multi-IAP Flat Mode branch architecture would look like:

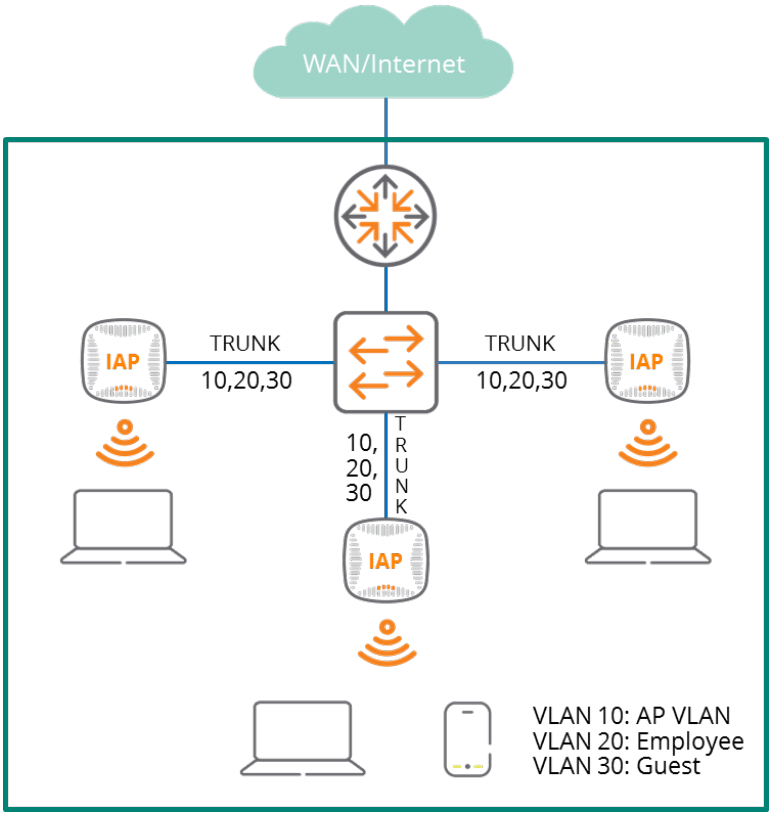


Figure 2-3 *Typical Multi-IAP Branch Flat Mode Deployment*

In general, the Hierarchical Mode design is more applicable to VPN-based branch deployments than it is to MPLS-based deployments. MPLS-based deployments typically employ either a single-IAP design or a Multi-IAP design in Flat Mode.

Aruba recommends deploying IAPs in a Flat Mode design if a managed switch is available.

VPN Branch Deployment

Connecting branches using MPLS certainly has advantages however is not always the best option for some branch office deployments due to cost and service availability concerns. Cost savings are a key driver in the adoption of distributed enterprise strategy and organizations seek a more cost-effective alternative to MPLS. Internet broadband service with high service availability and affordability provide an attractive alternative to an MPLS-based WANs.

In recent years both consumer grade and business grade broadband services have become faster, more reliable, and more affordable. This in turn has led many organizations to switch to a broadband service for branch and home office connectivity. In the case of organizations that support home-based employees broadband is the only choice as connecting home offices with an MPLS-based WAN is not a viable solution.

If an organization is using MPLS for branch connectivity the service provider ensures data security over the WAN on their behalf. However, when using the public internet for branch connectivity the responsibility for ensuring data security is the responsibility of the corporate IT team. The most common VPN technologies that provide secure remote access are SSL VPN and IPsec VPN. SSL VPN is well suited to provide remote access to a specific application, however it is not suitable for connecting enterprise networks. For that reason IPsec VPN is the most common choice for securely extending corporate networks and resources to remote sites. IPsec VPN protects sensitive data by interconnecting the remote sites with secure encryption tunnels over the Internet.

Historically, the implementation of IPsec VPNs were site-to-site. Implementing IPsec VPN requires IPsec-capable hardware at each remote site and involves complex configurations. Most branch sites have limited or no IT staff onsite, so interconnecting branches using IPsec VPN can be challenging.

Aruba Instant is designed to alleviate the complexity associated with deploying site-to-site IPSec VPNs. Aruba Instant's native VPN capabilities and zero-touch provisioning greatly reduce the challenges that normally come along with deploying IPSec VPN. Instant's zero-touch provisioning capabilities reduce deployment costs and eliminate the complexity that is normally associated with traditional IPsec VPN deployments.

Since IAPs have a virtual controller architecture the Instant network there is no need for a physical controller to provide the configured WLAN services at remote sites. However, a physical controller is required for terminating VPN tunnels from the Instant AP networks at branch locations to data centers where the Aruba controller acts as a VPN concentrator (VPNC).

When a VPN is configured, the IAP acting as the VC creates a VPN tunnel to an Aruba Mobility Controller in a corporate office. The controller exclusively functions as a VPN endpoint and does not supply the IAP with any configuration. Aruba recommends deploying IPSec VPNs with Instant for the following scenarios:

1. Enterprises with many branches that do not have a dedicated VPN connection to the corporate office.
2. Branch offices that require multiple Instant APs.
3. Individuals working from home and, connecting to the VPN.

The survivability feature of Instant APs with the VPN connectivity of Remote APs allows you to provide corporate connectivity on non-corporate networks

The WLAN controller is not responsible for anything other than acting as a VPNC for IAP networks in remote branches.

Architecture

The IAP TUNNEL architecture includes the following two components:

1. Instant APs at branch sites
2. Controller at the Data center

The Master IAP at the branch site serves as the VPN endpoint and the controller located in the datacenter serves as the VPN concentrator. When an IAP is set up for VPN it forms an IPsec tunnel to the controller in the datacenter to secure sensitive corporate data.

IPsec authentication and authorization between the controller and the IAP is based on the Remote AP whitelist configured on the controller. Only the Master IAP of the cluster forms the VPN tunnel to the VPNC. From the controller's perspective, the Master IAPs that form the VPN tunnels are considered VPN clients.

The controller's purpose in this scenario is to terminate VPN tunnels as well as route or switch VPN traffic. The IP cluster creates an IPsec or GRE VPN tunnel from the VC to a Mobility Controller in a branch office. The controller only acts as an IPsec or GRE VPN endpoint. It does not provide any configuration or management of any kind for the IAP. The figure below provides a visual depiction of the IAP TUNNEL architecture:

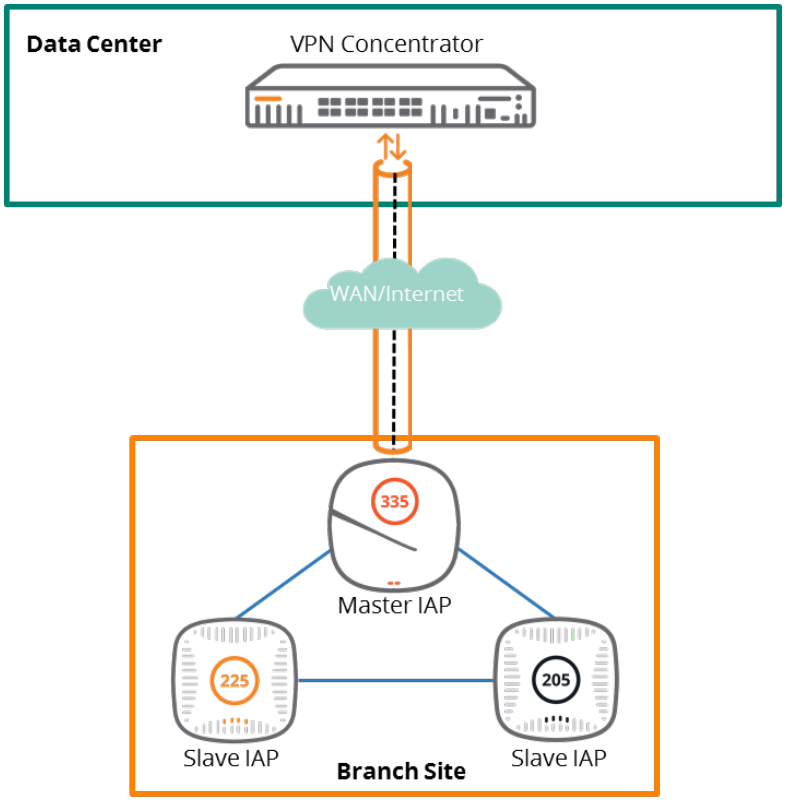


Figure 2-4 *IAP Tunnel Architecture*

When an IPsec connection is established between the WLAN controller and an IAP, each end of the IPsec tunnel has two IP addresses: an Inner IP address and an Outer IP address. By default, the WLAN controller assigns them the following roles:

- **Outer IP address:** Logon
- **Inner IP address:** Default VPN with an "allow all" access control list (ACL)

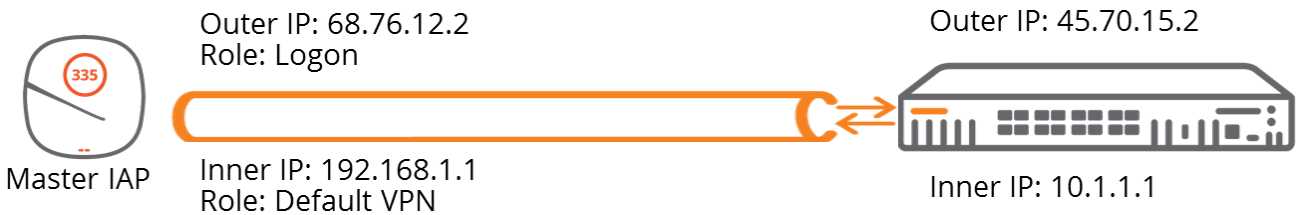


Figure 2-5 *IP Address Role Assignment*

Licensing

The WLAN controller considers the Master IAP that establishes a tunnel as a VPN client and not an AP which means that licenses such as the AP capacity license, PEFNG license, and RFProtect license are not required. However, a PEFV license is required in one of the following scenarios:

- Changing the ACLs in the default VPN role present in the controller
- Changing the role that is applied to the inner IP address and the ACLs within that role

Licenses	Features
Base ArubaOS	IAP can terminate a VPN tunnel and pass VPN traffic. Roles and polices cannot be edited.
ArubaOS with a PEFV license	IAP can terminate a VPN tunnel and pass VPN traffic. The default role in the default IAP VPN authentication profile of a WLAN controller can be edited. New user roles with custom firewall policies can be applied.

Table 2-1 *IAP License Functionality Descriptions*

Tunneling Options

Instant supports the following tunneling protocols for remote access:

- **Aruba IPSec** - IPsec is a protocol suite that secures IP communications by authenticating and encrypting each IP packet of a communication session. IPsec tunnels can be configured to ensure that the data flow between the networks is encrypted. However, a split-tunnel can also be configured which will only encrypt the corporate traffic. When IPsec is configured it is important to add the Instant AP MAC addresses to the whitelist database stored on the controller or external server. IPsec supports Local, L2, and L3 modes of IAP TUNNEL operations

Instant APs only support IPSec with Aruba Controllers.

- **Layer-2 GRE** - GRE is a tunnel protocol for encapsulating multicast, broadcast, and L2 packets between a GRE-capable device and an endpoint. Instant APs support the configuration of L2 GRE tunnel with an Aruba controller to encapsulate the packets sent and received by the Instant AP

  The GRE configuration for L2 deployments can be used when there is no encryption requirement between the Instant AP and controller for client traffic. Instant APs support two types of GRE configuration:

  - **Manual GRE** - The manual GRE configuration sends unencrypted client traffic with an additional GRE header and does not support failover. When manual GRE is configured on an Instant AP it is important ensure that the GRE tunnel settings are enabled on the controller

- **Aruba GRE** - Aruba GRE does not require any configuration on the controller except for adding the Instant AP MAC addresses to the whitelist database stored on the controller or an external server. Aruba GRE reduces manual configuration when the **Per-AP tunnel** configuration is required and supports failover between two GRE endpoints. Aruba GRE is only supported by Aruba Controllers running ArubaOS 6.4.x.x or later versions

Instant APs support manual and Aruba GRE configuration only for L2 mode of operations.

Instant APs can send IPsec and GRE heartbeat packets to Aruba Controllers. By default, Instant APs verify the status of heartbeat messages every 5 seconds and look for lost packets 6 times before marking the IPsec tunnel as down. The time intervals are fully configurable and can be modified according to the needs of network administrators.

- **L2TPv3** - The L2TPv3 feature allows the Instant AP to act as an L2TP Access Concentrator and tunnel all wireless client L2 traffic from the Instant AP to the L2TP Network Server (LNS). In a centralized L2 model the VLAN on the corporate side is extended to remote branch sites. Wireless clients associated with an Instant AP receive the IP address from the DHCP server running on the LNS. In order to receive the address the Instant AP has to transparently allow DHCP transactions through the L2TPv3 tunnel. Some important points to note about L2TPv3 in the context of Instant APs are as follows:
  - Instant supports tunnel and session configuration and uses Control Message Authentication (RFC 3931) for tunnel and session establishment. Each L2TPv3 tunnel supports one data connection and this connection is termed as an L2TPv3 session
  - IAPs only support tunneling over UDP
  - If the primary LNS goes down it will fail over to the backup LNS. L2TPv3 has one tunnel profile under which a primary peer and a backup peer are configured. If the primary tunnel creation fails or if the primary tunnel gets deleted then the backup is engaged. The following two failover modes are supported:
    - **Preemptive:** Preemptive mode means that if the primary peer comes back up while the backup is active then the backup tunnel is deleted and the primary tunnel resumes its role as an active tunnel. If preemption is configured when the primary tunnel goes down a persistence timer is triggered which will attempt to bring up the primary tunnel.
    - **Non-Preemptive:** In non-preemptive mode the backup tunnel will continue to operate after taking over from the primary tunnel even if the primary comes back up again.

L2TPV3 is not supported on IAP-205 devices.

Forwarding Modes

IAP forwarding modes determine whether the DHCP server and default gateway for clients reside in the branch or at the datacenter. These modes do not determine the firewall processing or traffic forwarding functionality. The virtual controller enables different DHCP pools (various assignment modes) in addition to allocating IP subnets for each branch. The virtual controller allows different modes of forwarding traffic from the clients on a VLAN based on the DHCP scope configured on the Instant AP.

The following forwarding modes are supported for IAP TUNNEL deployments:

1. Local mode
2. L2 Switching mode
3. L3 Routing mode

The DHCP scopes associated with these forwarding modes are described in the following sections. When configuring forwarding modes it is important to ensure that VLAN 1 is not configured for any of the DHCP scopes as it is reserved for a different purpose.

- **Local Mode** - In Local Mode the IAP cluster at that branch uses a local subnet and the Master IAP of the cluster acts as both the DHCP server and default gateway for clients. Local Mode provides access to the corporate network using the inner IP of the IPsec tunnel. The traffic destined for the corporate network is translated at the source with the inner IP of the IPsec tunnel and is then forwarded through the tunnel. All other non-corporate network traffic is translated using the IP address of the IAP and is forwarded through its uplink. When Local Mode is used for forwarding client traffic, hosts on the corporate network cannot establish connections to the clients on the Instant AP since the source addresses of the clients are translated.
- **Distributed L2 Mode** - In this mode, the Master IAP assigns IP addresses from the configured subnet and forwards traffic to both corporate and non-corporate destinations. The Master IAP acts as a DHCP server for the clients while the gateway for clients resides in the datacenter. Distributed L2 Mode can be thought of as an L2 extension of the corporate VLAN to remote sites. Either the controller or an upstream router can serve as the gateway for clients. Client traffic destined for datacenter resources is forwarded by the Master IAP through the IPSec tunnel to the default gateway in the datacenter. When an IAP registers with the VPNC it automatically adds the VPN tunnel associated to that IAP into the VLAN multicast table. This allows the clients connecting to the L2 Mode VLAN to be part of the same L2 broadcast domain on the controller.
- **Distributed L3 Mode** - Distributed L3 mode restricts all broadcast and multicast traffic to a branch which eliminates the cost and the complexity associated with a classic site-to-site VPN. Each branch location is assigned a dedicated subnet. The Master IAP in the branch manages the dedicated subnet in addition to serving as the DHCP server and default gateway for clients. Client traffic destined for datacenter resources is routed to the

controller through the IPsec tunnel, which then routes the traffic to the appropriate corporate destination. When an IAP registers with the controller a route is added to enable the routing of traffic from the corporate network to clients on the local subnet of the branch.

- **Centralized L2 Mode -** Centralized L2 Mode extends the corporate VLAN or broadcast domain to remote branches. The DHCP server and the gateway for the branch clients reside in the datacenter. Either the controller or an upstream router acts as the gateway for clients. Aruba recommends using an external DHCP server in this mode in lieu of the DHCP server on the controller. Client traffic destined for datacenter resources is forwarded by the Master IAP through the IPsec tunnel to the client's default gateway in the datacenter.
- **Centralized L3 Mode** - In Centralized L3 Mode the Master IAP acts as a DHCP relay agent by forwarding client DHCP traffic through the IPSec tunnel to a DHCP server located behind the controller in the corporate network. The Centralized L3 VLAN IP is used as the source IP. IP addresses are obtained from the DHCP server.

Forwarding Mode	DHCP Server	Client Default Gateway	Corporate Traffic	Internet Traffic	Branch Access from Datacenter
Local	Virtual Controller	Virtual Controller	Source NAT with inner IP of the IPSec tunnel	Source NAT performed with the local IP of the VC	No
Centralized L2	DHCP server in the datacenter	Datacenter controller or router	L2 reachable	Source NAT performed with the local IP of the VC	Yes
Centralized L3	DHCP server in the datacenter, VC acts as a DHCP relay	Virtual Controller	Routed	Source NAT performed with the local IP of the VC	Yes
Distributed L2	Virtual Controller	Datacenter controller or router	L2 reachable	Source NAT performed with the local IP of the VC	Yes
Distributed L3	Virtual Controller	Virtual Controller	Routed	Source NAT performed with the local IP of the VC	Yes

Table 2-2 *Forwarding Modes Feature Matrix*

NOTE

Local Mode, Centralized L2 Mode, and Distributed L3 mode are covered in depth as they are the most commonly employed forwarding modes.

Local Mode

Local Mode with Aruba Instant is similar to the local network of a home wireless router with the exception that it has VPN capabilities in addition to other enterprise grade features. The IAP cluster at the branch has a local subnet (e.g., 192.168.200.0/24) and the Master IAP of the cluster functions as the DHCP server as well as the default gateway for clients. Local Mode enables VPN capabilities by using the inner IP address of the Instant-VPN IPsec tunnel. Client traffic destined for corporate destinations is source NATed by the Master IAP using the inner IP address of the IPsec tunnel. Traffic that is destined for the Internet or local destinations is source NATed using the local IP address of the Master IAP. It is essential that the IP addresses that are defined in the VPN address pool of the WLAN controller (which is used for inner IP addresses of IPsec tunnels) are routable from the upstream router in the data center. If required, all client traffic can be forwarded through the IPsec tunnel or bridged locally.

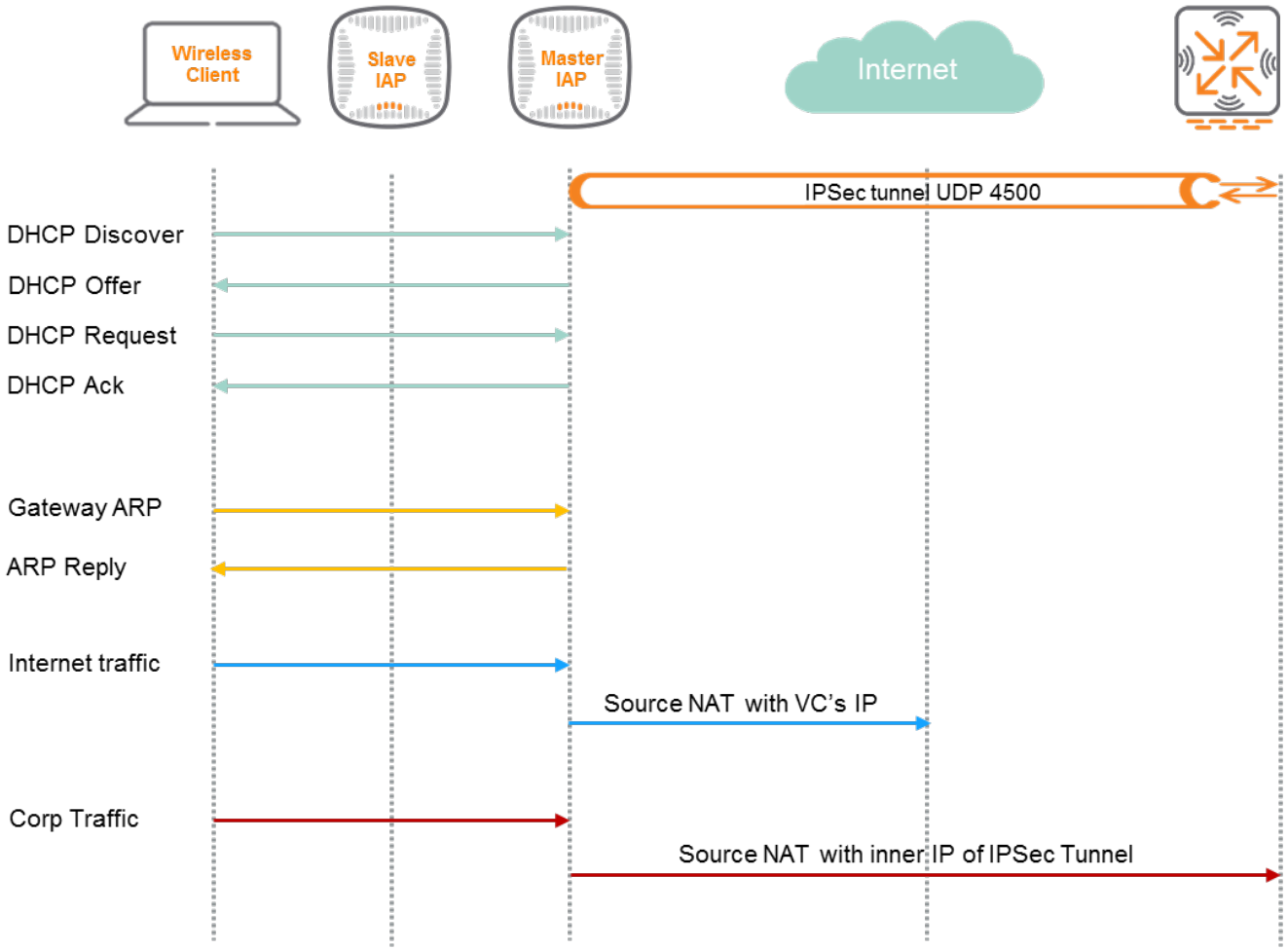


Figure 2-6 *Local Mode Forwarding*

In Local Mode, clients in the branch can initiate connections to a server in the data center, however connections cannot be initiated from the datacenter to remote clients. The behavior is similar to that of a NAT device. The WLAN controller and the upstream routers have no visibility or direct route to the branch subnet. Therefore, connections cannot be initiated from the data center to remote clients for troubleshooting purposes.

Local mode is ideal for branch guest networks using a captive portal sever in the datacenter for guest authentication.

Centralized L2 Mode

Centralized L2 Mode extends the corporate VLAN and broadcast domain to remote branches. The DHCP server and the gateway for branch clients both reside in the data center. Either the WLAN controller or an upstream router act as the gateway for clients. Aruba recommends using an external DHCP server for DHCP services in Centralized L2 mode rather than the DHCP server on the WLAN controller.

Centralized L2 mode has two options for forwarding traffic:

1. All traffic including guest traffic is forwarded by the Master IAP through the IPsec tunnel to the default gateway in the data center. This option is typically selected for organizations that prefer to exercise more control over guest traffic by having it forwarded to the data center
2. Alternatively, a split-tunnel can be used which forwards traffic destined for corporate resources through an IPsec tunnel to the VPNC while internet traffic is bridged locally. This option is effective for scenarios where control over guest traffic is less of a concern while also alleviating overhead on the corporate network

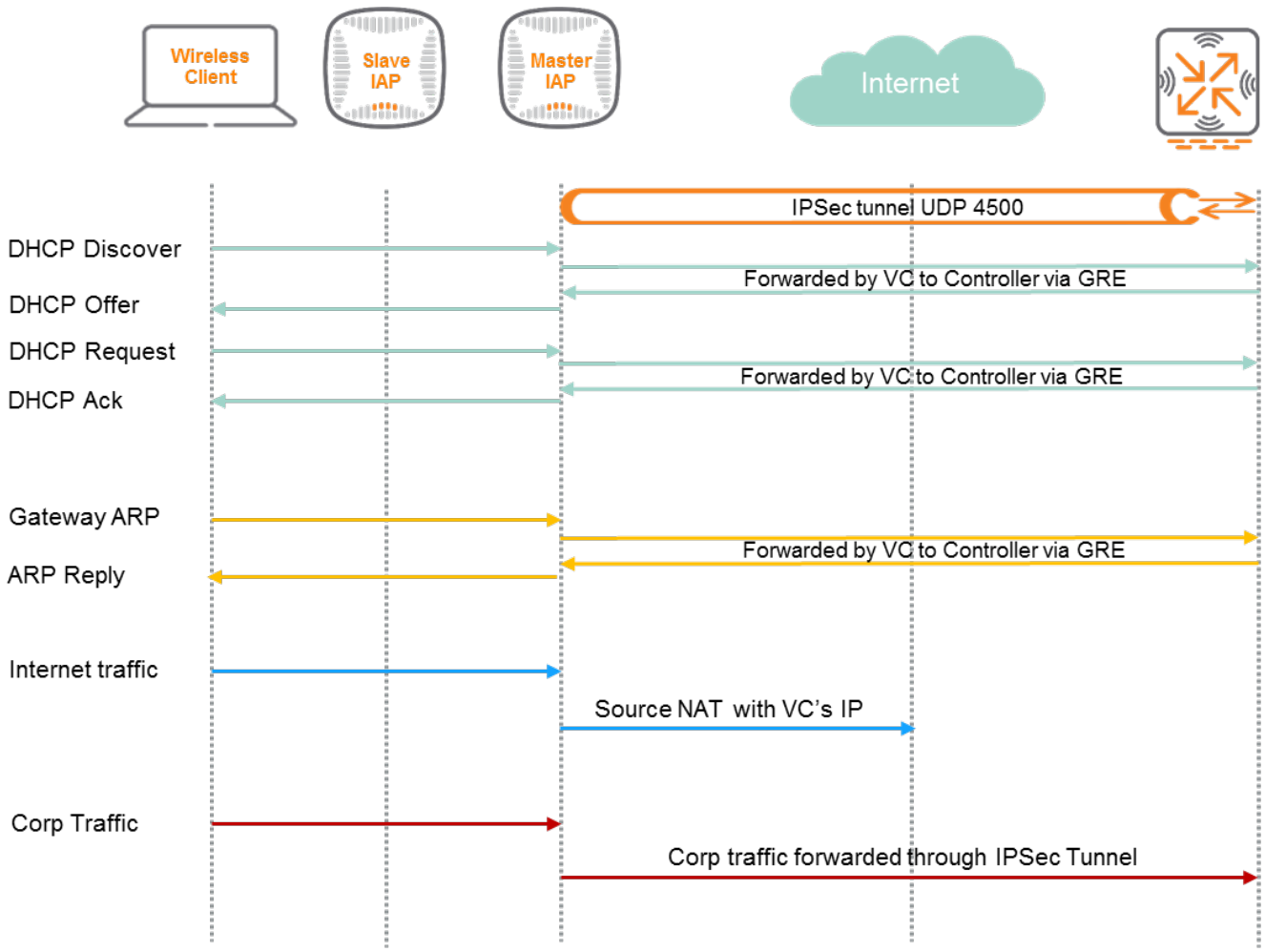


Figure 2-7 *Centralized L2 Mode Forwarding*

In Centralized L2 Mode connections can be initiated from the data center to remote clients for troubleshooting purposes. If RADIUS traffic is not source NATed at the WLAN controller, the VPN pool for inner IP addresses must be made routable for RFC 3576-compliance and 802.1X. A routable VPN address pool also allows access to the local WebUI of the Aruba Instant cluster from the datacenter.

NOTE

Aruba recommends using Centralized L2 Mode only if Layer 2 extension is mandatory for branches.

BID Allocation

When an Instant cluster in a branch comes up for the first time, one IAP is elected as the Master IAP through the master election algorithm. The designated Master IAP in a cluster generates a branch key by hashing its own MAC address and proceeds to distribute the key to all IAP cluster members. The branch key plays a significant role in ensuring that a branch is allocated the same subnet and IP addresses regardless of which IAP becomes the Master IAP of the cluster at a later point. This key is generated even for IAP clusters that are not configured for IAP TUNNEL.

After generating the branch key, the Master IAP forms an IPsec connection to the WLAN controller and obtains an inner IP address from its VPN address pool. The BID allocation process is initiated when the Master IAP sends a registration message to the WLAN controller. This registration message includes the following attributes:

- **Inner IP:** The inner IP address of the Master IAP that established the IPsec tunnel
- **Branch Key:** The key that was generated and distributed to all member IAPs by the Master IAP
- **MAC:** The MAC address of the Master IAP participating in the BID process
- **MAX_BID and subnet name:** The maximum number of subnets or IP address blocks that can be created based on the subnet size and the client count configured on the IAP

In addition to the *MAX_BID*, the IAP sends the corresponding subnet name to the VPNC. The subnet name is derived from IP address range in the configuration as well as the client count for each mode. E.g., if an organization uses 10.10.0.0/16 with 250 clients per branch, the IP configuration on the IAP is 10.0.0.0 - 10.10.255.255 instead of 10.10.0.0/16. The name of the L3 subnet will appear in the CLI as “10.0.0.0 – 10.10.255.255,250”.

The subnet name keeps track of which MAX_BIDs apply to which distributed mode configurations. If a branch is configured for multiple distributed modes, the IAP sends multiple combinations of MAX_BID and corresponding subnet names to the WLAN controller. This method allows a branch to have multiple SSIDs that use different distributed modes and different subnet sizes. For example an organization can have an SSID_1 with distributed L3 mode and a configuration of "10.10.0.0 /16” with 250 clients per branch and SSID_2 with distributed L3 mode and a configuration of "10.20.0.0 /16” with 100 clients per branch. The configuration on an Aruba IAP assumes the following definitions:

- **BID:** Value that specifies whether a branch is new or existing. A new branch uses a unique value in this field to specify that it requires a BID from the MAX_BID range. If the Master IAP of a branch that has already received a BID fails then a new IAP will be elected as the Master. When the newly elected Master IAP connects to the WLAN controller it will use the previously allocated BID in this field.
- **Backup:** Value that specifies whether the Master IAP is communicating with a backup host. A backup host is a backup WLAN controller where the Master IAP can initiate an IPsec connection. A backup host is similar to a backup local management switch BLMS controller in an ArubaOS campus network. It does not represent a VRRP backup to a WLAN controller.

The BID allocation process occurs between the primary host and the Master IAP. The WLAN controller serving as the primary host must be operational when a branch comes up for the first time. Any IAP TUNNEL branch brought up from a factory default configuration that is configured for Distributed L3 mode must exchange its first BID process with its primary host to receive its required address space and subnet.

Upon receiving a BID registration message, the WLAN controller determines whether a branch is new or existing by examining the BID field. If the branch is new, the WLAN controller verifies whether the branch key in the registration message is present in its database. If the branch key is not found then the WLAN controller selects an unused BID from the MAX_BID range and returns it to the Master IAP. If the branch key is already present in the WLAN controller's database, then the WLAN controller returns the BID that is already associated with the branch key. When the BID is allocated, the Master IAP uses the BID to determine the IP subnet or IP addresses that may be used. The following examples describe how the subnets are determined, based on BID value:

Consider an organization that uses a "10.10.0.0 /16" configuration with 250 clients per branch as the Distributed L3 mode configuration on IAPs in 200 branches. This configuration can support 256 branches. If a branch is assigned a BID of 0, it takes the first available /24 subnet. The subnet for the branch is 10.10.<bid>.0/24 = 10.10.0.0 /24. If a branch is assigned a BID of 50, the subnet for the branch is 10.10.<bid>.0 /24 = 10.10.50.0 /24.

After determining the IP address or the subnet that must be used, the Master IAP registers the IP addresses and IP subnet with the WLAN controller using ROUTE ADD and VLAN ADD messages. The ROUTE ADD and VLAN ADD messages notify the WLAN controller about the L3 subnet and L2 VLAN used at the branch. The Route ADD and VLAN ADD messages are not part of the BID process. These datapath programming messages are used to add the appropriate VLAN and route information to the WLAN controller datapath. If the Master IAP fails and a slave IAP becomes the new Master, then the branch key and BID will not change and the branch will continue to use the same subnet and IP addresses. The BID allocation process is depicted in the figure below:

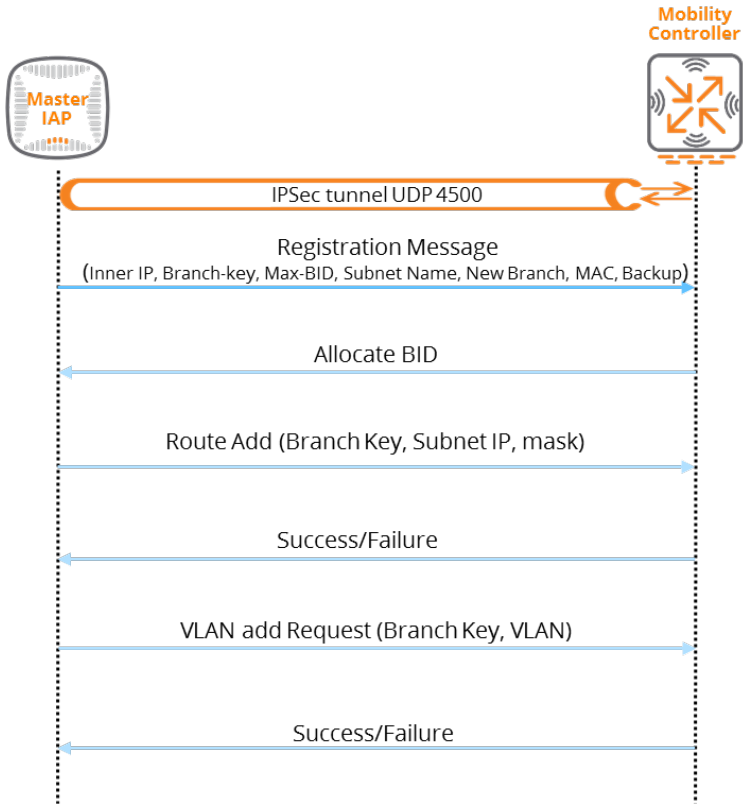


Figure 2-8 *BID Allocation process*

Distributed L3 Mode

In Distributed L3 mode, each branch location is assigned a dedicated subnet. The Master IAP in the branch manages the subnet, functions as the DHCP server, and acts as the default gateway for clients. Client traffic destined for datacenter resources is routed to the WLAN controller through an IPsec tunnel. The WLAN controller then routes the traffic to the appropriate corporate destinations as needed.

Any traffic destined for the Internet or a local destination is source NATed using the local IP address of the Master IAP and locally bridged. The WLAN controller in the datacenter is aware of the Layer 3 subnet at each branch and can redistribute these routes to upstream routers through the Open Shortest Path First (OSPF) routing protocol. All client traffic can be forwarded through the IPsec tunnel or bridged locally if required.

Distributed L3 mode allows connections to be initiated from the data center to remote clients for troubleshooting purposes. If RADIUS traffic is not source NATed at the WLAN controller then the VPN pool that is used for inner IP addresses of the IPsec tunnel must be routable for RFC 3576-compliance and 802.1X.

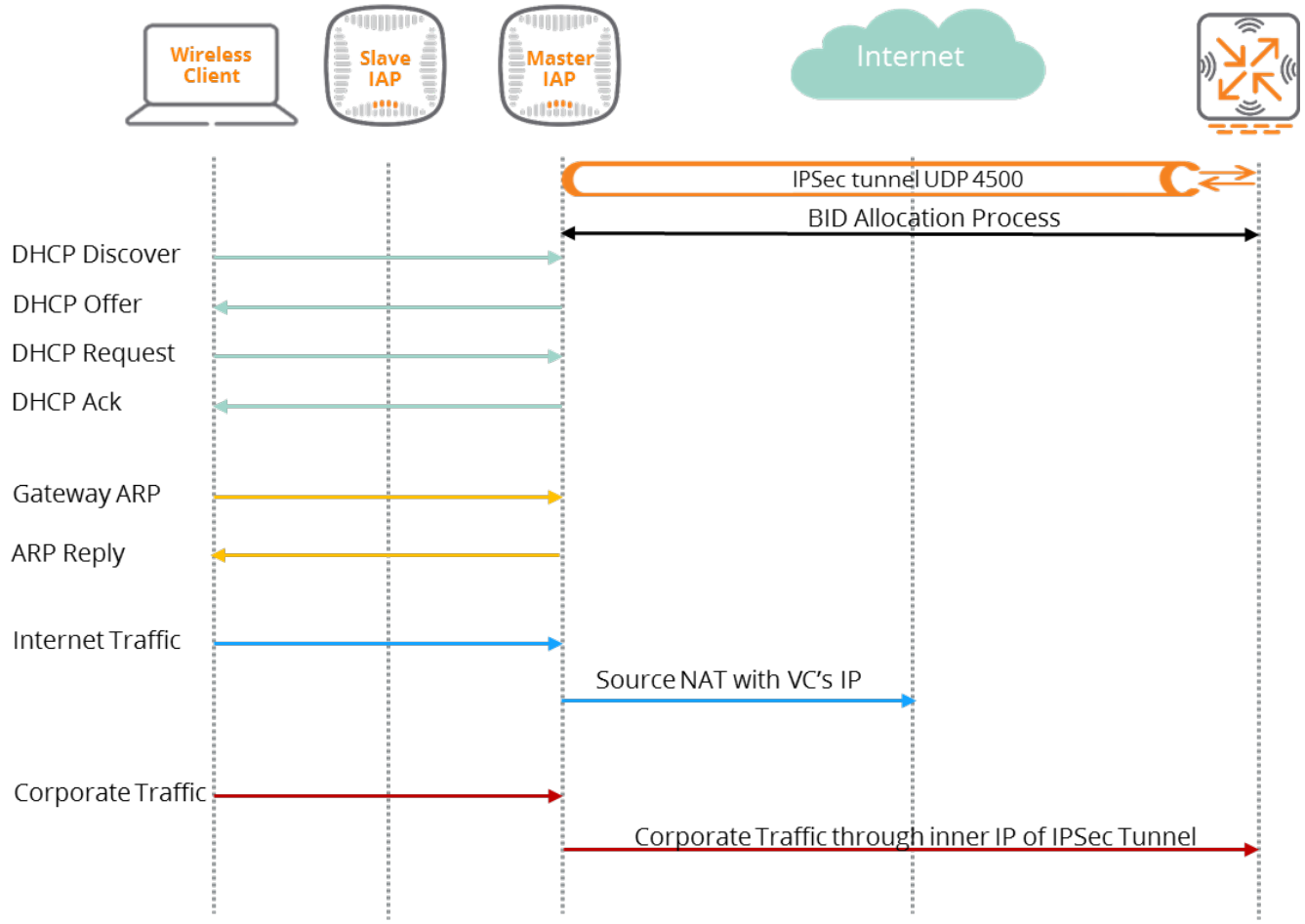


Figure 2-9 *Distributed L3 Mode Forwarding*

NOTE

Split-tunnel Mode cannot be configured in Distributed Layer 3 mode as it can in Centralized Layer 2 Mode. In Centralized Layer 2 deployments Split-tunnel Mode more frequent use case. Routing profiles can be used to achieve similar functionality with a Distributed Layer 3 deployment

NOTE

Distributed L3 mode is the recommended mode of operation for Instant-VPN networks. Centralized L2 mode should only be used by organizations which require the extension of corporate VLANs to branch networks.

Scalability

The table 9 below outlines scalability numbers for each controller model for an IAP TUNNEL deployment. The table assumes the following definitions:

- **IAP TUNNEL Branches** –The number of IAP TUNNEL branches that can be terminated on a particular controller platform
- **Route Limit** – The number of L3 routes supported on a controller
- **VLAN Limit** – The number of VLANs supported on a controller

Platforms	IAP TUNNEL Branches (Preferred)	Route Limit	VLAN Limit
7280	8192	32,769	4,094
7240	8192	32,769	4,094
7220	4096	32,769	4,094
7210	2048	32,765	4,094
7205	1024	16, 381	2,048
7030	256	8,189	256
7024	128	4,093	128
7010	128	4,093	128
7008	64	4,093	128
7005	64	4,093	128

Table 2-3 *IAP Tunnel Scalability*

IAP Tunnel Authentication

In an Instant tunnel branch network users can be authenticated either through a local RADIUS server or a RADIUS server in the data center. The Master IAP in an Instant tunnel branch determines which RADIUS server is used by checking its own routing profile. Traffic destined for a RADIUS server in the datacenter is sourced using the inner IP address of the IPsec tunnel. The VPN address pool that is used for inner IP addresses of IPsec tunnels must be routable from the upstream router in the data center. If dynamic authorization extension to RADIUS (RFC 3576) is not required then a rule can be placed on the WLAN controller to source NAT all RADIUS traffic with the IP address of that WLAN controller. If a branch network has a local RADIUS server and if dynamic RADIUS proxy (DRP) is enabled on the IAP, then 802.1X traffic is source NATed with the Master IAP's IP address.

RFC 3576-compliance dictates that CoA messages must be initiated by the RADIUS server. Rules should never be enabled on the WLAN controller to source NAT all RADIUS traffic with the IP address of that WLAN controller. If the RADIUS server is located in the datacenter then the inner IP addresses of the IPsec tunnels must be listed as RADIUS clients. If RFC 3576-compliance is used with a local RADIUS server, the Master IAP's IP address must be added as the RADIUS client. DRP must be enabled for Instant networks consisting of multiple IAPs to tunnel the RADIUS traffic from the member IAPs to the authentication server in the datacenter.

When DRP is enabled, the 802.1X transactions for clients connecting to the member IAPs are forwarded to the Master IAP functioning as a RADIUS proxy. With DRP enabled, the NASIP attribute in RADIUS packets destined for the RADIUS server in the datacenter contain the inner IP address of the IPsec tunnel. DRP is not required for single IAP deployments. However, if DRP is enabled in such a deployment then the NASIP attribute in RADIUS packets destined for the RADIUS server in the datacenter will contain the local IP address of the IAP rather than the inner IP address of the IPsec tunnel. As a best practice, Aruba recommends enabling DRP in single IAP deployments with RADIUS servers that use the NAS IP attribute as a filter for authentication. The following table outlines authentication options in various Instant deployment scenarios:

RADIUS Server Location	DRP	VPN Pool Routable From DC	ACL Source NATs Traffic to Controller IP	Source IP	NAS IP	RFC 3576 Compliant
DC	Enabled	Yes	No	Inner IP of IPsec Tunnel	VPN Tunnel IP	Yes
DC	Enabled	No	Yes	Controller	VPN Tunnel IP	No
Local	Enabled	N/A	N/A	Master IAP Local	Master IAP IP	Yes
Local	Disabled	N/A	N/A	Master or Slave IAP	Master/Slave IAP IP	Yes

Table 2-4 *802.1X and RFC 3576 Options*

IAP Tunnel DNS

In a typical IAP deployment without tunneling all DNS requests from a client are forwarded to the client's DNS server by default. However, this behavior changes if an IAP is configured for tunneling.

The DNS behavior for both wired and wireless clients on an IAP network configured for tunneling is determined by the enterprise domain settings. The enterprise domain setting on the IAP specifies the domains for which DNS resolution must be forwarded to the default DNS server of the client. E.g., if the enterprise domain is configured for arubanetworks.com, the DNS resolution for host names in the arubanetworks.com domain would be forwarded to the default DNS server of the client. The DNS resolution for host names in all other domains is source NATed to the local DNS server of the IAP.

If no enterprise domain configuration exists and the client is on an SSID for IAP VPN then all DNS traffic will be source NATed to the DNS server of the IAP. If a non-VPN SSID is present, its traffic will be forwarded to the default DNS server for the client that initiated the request. If Split-tunnel Mode has been disabled, all DNS traffic will be forwarded over IPSec tunnel to DNS server of the client regardless of the enterprise domain configuration. If an asterisk is configured in the enterprise domain list instead of a domain name then all DNS requests are forwarded to the default DNS server of the client.

Branch Connectivity Scenarios

Internet Connectivity

The Internet branch connectivity scenario consists of a deployment with multiple DCs with a requirement for redundancy between the DCs and branch offices. Internet traffic is locally bridged in branch offices while corporate traffic is secured and routed to the DC. Split-tunneling of client DNS traffic is preferred for the Internet branch connectivity scenario.

Aruba IPSec is used to securely transmit data between branch offices connected to the DC through the Internet. Distributed Layer 3 mode is the preferred forwarding mode as there is no need to extend the corporate VLAN or multicast traffic from DC to branch offices. The primary and backup IPSec VPN tunnels are configured with preemption and fast failover from the branches to the DC for redundancy purposes. The IPSec VPN tunnels terminate on the controllers in the DMZs. Clients connected to the branch offices obtain their IP address either from the local DHCP server on the switch or from DHCP server on the IAP (depending on whether the branch has a Flat or Hierarchical Mode topology).

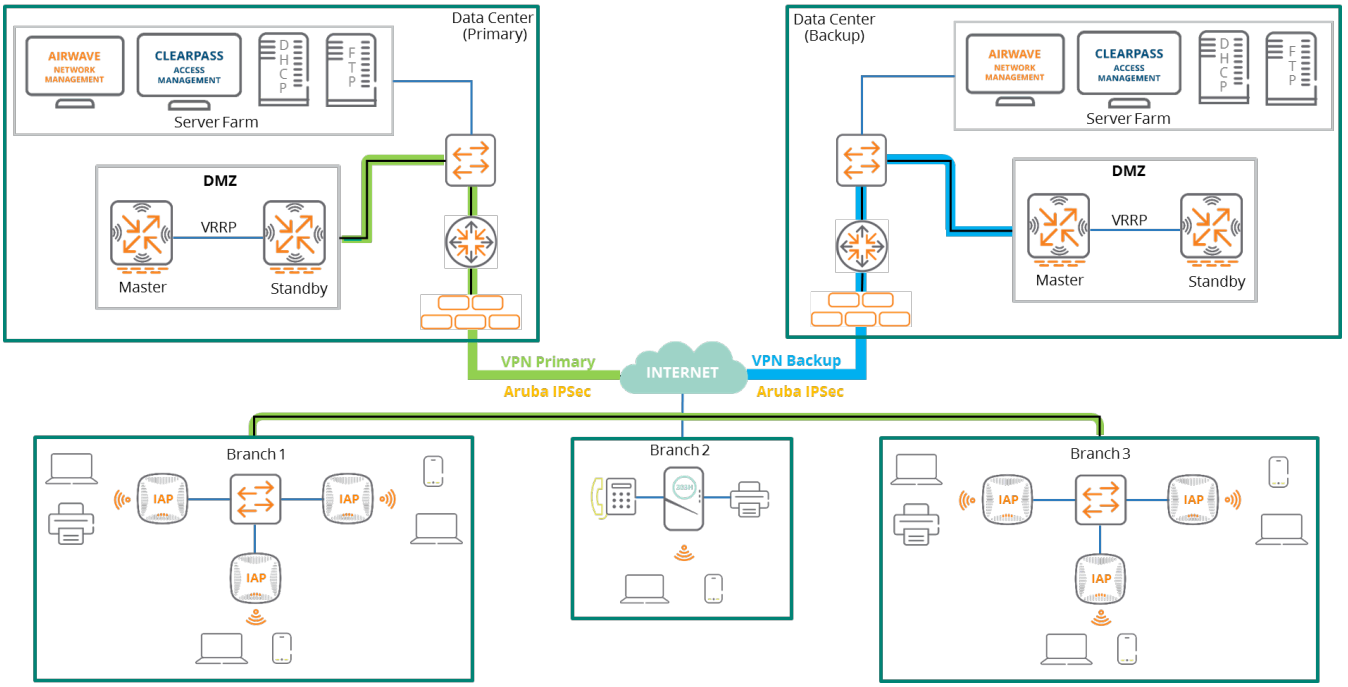


Figure 2-10 *Branch Connectivity through Internet*

Employees are authenticated with 802.1x through the ClearPass server in the DC. Guests can be presented with a captive portal from the ClearPass server as well with internet traffic bridged locally at the branch using a separate guest VLAN. Split-tunnel DNS is configured under the enterprise domain tab with a rule created only corporate domain name queries are tunneled to the DC.

MPLS Connectivity

The MPLS branch connectivity scenario consists of a deployment with multiple DCs with a requirement for redundancy between the DCs and branch offices. All employee and guest traffic is forwarded to the DC for processing.

Since the traffic from branch offices flows through MPLS network, the security of the data packets is handled by the service provider. Aruba GRE is the preferred tunneling mode and only control packets are encrypted using IPsec.

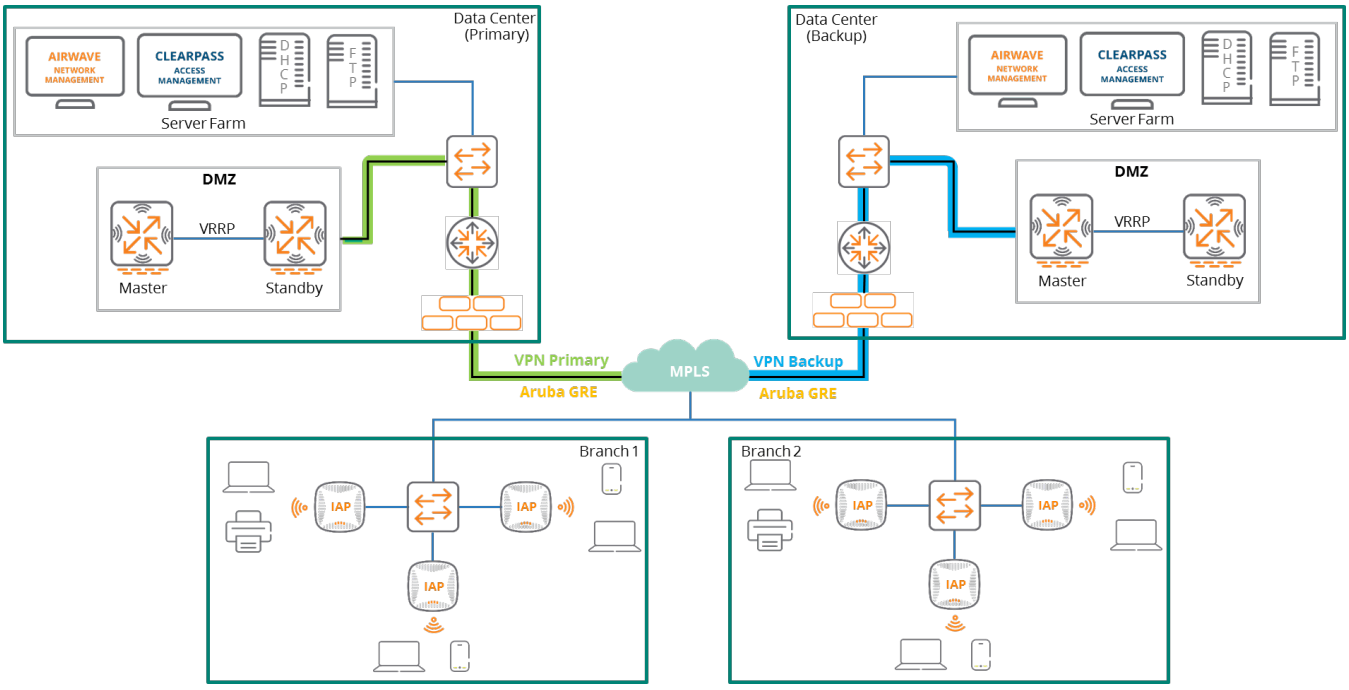


Figure 2-11 *Branch Connectivity through MPLS*

Centralized L2 Mode is the preferred forwarding mode for this scenario since the DHCP and DNS servers are centralized and employee as well as guest traffic needs to be forwarded to the DC. The ClearPass server provides 802.1X authentication so employees in the branch office can access the network.

Guest users are provided with a captive portal through the ClearPass server in the DC. All guest traffic is tunneled to the controller in the DMZ. Appropriate firewall policies should be applied to restrict guests from gaining access to internal resources. The IAPs where clients are connected tunnel the guest traffic to the controller in the DMZ. As the DNS server is also centralized an asterisk is placed in the enterprise domain list to ensure that all DNS queries are forwarded to the servers in the DC.

Aruba Central

Aruba Central is a Software as a Service (SaaS) offering that provides simple, cost-effective, wireless, wired, and WAN management for Aruba Instant APs, switches, and gateways. Central also offers value added services such as customized guest access in addition to detailed location and service assurance analytics. With Aruba Central, distributed enterprises are operational in minutes rather than hours or days. Simple, functional, and workflow driven features simplify traditional management tasks which allows organizations to focus on value creation. Additional information about Central can be found on Aruba's website.

Key Features

1. **Unlimited and Immediate Scalability** – There is virtually no limit to how many devices can be managed with Central since it is elastically scalable.
2. **Zero Impact Upgrades** – Due to Central's compartmentalized nature it gets upgraded without impacting any services. There are major upgrades every few month with some issues resolved on the go using hot fixes.
3. **Ease of Communication** – Devices initiate communicate with Aruba Central via WebSocket and create a two-way communication channel allowing any communication by Central to be immediately delivered to devices.
4. **Cloud-based Solution** – Central is hosted securely in cloud and does not require an on premise installation. This also eliminates the need to set up backup mechanisms since Central is a fully-redundant solution.
5. **Subscription based Model** - Central is a subscription based model and does not require the substantial investment of traditional on premise solutions. Subscription based models do not require upfront costs and can be purchased in increments of one, three, or five years.
6. **Device Support** – The Supported Device List increases with every release of Aruba Central.
7. **Evaluations** – Free trials are available which allow organizations to test Central without requiring a full commitment.
8. **High Availability** - Central automatically provisions and maintains a synchronous standby replica in a different availability zone which provides reliable redundancy in the cloud with a 99.95% uptime service level agreement.
9. **Versatile Capabilities** – Central does far more than just network management. Additional applications include guest wireless, presence analytics, clarity, and UCC.
10. **Support Included** - Support fees and software updates are bundled into Central subscriptions if the device is being managed through Central. This does not affect product hardware warranty or replacement.

Architecture

Aruba Central is deployed in a Virtual Private Cloud (VPC) within the data center of a leading public cloud provider. The physical infrastructure Aruba Central SaaS runs on is not shared with any other vendor. Central's status can be checked at any time by visiting the following URL http://status.central.arubanetworks.com/.

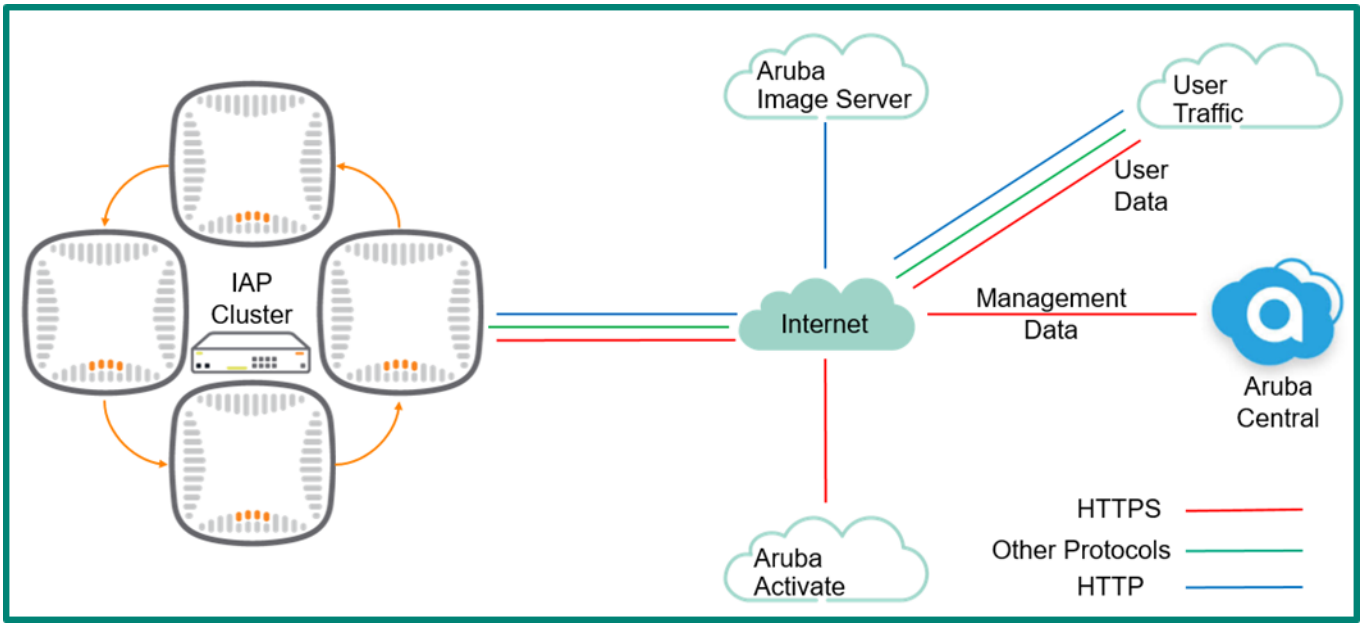


Figure 3-1 *Aruba Central Architecture*

Device Communication

Aruba devices connect to Aruba Central via HTTPS using Secure Sockets Layer (SSL) version 1.2 to protect against eavesdropping, tampering, and message forgery. All Aruba devices have a TPM module built in the hardware which controls the end device security at the hardware level. It can store certificates and keys for encryption which are used in the HTTPS tunnel to Central. Central only consumes management data from devices; user data is completely excluded from the communication plane between Central and devices.

It is important to note that Central acts as a management server by pushing configuration down to the devices and consuming monitoring information from them via WebSocket. Management related messages such as configuration, image upgrade, and status are transmitted via WebSocket only to the master IAPs. Other messages such as AppRF, debug, support commands, RSSI information, Clarity etc. are sent via WebSocket to all IAPs, regardless of whether they are master or slave.

If an IAP is connected to Central then its local UI is available, however configuration options will be blocked and Central retains absolute authority for configuration. If Central connectivity goes down due to Internet connectivity issues or subscription expiration, then the configuration options in the IAP's local UI will be completely functional. When connectivity to Central is re-established it will

override any local configuration changes that were made during the time communication was lost. A list of the URLs that need to be opened in the firewall to permit Central to manage devices can be found here.

Image Server

Aruba Image Server communication takes place over HTTP. Aruba Instant images are digitally signed by an Aruba image signing Certificate Authority (CA) when they are built. An image's digital signature is verified prior to being loaded. If the digital signature verification fails then the image is not loaded. This verification is performed while the device boots before loading the image as well as prior to performing an image upgrade. Modifying the image will result in digital signature verification failure and the image will not be able to be loaded on an IAP.

Image server URLs are different for IAPs and switches.

Activate

Every device sold to a customer is automatically recorded into Aruba Activate (Aruba's provisioning and inventory service). Customers may request an Activate login free of cost for purposes of inventory management and provisioning. Aruba devices automatically initiate communication to Aruba Activate via HTTPS tunnel when they boot up. Activate can then guide the device to a management service such as Central. Central natively interfaces with Activate without any intervention required from the customer. The only requirement is adding the credentials for the Activate account in Central. A Central account can only be tied to one Activate account.

Version

Central utilizes a service-oriented architecture and is therefore not subject to traditional version number conventions. Different pages in Central could each be served by different applications so Central does not have a single version number.

User Interface Landscape

The Central UI supports all major browsers (IE, Chrome, Firefox, Safari, etc.).

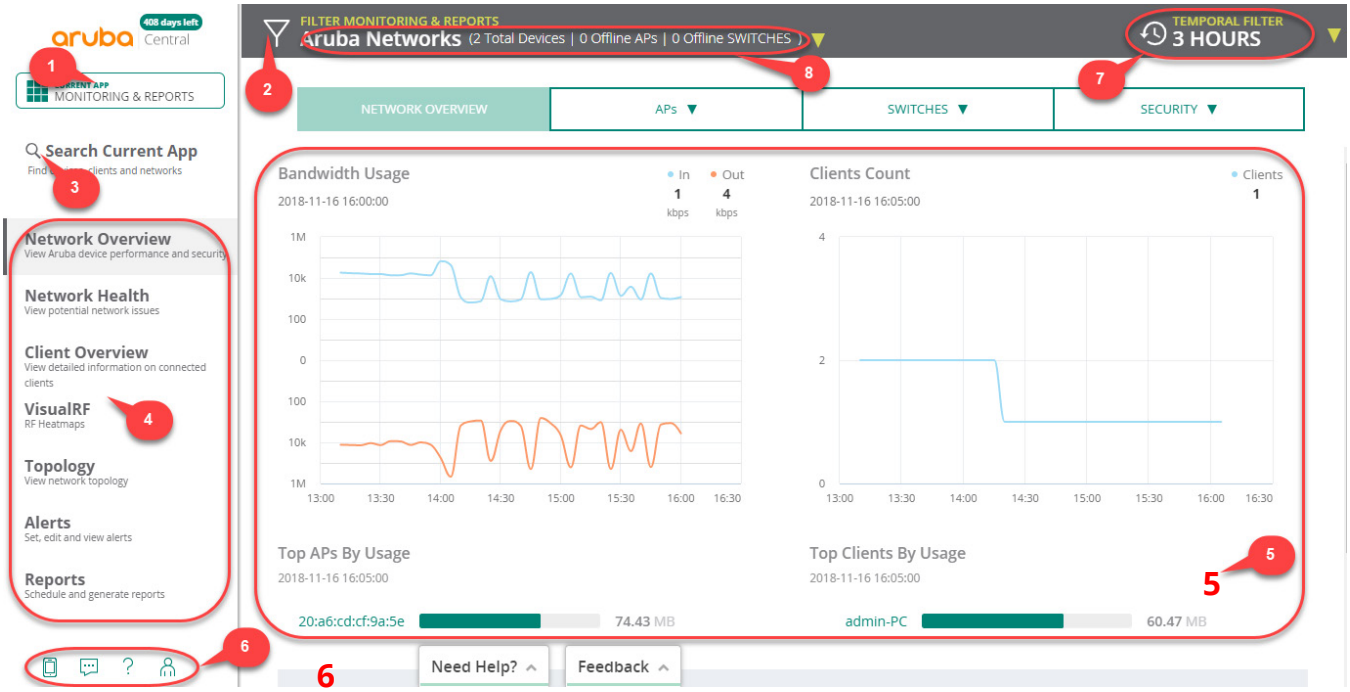


Figure 3-2 *Central User Interface Landscape*

The Central UI has the following major sections:

1. **App Selector** – Used to switch between Central applications
2. **Filter Pane** - Used to select a Group, Device, Label, etc.
3. **App Search** – Used for searching within an app
4. **Navigation Pane** – Allows selection of app-specific options
5. **Data Pane** – Displays contents based on the selected navigation pane option
6. **User & Resource Pane** – Online documentation, release notes, user settings, and help
7. **Time Selector** – Can display data in intervals of 3 hours, 1 day, 1 month, and 3 months
8. **Summary Pane** – Provides a summary of device status

Account ID

All that is required to create a Central account is a valid email address. However email addresses can be added or removed at any time and multiple email addresses may exist in a single Central account to enable management by multiple administrators. The Account ID is a unique number which remains static and was specifically created for purposes of distinguishing between different Central accounts and for troubleshooting. To view the Account ID, navigate to the **User & Resource Pane** and select the **User Icon** shaped like a human:

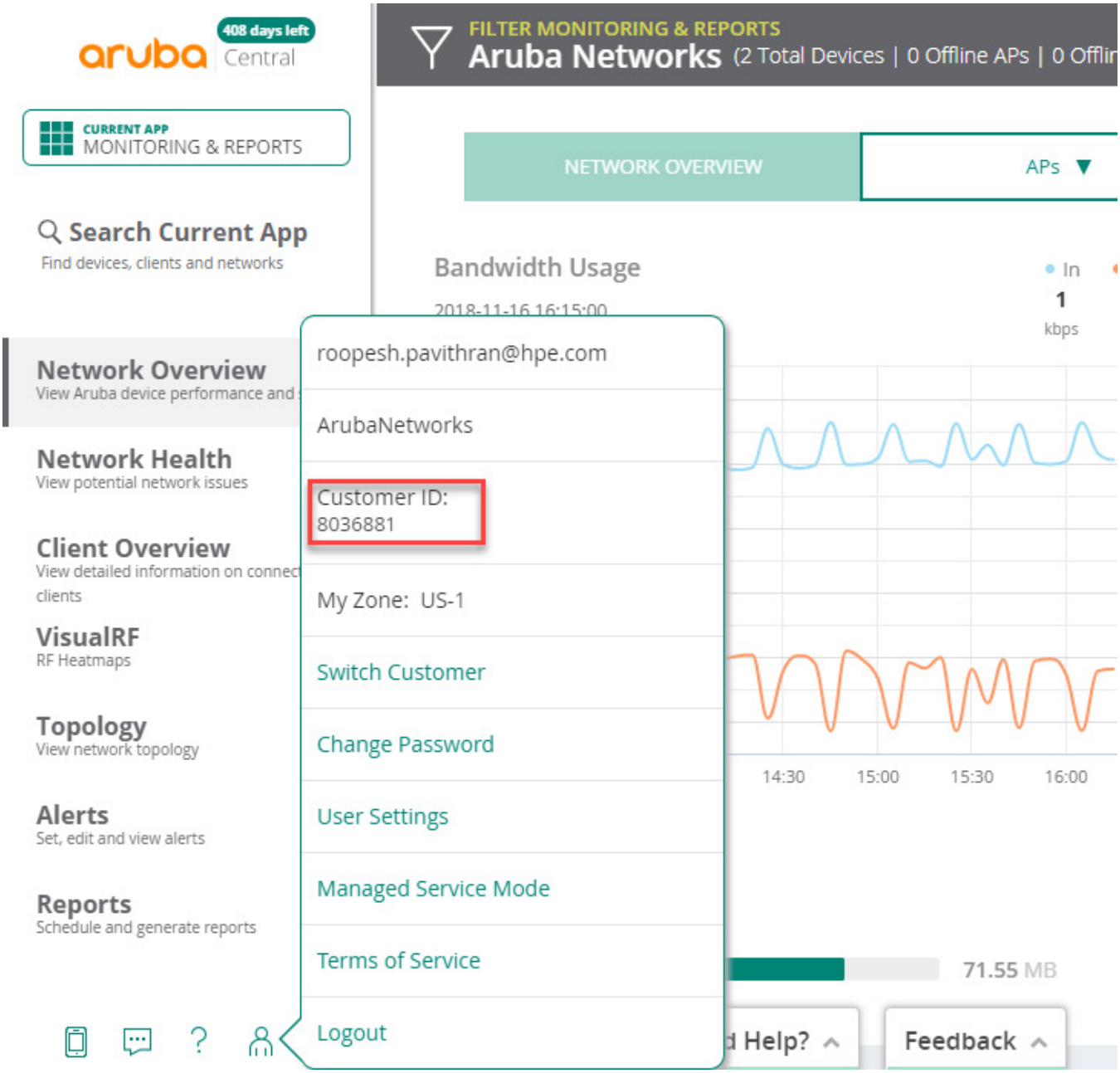


Figure 3-3 *Locating the Central Account ID*

Multiple Accounts

A single email address can be tied to multiple Central Account IDs e.g., a partner providing managed services for customers added as a user in each of their Central accounts. A screen such as the one shown in Figure 3-4 will be displayed when the partner logs into Central so they may choose the correct account. While users can be added to multiple Central accounts, that is not a solution for multi-tenancy. Multi-tenancy solutions are offered through **MSP** mode.

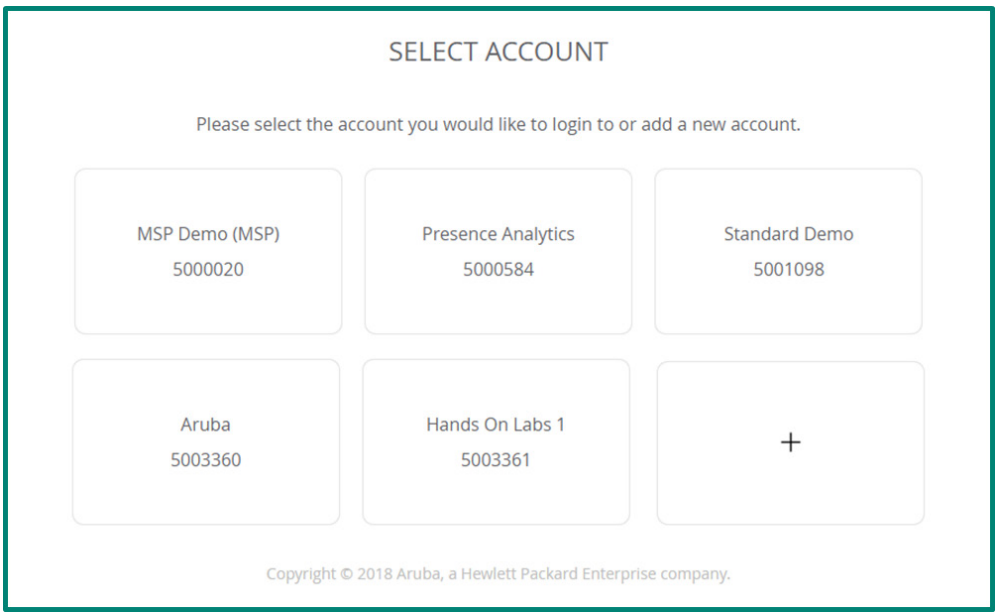


Figure 3-4 *Login Screen for a Single Account Mapped To Multiple Accounts*

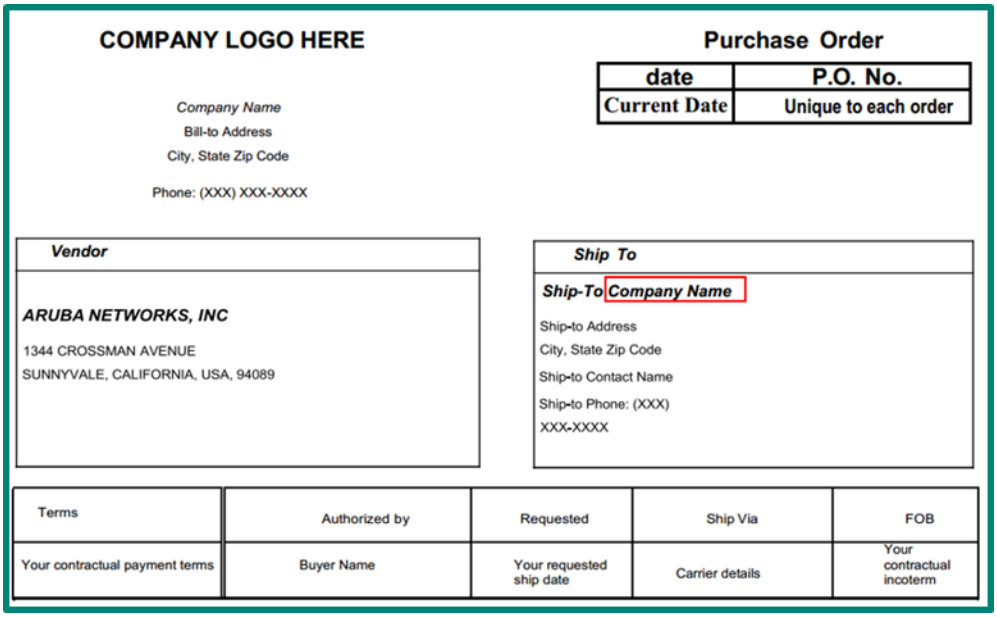
Inventory

A device can only exist in the inventory of only one Central account at one time. There are three methods of populating Central inventory:

- Activate
- MAC Address and Serial Number
- Cloud Key and Serial Number

Activate

All devices sold to a customer are automatically moved to the inventory of an account in Activate with the same name as the “Company Name” field listed on the purchase order. It is critical to ensure that the Company Name value on the purchase order is accurate:



COMPANY LOGO HERE

Purchase Order

date	P.O. No.
Current Date	Unique to each order

Company Name
Bill-to Address
City, State Zip Code
Phone: (XXX) XXX-XXXX

Vendor	Ship To
ARUBA NETWORKS, INC 1344 CROSSMAN AVENUE SUNNYVALE, CALIFORNIA, USA, 94089	***Ship-To Company Name*** Ship-to Address City, State Zip Code Ship-to Contact Name Ship-to Phone: (XXX) XXX-XXXX

Terms	Authorized by	Requested	Ship Via	FOB
Your contractual payment terms	Buyer Name	Your requested ship date	Carrier details	Your contractual incoterm

Figure 3-5 *Sample Purchase Order*

Once the Activate credentials have been entered Central's inventory is synced with all the devices in that Activate account. The following points outline how the process works:

1. A customer called Acme Inc. has an Activate account called "ACME" with folders that have names such as "default" and "AW" .The AW is not manged by Central and has a redirection rule to AirWave. Devices are present in both the default and AW folders.
2. ACME administrators map the Activate credentials into a Central account.
3. Central creates an additional folder called "athena-f-ACME" with a redirection rule to Central in ACME's Activate account.
4. ACME's Activate account now contains the "default", "AW", and "athena-f-ACME" folders.
5. Central syncs all the devices present in ACME's Activate account (i.e. the devices present in the "default" and "AW" folders) which will then be displayed in the Device Inventory page in Central.
6. When a subscription is assigned to devices in Central, then they will be moved to ""athena-f-ACME" from the "AW" and "default" folders.
7. If devices are moved out of ACME's Activate account then they will be deleted from Central's Device Inventory during the next sync.
8. As long as the devices are present in "ACME" then Central will sync them and they will be displayed in the Device Inventory page.
9. Activate sync runs in the background and it occurs automatically once every 4 hours.
10. Synchronization with Central can also be manually initiated from Central UI in the **Device Inventory** page once every 30 minutes.

NOTE

Aruba recommends adding Activate credentials as the method to populate the device inventory in Central. It is also highly recommended to allow Central to create Activate folders and move devices around in them.

MAC Address and Serial Number

A device can also be added in Central using its MAC address and serial number as long as the device is not subscribed in any other Central account.

Cloud Key and Serial Number

When a device communicates with Activate it generates a cloud key for itself which can be found using that device's CLI. Only the Master IAP in a cluster communicates with Activate and generates the cloud key used to add the device to Central. Central is able to query Activate using the cloud key and pull all devices in the purchase order into Central inventory.

NOTE

Being a part of Central's inventory does not mean the device is managed by Central. It gives the Central administrator the option to assign a subscription to the device in inventory which makes the device manageable via Central.

Subscriptions

Aruba Central has a simple and easily applied subscription model consisting of two components for each device:

- 1 Device Management Subscription
- 1 Service Subscription per device for each service

Figure 3-6 *Central Subscription*

Device Management Subscription

Each device requires a Device Management Subscription at a minimum in order for the device to be managed by Central which can then be assigned to an IAP, switch, or SD-branch gateway. The act of assigning a subscription to a device will automatically move the device to the Central folder in Activate make it manageable via Central. Central has an “Auto Assignment” feature which if enabled will assign a device management subscription to all devices in its inventory.

Devices periodically contact Central every 5 minutes. When the device reaches out to Activate in the next period, it learns the new provisioning rule and sets up HTTPS tunnels with Central. Slave IAPs also set up tunnels to Central for monitoring and troubleshooting purposes. Configuration is propagated from Central to Master IAPs only and from there is coordinated between Master and slave IAPs.

A Central evaluation lasts for 90 days and provides 10 device management and 20 service subscriptions including WebCC.

NOTE

Every IAP in the cluster must be assigned a device management subscription, not just the Master IAP.

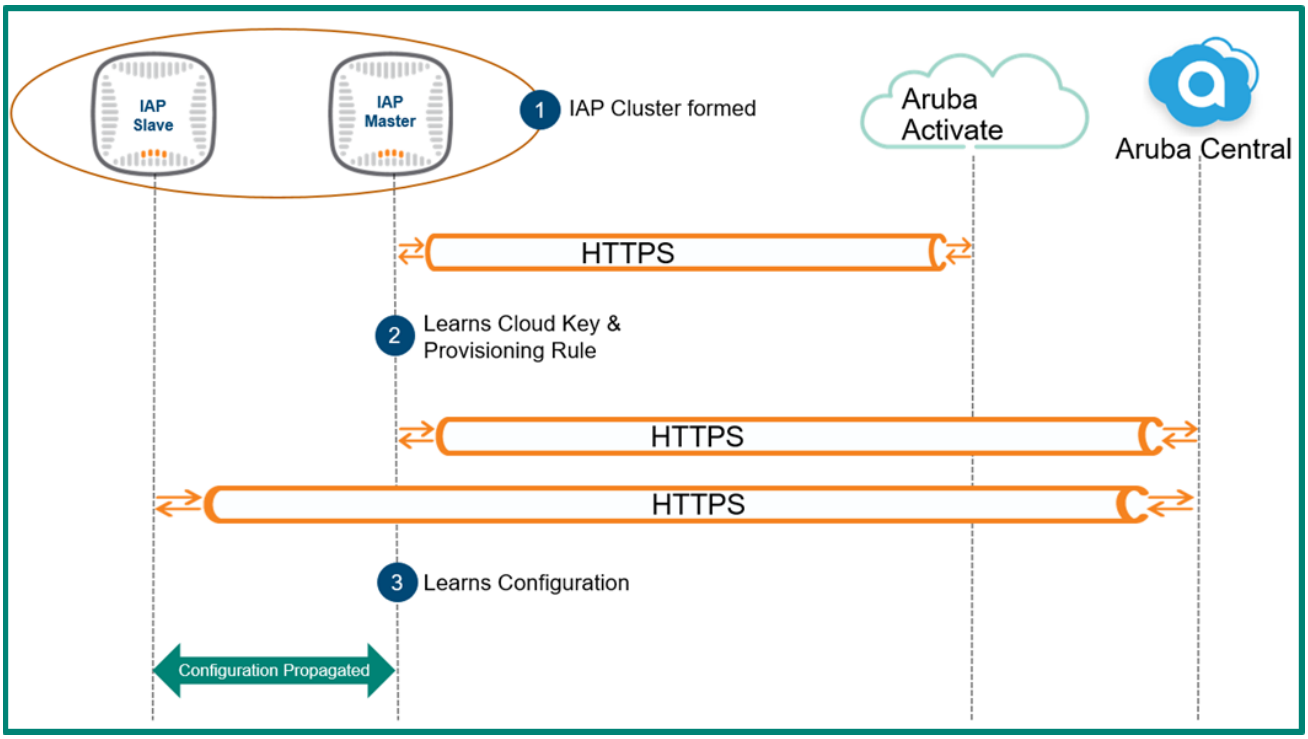


Figure 3-7 *Device Provisioning Process*

Service Subscription

Some organizations may require additional functionality for depending on the services needed for the network which may be added using service subscriptions. These subscriptions are different than Device Management subscriptions and cannot use the “Auto Assignment” feature. E.g., if three services are required in an IAP cluster of 4 IAPs then 12 service subscriptions are needed (3 service subscriptions for each of the 4 IAPs) in addition to 4 Device Management subscriptions. These services are highly customizable and organizations may pick and choose which are relevant for their deployment. E.g. if presence data doesn’t need to be collected for warehouse APs, then those APs will not be assigned a service license.

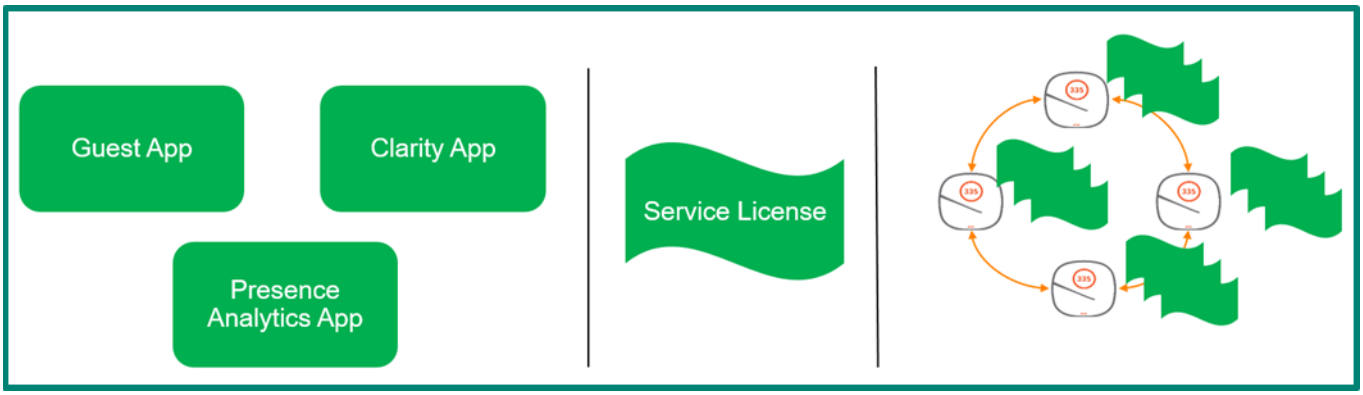


Figure 3-8 *Service Subscription Assignment*

Subscription Expiration

If the subscription of a device being managed by Central expires and a valid subscription is available then the device is automatically assigned to that license and will remain connected to Central. There is no device specific expirations, rather only the expiration subscription key will expire. If no valid subscription is available then the device is disconnected from Central and will wait for next provisioning cycle update from Activate and is moved to default folder. During the next provisioning cycle the device will not receive a provisioning rule from Activate since it is in the default folder and therefore will not connect to Central.

The local UI of the IAP will be fully functional and the device will operate using the last good configuration received from Central. It will not be reset to factory defaults. Central users will still be able to login into the Central portal where new subscriptions may be added and assigned to devices. Devices with the expired subscription will be displayed as down in Central and if needed can be removed by following the method outlined here. If a subscription will expire within 90 days an email is sent to Central admin users.

Central Subscriptions commence their countdown from the date of purchase, not the date when they are entered into Central system.

Organization

There are three major non-hierarchical (cannot be nested) categories used to define devices for purposes of configuration and monitoring which are referred to by Central as Constructs:

- Groups
- Labels
- Sites

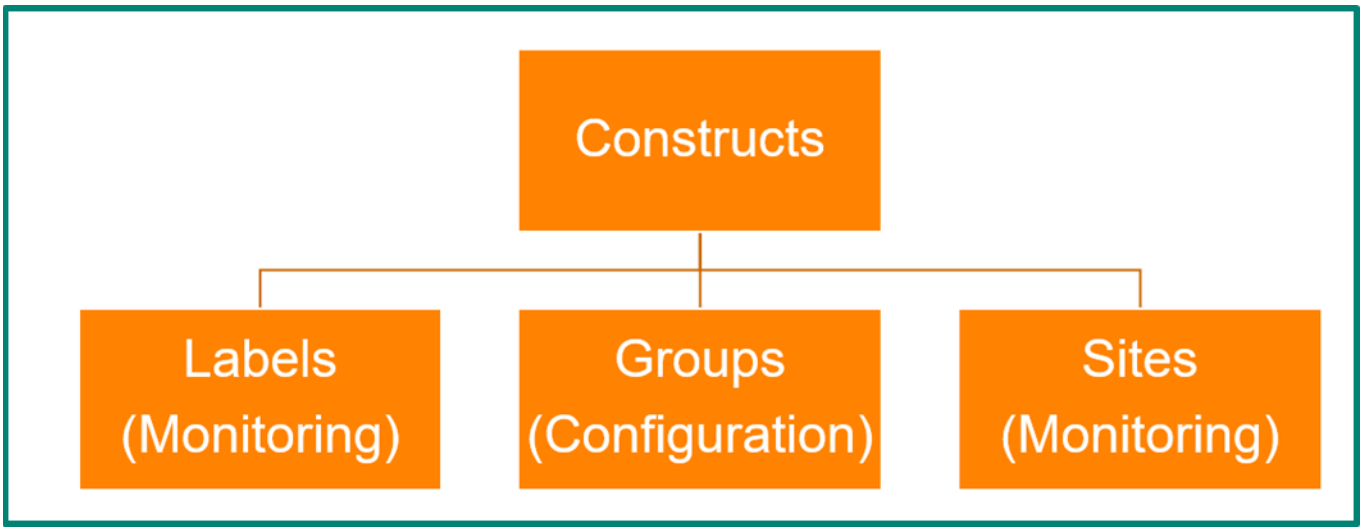


Figure 3-9 *Constructs in Aruba Central*

Aruba recommends planning and creating constructs for devices prior to onboarding. Constructs can be created after device onboarding as well however doing so prior to the onboarding process will facilitate the process.

Groups

Groups are mutually exclusive configuration containers in Central which can also defined as a group of devices sharing common configuration settings. Additional information about groups can be found here. Groups may be defined according to the following criteria:

1. There can be several different groups defined in Central.
2. A group can have multiple devices and multiple device types.
3. A device can be part of only one group at one time.

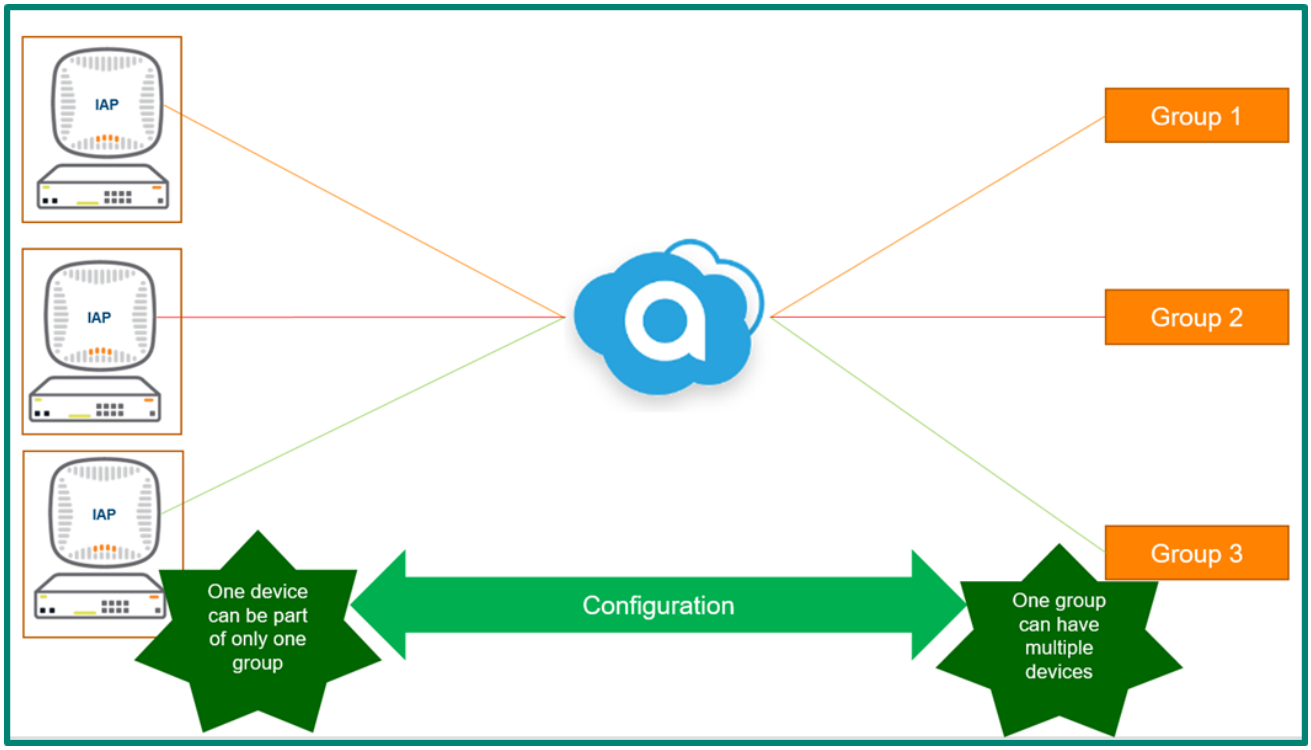


Figure 3-10 *Groups and Configuration in Central*

In addition to configuration, groups are used for other structures and monitoring as well. E.g.:

- **User management** - A user can be granted a role and limited per group
- **Device status and monitoring** - View status and performance for devices in a group
- **Report generation** - Run reports per group
- **Alerts and notifications** - View and configure notification settings for groups
- **Firmware upgrades** - Enforce firmware compliance across all devices in a group

There are two types of Groups in Central:

- **User Interface Groups** - UI groups refer to the device configuration constructs that allow customization and management of configuration parameters through the UI. E.g., the APs in a UI group can be configured through the Wireless Management app while Aruba switches can be configured using the Wired Management app.
- **Template Groups** - Template groups allow admins to customize and manage device configurations through CLI-based configuration templates. Devices with similar configuration requirements may be combined into a single template group and a common configuration template can be pushed to all group members.

Template groups as well as UI groups may both exist together in one Central account.

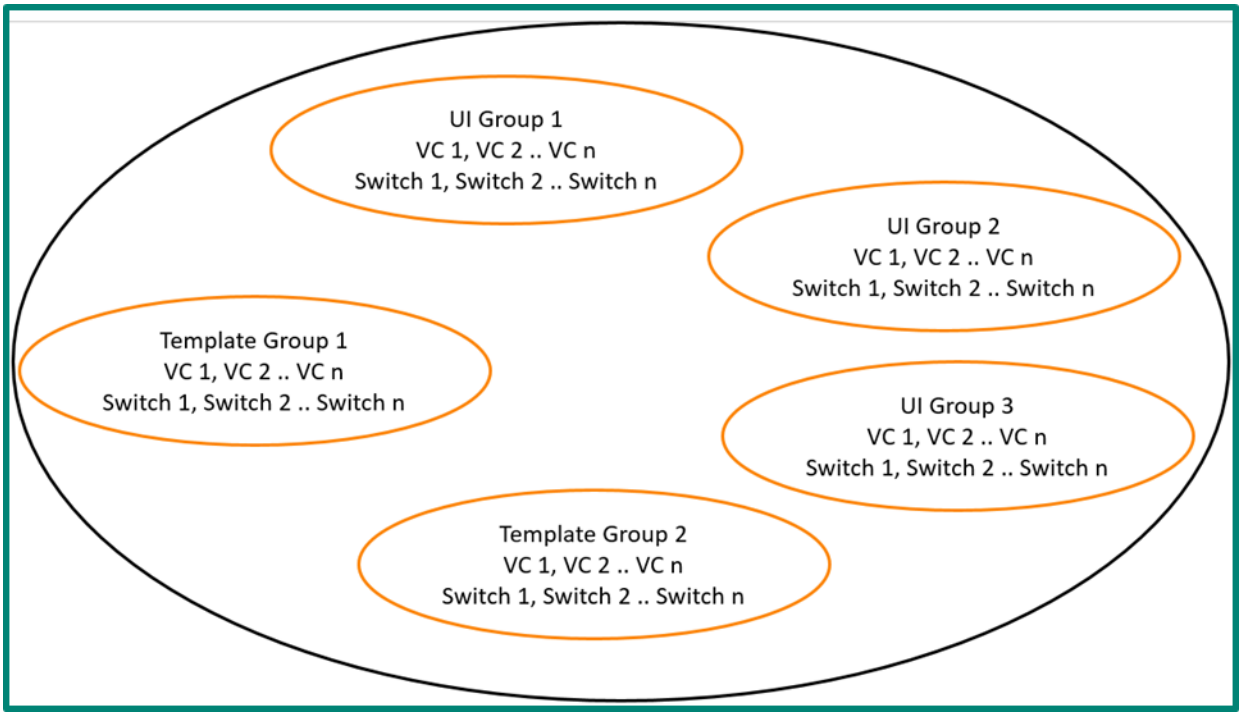


Figure 3-11 *Multiple VCs and Switches in a Single Group*

User Interface Groups

User Interface Groups are Groups that allow users to customize and manage device configuration through GUI workflows. Each UI Group can hold configurations for multiple different device types. E.g., the IAPs in a group can be configured using the menu options under the **Wireless Management** application. Similarly, Aruba switches can be configured using the **Wired Management** application.

Not every configuration possible in a device's local UI will necessarily be available as a knob in Central UI groups. In such cases it may make sense to use Template Groups or use the following method to configure IAPs with options not available through Central.

A password is required for creating a UI group which Central will also use as the password for all group members in lieu of the default password. As a result the group password becomes the device login password as well. The password may can be changed in future from Central UI at any time.

The same wireless configuration is propagated down to all IAP clusters within a UI group and the same wired configuration is propagated down to all Switches. It is possible to define device-specific configurations in addition to group configurations, e.g. changing the hostname of device.

Virtual Controller (VC) parameters such as the VC name can be defined at the group level. These configurations do not cause an override in the group configuration and are a built in feature of groups since groups allow specific per device fields to be changed for each device and VC.

The diagram depicts two clusters: one in San Francisco with two IAPs and one in Los Angeles with one IAP with the hostname and VC name are configured as examples. Note that this does not cause an override:

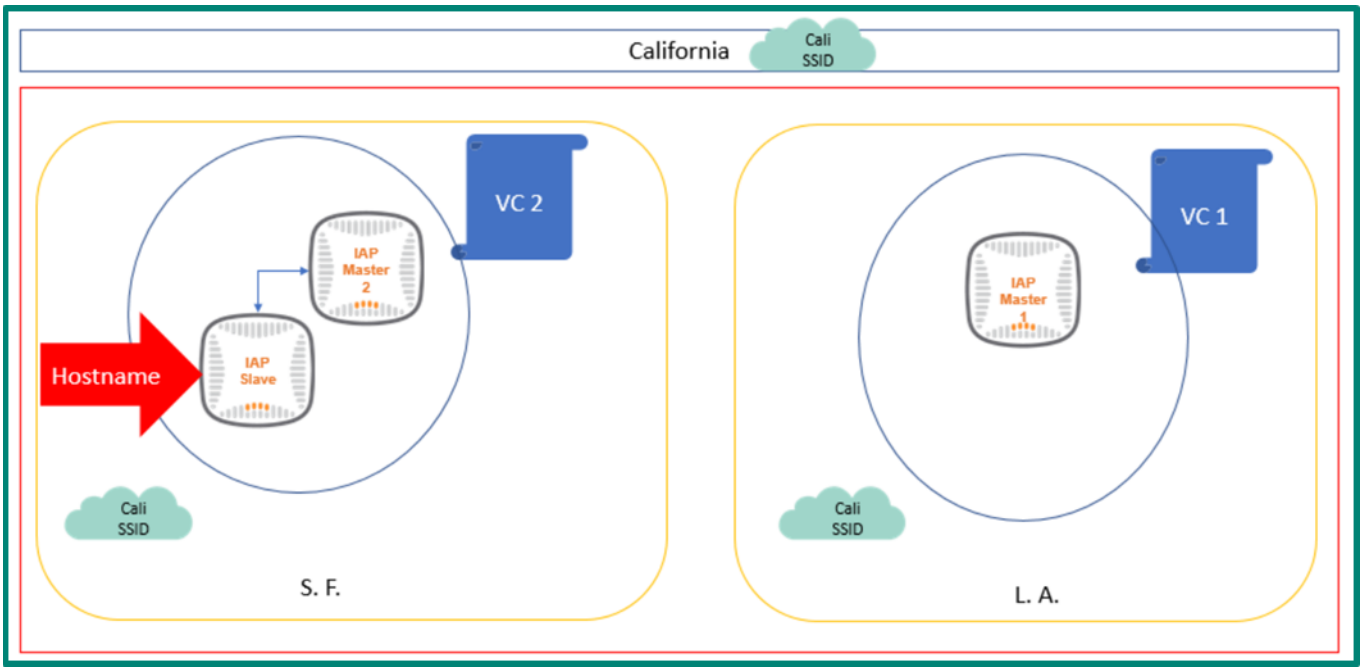


Figure 3-12 *Group Configuration without an Override*

A group's complete wireless and wired configuration can be overridden at an IAP cluster level or switch level if required. E.g., the SSID to VLAN mapping for the San Francisco cluster can be overridden from the group mapping of 10 to 20 and the SSID to VLAN mapping for the Los Angeles cluster can be overridden from the group mapping of 10 to 30.

Nearly can every group configuration element can be overridden for each cluster. E.g., RADIUS server configurations for the San Francisco cluster can be overridden to 192.168.20.100 and for can be overridden to 192.168.30.100 for the Los Angeles cluster.

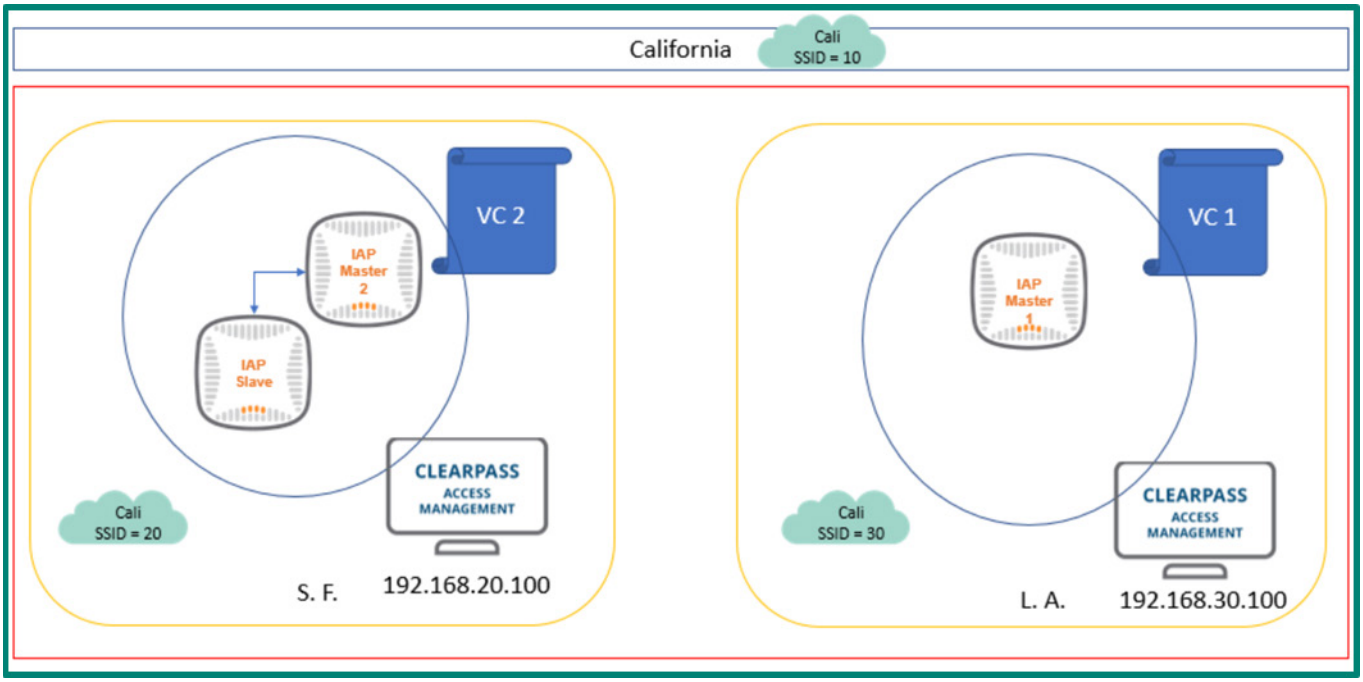


Figure 3-13 *Group Configuration with an IAP Cluster Local Override*

Similarly two switches that are part of the same group could have every element of their configuration overridden. E.g., a San Francisco switch has VLAN 1 while a Los Angeles switch has VLANs 1 and 2. Local ports on switches can also be shut down if desired.

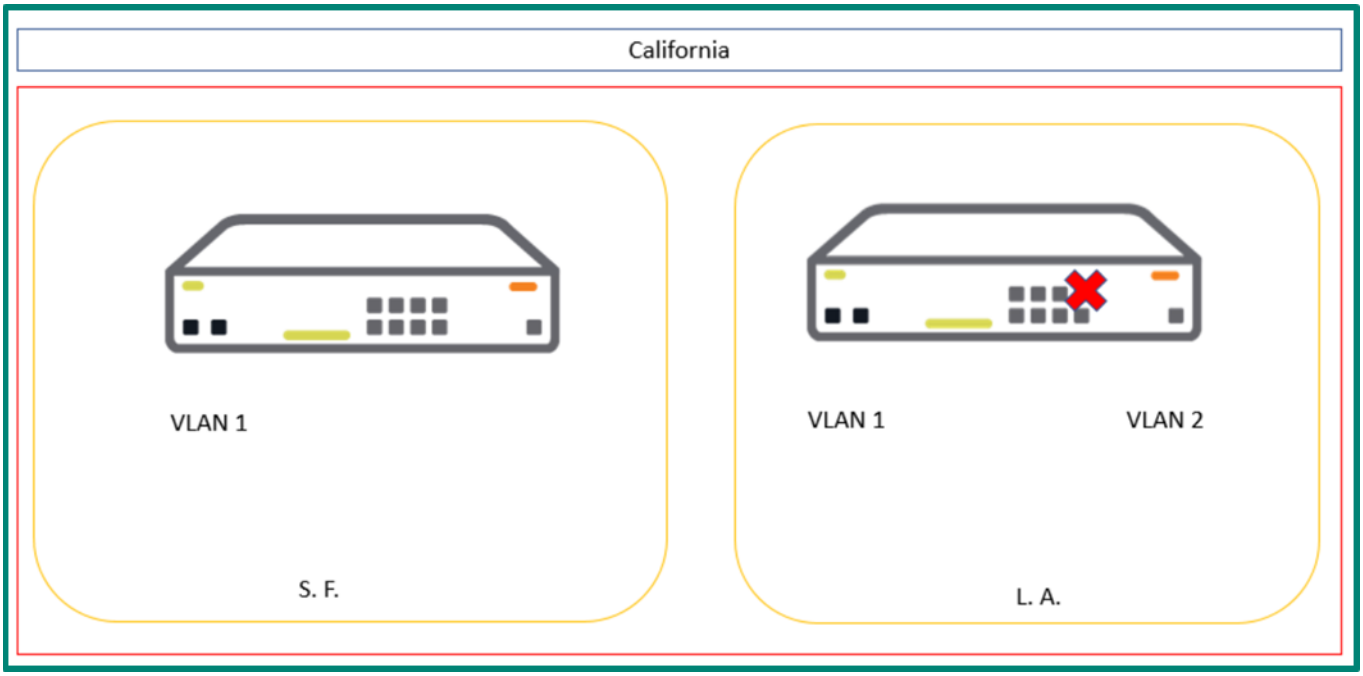


Figure 3-14 *Group Configuration with a Switch Local Override*

These configurations are referred to as *local overrides* and can be resolved using the configuration audit feature in Central. Upon removing a local override, the group configuration is enforced again on the devices.

NOTE

The override feature for groups should be used to treat exception configurations only and should be used rarely.

Aruba Switches have a feature in UI groups called CLI snippets that can be used to push CLI configuration snippets to the following devices:

1. All switches in a group
2. All switches of a specific model in a group
3. All switches running a particular software version in a group
4. A particular switch in a group

Nearly any configuration that can be entered on the CLI prompt of the switch can be pasted in the CLI snippet box, pushed to the device, and saved in memory. However, this process can only be performed once and will not be implemented on any new switch added to the group in Central. In addition, if the switch is factory defaulted then the CLI snippets will not be pushed again.

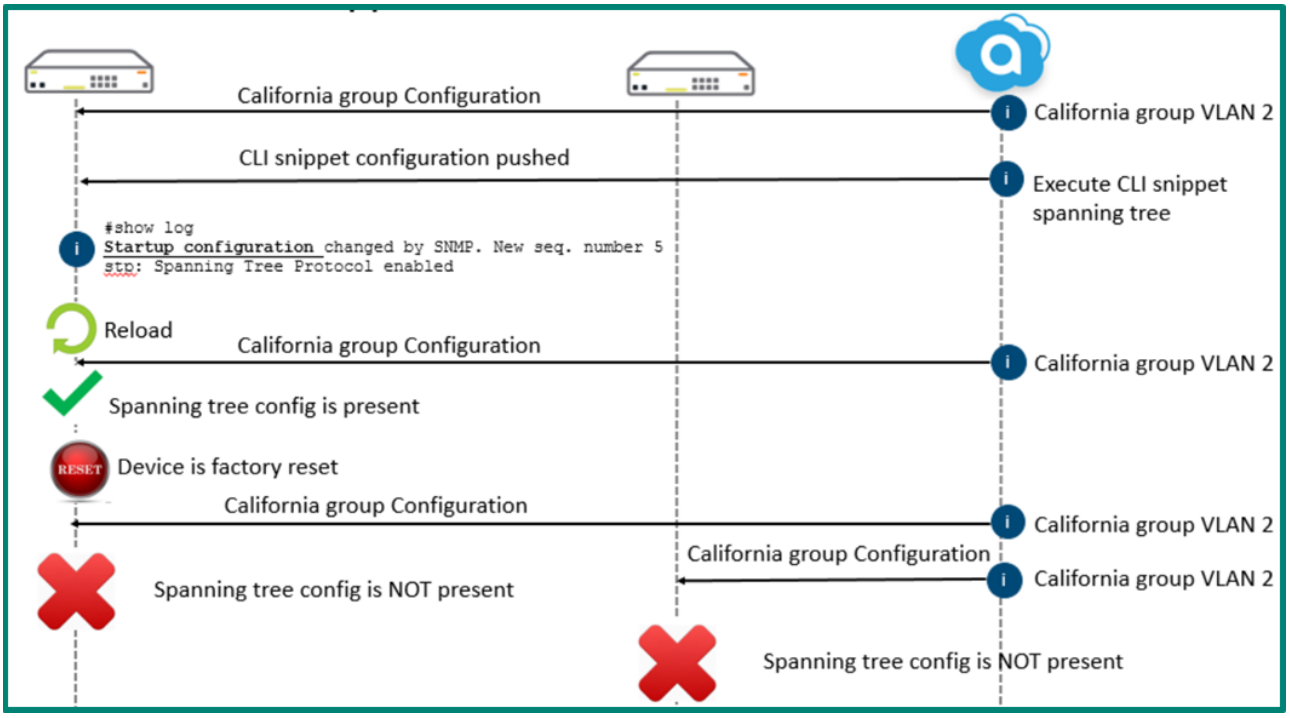


Figure 3-15 *CLI Snippets are not pushed upon a Switch Factory Reset*

The CLI snippet feature should only be used for configurations which are not managed by Central UI groups since configurations managed by Central UI groups are audited by Central. E.g., VLAN configuration is supported in Central UI Groups and the whole VLAN section and sub commands would be audited and overwritten so CLI snippet would not be useful. Additional information on CLI snippet configuration can be viewed here.

Template Groups

Template groups are based on industry standard method of automated network deployments where a template and variables are combined to generate configuration for devices. They are based on CLI configurations with a minimal usage of the UI, therefore it is imperative that administrators implementing Template Groups have strong knowledge of CLI configurations. There are less knobs to control compared to UI groups and they can be easily controlled with APIs which makes Template Groups suitable for automation. Since Central generates a complete CLI configuration for the device, practically any feature that can be configured on device CLI can be achieved.

Template groups are ideal for large scale deployments with cookie cutter designs e.g. a service provider with thousands of stores to manage that have similar configuration in stores and a small number of differing configuration elements. Template groups also allow an administrator to define individual device settings, e.g. hostname, channel, power etc. before the device comes online and is active in Central. UI groups on the other hand require the device to be up in Central before the same settings can be configured. Central administrators typically need to create multiple groups. The following operations help to simplify the process:

- **Clone** – A group's configuration can be cloned completely into a new group with a different name. It is not possible to clone a template group.
- **Delete** – A group can be deleted. It is not possible to delete the Default Group.
- **Move Devices** – Devices can be moved from one group to another group. It is possible to move devices from a UI group to a template group.

Additional details regarding groups can be found here.

Sites

A site in Central refers to a physical location where a set of devices are installed; for example, campus, branch, or venue. Sites have the following attributes:

- A site has a unique address associated to it
- Sites can be used to simplify device onboarding via Install Manager app
- Sites can be used to monitor the Network via Health Dashboard and Clarity app
- A device can only be assigned to one site at a time
- Central supports bulk creation of sites via CSV upload

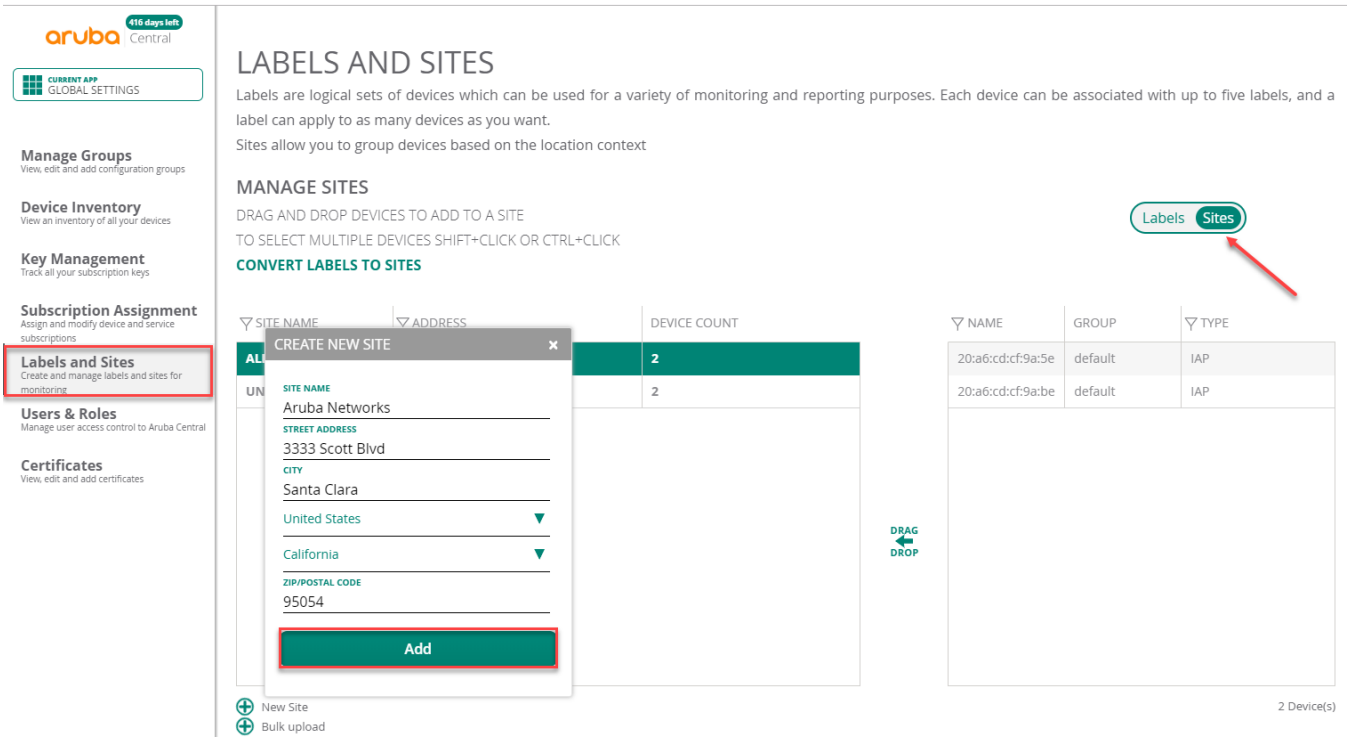


Figure 3-16 *Adding Sites*

Labels

Labels are tags attached to a device provisioned in the network. Labels determine the ownership, departments, and functions of the devices. Labels may be used for creating a logical set of devices and as filters when monitoring devices and generating reports.

E.g., consider an IAP labeled with the labels “Building 25” and “Lobby”. These tags identify the location of the IAP within the enterprise campus or a building. The IAPs in other buildings within the same campus can also be tagged as Lobby. To filter and monitor IAPs in the lobbies of all the campus buildings, you can tag all the Instant APs in a lobby with the label of Lobby. Labels are primarily used as a filter for monitoring data and have a dedicated Health Dashboard. A device can only be assigned maximum of five label tags.

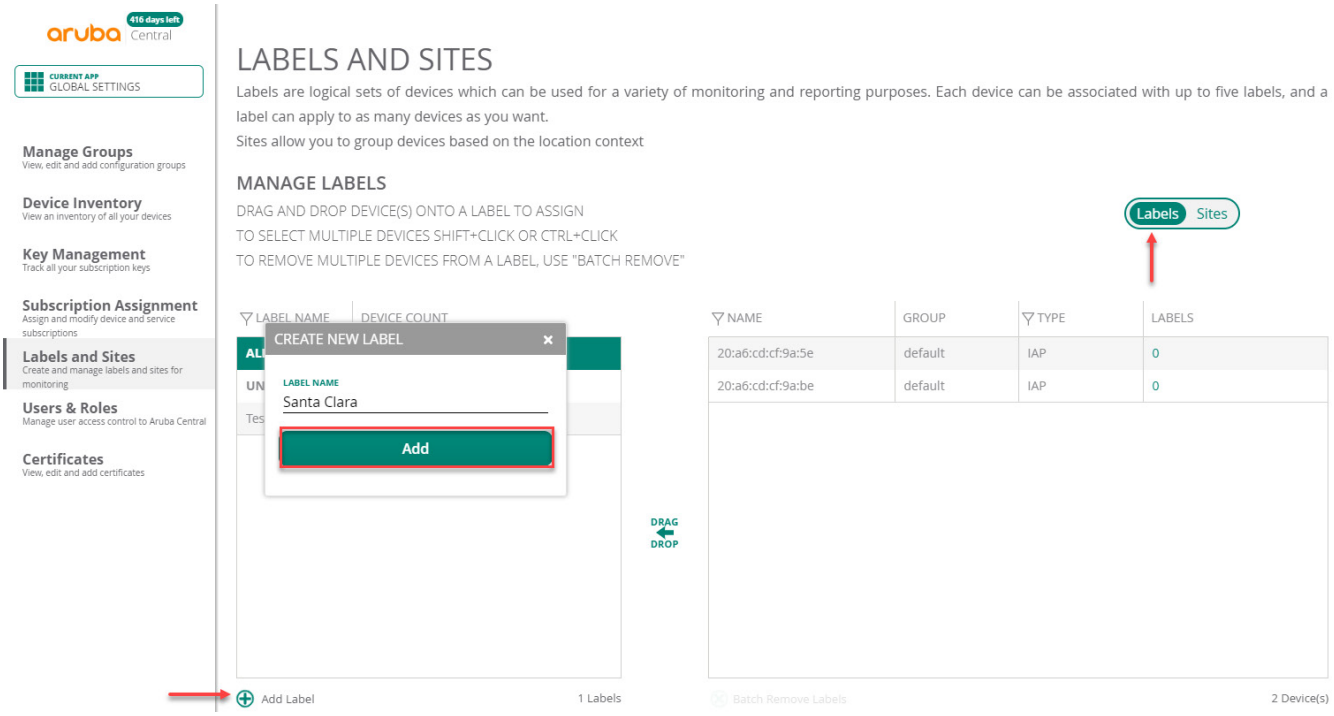


Figure 3-17 *Adding Labels*

Organizational Comparison

Topic	Label	Site	Group
Purpose In Central	Monitoring Construct	Monitoring Construct	Configuration Construct
Hierarchical	No	No	No
Bulk Creation	API only	Yes	API only
Location Context	No	Yes	No
Number per Device	5	1	1
Contains Multiple Devices	Yes	Yes	Yes
Assignment Prior To Central	No	Via Install Manager App	Via Pre Provisioning and Install Manager Apps
Install Manager Can Assign	No	Yes	Yes
Client Overview	Yes	Yes	Yes
Generates Searchable Reports	Yes	Yes	Yes
Creates Filterable Alerts	Yes	Yes	Yes
Topology View	Yes	No	No
Granular AppRF Information	No	No	Yes
Health Dashboard	Label Health	Network Health	No
Maintenance App	No	No	Yes
Presence Analytics App	No	Yes	No
Clarity App	Yes	Yes	No
Users Limited To A Construct	No	No	Yes

Table 3-1 *Organizational Comparison*

On-boarding Workflows

The process of aligning devices into different constructs can is referred to as onboarding. There are many ways to onboard devices in Central which will be outlined below:

Greenfield Deployment

New installations generated from scratch are called Greenfield deployments.

1. Devices are packed in boxes and shipped directly to the actual site/location/branch

Step	Details
Groups	Use Install Manager and Installer app to assign group
Sites	Use Install Manager and Installer app to assign site
Labels	Drag and drop devices to labels after they come up on Central

2. Devices are packed in boxes and shipped to one central staging location

Step	Details
Groups	Pre Provision devices into groups
Sites	Drag and drop devices to sites after they come up on Central
Labels	Drag and drop devices to labels after they come up on Central

3. Devices are plugged in and powered up with their default configuration and can access internet

Step	Details
Groups	Devices are moved to a different group after they show up
Sites	Drag and drop devices to sites after they come up on Central
Labels	Drag and drop devices to labels after they come up on Central

The workflow depicted below is recommended by Aruba and consists of the following key features:

- Devices are shipped directly to branch site locations
- No manual overhead of tracking device inventory and their shipped sites
- Installers can self-validate device installation status
- Network administrators can track site installation progress using the install manager app

The diagrams below explain the complete process of an install done via using this workflow:

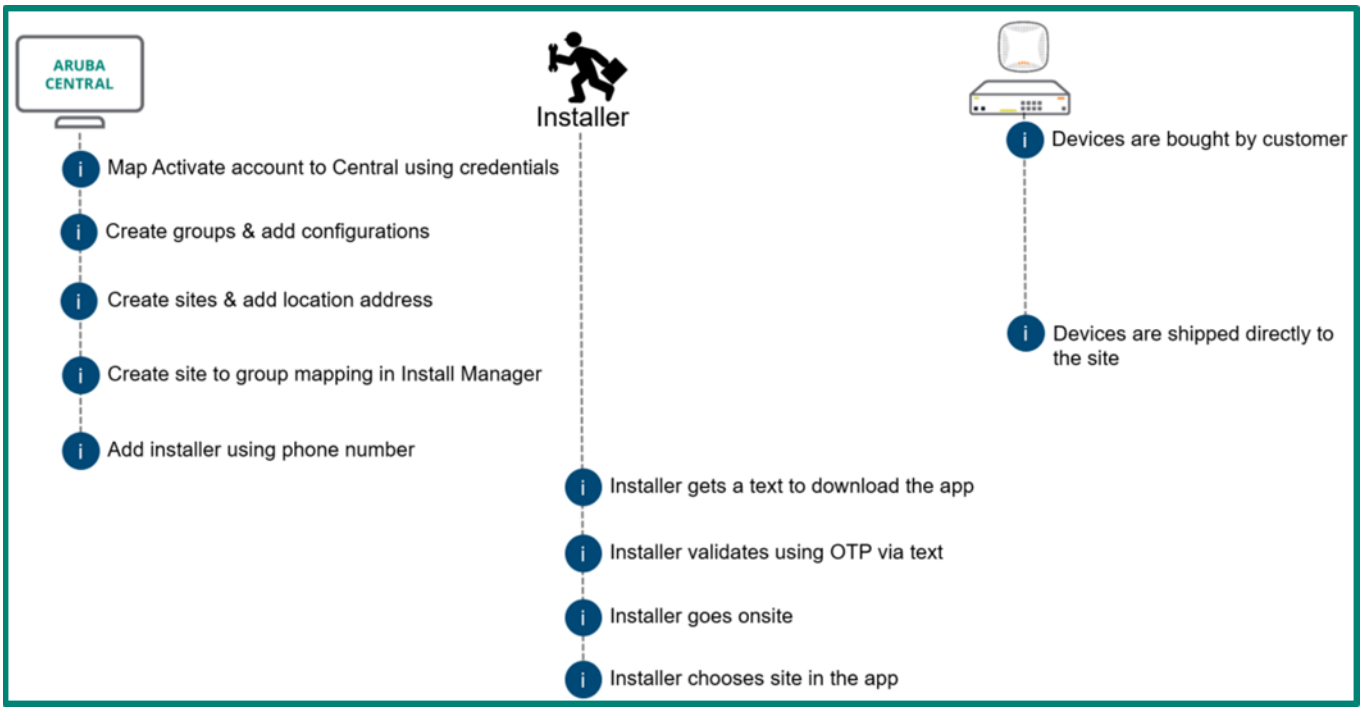


Figure 3–16 *Installer Workflow*

1. Customer buys the devices and Central subscription key from Aruba
2. Devices are shipped directly to the branch site locations
3. An Activate account is automatically created based on customer information on the purchase order and the devices are added so said account
4. Customer requests access to Activate account and creates a login
5. Customer registers for a Central evaluation
6. Customer adds the Central subscription key in the account created in previous step
7. Customer adds the Activate credentials in the Central account to create a mapping
8. Central's device inventory is populated with all devices sold to the customer
9. Customer designs Central constructs based on requirements i.e. label, site, groups
10. Create groups in Central and add configuration
11. Create sites in Central and add location information
12. Map groups to sites in the Install Manager app in Central
13. Add installer using phone number and assign sites in Install Manager app in Central
14. Installer receives a text prompting them to download the Installer app

15. Installer validates using OTP via text
16. Installer goes onsite and chooses the correct site in the Installer app

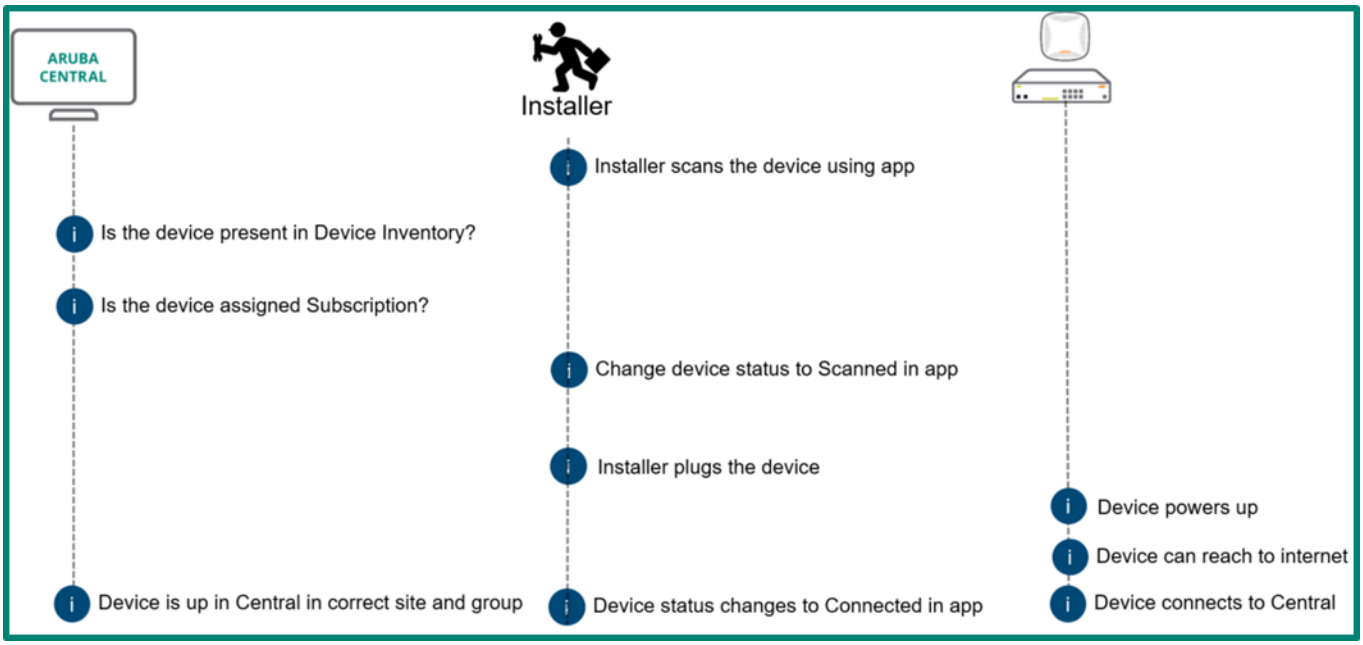


Figure 3–17 *Installer Workflow Cont.*

17. Installer scans the device using Installer app
18. Central checks to see if the device is present in the inventory of the Installer's Central account
19. Central checks to see if the device is assigned a device management subscription
20. The device's status changes to "scanned" in the Installer app
21. Installer connects the device to the network
22. Device powers up, checks its reachability to internet, and connects to Central
23. Device comes up in Central under the correct site and group
24. Device status changes to "Connected" in the Install app

Brownfield Deployment

Installations where customers migrate from another other management device e.g. AirWave are called Brownfield deployments.

1. Devices are plugged in and powered up with a Non-default configuration and can access internet. Their configurations need to be overwritten with configuration in Central.

Step	Details
Groups	Devices show up in an unprovisioned group, then are moved to another group
Sites	Drag and drop devices to sites after they come up on Central
Labels	Drag and drop devices to labels after they come up on Central

2. Devices are plugged in and powered up with a Non-default configuration and can access internet. The configuration on the device has to be preserved and converted into a Central group.

Step	Details
Groups	Devices show up in un provisioned group and then used to create a group
Sites	After devices come up in Central, drag and drop to sites
Labels	After devices come up in Central, drag and drop to labels

Any device currently managed by AirWave will not go out to Activate to learn about the new provisioning rule because if an AirWave configuration is present on an IAP, then the IAP will assume it has already been provisioned and will skip any provisioning steps.

AirWave either has to reset the device to factory defaults or remove the current AirWave configuration and provisioning method from the device which will make the device to reprovision itself using Activate.

Device Group Provisioning Pre-Installation

Automatic Provisioning

If a site to group mapping already exists in the install manager app then when the device is assigned the mapped group when it comes online at the site. For additional details please refer to Greenfield Deployment.

Manual Provisioning

Once groups have been configured, the inventory has been populated, and licenses have been allocated, the devices can be provisioned into their respective groups. This can be done prior to device installation.

E.g., the ACME Company has created 3 groups based on user access requirements, monitoring, and configurations. Each group has a different SSID based on the state where the IAPs will operate:

- California
- Texas
- New York

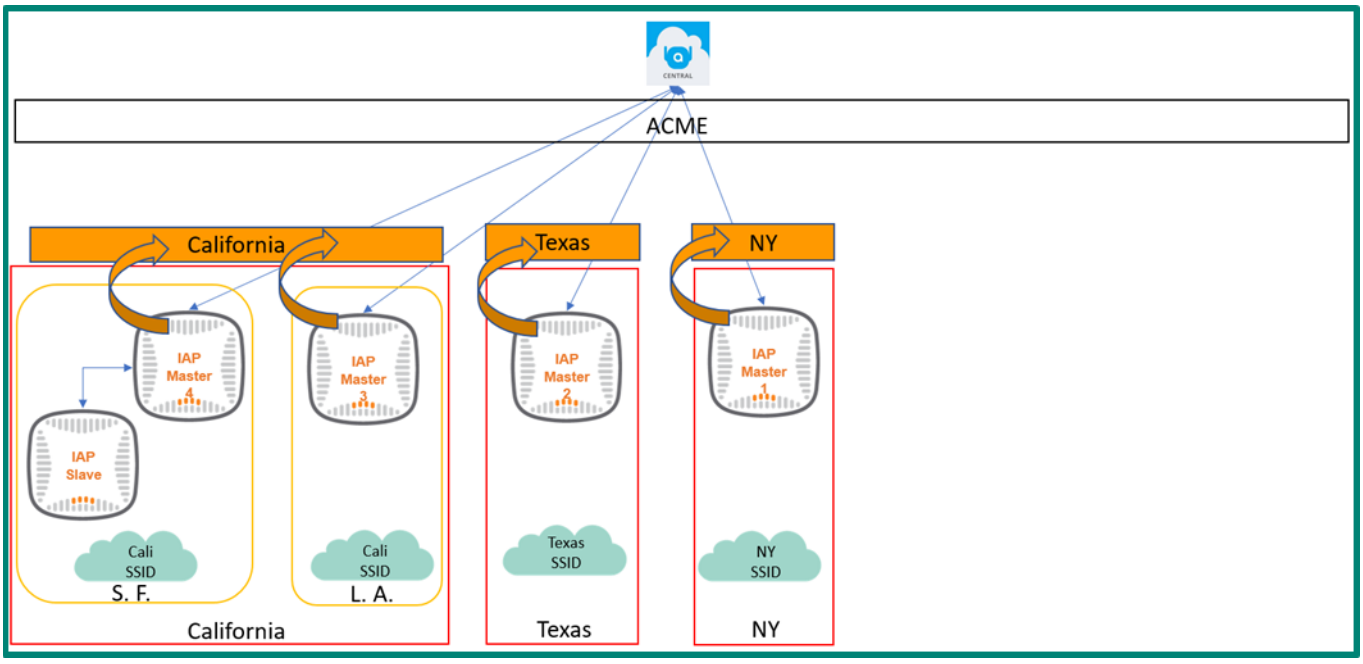


Figure 3-18 *Manually Provisioning Multiple Groups*

In the example above the California location has multiple clusters whereas Texas and New York have only one cluster each. Devices land into their respective groups since they have been preprovisioned with their respective groups.

Device Group Provisioning Post-Installation

Default Configuration

A default group is already defined in Central. If a device is not preprovisioned with a group but still assigned a subscription it will be placed in the default group when it comes online if it has a default configuration.

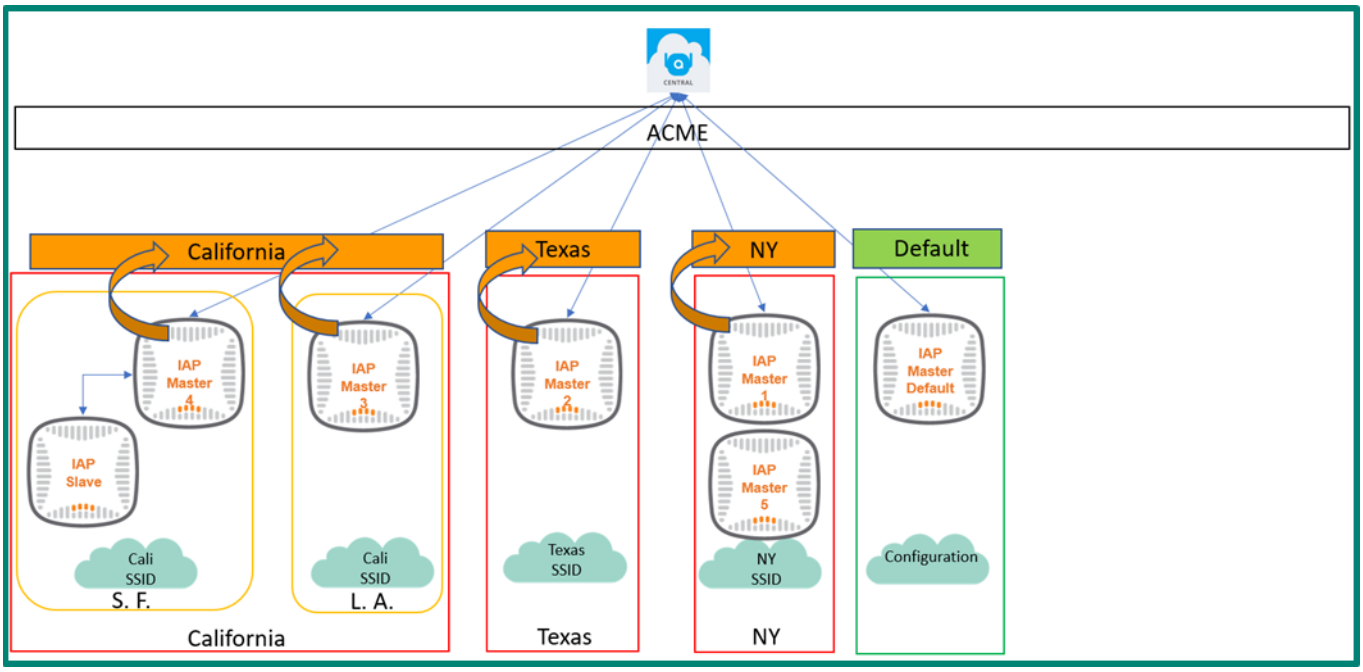


Figure 3-19 *Unprovisioned Device on Default Configuration Placed in Default Group*

Non Default Configuration

If device has any existing configuration such as in the case of a migration customer then it is moved to the unprovisioned section. A group configuration can then be generated and a new group created from the existing device configuration in the unprovisioned section. This unprovisioned workflow is typically appropriate and useful for customers migrating to Central. In this example a new group named “Portland” is created using existing configuration on IAP Master 5.

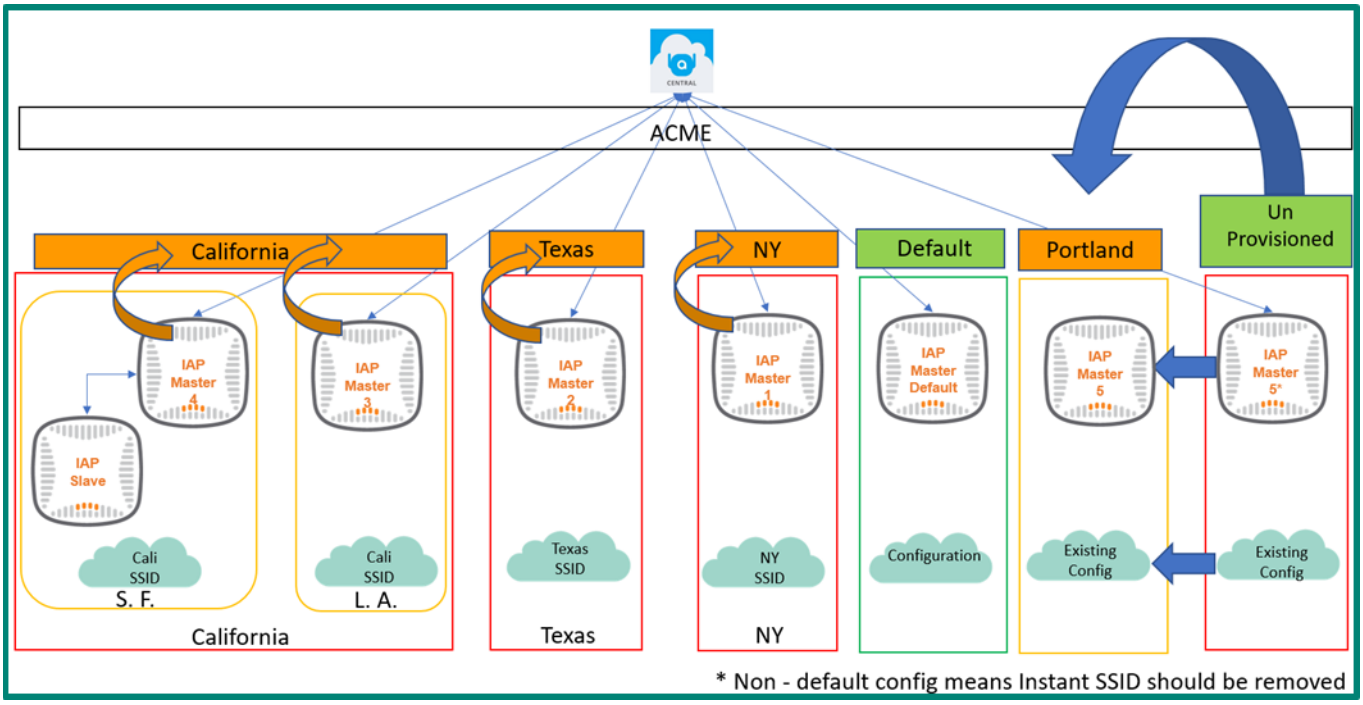


Figure 3-20 *Creating a Group Using Existing Configuration via Unprovisioned Group*

NOTE

The workflow shown above does not apply to switches. Aruba switches can only join Central during ZTP if they are running the factory default configuration with a valid IP address and DNS settings from a DHCP server.

Devices in the unprovisioned section can also be moved directly to a pre-existing group.

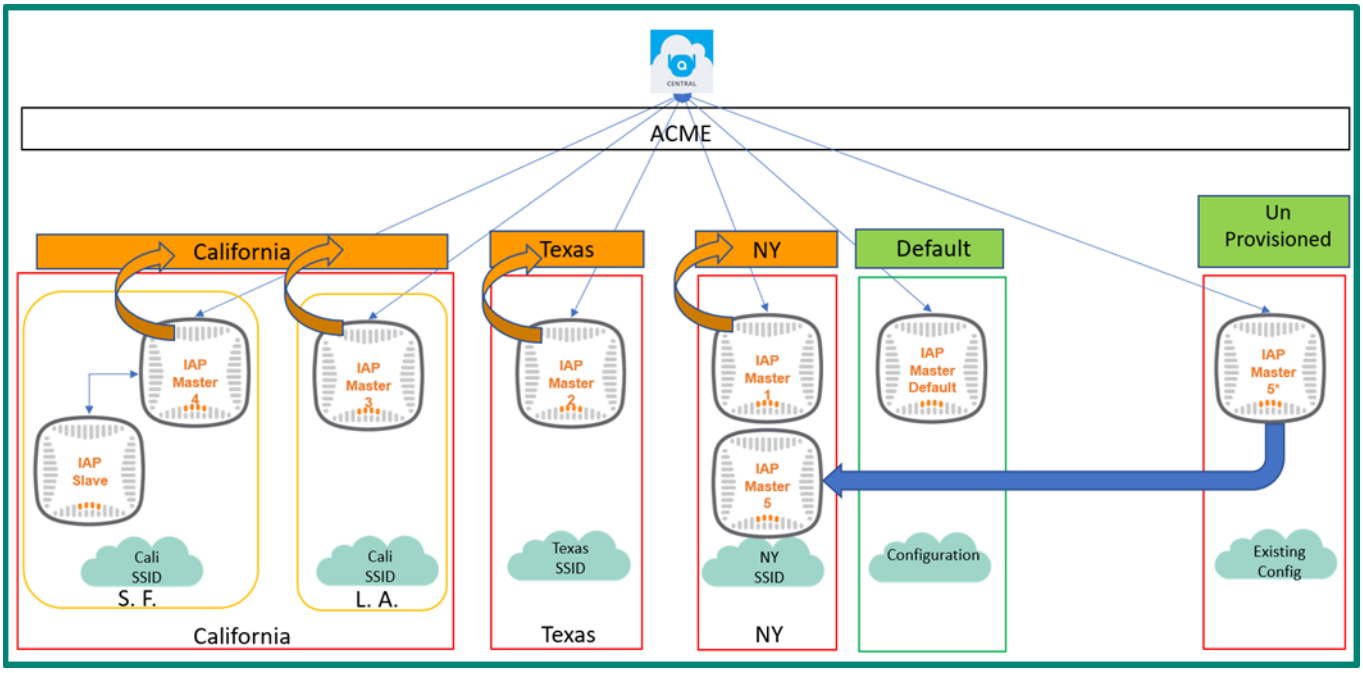


Figure 3-21 *Moving a Device in an Unprovisioned Section to an Existing Group*

Cluster Formation and Auto Join

The figure below depicts a summary of the device provisioning process:

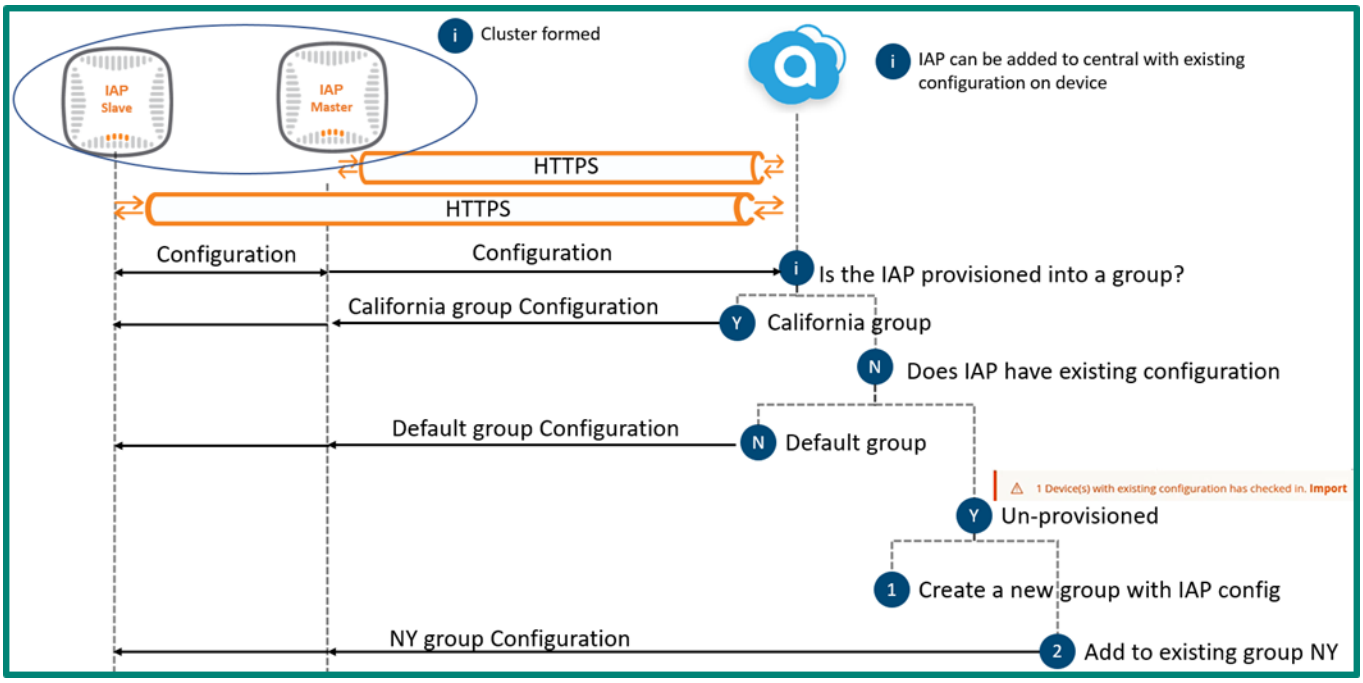


Figure 3-22 *Provisioning Flows*

As seen in the above example, an IAP cluster must be formed before a connection can be established between IAPs and Central. The rule of thumb for IAP cluster election is the IAP with longer uptime generally becomes the Master IAP and all the other IAPs become slave IAPs. There are no primary, secondary, or tertiary Master IAPs, because Aruba believes in a truly distributed controllerless solution where controller functionality is divided between the whole cluster and not just a function of a single IAP. Any IAP in the cluster can play the role of Master IAP. However, the election can still be influenced if needed by using the preferred master feature. For additional details please refer to Chapter 1 of this VRD.

Another important aspect of cluster formation is the software image on the IAPs. Each IAP model could potentially have a different image. E.g., the image of an IAP 325 will differ from image of an IAP 225. However, if both IAPs have to form a cluster, they must run the same software version. An IAP trying to join a cluster will first try to find an existing cluster member of the same model by consulting the master IAP. If it successfully finds one then the IAP attempting to join the cluster will download the image from the existing IAP in the cluster of the same model.

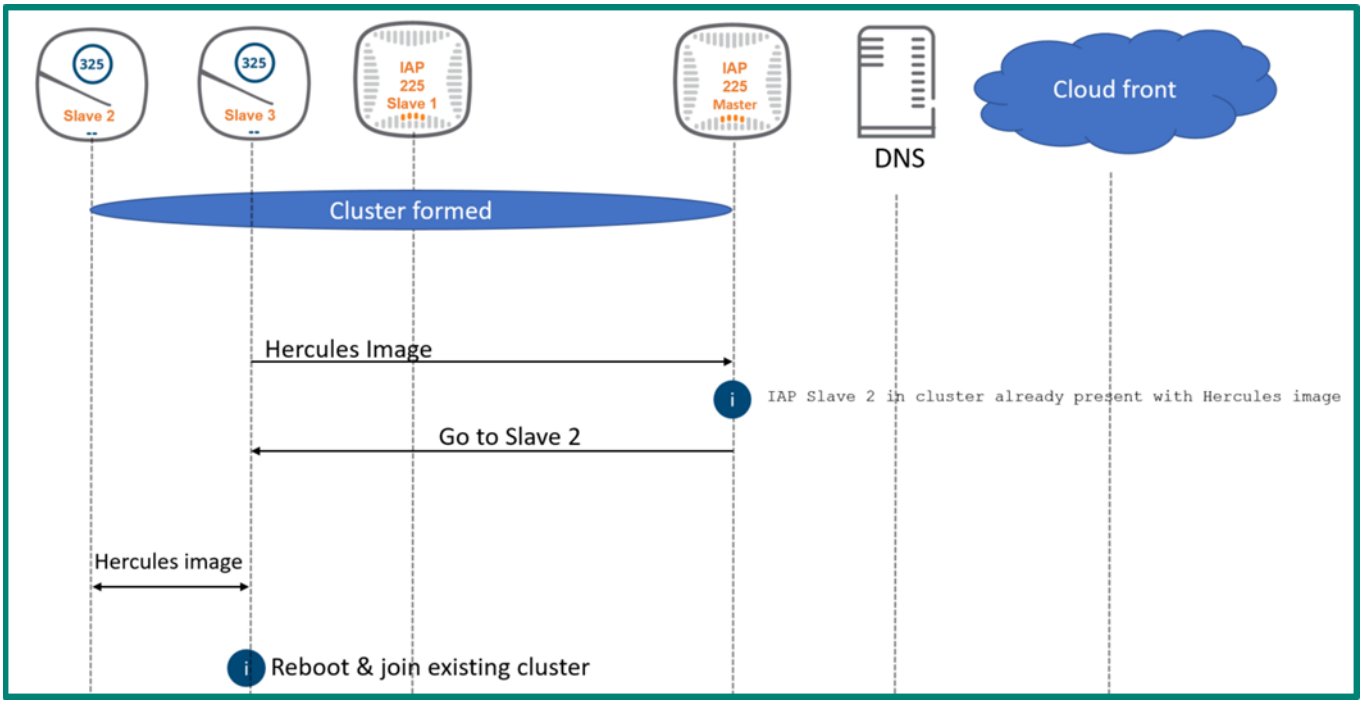


Figure 3-23 *IAP Cluster Formation and Image Upgrade from IAP Cluster Member Seed*

If an IAP of the same model is not present in the cluster then the Master IAP will direct the IAP trying to join to fetch the image from Aruba Cloud Image Server:

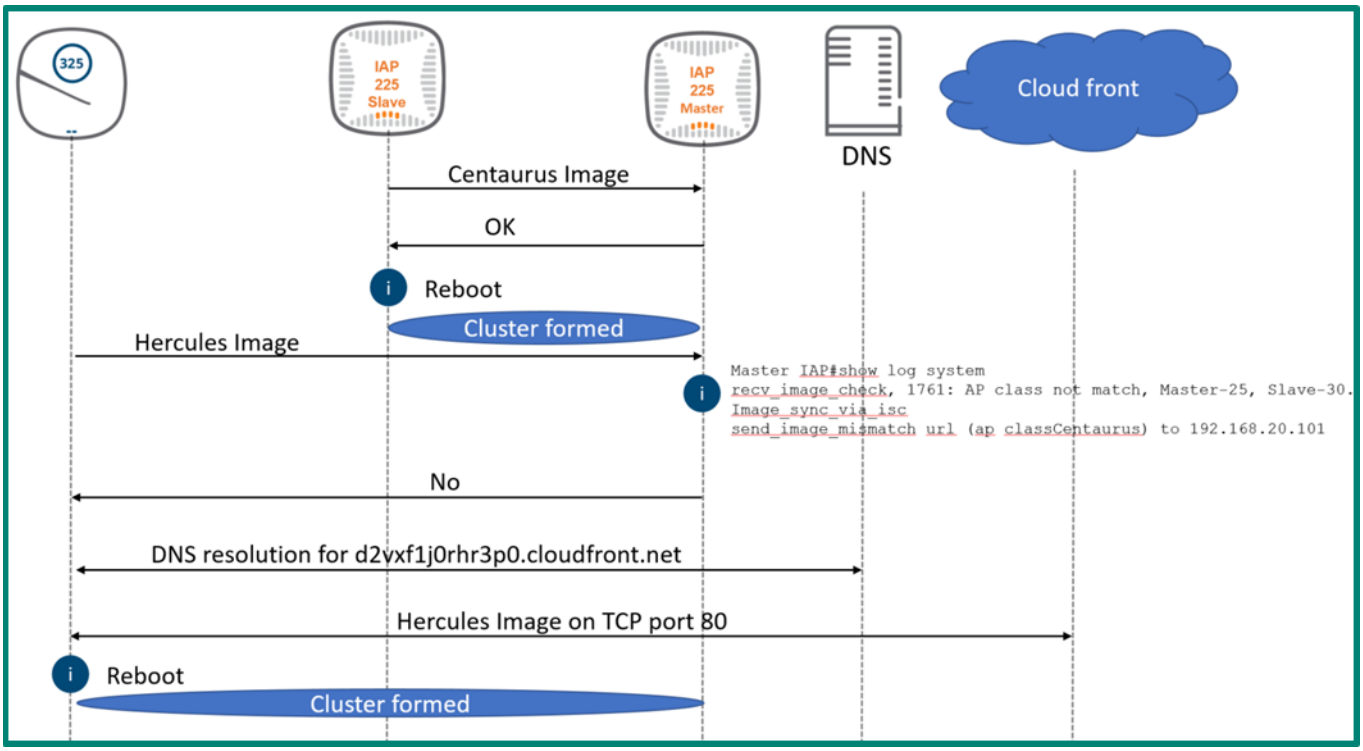


Figure 3-24 *IAP Cluster Formation and Image Upgrade from Cloud*

Aruba recommends creating clusters where all IAPs are of the same model.

Following commands can be used on IAPs to debug any provisioning or cluster formation issues:

```
Show log ap-debug
Show log provision
```

After cluster formation both slave and Master IAPs reach out to Activate but only the Master IAP learns the provisioning rule. The master IAP drives the provisioning process for the whole cluster. HTTPS Tunnel formation consists of exchanging SSL certificates which need the device time to be accurate. When devices communicate to Activate upon bootup they ensure their time is accurate using HTTP headers eliminating dependency on NTP.

An IAP's running configuration has following parameters enabled:

```
allow-new-aps <Enabled Auto Join>
allowed-ap <MAC-address>
```

The MAC addresses are populated based on cluster members. Once cluster is formed Central learns about all current cluster members and adds them as allowed APs. However, to avoid any invalid future cluster members it is recommended to disable the Auto Join feature. Additional details can be found through the following link.

If any new IAPs need to be added in a predetermined window of time administrators have two options:

1. Add the MAC address in the Central UI for the cluster
2. Enable auto join, let IAPs Central learn about the new IAPs and add them in whitelist, then disabling auto join

Monitoring

Central validates device connectivity through the network Websocket connection that device maintains. If Central doesn't receive a status update from device for 5 mins then it marks that device offline. This interval is currently not configurable.

Central provides multiple options to monitor the network:

Health Dashboard

- Context
  - Site
  - Label
- Data Source
  - Summary (All Devices supported by Central)
  - Gateway
- Views
  - Summary View
  - Detailed View
- Indicators
  - Grid
  - Status

The Summary View has a tabular summary of all context elements. E.g. all sites.

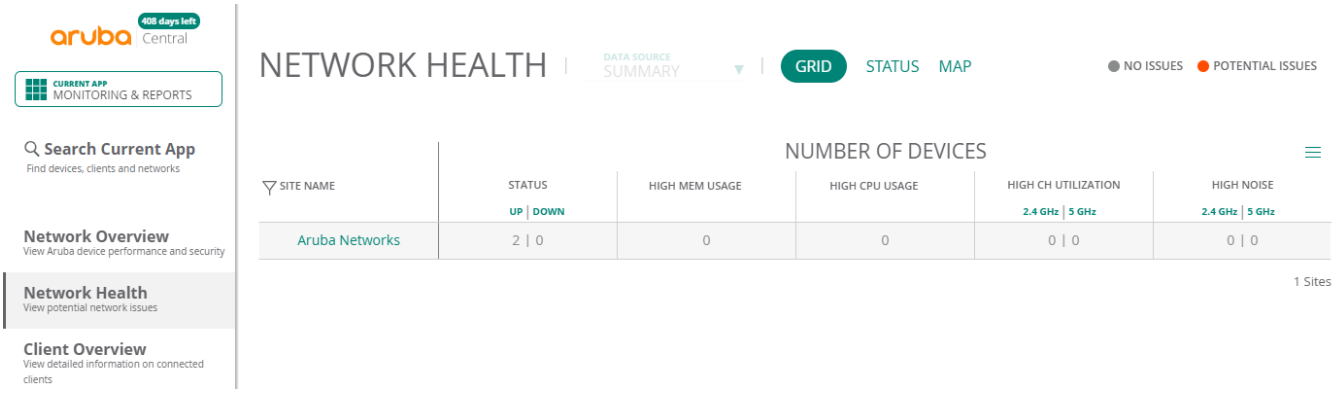


Figure 3-25 *Summary View*

The Detailed View provides more information on each site and is connected to the Topology View as well.

- Change Log
  - Configuration
  - Firmware
  - Reboot
- Summary Statistics
  - Number of wireless clients
  - Wireless bandwidth
- System Health
  - Device Up & Down Status
  - High CPU
  - High Memory
- RF Health
  - 2.4 Ghz Utilization
  - 5 Ghz Noise
- Client Health
  - Connectivity Score – Borrowed from Clarity app

Alerts

Set of combined events can generate an alert with an associated severity level and can be delivered via an email or HTTP webhooks. The following alerts are enabled by default in Central:

Alert	Severity
VC Disconnected	Major
Rogue AP Detected	Major
User Account Added	Major
Switch Disconnected	Major
Switch Detected	Major

Table 3-2 *Alert Summary*

Reference Architecture

There are many ways Central can be deployed to manage networks. This section outlines a couple of use cases that have been solved by using Central as a management solution. The following factors may vary from deployment to deployment:

- Additional Service Apps used e.g. Presence Analytics, UCC
- Groups: UI Groups or Template Groups
- Site Group & Label Structure
- On Boarding Workflow
- Operating Mode: Standard Enterprise or MSP

Consider a scenario where ACME Inc. wants to provide its 10,000 employees across the country an option to work from home.

- Wireless connectivity at employee homes should have access to resources at their redundant corporate data centers, making IAP VPN a better fit
- The UCC app will be used to find voice quality of on premise skype for business calls
- The Guest app will be used to create an additional SSID for each home network
- Each home will be called a site with an associated address. Sites will be created via bulk upload
- Each employee is considered an installer and provided an IAP
- Each employee's name will be a label attached to the AP along with labels of the employee's organization
- Since every feature can be supported via UI groups and there is no need for automation of configuration via API UI groups are a better fit
- Every employee acts as an installer and is given an AP303H to into their home's DSL router
- This is a standard enterprise mode operation of Central
- ACME will create one group consisting of all devices since configuration of each employee's home is identical and employees do not require access to the Central UI
- The IAP VPN SSID will operate in CL2 - full tunnel mode with the exception of IAP - Central communication as it stays outside the tunnel
- The IAP VPN SSID is authenticated from CPPM in the redundant data centers
- IAP VPN tunnels will be created to both controllers in both data centers, however since the IAPs will be able to use only one tunnel at one time load balancing will not be used
- IAP to Central traffic stays outside the IAP VPN tunnel due to the following 8.3 enhancement

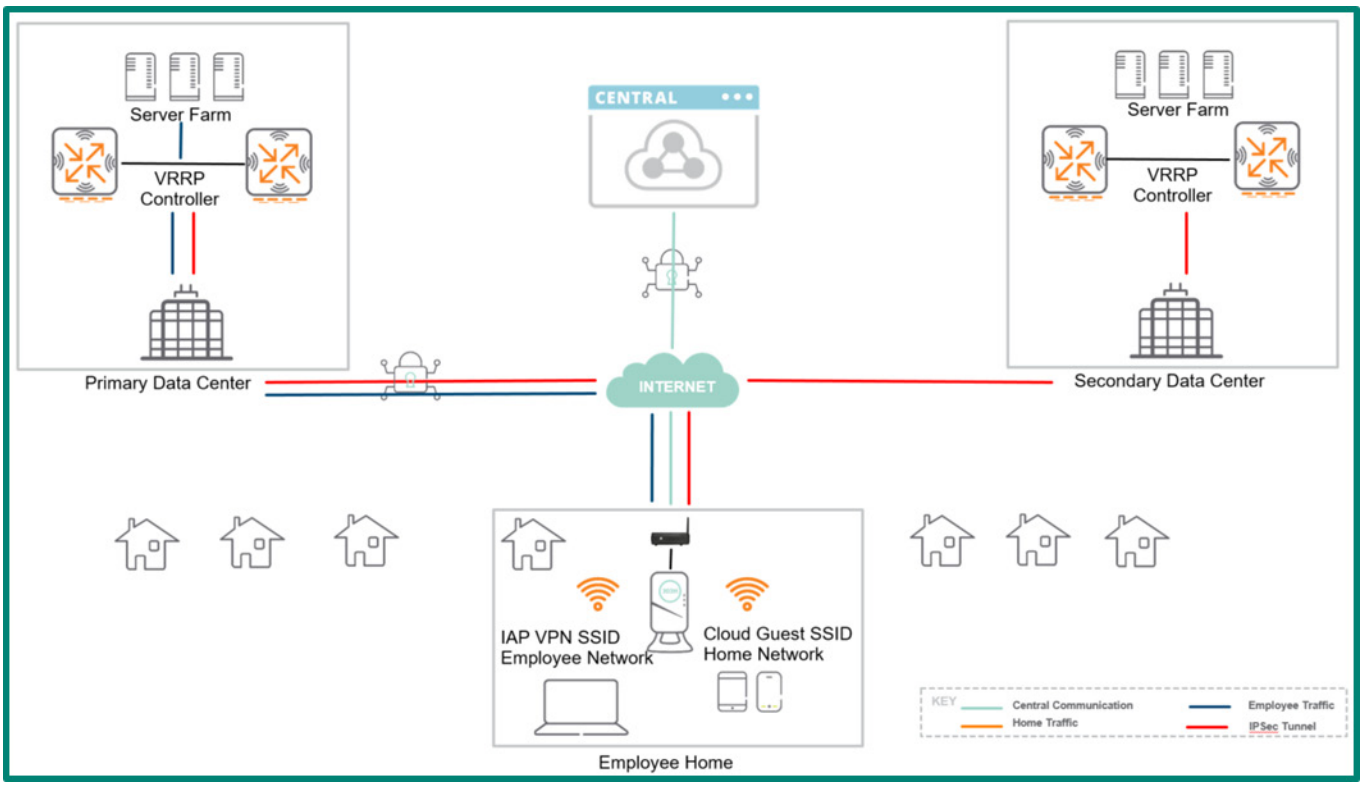


Figure 3-26 *Reference Architecture 1*