ArubaOS 8 Fundamentals Guide

a Hewlett Packard
Enterprise company

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
6280 America Center Drive
San Jose, CA 95002
USA

The following table lists the revisions of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 08	Updated the **Stateful Failover** section of the **Clustering** chapter.
Revision 07	Updated the **Migration to ArubaOS 8** and **AP Modes** chapters.
Revision 06	Removed references of Migration Tool as the Migration Tool is no longer supported.
Revision 05	Updated to the migration from ArubaOS 6.x master-master redundancy to a pair of ArubaOS 8.x standalones.
Revision 04	Updated the reference architecture section to reflect scaling. Also updated clustering sections based on ArubaOS 8.5.0.0 enhancements.
Revision 03	Updated content to reflect changes added in ArubaOS 8.4.0.0.
Revision 02	Updated Controller Mode Comparison, Change of Authorization, and Licensing Concepts.
Revision 01	Initial release.

Chapter 1
About this Guide

Aruba Deployment Guides are best practice recommendation documents specifically designed to outline how Aruba technology works and to enable customers who deploy Aruba solutions to achieve optimal results. This document is not only intended to serve a deployment guide but also to provide descriptions of Aruba technology, recommendations for product selections, network design decisions, configuration procedures, and best practices. Together, Aruba documentation suite for ArubaOS 8 comprises a reference model for understanding Aruba technology and designs for common customer deployment scenarios. 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.

Intended Audience and Assumptions

This guide is intended for administrators who are responsible for deploying and configuring AOS 8 solutions on customer premises. Readers should have at least a basic understanding of WLAN concepts. This is a base design guide for ArubaOS and it is assumed that readers have at least a working understanding of fundamental wireless concepts as well as Aruba technology.

Related Documents

The following documents may be helpful as supplemental reference material to this guide:

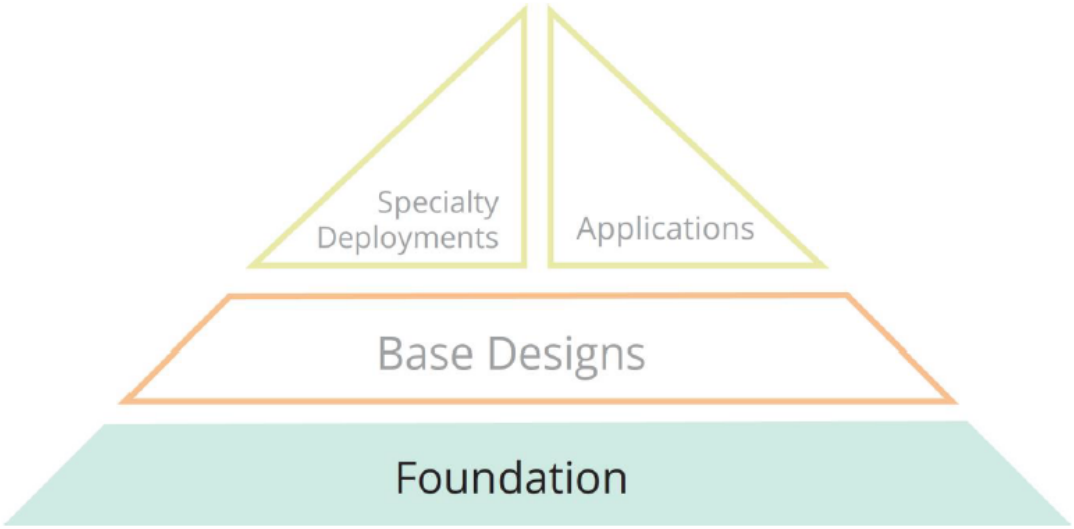
- ArubaOS 8 User Guide
- ArubaOS 8 CLI Reference Guide
- Aruba Solution Exchange

Scope

The Validated Reference Design series documents focus on particular aspects of Aruba technologies and deployment models. Together these guides provide a structured framework to understand and deploy Aruba Wireless Local Area Networks (WLANs). The VRD series has four document categories:

- Foundation guides explain the core technologies of an Aruba WLAN. These guides also describe different aspects of planning, operation, and troubleshooting deployments
- Base Design guides describe the most common deployment models, recommendations, and configurations
- Application guides build on the base designs. These guides deliver specific information that is relevant to deploying particular applications such as voice, video, or outdoor campus extension.
- Specialty Deployment guides involve deployments in conditions that differ significantly from the common base design deployment models, such as high-density WLAN deployments.

Figure 1 *Aruba Reference Architecture*



Information Icons

The following informational icons are used throughout this guide:

NOTE

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

CAUTION

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

WARNING

Indicates a risk of personal injury or death.

Typographical Conventions

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

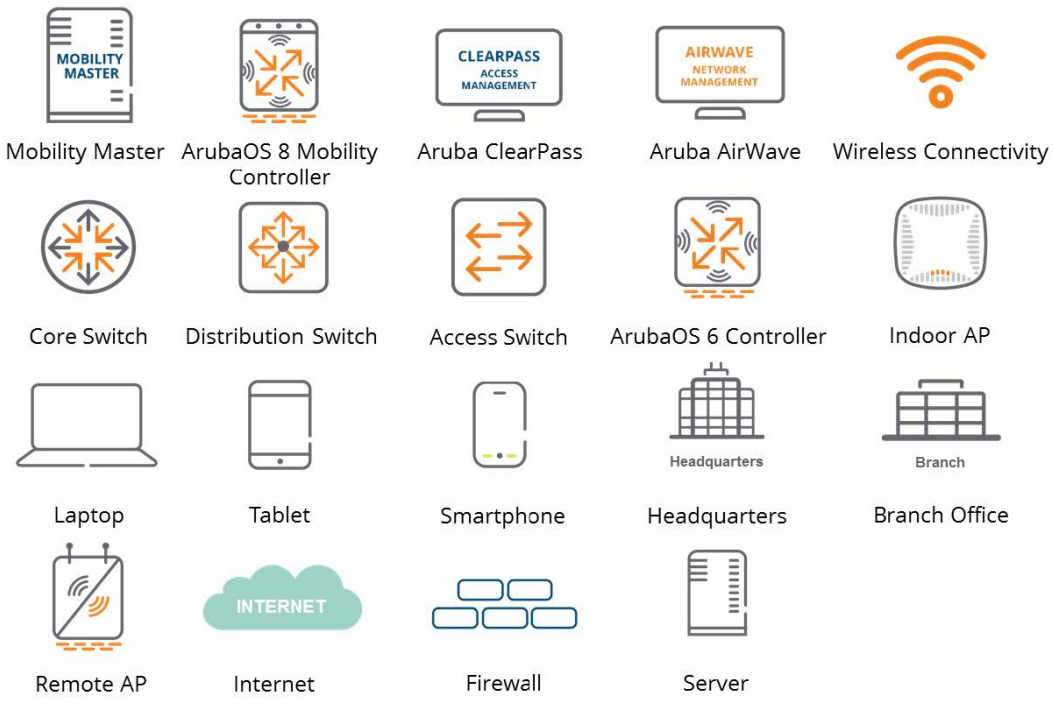
Table 2: *Typographical Conventions*

Style Type	Description
Italics	Italics are used to emphasize important terms and to mark the titles of documents.
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).

Style Type	Description
<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 curly braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

Graphical Icons

Figure 2 *VRD Icon Set*



Acronym List

Acronym	Definition
A-MPDU	Aggregated Media Access Control Packet Data Unit
A-MSDU	Aggregated Media Access Control Service Data Unit
AAA	Authentication, Authorization, and Accounting
AAC	AP Anchor Controller
ACL	Access Control List
ACR	Advanced Cryptography
AM	Air Monitor
AP	Access Point
API	Application Programming Interface
ARM	Adaptive Radio Management
ASP	Aruba Support Portal
BLMS	Backup Local Management Switch
CoA	Change of Authorization
CLI	Command Line Interface
CPSec	Control Place Security
CPU	Central Processing Unit
DC	Data Center
DLNA	Digital Living Network Alliance
DNS	Domain Name Service
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DPI	Deep Packet Inspection
FQDN	Fully-qualified Domain Name

Acronym	Definition
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
HA	High Availability
HMM	Hardware MM
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IAP	Instant Access Point
IDF	Intermediate Distribution Frame
IKEq	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
JSON	JavaScript Object Notation
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LAG	Link Aggregated Connection
LMS	Local Management Switch
LSM	Loadable Service Module
MAC	Media Access Control
MC	Mobility Controller
MCM	Master Controller Mode
mDNS	multicast Domain Name Service
MD	Managed Device

Acronym	Definition
MD	Mobility Device
MDF	Main Distribution Frame
MM	Mobility Master
MM-HW	Mobility Master - Hardware
MM-VA	Mobility Master – Virtual Appliance
MN	Managed Node
MNP	MyNetworking Portal
NAS	Network Access Server
NAT	Network Address Translation
NBAPI	Northbound Application Programming Interface
NVF	Network Virtualization Functionality
PAPI	Proprietary Access Protocol Interface
PAT	Port Address Translation
PEF	Policy Enforcement Firewall
PSK	Pre-shared Key
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RAP	Remote Access Point
RF	Radio Frequency
RFP	RF Protect
S-AAC	Standby AP Anchor Controller
S-UAC	Standby User Anchor Controller
SDN	Software Defined Network

Acronym	Definition
SfB	Skype for Business
SIP	Session Initiation Protocol
SSID	Service Set Identifier
SVI	Switch Virtual Interface
UAC	User Anchor Controller
UCC	Unified Communications and Collaboration
UCM	Unified Communication Manager
UDLD	Unidirectional Link Detection
URL	Uniform Resource Locator
VAP	Virtual Access Point
VIA	Virtual Internet Access
VIP	Virtual Internet Protocol address
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMC	Virtual MC
VMM	Virtual MM
VPN	Virtual Private Network
VPNC	Virtual Private Network Concentrator
VRRP	Virtual Router Redundancy Protocol
VSF	Virtual Switching Framework
WLAN	Wireless Local Area Network
XML	Extensible Markup Language
ZTP	Zero-touch Provisioning

Most of the end user devices in modern production networks are wireless devices, including laptops which are shipped without an ethernet port. Wired phones are now being replaced with unified communication applications such as Skype for Business (SfB) and these trends force enterprises to be increasingly reliant on wireless Local Area Networks (LANs) to address their business needs. With crucial dependencies on wireless LANs, network administrators are required to design complex networks to support various types of applications, users, and devices without compromising security. This deployment guide will outline all the features enabled through the Aruba's state-of-the-art ArubaOS 8 which helps addressing the challenges encountered in modern production networks.

AruabOS is the operating system for all Aruba Mobility Controllers (MCs) and controller-managed wireless access points (APs). With an extensive set of integrated technologies and capabilities, ArubaOS 8 delivers unified wired and wireless access, seamless roaming, enterprise grade security, and a highly available network with the required performance, user experience, and reliability to support high density environments.

Product Portfolio

The following table lists the controllers supported in ArubaOS 8 and their capabilities:
Table 3: *Controller Portfolio*

Controller Series	Controller Model	Number of APs	Number of Users	Firewall (Gbps)
70xx	7005	16	1,024	2
	7008	16	1,024	2
	7010	32	2,048	4
	7024	32	2,048	4
	7030	64	4,096	8
72xx	7205	256	8000	12
	7210	512	16000	20
	7220	1,024	24000	40
	7240	2,048	32000	40
	7280	2,048	32000	100

CAUTION

ArubaOS 8.x does not support 3000 or 600 series controllers.

ArubaOS 6 Controller Modes

ArubaOS 6 supports the following controller modes:

Master Mode

If a controller is deployed in master mode, the administrator is responsible for all configuration including IP addresses, licenses, WLANs, AP groups, user roles, etc. The administrator applies the configurations by connecting to the console of the controller and navigating through the Command Line Interface (CLI) wizard.

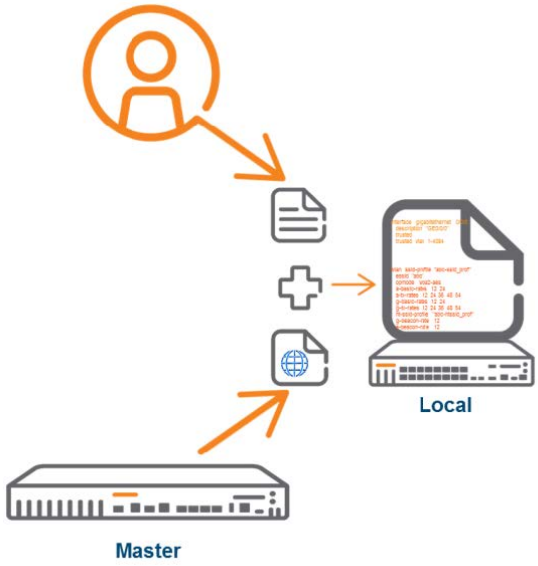
A master mode controller partially manages a local controller and fully manages a branch controller. 70xx series controllers and 72xx series controllers can operate in master mode. However, a 70xx series master controller cannot manage another 70xx series branch controller.

Figure 3 *Master Mode*

Local Mode

Similar to master controllers, local controllers should also be initially configured by an administrator using the serial console to assign IP addresses, to configure Virtual Local Area networks (VLANs), and other network related parameters. The global configuration parameters such as Wireless Local Area Networks (WLANs) and AP Groups are inherited from the master controller. and the inherited global configurations cannot be modified using the local controller Graphical User Interface (WebUI) . 70xx series controllers and 72xx series controllers can operate in local mode.

Figure 4 *Local Mode*

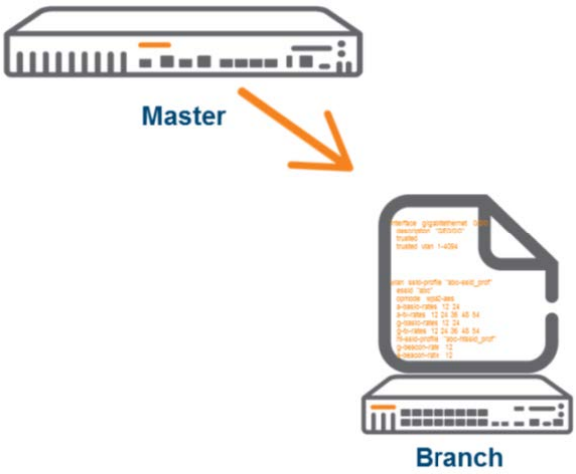


Branch Mode

Branch Mode is relatively a new controller operating mode which was introduced in the ArubaOS 6.4.3 version. It is typically used in distributed enterprises with geographically separated branch and remote offices. unlike master Mode and local mode, branch mode is enabled by default and it is only supported on 70xx series controllers. By default, 70xx series controllers are shipped with Dynamic Host Configuration Protocol (DHCP) client functionality enabled on last port on VLAN 4094. A Master controller can assign IP addressed to a branch controller using DHCP option 43. Alternatively, a branch controller can use Zero Touch Provisioning (ZTP) through Aruba Activate to obtain the master controller IP address.

In contrast to local controllers, branch controllers receive the entire configuration from the master controller. There are no write permissions permitted on the branch controller's WebUI or CLI. A special WebUI called Smart Config is enabled on the master controller for branch controller management and configuration. Controllers operating in branch mode have all the same features of other controllers yet only the features exposed in Smart Config can be enabled. The figure below illustrates how a branch controller is configured.

Figure 5 *Branch Mode*



Standalone

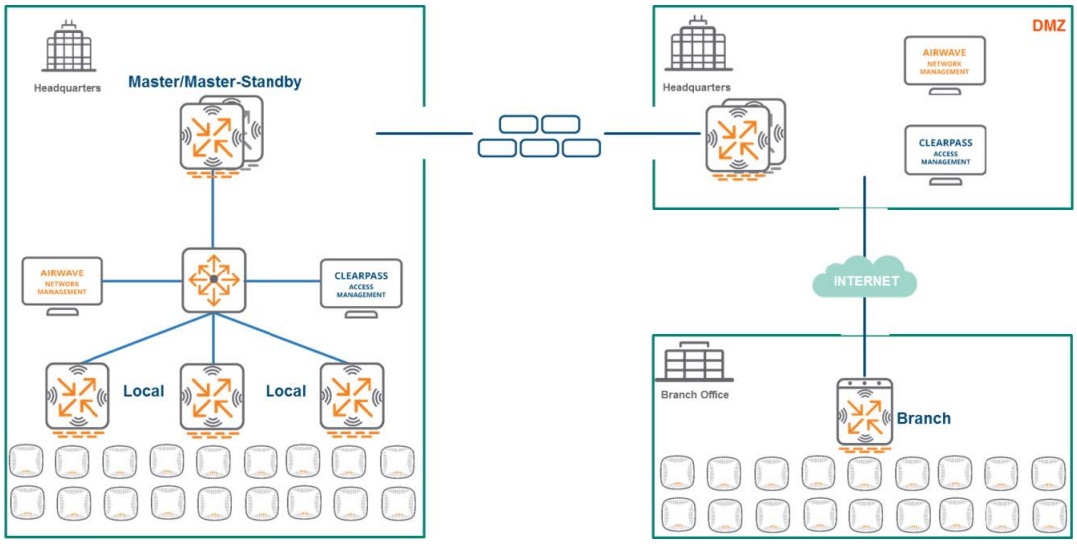
Stand-alone controllers are employed when an architectural design requires a deployment consisting of single controller. Stand-alone controllers cannot manage local or branch controllers and are very rarely used in production environments due to their inherent lack of redundancy. They have all the same functionality of a master controller with the notable exception that they cannot manage other controllers.

Figure 6 *Standalone*

ArubaOS 6 Topology

A typical ArubaOS 6 controller topology is characterized by two Master controllers located at the headquarters campus location in a Master / Standby configuration. The Master controllers are connected to several local controllers at the headquarters campus and to branch controllers deployed at remote locations. AirWave and ClearPass are deployed for network management and network access control.

Figure 7 *ArubaOS 6.x Topology*



ArubaOS 8 Controller Modes

Mobility Master

The concept of the Mobility Master (MM) is new to ArubaOS 8. Mobility Masters can be categorized as Virtual Mobility Master (VMM) and Hardware Mobility Master(HMM). The Mobility Master is designed to run on an x86-based platform and the features introduced in ArubaOS 8 require random access memory (RAM), central processing unit (CPU), and storage space that are not supported by physical controllers. The Mobility Master should be completely configured by a network administrator, similar to how a master controller would be configured in ArubaOS 6. The primary role of Mobility Master is to serve as the single point of configuration and image management for the network. In addition, the Mobility Master can be configured using a Northbound Application Programmable Interface (NBAPI). A Virtual Mobility Master can be installed on VMWare, KVM, or Hyper-V depending on what is most appropriate for the deployment. HMMs and VMMs may alternatively be referred to as MM-HW and MM-VA meaning MM-Hardware and MM-Virtual Appliance, respectively.

Access Points cannot be terminated on a MM.

Figure 8 *ArubaOS 8.x Topology*

Master Controller Mode

ArubaOS 8 also introduces the concept of master controller mode (MCM) to enable a seamless transition from ArubaOS 6 without requiring an x86-based appliance (HMM) or a VMM. Master controller mode can manage other Mobility Controllers (MC), however only a subset of MM features is available and APs cannot be terminated as they would be configured with a Mobility Master. Only 7030 controllers and 72xx series controllers support master controller mode.

Figure 9 *Master Controller Mode*

The following table outlines the features supported and unsupported on master controller mode:

Table 4: *Master Controller Mode Feature Matrix*

Supported Features	Unsupported Features
New WebUI, Workflows, and Hierarchical Configuration	Clustering
Multizone	AirMatch
Multi-threaded CLI with auto-completion	Centralized App Support (UCC, AppRF)
WAN Link Bonding and Load Balancing	Live Upgrade
Distributed UCC, AppRF, ARM and AirGroup	Centralized Visibility

Mobility Controller

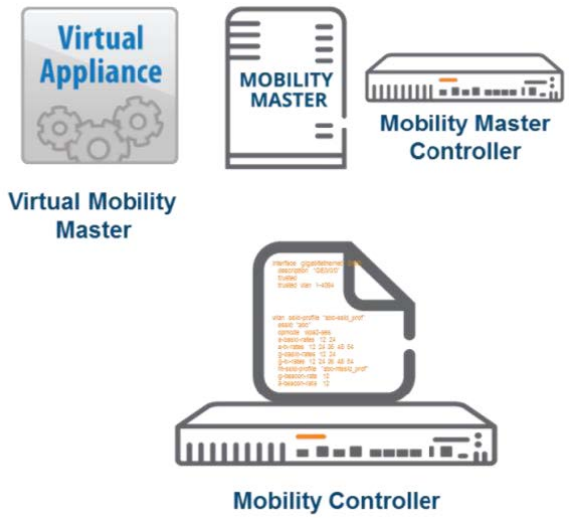
The concept of the Mobility Controller or MC is also new to ArubaOS 8. Mobility Controllers have been historically referred to as Managed Nodes (MN), Managed Devices (MD), or Mobility Devices (MD) in a few Aruba documentation. A Mobility Controller is similar to a branch controller in ArubaOS 6 as it can be configured using ZTP and Aruba Activate. The last port of a Mobility Controller is enabled as a DHCP client on VLAN 4094 in its factory default configuration.

NOTE

MMs and MCMs cannot adopt an MC using DHCP Option 43 since MM or MCM certificate distribution is not supported with DHCP Options.

Unlike the ArubaOS 6 local controllers, mobility controllers can be fully managed by a Mobility Master or Master Controller Mode. In addition, an administrator can configure all features of a mobility controller. 70xx series controllers and 72xx series controllers are shipped as Mobility Controllers. ArubaOS 8 also supports Virtual Mobility Controllers (VMC). A Virtual Mobility Controller can be deployed either on VMWare, KVM, or Hyper-V. Mobility Controllers can also be configured as Virtual Private Network Concentrators (VPNCs).

Figure 10 *MC Management*



Stand-alone Controller

ArubaOS 8 can also configure a stand-alone controller. A stand-alone controller cannot be managed by a Mobility Master and cannot be clustered with other stand-alone controllers. It is very similar to stand-alone controllers in ArubaOS 6 and supports Multizone feature.

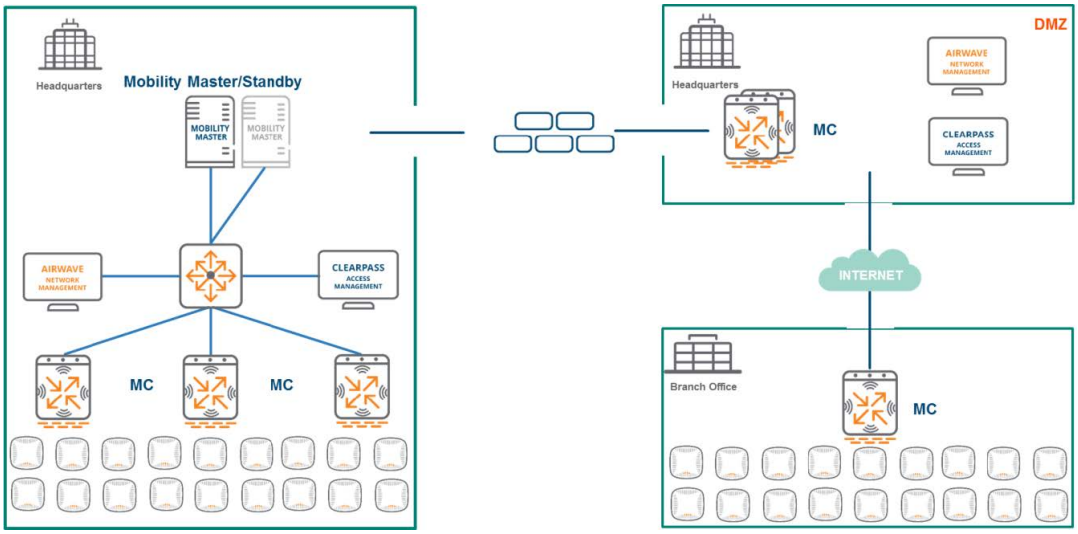
AirMatch and clustering are not enabled on stand-alone controllers because they can only be implemented with the assistance of a virtual machine (VM). ARM is the only available RF optimization method. Other features such as WebCC, AppRF, UCC, AirGroup, Northbound API, UCM, and WMS will function as how they do on an ArubaOS 6 local controller.

Figure 11 *ArubaOS 8 stand-alone controller*

ArubaOS 8 Topology

Migration from a an ArubaOS 6 topology to an ArubaOS 8 topology primarily consists of replacing the Master controller with a Mobility Master and replacing all local and branch controllers with Mobility Controllers.

Figure 12 *ArubaOS 8 Topology*



ArubaOS 8 topology has the following key points of differentiation when compared to an ArubaOS 6 topology:

- Introduced the VM-based Mobility Master as a single point of configuration and image management.
- Introduced Mobility Controllers which are entirely managed by a Mobility Master using ZTP.
- The Mobility Master does not terminate APs.
- 72xx and 70xx controllers can be set up as mobility controllers or stand-alone controllers.
- Introduced Master Controller Mode as a migration path.

Controller Mode Comparison

The following table outlines how the previous designations for controller devices in an ArubaOS 6-based deployment have changed and been identified with their appropriate counterparts in an ArubaOS 8-based deployment:

Table 5: *Controller Mode Summary*

ArubaOS 6	ArubaOS 8
Master Controller	Mobility Master (VM or hardware) or Master Controller Mode (only 72xx and 7030 controllers)
Local Controller	Mobility Controllers
Branch Controller	Mobility Controllers
Stand-alone Controller	Stand-alone Controller

The following key points should be noted about the ArubaOS 8 controller modes:

1. ArubaOS 6 master controllers partially manage local controllers and fully manage branch controllers.
2. Mobility Masters in ArubaOS 8 manages all types of controllers regardless of where they are deployed.
3. The key distinction between a Mobility Master in ArubaOS 8 and a Master controller in ArubaOS 6 is that an Mobility Master can neither adopt APs nor point an AP to a Mobility Controller.
4. Master Controller Mode was introduced as a migration path to ArubaOS 8 as it doesn't require a Virtual Mobility Master.
5. Stand-alone mode functions in the same manner in ArubaOS 8 as it does in ArubaOS 6. It is supported only on hardware controllers.
6. ArubaOS 6 based local controllers receive only a partial configuration from their master and do not support ZTP. All ArubaOS 8 hardware controllers support ZTP.
7. Branch controllers from ArubaOS 6 are replaced by mobility controllers in ArubaOS 8 and have full configuration capabilities unlike the limited functionality of Smart Config in ArubaOS 6.

Campus APs

In most of the ArubaOS 8 topologies, campus APs typically operate either in tunnel mode or decrypt tunnel mode to communicate with the mobility controller. The advantage of these modes is that the user VLANs reside on the controller and do not have to be managed at the edge. If necessary, additional VLANs can be added to the core switch where the uplink of the mobility controller is connected. There is no need to add them to the edge switch where the APs terminate. Both of these operating modes simplify network design and allow flexibility in terminating users.

Tunnel Mode

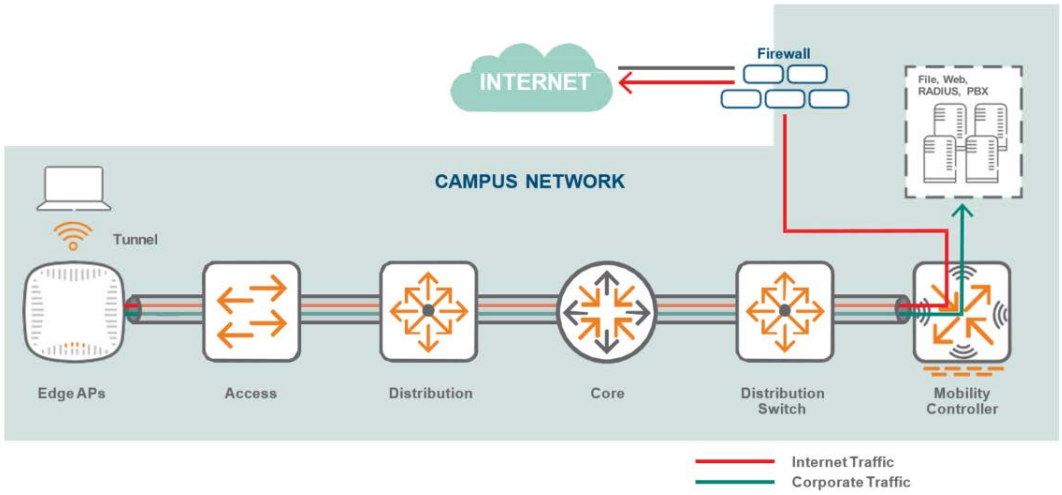
When operating in the tunnel forwarding mode, APs handle all 802.11 association requests and responses and all 802.11 data packets, action frames, and EAPOL frames are sent over a GRE tunnel to the mobility controller for processing. The mobility controller then removes or adds GRE headers, decrypts or encrypts 802.11 frames, and applies firewall rules to user traffic.

Due to the increased aggregation introduced in IEEE 802.11ac standard, end-to-end jumbo frame support should be enabled on a wired switch to achieve maximum performance in tunnel mode. Control Plane Security (CPSec) is not mandatory in tunnel mode. The majority of production deployments use tunnel mode for AP forwarding where the AP sends 802.11 traffic to the controller. Control and data plane traffic between the AP and the mobility controller is always encrypted. Aruba recommends using tunnel mode as the majority of traffic fits in a standard 1500 byte ethernet frame and no special handling is required on the wired network to achieve maximum aggregate performance.

When jumbo frames are used in tunnel mode, the network should support Maximum Transmission Unit (MTU) size of at least 4500 bytes. If the network cannot support an MTU of 4500 bytes, the benefits of aggregation efficiency over air will be lost due to fragmentation. if there are no end-to-end jumbo frames on the wired network, 802.11ac networks might experience performance degradation in a few cases. It should also be noted that this adverse impact in performance is noticed only when the peak network performance is measured during technology demonstrations. The day-to-day operations in a real world production networks are typically unaffected when jumbo frames are not enabled.

Aruba recommends enabling end-to-end jumbo frames as a best practice.

Figure 13 *Tunnel Forwarding Mode*



Decrypt-Tunnel Mode

Decrypt-tunnel mode allows an AP-client pair to take full advantage of Aggregated-Media Access Control (MAC) Service Data Units (A-MSDUs) and Aggregated-MAC Packet Data Units (A-MPDUs) without requiring the wired network to transport jumbo frames. APs can locally perform decryption and de-aggregation. It is mandatory to enable control plane security (CPSec) between APs and Controllers while using decrypt-tunnel mode.

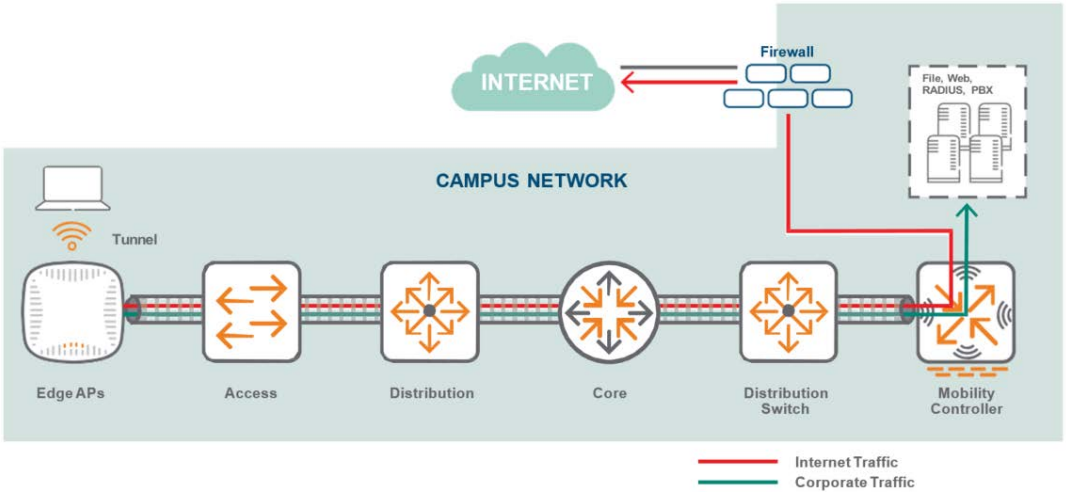
CAUTION

Decrypt-tunnel mode does not provide end-to-end encryption. Only the control plane traffic between APs and Mobility Controllers is encrypted in decrypt-tunnel mode.

In addition to performing encryption and decryption, APs in decrypt-tunnel mode act as a bridge between clients and the controller. The mobility controller still acts as the aggregation point for terminating data traffic. This allows the AP-client pair to take advantage of A-MSDU and A-MPDU on the WLAN radio side without requiring the wired network to transport jumbo frames, since the AP performs all assembly aggregation and de-aggregation locally. The payload is then sent to the controller for firewall processing and L2/L3 forwarding.

Decrypt-tunnel mode is functionally equivalent to tunnel Mode with jumbo frames enabled and is typically used for technology demonstrations. It is important to keep in mind that the AP wireless chipset performs cryptography for up to 50 clients which is offloaded to the AP hardware. Scenarios involving more than 50 clients will likely experience minor performance degradation due to this offload process.

Figure 14 *Decrypt-Tunnel Mode*



Control Plane Security

The CPSec feature has two main functions:

1. Securing the control channel between Aruba Mobility Controllers and their attached APs.
2. Preventing unauthorized APs from joining the Aruba WLAN network.

The above mentioned goals are achieved in the following manner:

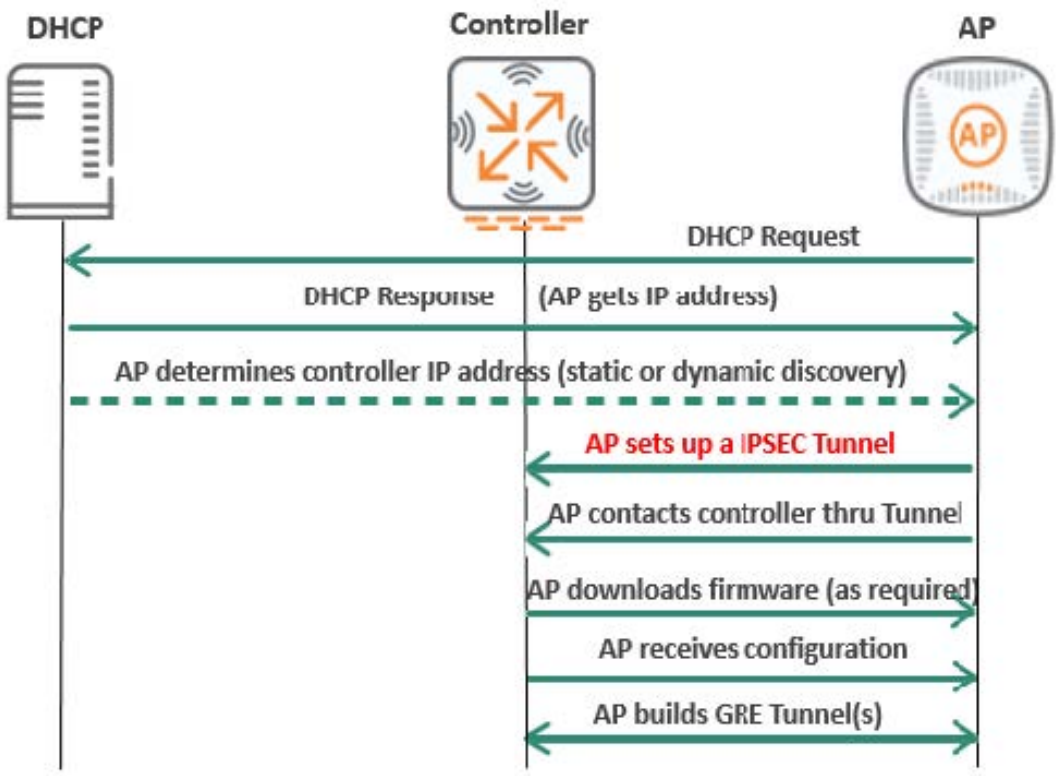
- The control traffic transported using Proprietary Access Protocol Interface (PAPI) is secured using a certificate-based Internet Protocol Security (IPsec) tunnel in transport mode.
- A CPsec whitelist database has the list of authorized APs to connect to the Aruba controllers and join the WLAN network.

Since CPSec is enabled by default, the Mobility Master certifies its Mobility Controllers using the factory generated certificate after the boot up. Mobility Controllers , in turn certify their APs by signing their factory default certificates. Once the APs are authorized through the CPsec whitelist and enter the certified-factory-cert state, they will initiate a secure PAPI (UDP 8209 inside IPsec) communication with the controller, synchronize their firmware, and download their configurations.

Boot Process with Control Plane Security

The figure below illustrates the steps involved in the campus AP boot process with CPSec:

Figure 15 *AP Boot Process with CPsec*



The process includes the following steps:

1. AP sends a DHCP Request.
2. AP receives an IP address in the DHCP Response.
3. AP determines its controller's IP address either statically or dynamically.
4. AP establishes an IPsec tunnel with the controller.
5. AP exchanges PAPI (UDP 8209) over the IPsec tunnel with the controller.
6. If required, the AP downloads firmware from the newly discovered AP master to ensure version consistency.
7. AP receives the configuration from the controller.
8. AP creates a Generic Routing Encapsulation (GRE) tunnel for user traffic.

Local Management Switch

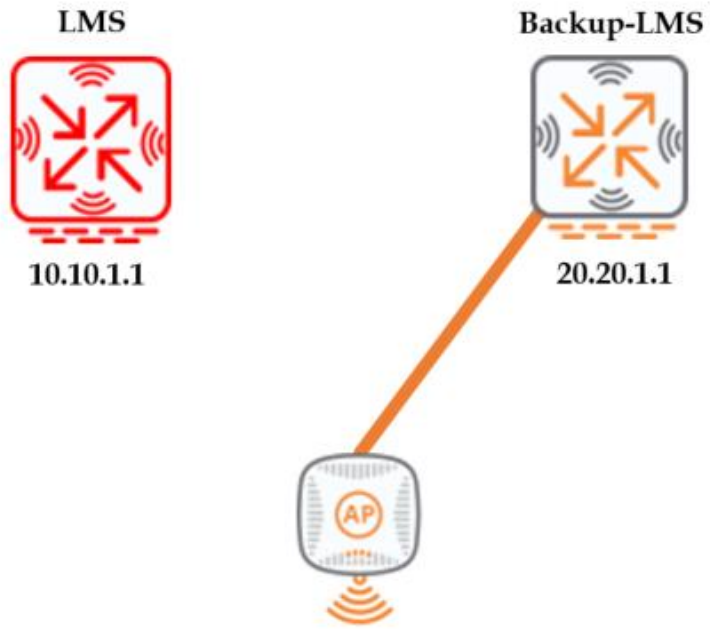
In multi-controller networks, each controller acts as a Local Management Switch (LMS) by terminating user traffic from the APs, and then processes and forwards traffic to the wired network. An LMS and a Backup Local Management Switch (BLMS) are the primary and secondary connection points for an AP. APs rely on heartbeat timeouts with the LMS controller to failover to a preconfigured BLMS controller.

When controllers are in a separate L3 networks, Virtual Router Redundancy Protocol (VRRP) cannot be used for redundancy. In such an instance, the LMS and BLMS should be used for redundancy.

In the most basic scenario of two L3 separated controllers:

- The AP finds aruba-master and obtains the LMS and BLMS IPs as part of its configuration.
- The AP terminates on the LMS controller.
- If the LMS controller fails, eight consecutive missed heartbeats will trigger an AP failover.
- The AP comes up on the BLMS.

Figure 16 *LMS and Backup LMS*



Another scenario would be an AP terminated on an LMS which is a cluster of controllers. In this scenario, AP finds the aruba-master and obtains the IP addresses of its LMS and BLMS as part of its configuration. If the LMS is located in a cluster of controllers and the LMS fails, any APs terminated on that LMS will attempt to failover to the other members of the cluster. The AP will failover only to its BLMS if all of the other members in the cluster have failed. The BLMS could either be a single controller or a member of a cluster.

The concept of clustering is covered in detail in the in the Clustering chapter of this document

Figure 17 *LMS and BLMS Architecture with Clusters*

Remote APs

Remote Access Points or RAPs are built for remote access use cases. Remote users are typically work from home offices, small satellite offices, medium-sized branch offices, or on the road from hotels, hot spots, or customer locations. Each of these remote locations has different connectivity, capacity, and usage requirements.

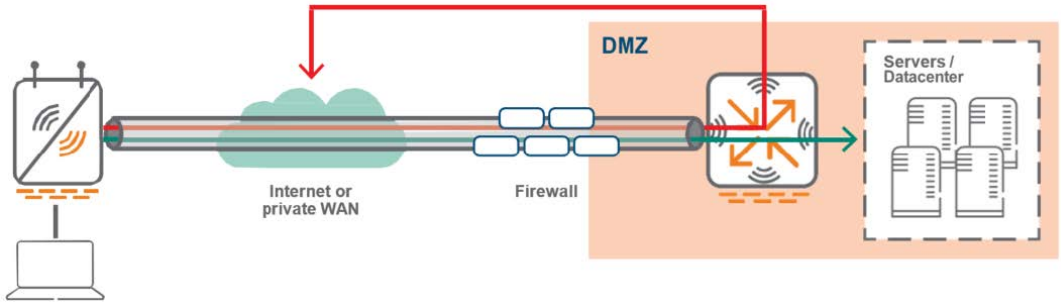
IT organizations have traditionally served each category using a different remote network architecture. For example, micro branches use a branch office router to interconnect an IP subnet at the remote site to the corporate network core, while telecommuters with only a single PC or laptop could be served with a software

VPN client. Aruba RAPs offer a solution for remote corporate users working from home or remote branches. These users are granted access to the same wireless network they would access at the main corporate office from wherever they are located.

Tunnel Mode

When RAPs operate in tunnel mode all traffic is tunneled back to the corporate network. There is a wireless encryption on the client and controller and a wired encryption on the RAP and controller. There is no access to local traffic, say a printer, home desktop, etc.

Figure 18 *RAP Tunnel Mode*

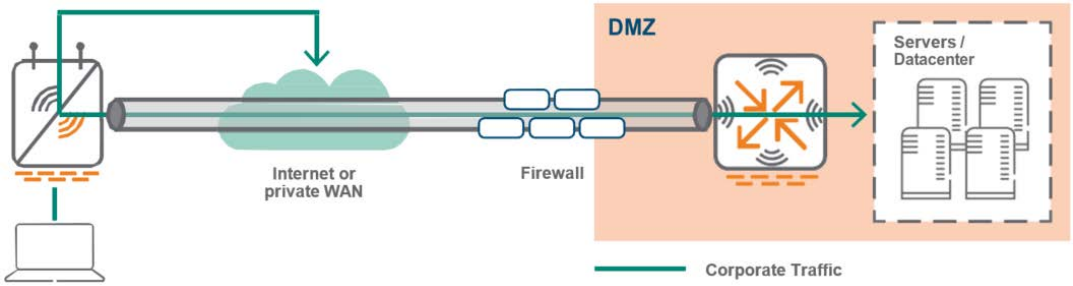


Split Tunnel Mode

Split tunnel mode allows non-corporate traffic to be bridged locally to the internet which reduces the tunnel bandwidth between the RAP and the controller that transports the corporate traffic. In split-tunnel mode, there is wireless (L2) encryption and decryption on the client and RAP.

Corporate traffic is tunneled to the controller in the demilitarized zone (DMZ) and the rest of the corporate network. Traffic is encapsulated using GRE to preserve VLAN tags. The tunnel is trusted and shared by all Virtual Access Point (VAP) and wired ports. Traffic between the RAP and the controller is encrypted using IPsec. Local traffic is source NATed (to enet0 address) and forwarded on both uplink and downlink wired interface ports according to the user role and session access control list (ACL).

Figure 19 *RAP Split Tunnel Mode*

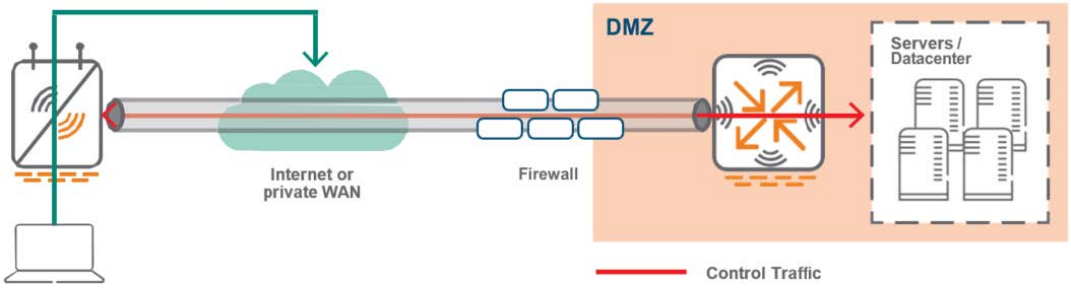


Bridge Mode

Bridge mode is primarily used on RAPs and Instant Access Points (IAPs). In bridge mode, there is no access to corporate traffic. There is user traffic bridge to the local network on the AP uplink. Traffic is not sent to the controller. User VLANs have to exist on the edge of the network and authenticated traffic is tunneled to the controller. CPSec is required for bridge mode. DHCP, Network Address Translation (NAT), and Port Address Translation (PAT) are provided either by the RAP or an external router.

Bridge mode is typically used so that non-corporate devices such as printers or family owned devices can access the internet directly via RAP uplink (similar to a home wireless router operation). This mode is not recommended for campus AP deployments as only a few features are supported in bridge mode.

Figure 20 *RAP Bridge Mode*



Secure Jack

On Aruba RAP that offers at least two ethernet ports, the additional port can be configured for bridging or secure jack operation. This configuration provides maximum flexibility and allows local wired access for remote sites. The additional ethernet ports on a RAP can be configured for all authentications and forwarding modes are also available which is similar to a wireless Service Set Identifier (SSID). A single SSID cannot be configured to provide 802.1X and MAC authentication simultaneously, but a wired port does not have the same limitation.

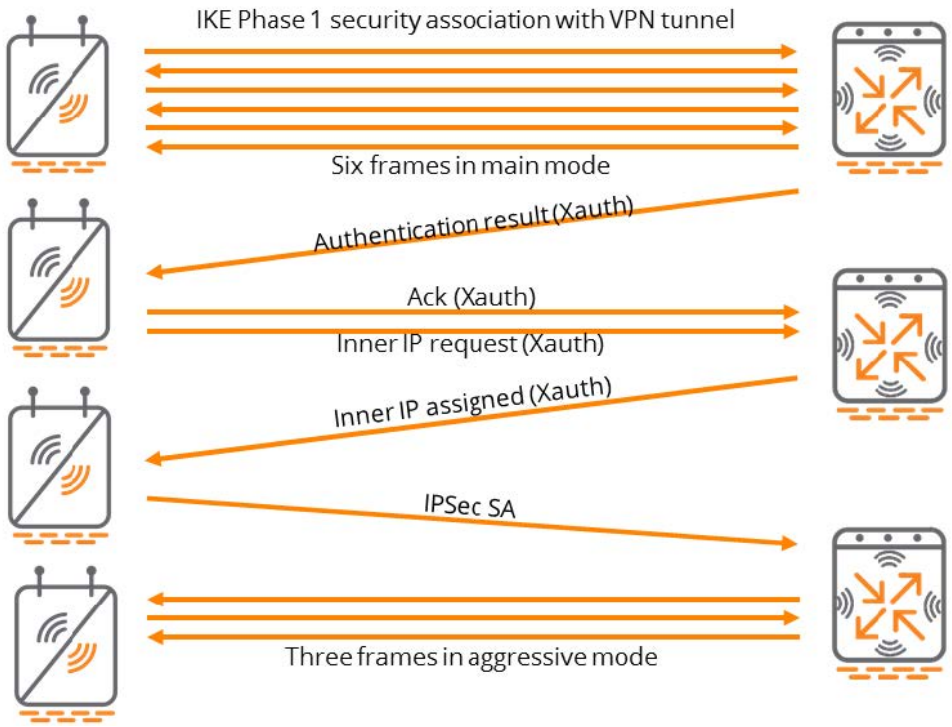
Client connectivity issues will be observed when 802.1X and MAC authentication are configured on the same SSID.

RAP Bootstrap Process

Following are the different phases of the RAP bootstrapping process:

1. Firstly. the RAP obtains an IP address on the wired interface (Eth 0) by using DHCP. In remote deployment scenarios, the IP address is typically provided by the Internet service provider (ISP) when it is directly connected to the internet.
2. The RAP can be provided with a Fully-Qualified Domain Name (FQDN) or a static IP of the mobility controller. If an FQDN is used, the RAP uses the DNS service provided by the ISP to resolve the host name.
3. The RAP attempts to establish an IPsec connection with the mobility controller through the ethernet interface. Depending on the provisioning type, either the RAP's certificate or Internet Key Exchange (IKE) Pre-shared Key (PSK) is used to complete phase 1 negotiation. XAuth (an extension to IKE phase 1) is used to authenticate the RAP.
   - If IKE PSK is used, XAuth will authenticate the RAP with username and password.
   - If a certificate is used, XAuth authenticates the MAC address in the certificate against the RAP whitelist.
4. An IPsec security association (SA) is then established between the RAP and the controller.
5. The mobility controller provides the RAP with the IP addresses of the controller (LMS and BLMS IP)
6. One or more IPsec encrypted GRE tunnels are formed between the RAP and the designated controller depending on the configuration.

Figure 21 *RAP Bootstrapping*



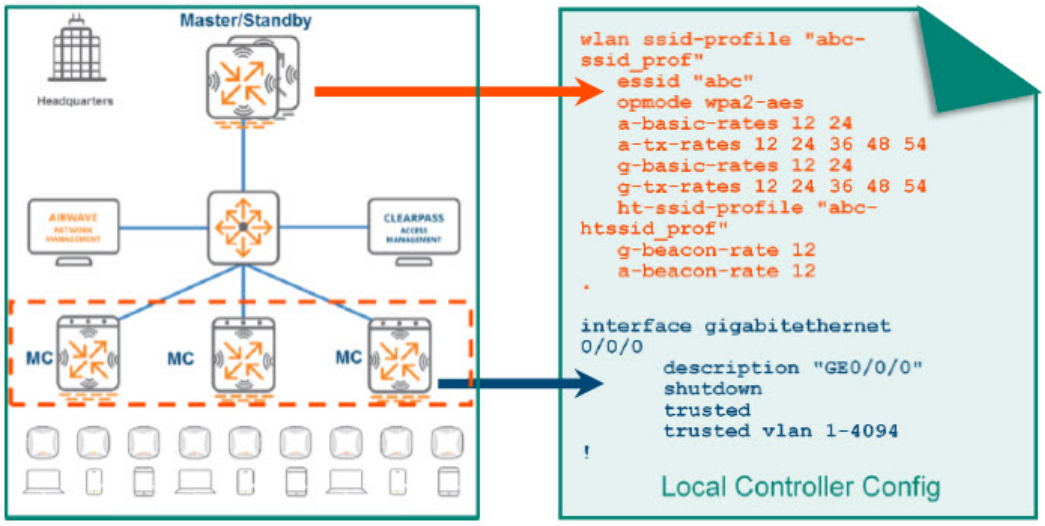
Hierarchical configuration is introduced in ArubaOS 8 to enhance the way the configurations are applied in multi-controller deployments.

ArubaOS 6 Configuration

In a typical ArubaOS 6 deployment, master controller manages the local controllers and each local controller is brought up with its own base configurations (interfaces, VLANs, and IP addresses). Once the base configurations have been applied on each local controller, the master then connects to the local controllers and pushes configurations such as AP Groups, SSIDs, and user roles. This involves numerous points of configuration in deployments with multiple controllers as configurations are not entirely centralized on the master and a single master can only manage a finite number of local controllers.

ZTP was introduced in ArubaOS 6, however is only applicable for branch controller networks and only a subset of features can be enabled using the Smart Config interface on the master controller.

Figure 22 *Typical AOS 6 Configuration*



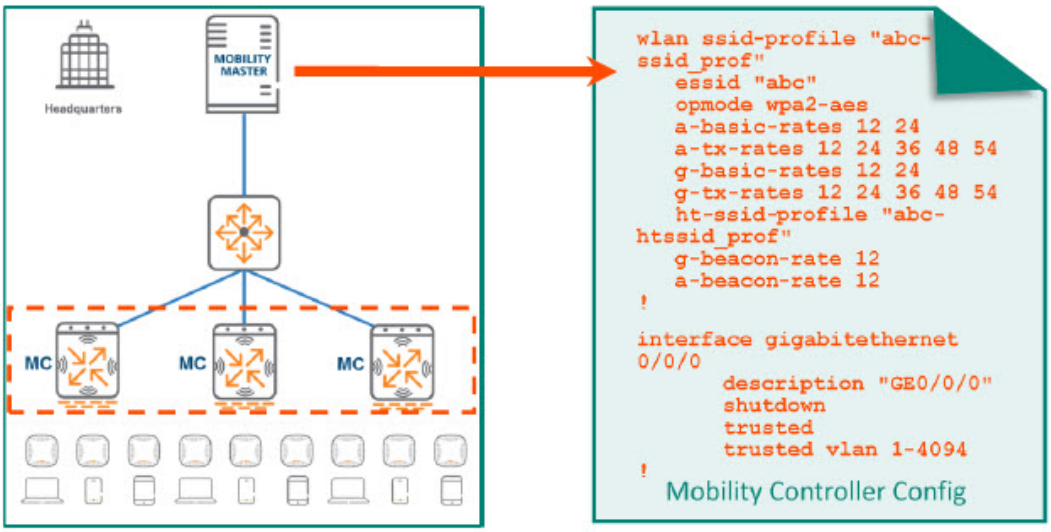
The configuration pushed from the master controller is consistent across all the local controllers. The master controller does not selectively push configurations for individual local controllers. The configurations pushed to each local controller will contain the SSID configurations for all the campuses. If local controllers are geographically separated across multiple campuses, each campus requires a unique SSID. In such cases , SSIDs pushed by the master controller will likely be redundant for the majority of deployments because APs subscribe to specific AP groups to broadcast the relevant SSIDs in each campus. Hence, the configuration intended for other campuses is irrelevant for the local controllers where that SSID will not be used.

In some cases, a uniform configuration approach may also present an operational concern as the entire master configuration is exposed across all regional local controllers. Since local network administrators need access to the master controller for configuration changes, a great amount of care needs to be taken to avoid mis-configurations which may affect the remaining controllers managed by the master controller.

AOS 8 Configuration Enhancements

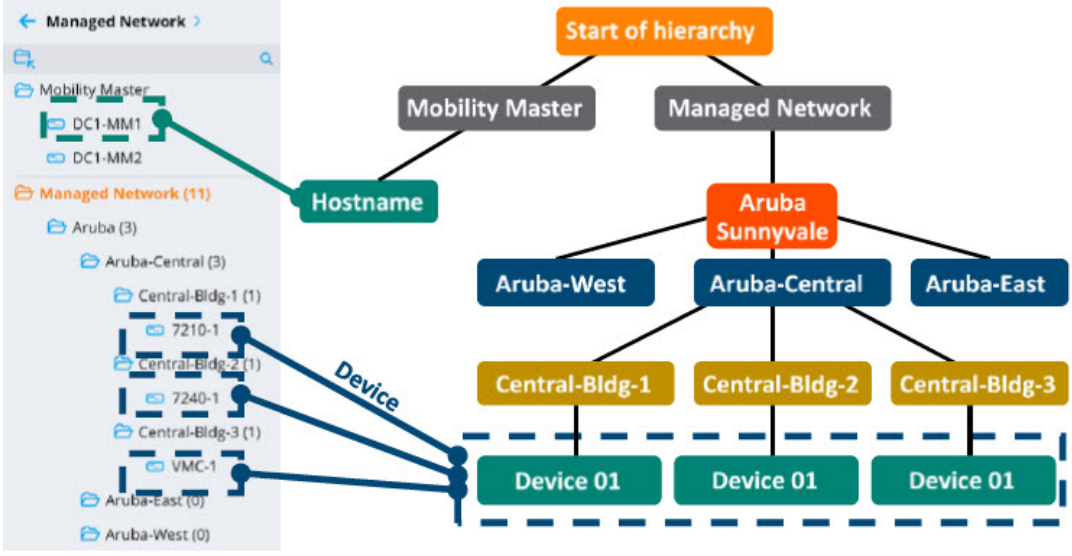
ArubaOS 8 introduces the concept of hierarchical configuration and ZTP for all deployment modes. New campus or branch controllers can discover the Mobility Master using DHCP options or Aruba Activate and receive their entire configuration from the Mobility Master. Regardless of the scale of controllers being managed, the Mobility Master acts as a single touch point for the entire deployment.

Figure 23 *Typical AOS 8 Configuration*



Hierarchical configuration allows configuration nodes to be created on the Mobility Master which has the common configurations for a specific region, campus, or building. Once a controller is whitelisted under a configuration node, device-level configurations can be added on the device configuration node. When the mobility controller contacts the Mobility Master for the first time, the group level configuration is merged with the device level configuration and then pushed to the mobility controller.

Figure 24 *Configuration Hierarchy*



The hierarchical configuration model has system-defined and user-defined configuration nodes.

System Nodes

By default, system level nodes are present on WebUI of the Mobility Master and it cannot be deleted. The system nodes are give below,

- **MM** – In the case of redundant Mobility Masters, the configuration defined at this node is common for both active and standby Mobility Masters.
- **Hostname (of MM)** – Holds configuration for the actual Mobility Master.
- **Managed Network** – Hierarchy under which all the user-defined nodes are created and controllers are configured.

User Nodes

User-defined nodes are created by administrators under the **Managed Network** system node. A node hierarchy can be created under this node where all the upper nodes hold common configuration for all controllers. The configuration becomes more specific (based on region, campus, or building) at lower levels of the hierarchy. The device nodes are defined at the very bottom. The following examples demonstrate hierarchical group and device node definitions:

Figure 25 *Group Node*

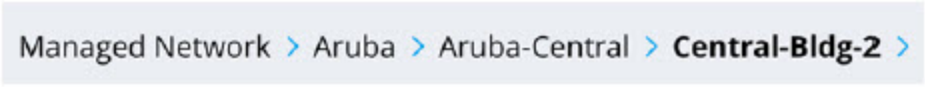


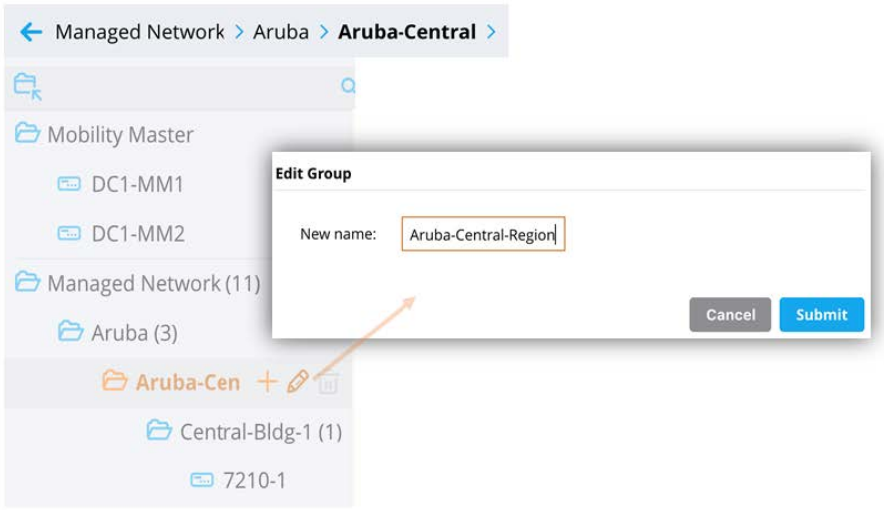
Figure 26 *Device Node*

Up to four nested child nodes can be created under the **Managed Network** node. For example:

Figure 27 *Four Nested Child Nodes*

Numerous child nodes can be created under the same parent node. In addition, child nodes can be freely moved to other nodes in the hierarchy as well as cloned from other nodes under the same parent node.

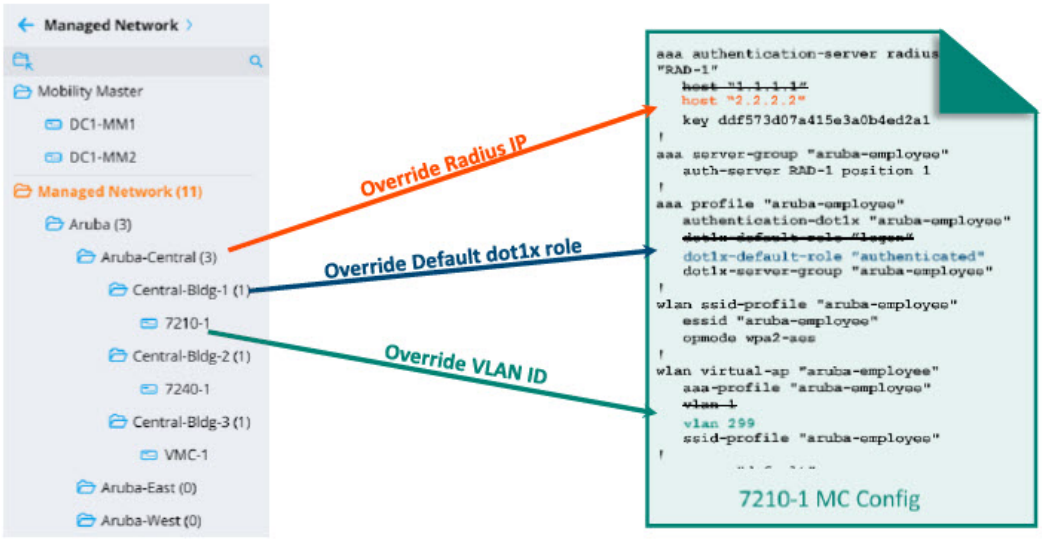
Figure 28 *Renaming a Node*



Configuration Inheritance

When a mobility controller initially contacts the Mobility Master, it will merge all the configuration sat the device node with the configurations in the higher node hierarchy to the **Managed Network** node. If there is a conflict or overlap in configuration on any node, the configuration defined on the lower nodes will take precedence over the configuration on the higher nodes when pushing the final configuration. The example below shows how a controller inherits its final configuration from the Mobility Master:

Figure 29 *MM Configuration Inheritance*



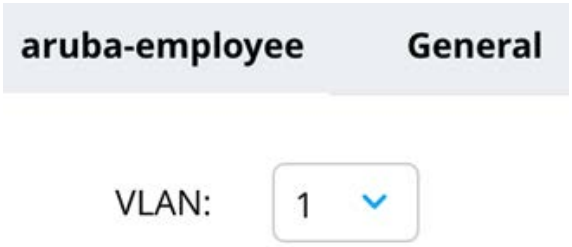
In the example above, the initial configuration is created on the user-defined **Aruba** node which will be common to all the controllers in the organization. Since the **Aruba-Central** Node is farther down the hierarchy it will receive its initial configuration from the **Aruba** node and then override the RADIUS IP address. Similarly, the **Cenral-Bldg-1** node and the **7210-1** device node will override the dot1x role and the VLAN ID defined in the original configuration, respectively. The following figures display some of the key elements which were configured using the **Managed Network > Aruba** path:

Figure 30 *RADIUS Server RAD-1 with RADIUS IP "1.1.1.1"*

Figure 31 *802.1X Default Role of Logon*

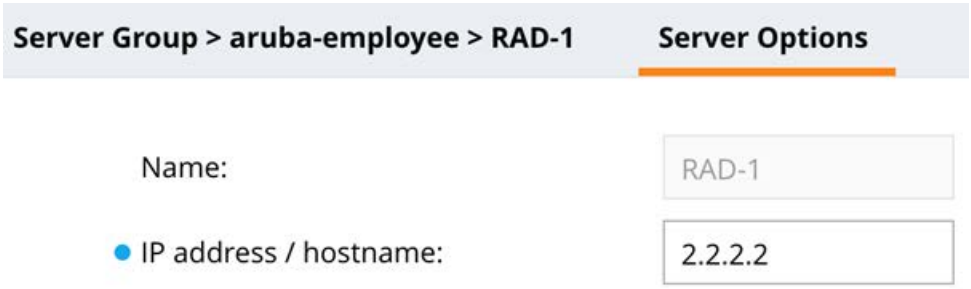
The presence of the blue dot next to a configuration parameter indicates the value was overridden such as in the case of a change to the configuration inherited from the parent node or a blank value that was replaced. Clicking on the blue dot displays additional details about the change and provides the option to either remove or retain the override.

Figure 32 *VLAN "1"*



In the figure below the **Aruba-Central** node inherited this configuration, however the IP of the RADIUS server **RAD-1** was changed to "2.2.2.2":

Figure 33 *RADIUS Server IP Override*

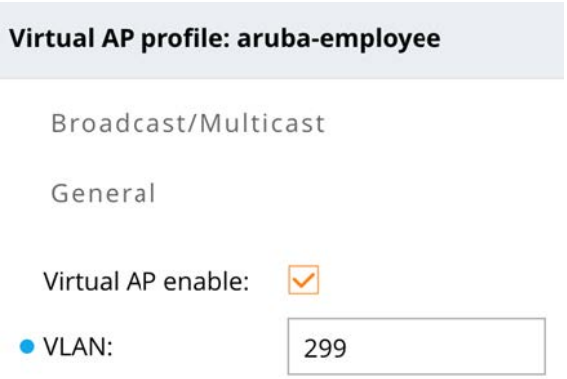


On the **Central-Bldg-1** node father down, the presence of the blue dot indicates that the default 802.1X role in the authentication, authorization, and accounting (AAA) profile was changed to "authenticated" and the configuration received from the parent node was overridden. **Managed Network > Aruba > Aruba-Central > Central-Bldg-1**:

Figure 34 *Authentication Default Role Override*

Lastly, the VLAN applied to the Virtual AP profile "aruba-employee" on the device node **7210-1** was changed to "299". **Managed Network > Aruba > Aruba-Central > Central-Bldg-1 > 7210-1:**

Figure 35 *VLAN Changed to 299*



When the 7210 controller assigned to the **Central-Blg-1** node contacts the Mobility Master for the first time, its inherited configuration will result in the following changes:

Table 6: *Summary of Inherited Configuration Changes*

	Original Configuration	Inherited Configuration
RADIUS Server IP	1.1.1.1	2.2.2.2
802.1X Default Role	logon	authenticated
VLAN	1	299

Node Level Administration

Hierarchical configuration allows to create node-level administration accounts on a Mobility Master. Network administrators can fully manage configuration for controllers preset in the node and below the configuration nodes for which they have the necessary permissions to access region, campus, or building level without affecting controllers elsewhere in the global hierarchy. This feature ensures that any undesirable configuration changes made at local sites are contained and do not affect the entire organization.

Proof-of-concept testing is another use case where custom ArubaOS builds and features need to be lab tested before bringing them into production. In such a scenario, test configuration nodes could be created along with node-level administration accounts. Since the nodes are created in a sandbox environment,

testing may be freely performed without creating any undesirable effects higher up in the configuration hierarchy.

Licensing Pools

Licensing in ArubaOS 8 is managed centrally from the Mobility Master and the global license pool will be used by default for all controllers under its management. However, if specific license pools have to be dedicated for a particular region, then custom license pools must be created on the Mobility Master in the appropriate hierarchical node and license counts definitions.

For additional information on please refer to the Creating Licensing Pools on the MM section.

Configuration Best Practices

Prior to deploying controllers there should be a defined plan on the configuration hierarchy for how a network will look like. The following sections provide a guidance for developing a configuration and deployment plan.

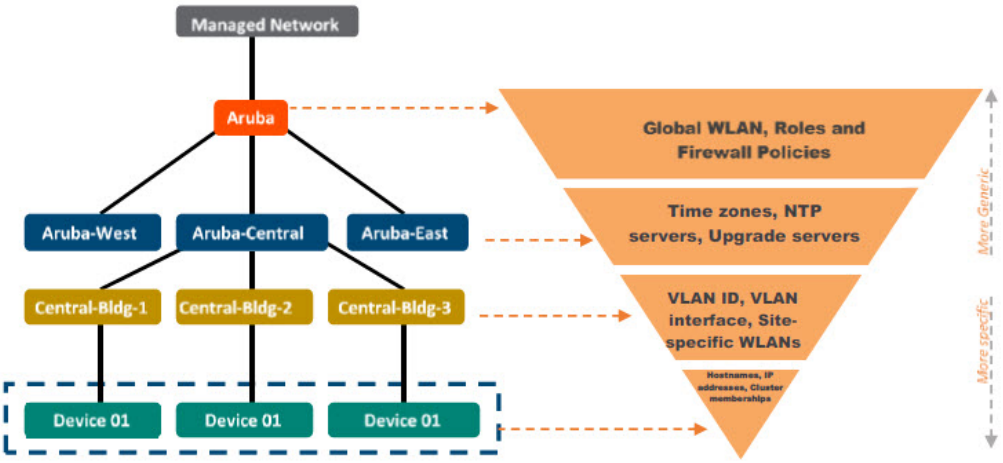
Node Hierarchy Design

Following are the approaches to implement a hierarchical design:

- A configuration hierarchy is typically created based on the geographical segmentation of controllers. If an organization has multiple offices across a country, then configuration nodes should be created for each region such as East, Central, and West. Each of these regions in turn may have multiple campuses, buildings, and devices which will have their own configuration node.
- An alternative way of organizing a hierarchy could be based on the type of services offered such as campus and remote with regional variations at the bottom of the tree.

Hierarchical configurations should be designed in a way that configurations which are common to the organization reside on the higher level nodes. The rest of the configuration will be inherited by the lower nodes of the hierarchy as network requirements become more specific. For example, a named VLAN can be defined at a higher level of the hierarchy and then assigned with specific VLAN IDs at the lower levels. Finally, configurations specific to individual controllers such as IP addresses, physical and virtual interfaces, and cluster membership are configured at the device level nodes. As a best practice, all configurations that are dependent on a single node should be always be defined together in a common node, for example, defining a VLAN ID and VLAN.

Figure 36 *Node Hierarchy Design*



Configuration Overrides

Generally, a configuration that is inherited from higher level nodes cannot be deleted, however it can be overridden on the lower level nodes. There are a certain configuration parameters that cannot be overridden at the lower level nodes. These parameters include the following:

- Net destinations
- IP access lists
- User roles
- AAA server groups
- AAA user derivation rules

CAUTION

Too many overrides across many hierarchy levels should be avoided as it can make troubleshooting challenging.

Depth of Hierarchy

A maximum of four nested child nodes can be created under the **Managed Network** node. To simplify configuration management, it is recommended to create only as many nested nodes that are actually required.

The Managed Network Node

As a best practice Aruba recommends defining configurations at a node below the **Managed Network** node and not on the **Managed Network** node itself. This is done to allow sufficient network growth and scalability while simultaneously maintaining a separate configuration hierarchy for new sites. Configuration on the **Managed Network** node should be kept as minimal as possible in order to prevent the spread of issues related to misconfiguration across every other node in the hierarchy.

CAUTION

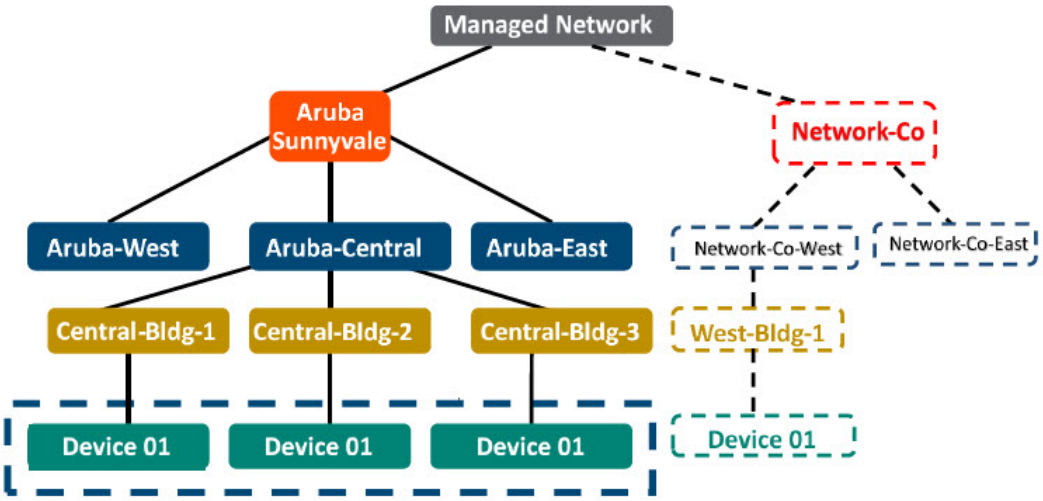
Aruba strongly discourages placing any configuration on the /md (Managed Network) node

CAUTION

under any circumstances. Modifying configurations at this level will permanently alter the configuration for every child node without any ability to determine the default settings. Configurations should always begin a level below the Managed Network node.

Sites can be differentiated either physically or by type. In the example below, if the organization “Aruba” acquired another company “Network-Co”, then a new configuration node would be defined under **Managed Network** called **Network-Co** parallel to the **Aruba Sunnyvale** node.

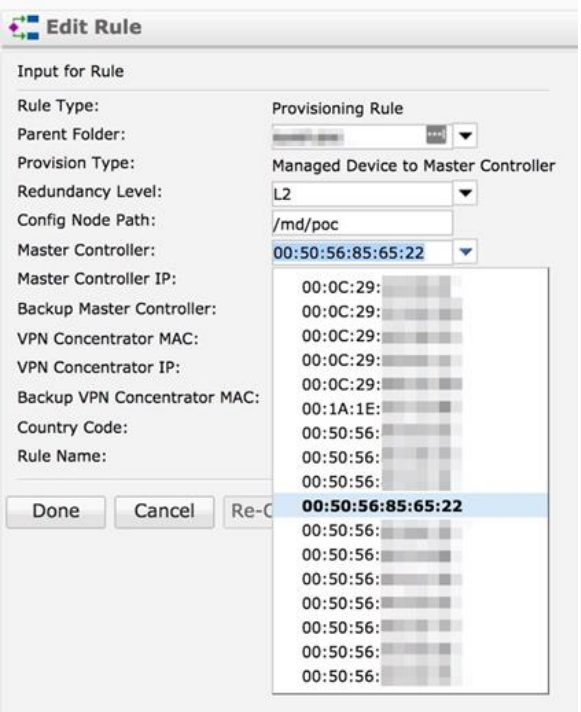
Figure 37 *Managed Network Node Hierarchy*



Configuration Notes

- When mobility controllers are manually brought up, it is important to ensure that they have been whitelisted on the Mobility Master under the appropriate configuration node.
- When ZTP is used to bring up mobility controllers, it is critical to ensure that the correct configuration node and MAC address of the Mobility Master are configured on Activate.
- Verify that the Mobility Master has learned about the mobility controllers from Activate and whitelisted them under the configuration nodes that were specified in the Activate provisioning rule.
- While specifying the MAC address of the Mobility Master for establishing an IPsec connection during initial configuration, always ensure that the management port hardware MAC address is used for a VMM and the hardware MAC address is used for an HMM.
- When the Mobility Master registers with Activate, the correct MAC address is automatically populated. If controllers are using ZTP to contact Activate and register with the Mobility Master, identify the MAC address of the Mobility Master and select it from the dropdown list while configuring the provisioning rule on Activate.

Figure 38 *Selecting the MM MAC Address*



Chapter 5
Loadable Service Module

Loadable Service Modules (LSMs) is a feature of ArubaOS 8 which allows administrators to dynamically upgrade or downgrade service modules on a system without requiring a controller firmware upgrade or total system reboot. Each application has its own compressed image and upgrades are performed in real time without requiring a controller reboot.

Unified Communication and Collaboration

Unified Communication and Collaboration (UCC) is a Aruba term describes the integration of real-time enterprise communication services such as instant messaging, voice, video conferencing, desktop-sharing, application sharing etc.

In the context of UCC as a feature on Aruba controllers, switches, and APs, it represents unification of various aspects of enterprise communication and collaboration applications. These aspects can be loosely categorized as media detection, media and traffic prioritization, monitoring and visibility, and media classification.

Aruba Controllers support the following UCC applications:

- Skype for Business
- Cisco Jabber
- Session Initiation Protocol (SIP)
- Wi-Fi Calling

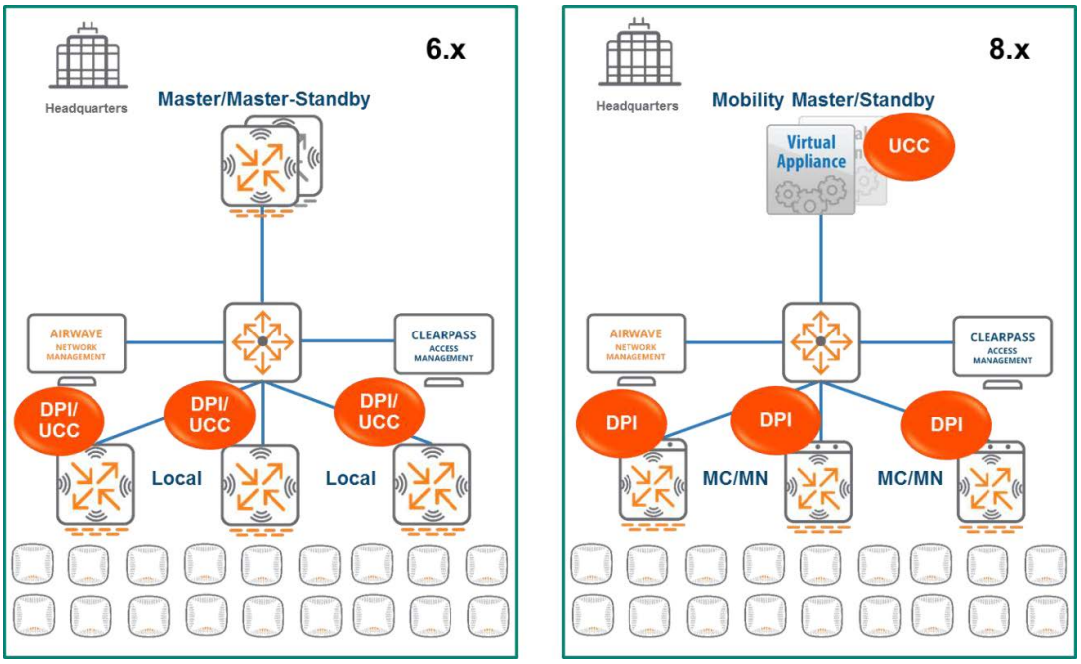
The list of application given above is not comprehensive. Please refer to the ArubaOS User Guide for a completel list of supported UCC applications.

UCC feature capabilities have not changed from ArubaOS 6 and UCC is not a new feature in ArubaOS 8. However, the architecture of the feature and the way it is deployed has been changed in ArubaOS 8.

Architecture Comparison

UCC consists of Deep Packet Inspection (DPI) engine that runs on local controllers in ArubaOS 6 and on mobility controllers in ArubaOS 8. In ArubaOS 6, both DPI and UCC processes run on the local controllers itself. In ArubaOS 8 a portion of the UCC processes which Aruba refers to as the UCC service or UCC application has been moved to the Mobility Master. The DPI functionality remains on the mobility controllers.

Figure 39 *UCC Architectural Comparison between ArubaOS 6 and ArubaOS 8*



New Features of UCC in ArubaOS 8

While UCC in ArubaOS 6 performs well, there are a few drawbacks in its design which were improved in ArubaOS 8 and this provides the following advantages for administrators to consider migrating to ArubaOS 8:

- **Lack of Visibility** – In ArubaOS 6, UCC visibility is not centralized on the master controller. Statistics and monitoring are maintained on the local controllers. This design is not ideal as it requires users to log into each local controller separately to monitor UCC data.
- **Challenging Upgrades** – Adding support for new applications in ArubaOS 6 involves an entire controller upgrade which can be disruptive to the network.
- **No SDN Aggregation** – Skype for Business Software Defined Network (SDN) API usage in ArubaOS 6 involves configuring the SDN Manager with the IP addresses of all subscribers in the network. This has an adverse effect on network scalability.

In contrast, ArubaOS 8 addresses the challenges listed above with improved functionality across the board through its superior architectural design and approach to UCC implementation. UCC now runs as an application (or a loadable service) on the Mobility Master. The DPI engine continues to run on the mobility controllers which function as local controllers in ArubaOS 6.

Classification and prioritization of decision making functionality has been moved to the Mobility Master along with the VoIP application layer gateway which operates as part of the UCC application. In addition, UCC feature can be upgraded independently without having to upgrade the all of the controllers in the network since it is one of the LSMs. This seamless upgrade process allows administrators to add support for newer voice and UCC applications without experiencing any of the adverse effects associated with rebooting a controller.

The Mobility Master brings an important value proposition to enterprises using SfB as their UCC application. SfB SDN APIs can now be aggregated at the Mobility Master for all mobility controllers. This eliminates the need to configure the SfB SDN manager with thousands of IP addresses of individual subscribers. The Mobility Master keeps track of the mobility controller and where the call was initiated and the matches the SDN API messages received from the SfB SDN manager to the call flows while programming datapath on that

particular mobility controller. Employing the Mobility Master-based architecture is introduced in ArubaOS 8 which provides centralized visibility into UCC through the Mobility Master's WebUI.

UCC Heuristics

In the context of UCC, heuristics is a method that the controller employs to detect and classify different types of media. It can be thought of as a form of advanced pattern matching for aspects such as packet size and ports used for flows. The UCC feature itself is comprised of two main processes, DPI and the Unified Communication Manager (UCM).

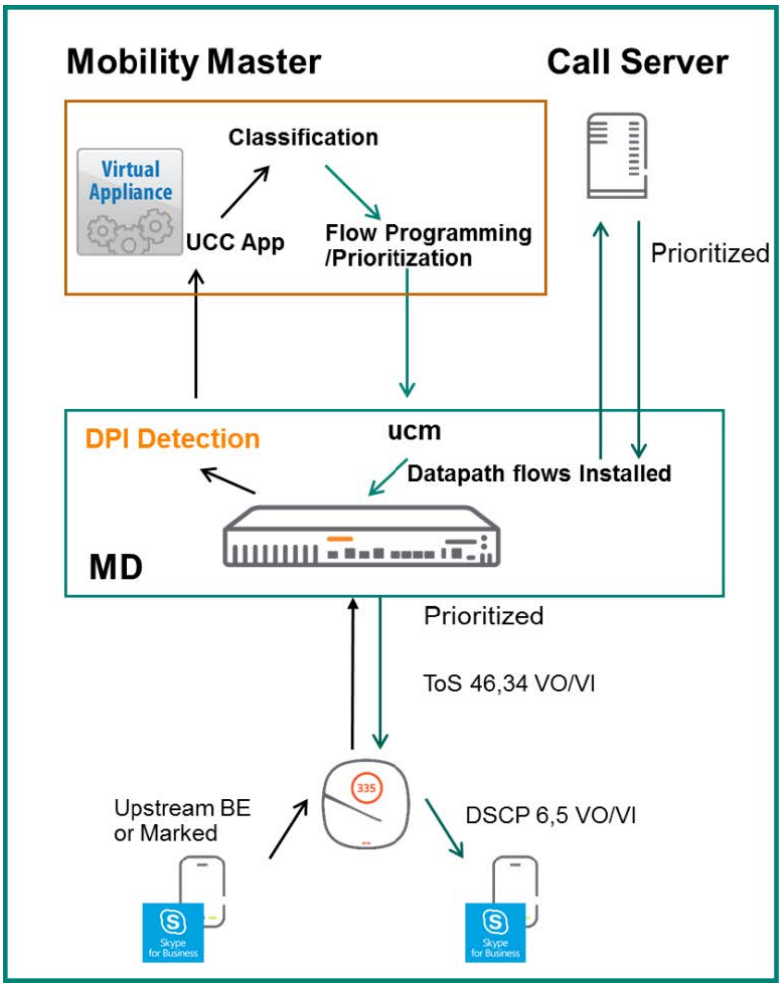
UCM is a process that handles the UCC classification and programs prioritized flows in the datapath of the controller. The following steps outline how UCC in ArubaOS 8 handles a call flow when using heuristics:

1. A client initiates a call and the flow is analyzed by the DPI engine on the mobility controller to detect the presence of media flows.
2. The detection of media flows is passed from the mobility controller to the UCC application on the Mobility Master.
3. The UCC application on the Mobility Master classifies these media flows into categories such as voice, and video.
4. The UCC application on the Mobility Master triggers an action on the mobility controller to program the datapath to prioritize the flow.
5. The prioritized flows are installed by the mobility controller from client to server and server to the call recipient. The result is end-to-end prioritization for both upstream and downstream traffic.

The steps listed above assume preset communication channels between the MM and MC which exchange information related to the call such as trigger flow programming actions

The figure below illustrates the steps described above in an ArubaOS 8 architecture:

Figure 40 *ArubaOS 8 Call Flow with Heuristics*



Skype for Business

Microsoft has developed a service that provides detailed call information to switches which they call the Skype for Business Software Defined Networking Application Programming Interface. This tool was formerly known as the Lync SDN API.

The SfB SDN API has the following three components:

- SfB SDN Manager - Resides next to the SfB front end server
- SDN Dialog Listener - Resides on the front end server
- Subscriber - In an Aruba architecture the subscriber would be the SfB SDN API-certified Aruba Controller (or switch)

NOTE

The SfB SDN API is not to be mistaken with the concept of SDN related to OpenFlow.

The subscriber (in this case the Aruba controller or switch) subscribes to the SDN API Manager which receives SDN API XML messages. These messages consist of XMLs containing detailed call information such as caller, recipient, port numbers, type of call, and endpoint client information.

SDN API Extensible Markup Language (XML) messages dramatically improve visibility into aspects of call quality as well as information that a controller is able to leverage for datapath flow prioritization. If SDN API XMLs used there is no need to engage heuristics for media classification as these flows provide such detailed information to the controller.

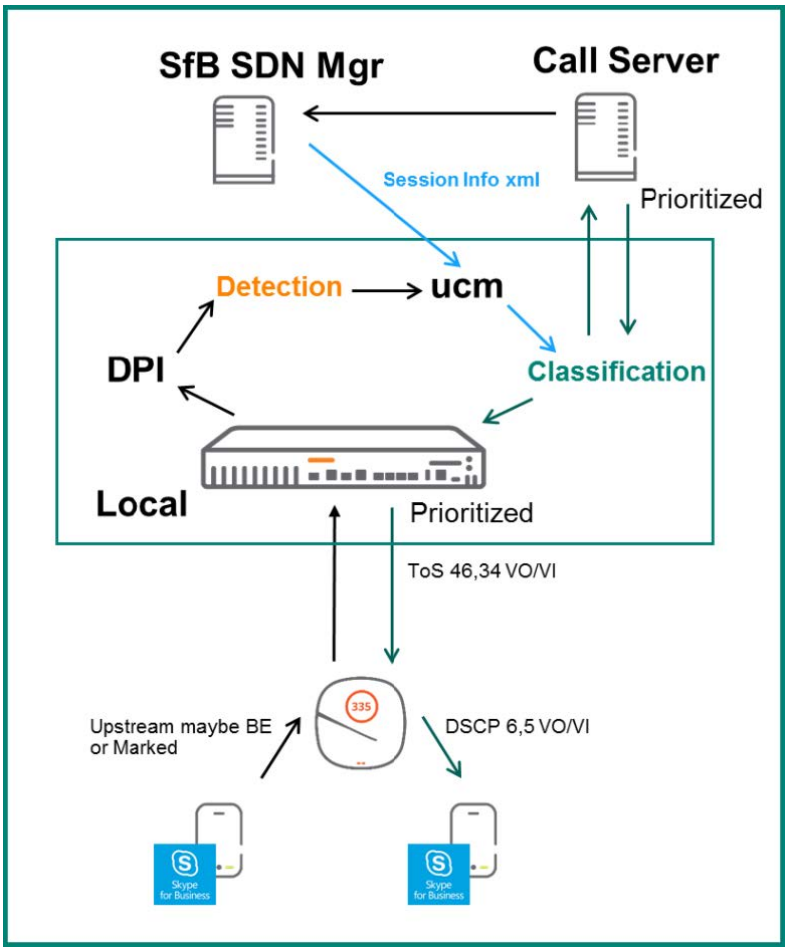
ArubaOS 6 SfB SDN API

In ArubaOS 6, the SfB SDN API is used to enable controllers to classify and prioritize media sessions by listening on a certain port over Hypertext Transfer Protocol (HTTP) or HTTP Secure (HTTPS). The SfB SDN Manager is in turn configured to send messages to the controller over the same port. The steps below outline the process for a call flow utilizing the SfB SDN API:

1. The client initiates a call. The SfB front end server triggers a session info XML and sends it to the SfB SDN Manager.
2. The SfB SDN Manager sends the SDN API XML to the controller that has subscribed to it.
3. DPI on the controller detects the presence of media flows.
4. The controller receives the session info XML which includes details such as caller, recipient, ports, MAC addresses, and media type.
5. The UCM process matches the SDN API XML it receives with the DPI result of the sessions which were identified as media.
6. The UCM programs flows in the datapath to prioritize traffic from the client to call server and from server to the call recipient.
7. Upon call termination, the SDN manager sends a call end message to the controller which includes a detailed statistics about call quality.

The process of how the SfB SDN API work is represented in the figure below:

Figure 41 *ArubaOS 6 SfB SDN API Call Flow*



ArubaOS 8 SfB SDN API

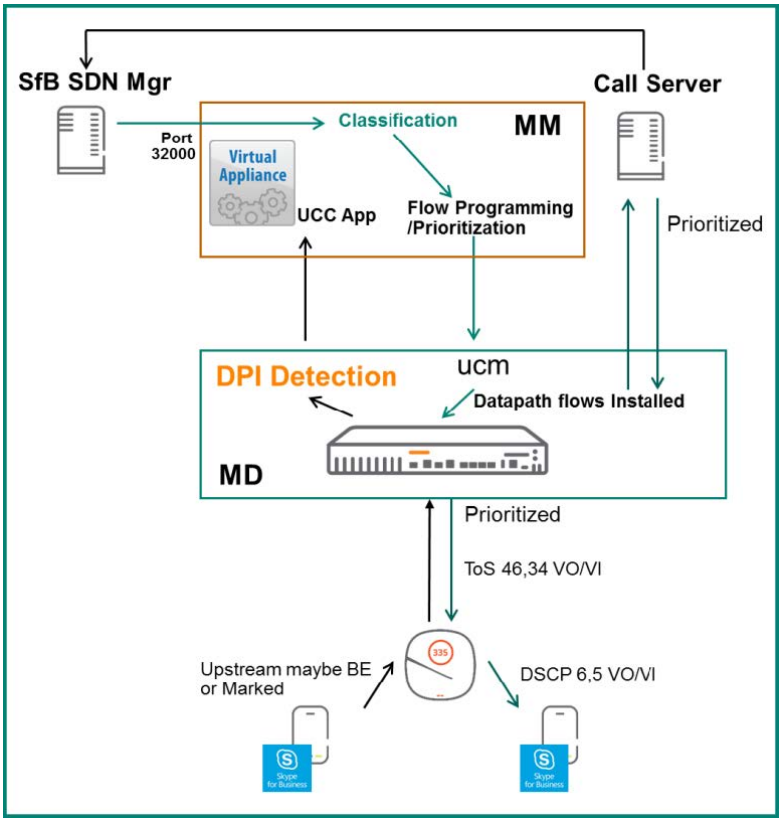
SfB SDN API functionality in ArubaOS 8 is similar to ArubaOS 6 with the key difference that the SfB SDN Manager needs to be configured with the subscriber IP address of the Mobility Master. By default, the Mobility Master is configured to listen to SfB SDN API messages on port 32000. In turn, the SfB SDN Manager sends messages over http or https to the Mobility Master using the same port.

The flow for an SfB call when using SfB SDN API with ArubaOS 8 is as follows:

1. The client initiates a call. Once the DPI engine of the mobility controller detects the presence of media flows, it triggers a notification to the UCC application on the Mobility Master.
2. In parallel, the SfB front end server will send a call session info XML message to the SfB SDN Manager which in turn forwards the message to the Mobility Master.
3. The Mobility Master consumes the XML and correlates it with the mobility controller that originally sent the DPI metadata.
4. The UCC application on the Mobility Master uses SDN session information to classify and program datapath flows.
5. The Mobility Master sends a flow programming action to the mobility controller for the client which initiated the call.
6. The mobility controller programs the datapath accordingly and installs priority flows for both upstream and downstream traffic.

With an ArubaOS 6-based architecture all UCC functionality resides on the local controller. ArubaOS 8 differs in the sense that only the DPI resides on the mobility controller while classification and prioritization decision making are moved to the Mobility Master. One of the key distinctions of UCC in ArubaOS 8 is the ability to aggregate the SfB SDN API messages at the Mobility Master. The figure below illustrates the SfB SDN API process in ArubaOS 8:

Figure 42 *ArubaOS 8 SfB SDN API Call Flow*



AirMatch

ARM in ArubaOS 6

Adaptive Radio Management (ARM) is the primary RF optimization technique used in ArubaOS 6. While ARM was a revolutionary technology when it was introduced, it did suffer a few shortcomings. Some of these are listed below:

- Excessively frequent channel changes that lead to client disconnection and RF network instability, channel plan coupling among proximate radio neighbors,
- Uneven use of available channels
- Asymmetric EIRP planning adversely affecting client roaming behavior
- Lack of 2.4Ghz/5Ghz distinction in EIRP planning
- Lack of automatic bandwidth planning

These drawbacks have led some customers to abandon the ARM solution by either turning off the feature or by manually setting radio parameters through a long and tedious configuration process. ARM had the following characteristics in ArubaOS 6:

- A decentralized service; each individual radio makes its own decision
- ARM is “reactive” in nature
- Future spectrum enhancements
- Asymmetric EIRP planning which may not provide optimal client roaming behavior

When ARM was conceived, the size of the networks was relatively small compared to a modern enterprise network and channel structures were very basic. While it was necessary to have automation in RF planning, it was not as critical for network stability and performance as it is today. At the time it was considered acceptable practice to design a decentralized algorithm where each individual radio makes its own decision based on local information. Perennial convergence time, cascading effects, and mutual coupling or back-off were natural outcomes and regarded as minor issues. In modern production networks such occurrences are no longer acceptable and can pose significant challenges for larger, denser, and increasingly heterogeneous networks.

AirMatch was created to address all the above mentioned challenges which ARM was incapable of addressing. AirMatch is a centralized, clean slate RF optimization service. Information collection and configuration deployment paths are newly defined. The algorithm targets long-term network stability and performance in order to model and address RF challenges for the network as a whole.

AirMatch in ArubaOS 8

AirMatch provides unprecedented quality for RF network resource allocation. It collects data from the past 24 hours of RF network statistics and proactively optimizes the network for the next day.

As a best practice, the RF plan change should be deployed at the time of lowest network utilization so that client disconnects have a minimal impact on user experience. In addition to proactive channel planning done every 24 hours, AirMatch also reacts to dynamic changes in the RF environment such as radar and high noise events. AirMatch results in a stable network experience with greatly minimized channel and EIRP changes. AirMatch is defined by the following key attributes:

- A centralized RF optimization service
- Newly defined information collection and configuration deployment paths
- Models and solves the network as a whole
- Results in optimal channel, bandwidth, and EIRP plan for the network

AirMatch only functions if the network is managed by an MM and is incompatible with an MCM architecture. In an MCM topology all channel, bandwidth, EIRP and other RF optimization decisions will continue to be made by ARM as they would be in an ArubaOS 6 architecture.

If the link between the Mobility Master and mobility controller goes down, Mobility Master will be unreachable and there will be an impact to performance. However, AirMatch will still continue to function. Most notably, the features which require the centralized coordination of the Mobility Master will be lost such as scheduled updates for RF optimization. The current RF solution will continue to function and changes resulting from high noise events and radar will still occur.

AirMatch Workflow

AirMatch is Aruba’s next generation automatic RF planning service which assigns channel, bandwidth, and power to radios in the entire network. The AirMatch service runs on the Mobility Master and generates an RF

solution which specifies new channel, bandwidth, and EIRP settings for each radio. The AirMatch workflow occurs using the following steps:

1. APs send RF statistics as AMON messages to mobility controllers.
2. The mobility controller forward the AMON messages to their Mobility Master.
3. AirMatch calculates the optimal RF solution.
4. The Mobility Master pushes the solution back down to the mobility controllers.
5. Mobility controller send dot11 radio profiles to APs.

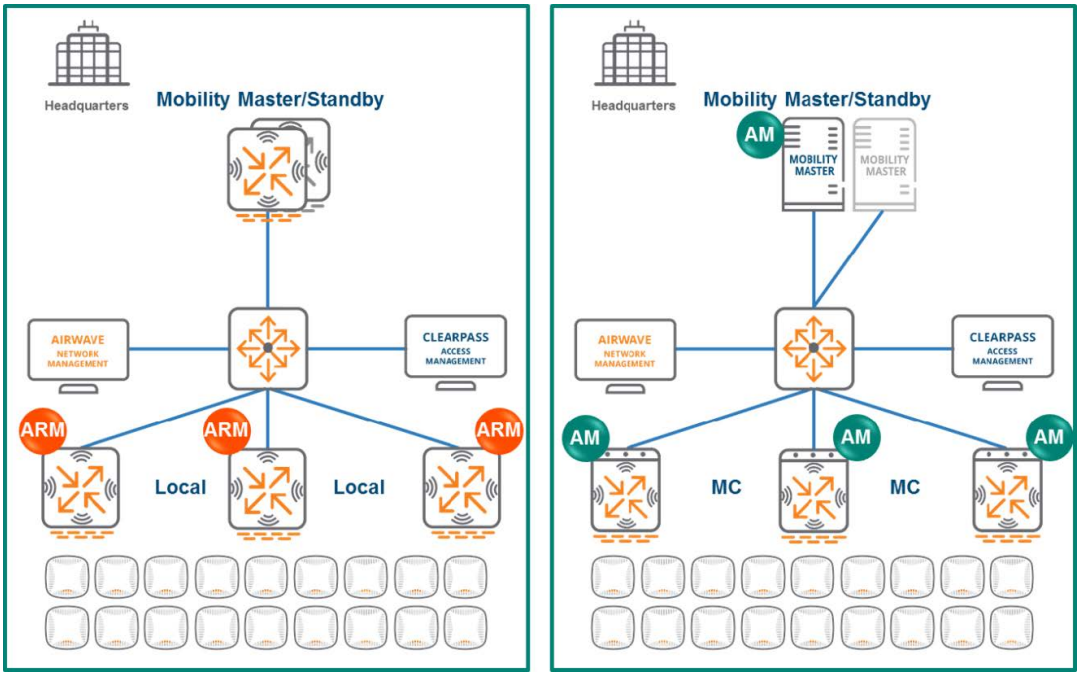
AirMatch and ARM Comparison

The following table and images provide an overview of how AirMatch in ArubaOS 8 differs and improves upon the functionality provided by ARM in ArubaOS 6:

Table 7: *AirMatch and ARM Comparison*

Feature	AirMatch	ARM
ArubaOS 8 Support	Mobility Master	Standalone or MCM
Computation	Centralized	Decentralized
High Noise Avoidance	Yes	Yes
Radar Avoidance	Yes	Yes
Optimization Scope	Entire RF network	Each AP
RF information Used	Past 24 Hours	Instantaneous snapshot

Figure 43 *ARM and AirMatch Comparison*

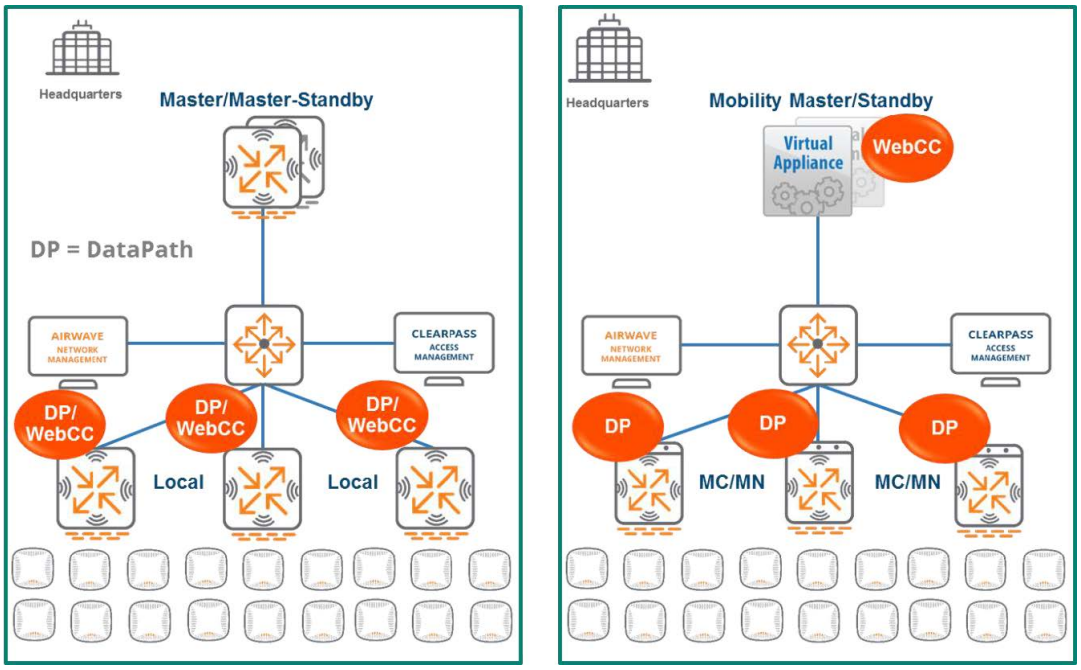


Web Content Classification

Web Content Classification (WebCC) is a feature on Aruba controllers and IAPs that was first introduced in ArubaOS 6. It classifies http and https traffic into category and reputation. Firewall rules can then be applied accordingly based on WebCC's classification. WebCC prevents spyware and malware by blocking access to dangerous and provide visibility into the web content categories and sites being accessed by users.

In an ArubaOS 6 deployment, the WebCC process runs on the local controllers. In ArubaOS 8, the underlying architecture has been changed by moving WebCC process to the Mobility Master in the form of an application or loadable service.

Figure 44 *WebCC Changes in ArubaOS 8*

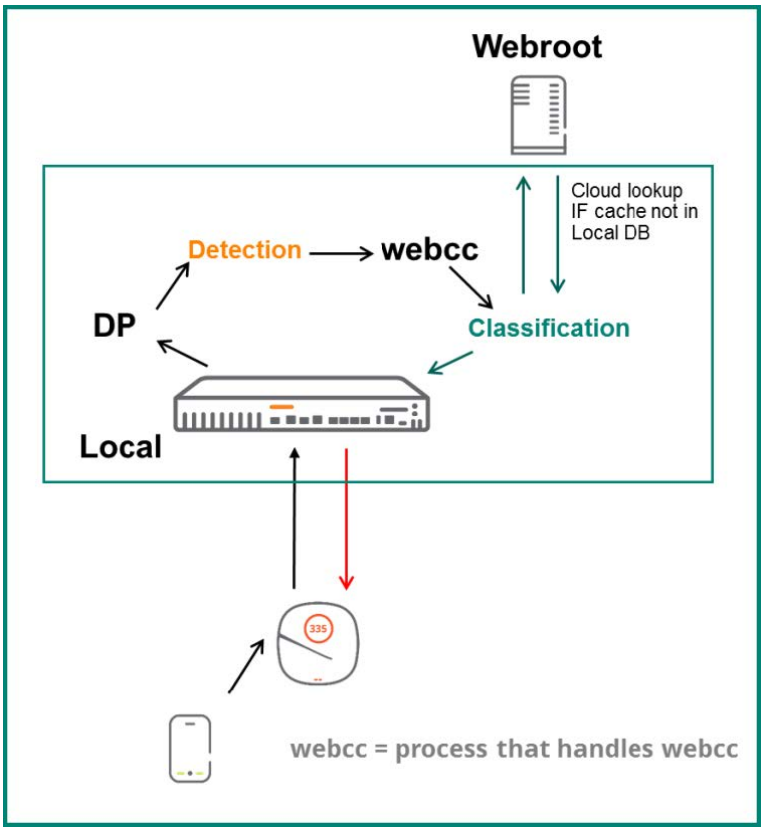


WebCC in ArubaOS 6

WebCC runs as a process on local controllers in ArubaOS 6 and works in conjunction with the datapath. Its primary role is to snoop http/https traffic in the datapath and inspect it to determine if further action is required. Once a client has IP connectivity and accesses a URL, the datapath intercepts http(s) traffic from client and checks against its local URL cache for a match. If datapath finds a match then classification and reputation rules are applied. The classification provided by WebCC is also used in a firewall access list which can take action to allow or deny access to the URL based on the additional information.

If the datapath cache does not find a match for the URL the client is attempting to access, then a URL-miss trigger is sent to WebCC. The WebCC process looks up the URL in the database maintained by the controller. If a match is found, the URL will be classified and the information will be provided to the datapath. This information is then used in an ACL to either deny or allow access to the URL. If the WebCC process does not find a match in the URL database, it performs a real-time cloud lookup from the Brightcloud repository and requests the URL's classification.

Figure 45 *WebCC Design in ArubaOS 6*



While WebCC in ArubaOS 6 offers significant advantages, there are a few drawbacks with the design. Each controller maintains a URL database, however controller sizes vary as do their database and memory sizes. The web URL database that can be maintained on a controller is dependent on the size of that controller. The probability of finding a URL in the local database decreases as controllers are reduced in size. This leads to a increase in the number of times a real-time cloud lookup is required for URL classification in the event of a URL miss. The time required to block a URL increases as well which allows users to access a URL which should have been blocked.

The other drawback of WebCC in ArubaOS 6 is each Local controller is required to individually contact Brightcloud. In addition, local controllers consume memory and space to maintain their URL database.

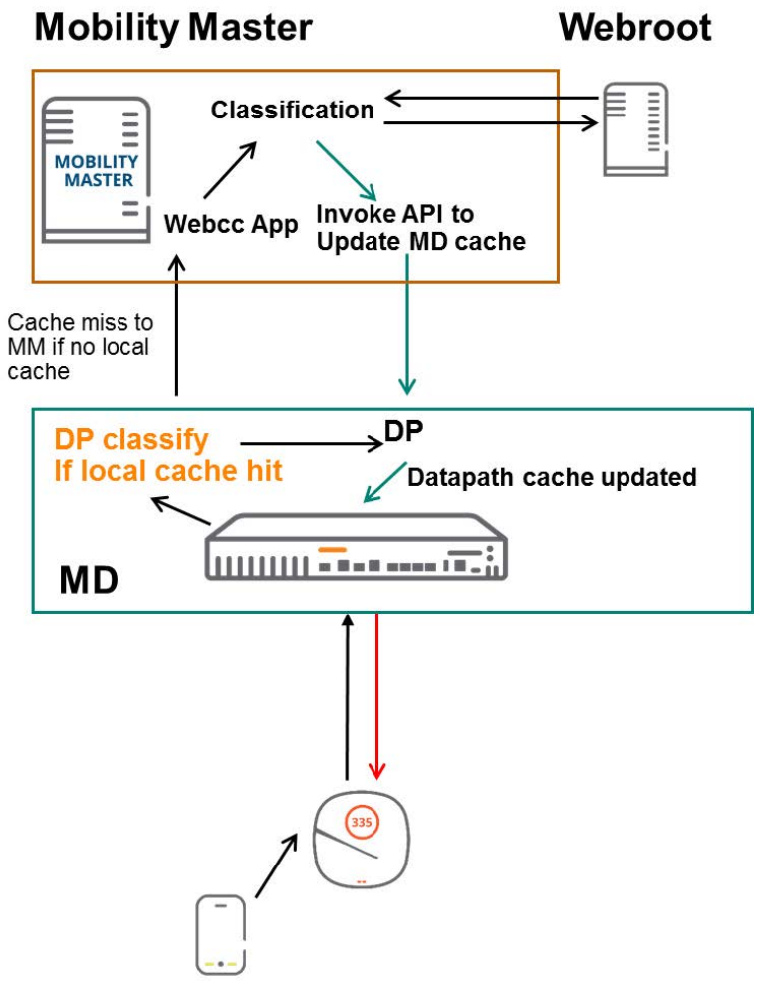
WebCC in ArubaOS 8

The design changes to WebCC in ArubaOS 8 offer numerous advantages compared to the drawbacks inherent in the design of WebCC in ArubaOS 6:

- WebCC runs as a loadable service module the Mobility Master.
- Mobility Controllers maintain only a shallow URL cache which saves memory.
- The Mobility Master has larger memory and is capable of maintaining a URL database of up to 1 million records.
- Cloud lookup for missed URL is performed only by the Mobility Master.

While the flow for WebCC in ArubaOS 8 looks similar to ArubaOS 6, there are some key distinctions to note. The most critical difference is that the WebCC process in ArubaOS 8 runs on the Mobility Master instead of the mobility controller. The flow for the WebCC feature in ArubaOS 8 can be seen in the figure below:

Figure 46 *WebCC in ArubaOS 8*



When a user attempts to access an http or https URL, the packet is snooped by the datapath on the mobility controller which maintains a local URL cache. If the URL is found in the mobility controller's local cache, then classification is applied and further action can be taken to either allow or deny access based on any ACLs that have been configured.

If the datapath of the mobility controller does not locate the URL in its local cache, then a URL-miss is triggered and sent to the Mobility Master. The Mobility Master looks for the URL in its database which is substantially larger than the local cache on the mobility controller. If a match is found, the classification result is sent back down to the mobility controller which will determine if action needs to be taken to restrict access or not based on existing ACLs. If the Mobility Master does not find a match in its local database, it will perform a cloud lookup through Webroot. The Mobility Master will update its local cache and the datapath of the mobility controller which initiated the lookup request.

The Mobility Master should be configured with a DNS server to access Webroot over the Internet.

AirGroup

AirGroup is a component of ArubaOS that resolves usability and performance issues related to the use of multicast Domain Name System (mDNS) services in enterprise and educational networks. Zero configuration networking services such as Bonjour and other mDNS services feature discovery, address assignment, and name resolution for desktop computers, mobile devices, and network services. They are designed for flat, single-subnet IP networks such as residential deployments. In large universities and enterprise networks, it is common for Bonjour-capable devices to connect to the network across VLANs. As a result, user devices such as an iPad on a specific VLAN cannot discover the Apple TV that resides on another VLAN. In order to utilize the mDNS services on mobile devices in an enterprise environment, AirGroup manages zero configuration networking multicasts to improve network throughput, simplify connections to devices that are relevant to the user and location, and be properly forwarded across subnets.

AirGroup in ArubaOS 6

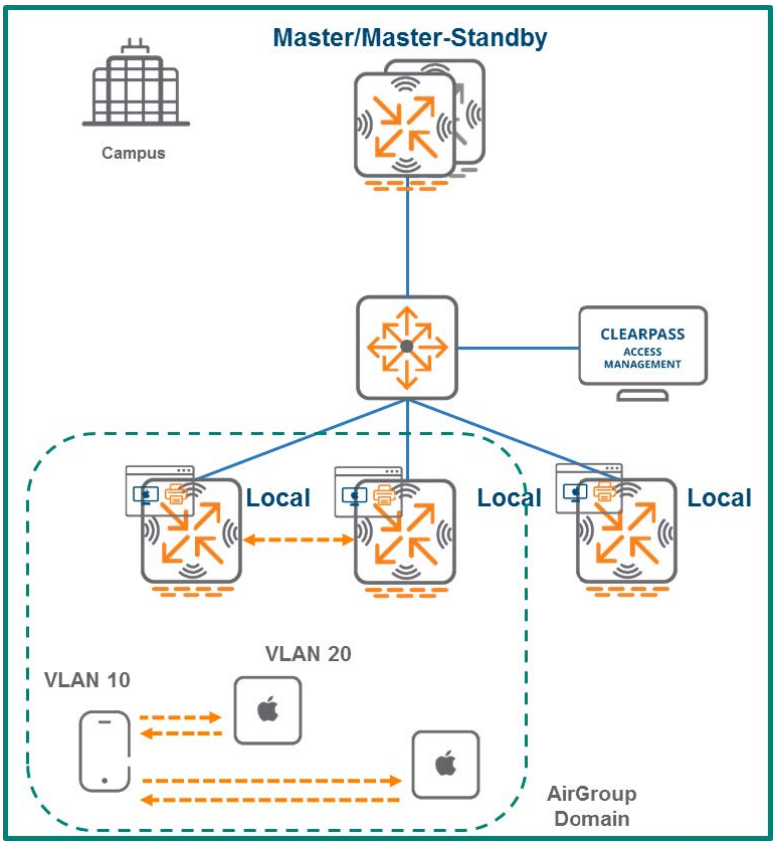
The mDNS protocol is designed to facilitate multicast communication and works well within L2 boundaries. However, only mDNS-capable devices in the same VLAN can communicate with each other. For example, an iPad in VLAN 10 cannot communicate with an Apple TV in VLAN 20.

Aruba created AirGroup to help facilitate communication for devices across VLANs and to provide filtering of peer-to-peer multicast traffic based on attributes including VLAN, user role, user name, user group, and location.

Each controller builds an mDNS cache table by learning and suppressing mDNS or Digital Living Network Alliance (DLNA) queries and advertisements over the air. For example, whenever an iPad sends an AirPlay query, the controller looks at its mDNS cache table and if an AirPlay service is available it responds to the iPad via unicast. Unicast packets help reducing channel utilization in the air.

AirGroup domains can be used for mDNS and DLNA communication between devices across different controllers. In addition, controllers are capable of integration with ClearPass to create Personal Area Networks. AirGroup servers can be defined on ClearPass and can optionally be shared along with usernames, user roles, user groups, AP group, AP name, and AP FQLN.

Figure 47 *AirGroup in ArubaOS 6*



AirGroup in ArubaOS 8

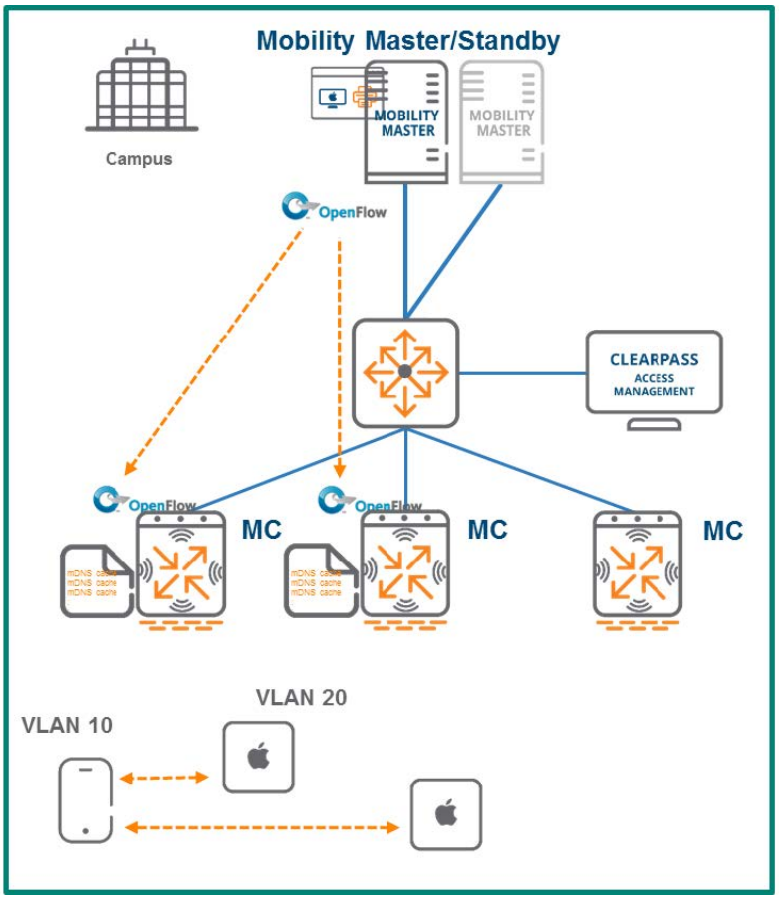
While AirGroup in ArubaOS 6 is capable of providing significant functionality enhancements it suffers from scalability limitations. ArubaOS 8 solves the platform scalability issues of AirGroup in ArubaOS 6, where scalability was limited by the platform capacities of controllers.

Unlike ArubaOS 6 where each controller runs AirGroup individually, AirGroup functionality has been moved to the Mobility Master in ArubaOS 8. The entire mDNS cache table resides on the Mobility Master. An OpenFlow controller is installed on the Mobility Master and OpenFlow agents are installed on mobility controllers for communication of mDNS and DLNA information. Whenever the mobility controllers intercept an mDNS or DLNA query or advertisement, it will be forwarded to the Mobility Master using the OpenFlow channel.

The Mobility Master creates the appropriate mDNS/DLNA flows based on its AirGroup policies and pushes these flows to the mobility controllers. The mobility controllers either allow or deny mDNS and DLNA communication for the AirGroup devices on the WLAN.

AirGroup is significantly more scalable in ArubaOS 8 as the Mobility Master is equipped with appropriate resources to handle large amounts of mDNS communication on the network compared to a hardware-based controller in ArubaOS 6.

Figure 48 *AirGroup in ArubaOS 8*



AirGroup Feature Enhancements

Table 8: *AirGroup Feature Enhancements*

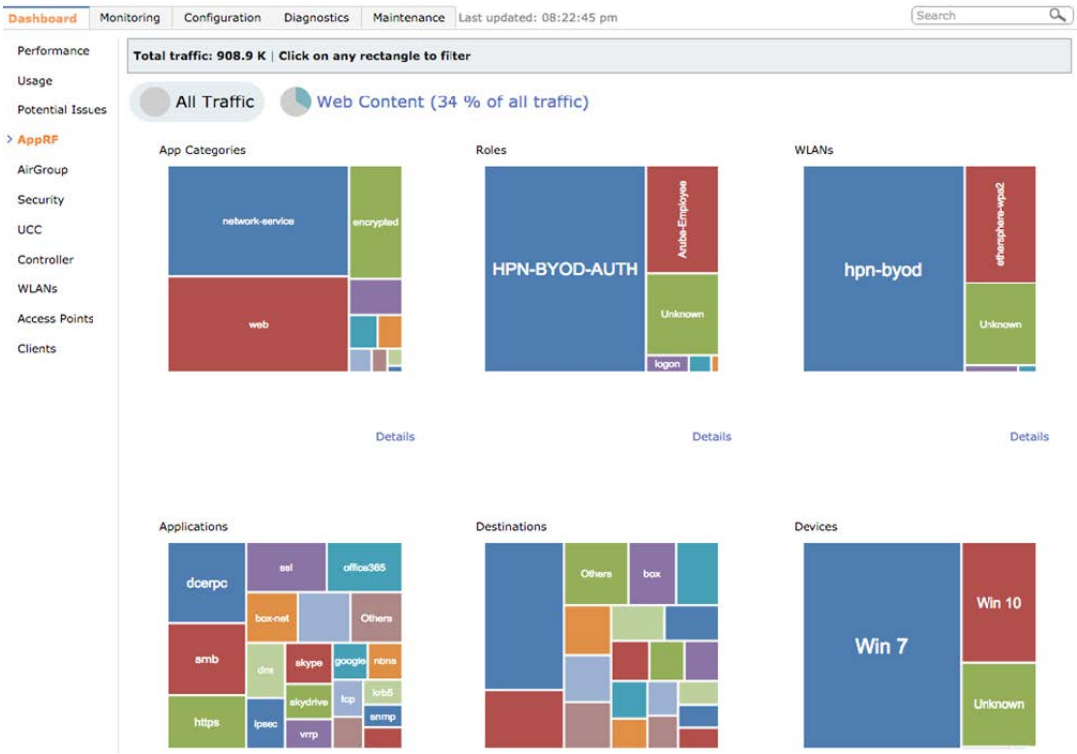
Feature	Comments
AirGroup support for wired users	Wired users can now search for AirGroup services.
AirGroup dashboard	Shows mDNS/DLNA traffic trends, server distribution, and user/server bandwidths.
Ability to define number of hops	Ability share services with users up to 3 RF hops away from AP.
Disallowed named VLAN	Allows to restrict AirGroup services across groups of VLAN IDs.
Disallowed VLAN ID (for users)	Ability to define disallowed VLAN ID for users in addition to the servers.
Disallowed user-role (for servers)	Ability to define disallowed user-role for users in addition to the servers.

AppRF

AppRF in ArubaOS 6

AppRF in ArubaOS 6 has the capability of identifying and applying policies to approximately 2000 applications including allowing, blocking, or rate limiting. Upgrading AppRF or adding new AppRF signatures in ArubaOS 6 requires a system-wide upgrade. For example, even if new signatures only need to be tested on one of the local controllers or a bug needs to be fixed in a Master-Local controller deployment, the master controller in the network needs to be upgraded along with all of the local controllers. This limitation causes network disruption and requires scheduling a downtime for the entire network. In addition, ArubaOS 6 cannot create custom AppRF policies or custom application categories.

Figure 49 *AppRF in ArubaOS 6*

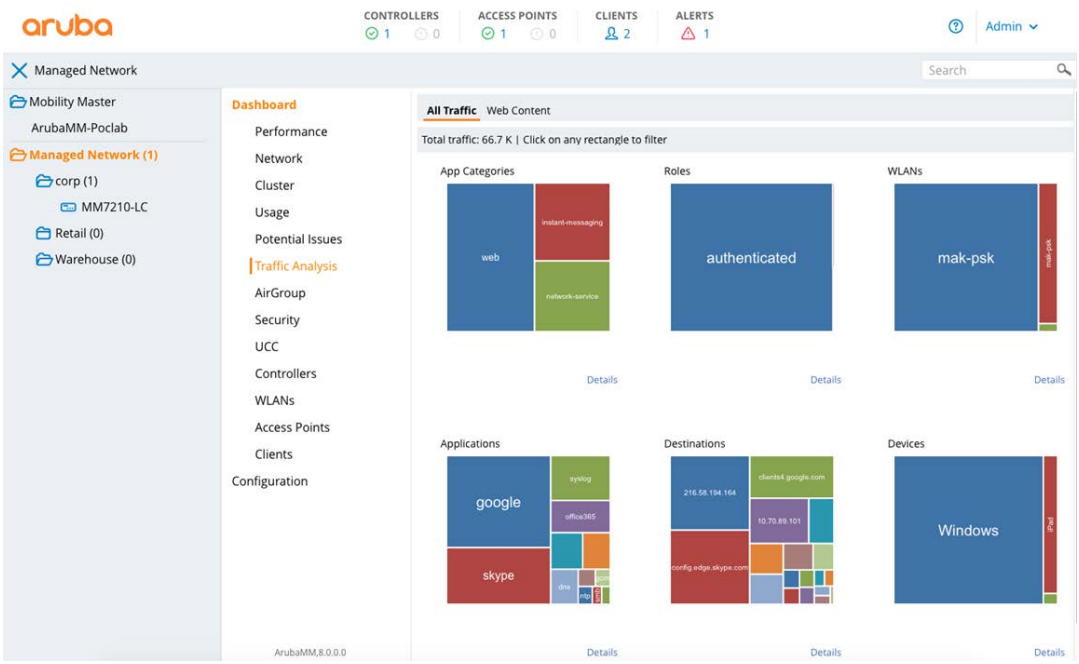


AppRF in ArubaOS 8

ArubaOS 8 provides the support for adding new applications to the controller without having to perform an upgrade. A proto bundle can be downloaded and activated at runtime to add support for new applications. DPI currently supports around 2,000 applications that can have rules applied to them. In ArubaOS 6, custom applications such as applications internal to the organization cannot be classified. ArubaOS 8 supports custom applications which can be pushed to the mobility controllers as desired.

New applications defined on the Mobility Master will be stored as application signatures in binary format and are delivered to mobility controllers when configurations are pushed down. The application signature is then added to the active signature set on the mobility controller providing the capability to support and define new applications as needed. The Mobility Master can configure up to 64 custom applications with 16 rules per application. Custom application categories can also be created and have policies applied to them. Even if a mobility controller loses connectivity with the Mobility Master and the standby Mobility Master , it will not lose application classification functionality.

Figure 50 *AppRF in ArubaOS 8*



Application Programming Interface

In ArubaOS 8, the following three methods can be used to automate configuration:

- Command Line Interface
- Graphical User Interface
- Application Programming Interface

ArubaOS 6 allows configuration automation only using the CLI and WebUI. Unfortunately, being limited to these methods imply that if the CLI output changes over time, the scripts should also be changed since not all outputs are generated using structured data. Modifying scripts every time there is a new code release can become tedious. Similarly, the WebUI is based on CLI and some WebUI pages are hardcoded.

ArubaOS 8 introduced structured APIs which are based on JavaScript Object Notation (JSON) model. The JSON model uses GET and SET messages in a structured format for all configurations. Structured data implies that all data is organized in a particular format where all elements that belong to a data type follow the same data model. This is achieved by separating schema from data. Schema (also called metadata) is a data model representation in JSON format which tells the user how to interpret the data.

Data in the context of ArubaOS 8 is the representation of the configuration state of the Mobility Master in JSON format. The Mobility Master arranges the data in the same order as the schema so that it can be interpreted according to the schema instructions.

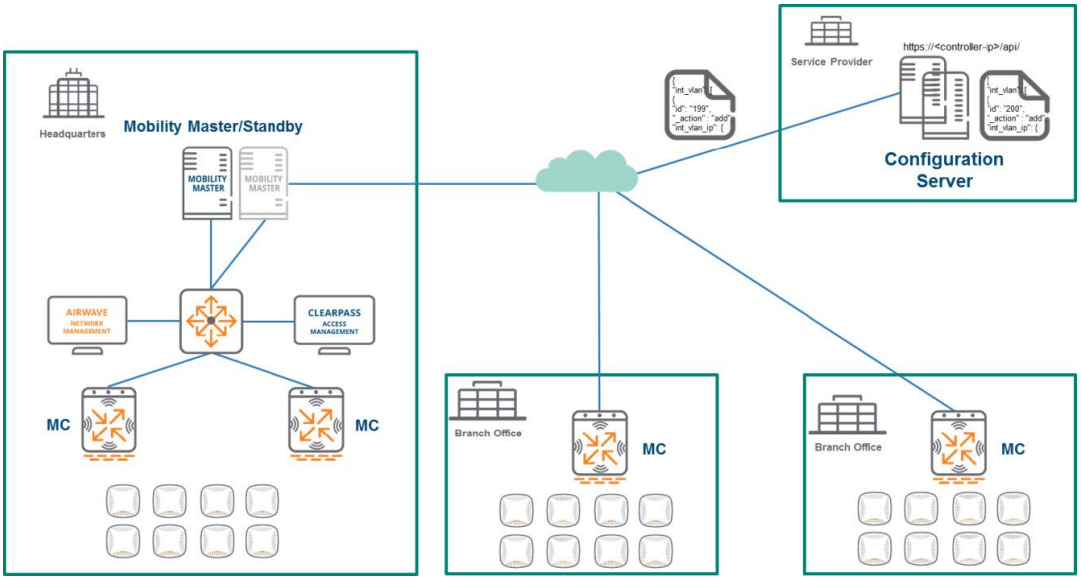
Configuration APIs

Configuration APIs use HTTPS to make GET and POST calls to the Mobility Master. GET APIs are used to learn the configuration status of mobility controllers and provide a similar output to show commands with the difference that they are in JSON format. POST APIs are used to configure mobility controllers. For example, the creation of new VLANs can be accomplished through POST APIs.

Configuration APIs may be appealing to service provider-oriented customers or customers who build their own large data systems using tools such as Elk Stack where they can use 3rd party APIs to interact with the

entire network from a single point of configuration. A complete list of APIs is available at https://x.x.x.x/api where x.x.x.x represents the IP address of the controller.

Figure 51 *Configuration APIs in ArubaOS 8*



Context APIs

Context APIs are similar to the northbound APIs in Aruba's Analytics and Location Engine (ALE). Its main purpose is network analysis. The predefined APIs in ArubaOS 8 are listed below:

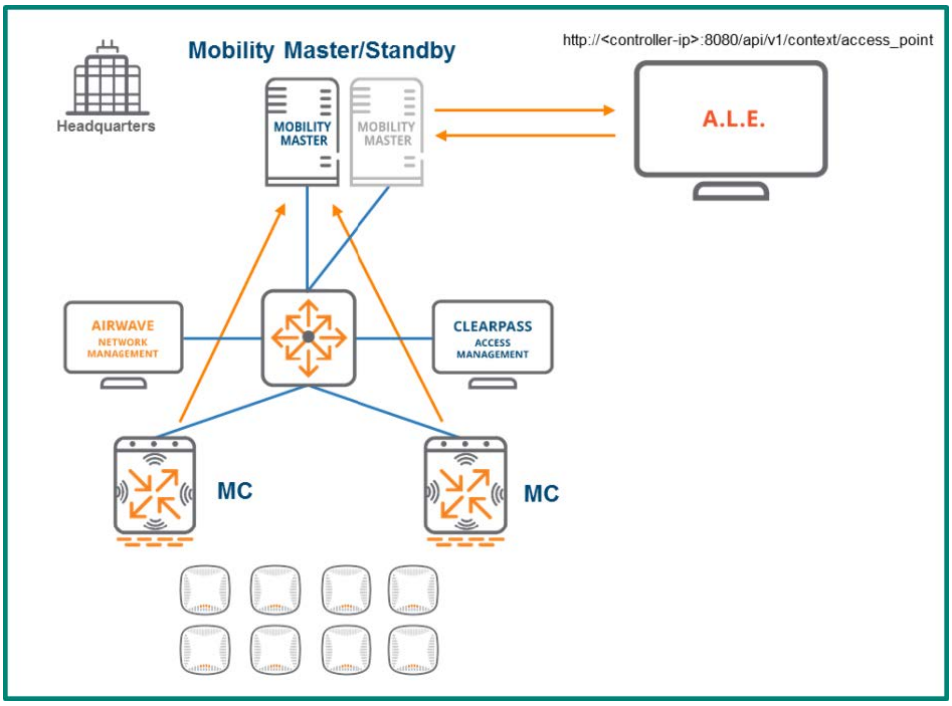
Context APIs

- Campus
- Building
- Floor
- Access_point
- VAP
- Station
- Radio
- Destination
- Application

From ALE

- Presence
- Location
- Geofence

Figure 52 *Context APIs in ArubaOS 8*

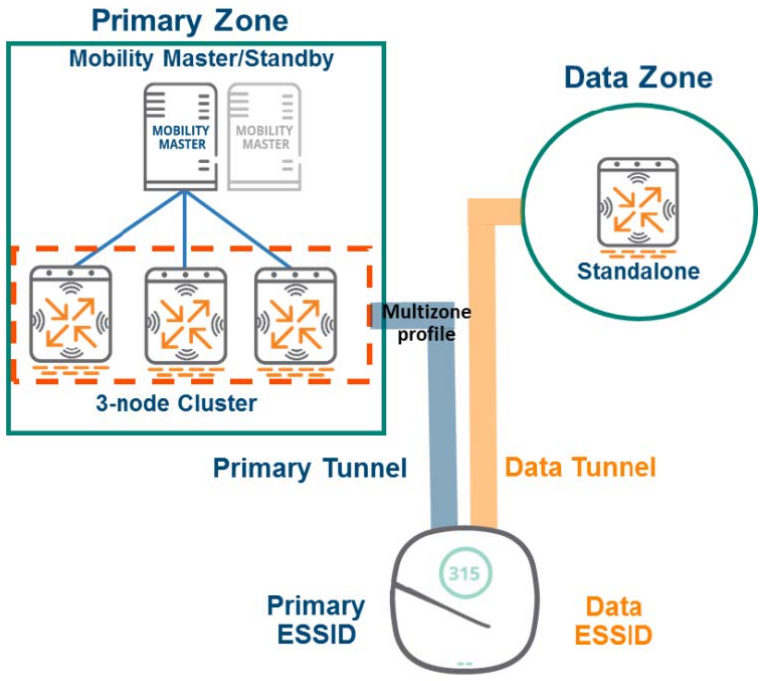


Multizone is a feature in ArubaOS 8 which allows IT organizations to have multiple separate and secure networks using the same AP. Historically, creating two secure networks in one physical location required separate APs. Multizone enables one AP to terminate two different SSIDs on two different controllers. The data from the client to the controller is encrypted, including when it flows through the AP. Multizone in ArubaOS 8 allows for complete secure network segregation and security even though the same AP might service traffic from multiple networks. A zone is a collection of mobility controllers under a single administration domain. The zone could consist of a stand-alone controller or a Mobility Master and its associated mobility controllers . A Multizone AP is an Aruba AP that is capable of terminating its tunnels on mobility controllers residing in different zones. An ArubaOS 6 deployment where an AP terminates its tunnels on a single controller would be considered a single zone deployment.

Architecture

In a Multizone deployment, a primary tunnel exists between the AP and the primary zone. In the below example, the primary zone is a Mobility Master with a 3 node cluster of mobility controllers. The Multizone profile is downloaded to the AP from the primary zone. When the Multizone profile is acquired, AP learns the IP address of the data zone controller (stand-alone) and establishes a data tunnel.

Figure 53 *Multizone Architecture*



Zone Roles

Multizone has several key objectives and abilities:

- Ability to leverage an existing AP deployment to broadcast SSIDs from different controller domains or zones.
- Creating secure containers for different Basic Service Sets (BSSs) belonging to different organizations.
- A wall is erected between zones where each administrative domain can only view and manage its own SSIDs.

Primary Zone

- Zone that the AP connects to while booting up.
- Retains full control of AP management and configuration (AP, WLAN, and RF profiles).
- Zone where the Multizone profile is configured to enable the feature.

Data Zone

- Secondary zone that an AP connects to after receiving the Multizone configuration from the primary zone.
- Cannot reboot, upgrade, or provision a Multizone AP.
- The only configuration allowed is the virtual AP configuration in tunnel mode.

The RFP license must be enable on the Primary Zone to enable the Multizone feature. No licenses are required on data zone controllers.

Key Considerations

- Mobility controllers in all zones need to run the same ArubaOS version.
- The data zone should use the same AP group and AP name used by the primary zone.
- The primary and data zone mobility controllers cannot be managed from the same Mobility Master.
- There can only be a maximum of 5 zones, 1 primary zone and 4 data zones respectively.
- There can only be a combined maximum of 12 controllers for all zones.
- The limit of 16 VAPs per radio still applies for all zones.
- Remote APs are not supported.
- All AP types are supported except for AP-9x.

Chapter 7
Mobility Master Redundancy

While designing mission critical networks, it is important to provide redundancy not only for the data plane but also for the management and control planes. In addition to losing ability to push configurations, there are services which may be adversely affected in the absence of a Mobility Master. Redundant Mobility Masters in a network ensure that configuration and service-related tasks are protected and will continue to perform as expected at all times.

The following list of services are impacted when the Mobility Master is unreachable:

- AirGroup operations (centralized mode only) and dashboard visibility
- UCC dashboard visibility
- Uncached WebCC lookups
- AirMatch recalibrations
- ClientMatch
- Configuration APIs
- Wireless intrusion detection and prevention

In ArubaOS 8, Layer 2 and Layer 3 are the two types of redundancy which can be configured for the Mobility Master. Layer 2 redundancy addresses redundancy within the data center (DC). The active Mobility Master manages all the mobility controllers in the network, the associated configuration and the service-related tasks. The active Mobility Master is backed up by a standby Mobility Master using VRRP. If the active Mobility Master fails, the associated controllers will failover to the standby Mobility Master immediately. The standby Mobility Master then assumes the role of the active Mobility Master.

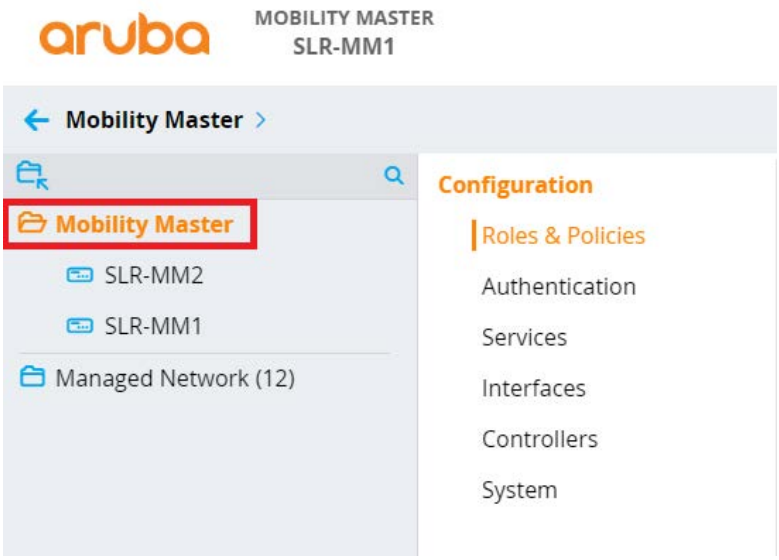
Layer 3 redundancy addresses disaster recovery across Layer 3 separated networks and typically applies to DCs. In an ArubaOS 8 architecture, this involves either one or a pair of Mobility Masters in each DC along with Layer 2 redundancy within the DC while using a pair of Mobility Masters. Within the context of Layer 3 redundancy, one DC is referred to as the primary DC and the other as the secondary DC.

Regardless of which type of redundancy is being used, licenses are configured on the active Mobility Master. These licenses will be automatically synchronized to the L2 and L3 redundant Mobility Masters.

Layer 2 Redundancy

Aruba Mobility Masters rely on VRRP as their layer 2 redundancy mechanism. The entire configuration hierarchy is automatically synchronized from the active Mobility Master to the standby Mobility Master except the configurations under the device configuration node of the active Mobility Master.

Figure 54 *Configuration for All Mobility Masters*



Configurations that are common to both the active and standby Mobility Masters are placed under the Mobility Master node so that they will be synchronized. Configurations specific to the Active Mobility Master like IP addresses and VRRP must be placed individually on its own specific device node. Mobility Master services and managed devices cannot be configured from the Standby Mobility Master.

Figure 55 *Configuration Specific to the Active MM*

Topology

Figure 56 *Layer 2 MM Redundancy*

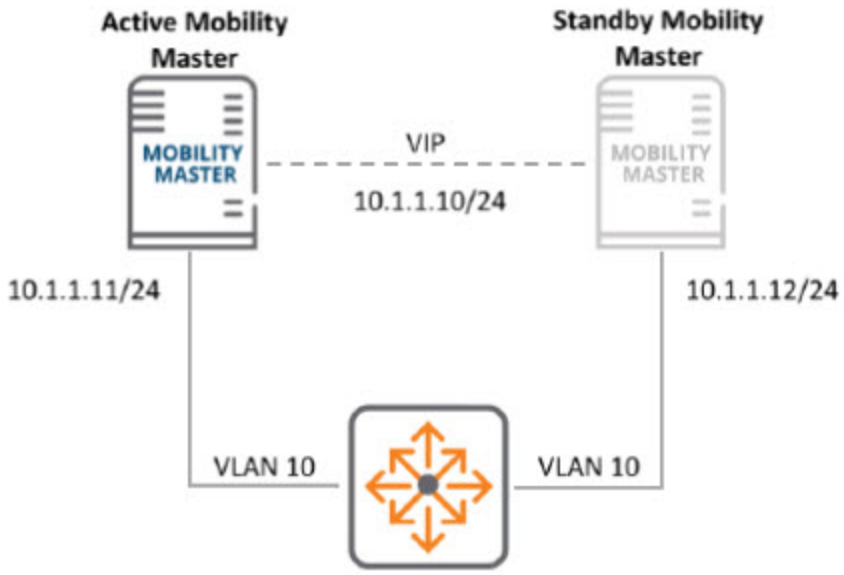


Figure 56 *Layer 2 MM Redundancy*

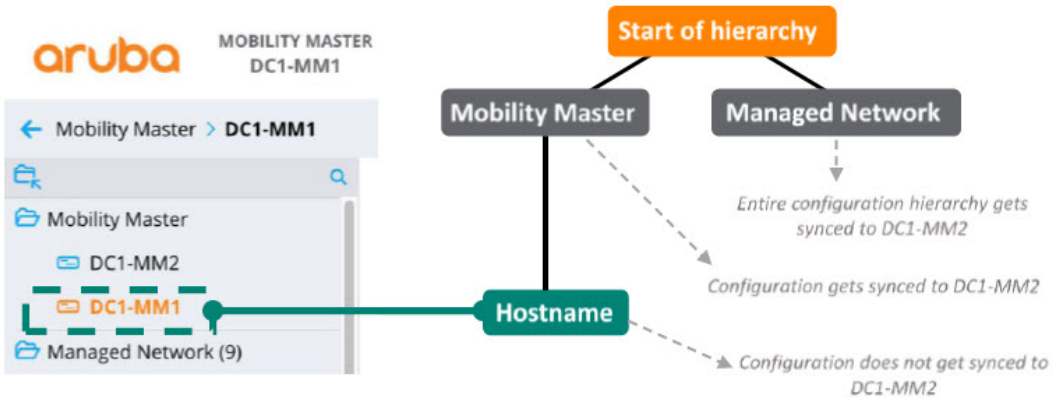
Synchronization

When the VRRP and master redundancy are configured between the active and standby Mobility Masters, the entire configuration hierarchy is synchronized. Following are the list of databases that are synchronized to the standby Mobility Master at periodic intervals when database synchronization is configured on the active Mobility Master:

- WMS Database
- Local User Database
- Global AP Database
- AirGroup Database
- License Database
- CPSec Database

The synchronization interval is specified as part of the database synchronization configuration. The database synchronization interval is configurable. As a best practice, Aruba recommends configuring the time interval of minimum 20 minutes. Configuring a more frequent time interval might add to a substantial amount of network overhead.

Figure 57 *Database Synchronization*



Once the active and standby Mobility Masters have performed their initial synchronization and reached a stable state, any incremental configuration change that is committed and saved on the active Mobility Master results in a configuration synchronization on the standby Mobility Master.

The exception to this behavior is that any change made on the device configuration node of the active Mobility Master (/mynode). These changes are not synchronized to the standby Mobility Master. The standby Mobility Master contains its own version of the device configuration and hence any desired changes must be made directly on its corresponding device configuration node (/mynode on the standby Mobility Master). Configuration changes for other nodes in the hierarchy are not permitted on the standby Mobility Master.

Mobility Controller Failover

Mobility Controllers communicate with their active Mobility Master using the Virtual Internet Protocol (VIP) address of the VRRP instance shared by the Mobility Master pair. By default, the active Mobility Master is master of the VRRP instance and sends out VRRP advertisements every second. The standby Mobility Master monitors these advertisements to ensure if the VRRP instance master functions properly. If the standby Mobility Master fails to receive VRRP advertisements from the master, such as in the event of a controller failure or reboot, the standby Mobility Master will wait until three consecutive advertisements are missed, after which it promotes itself to be the master of that VRRP instance. The mobility controllers continue communicating with the Virtual IP of their Mobility Master. The only impact on mobility controllers is the time taken to establish IPsec sessions with the Standby Mobility Master which has become active due to the change in VIP ownership. The mobility controllers continue to correspond with the owner of the VIP of the VRRP instance between the Mobility Masters. The actual device that owns VIP at any particular moment and therefore has assumed the role of the active Mobility Master is irrelevant to the mobility controllers. .

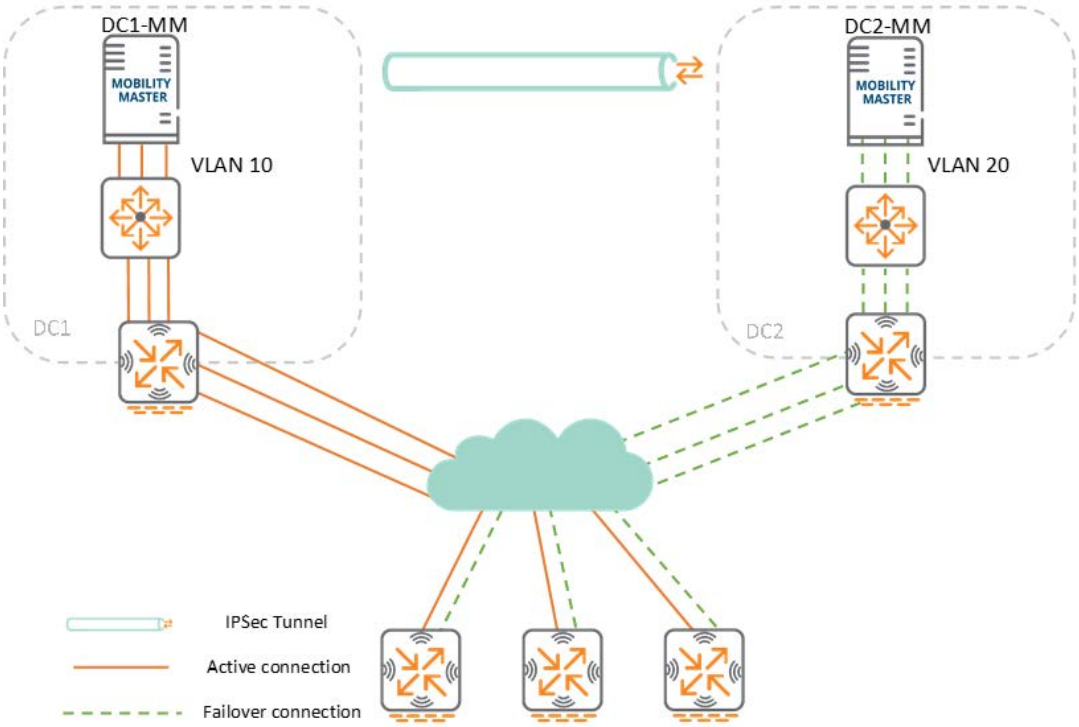
Layer 3 Redundancy

Layer 2 Mobility Master redundancy works well for single data center topologies where the active Mobility Master is supported by a standby Mobility Master. However, in the event of a data center power or network outage, the mobility controllers could potentially lose connectivity to both Mobility Masters which would result in a loss of functionality. Layer 3 Mobility Master redundancy was introduced to prevent the previously mentioned scenario. It involves a primary Mobility Master or MM pair backed up by a secondary Mobility Master or MM pair over a Layer 3 connection to provide service continuity for controllers, if the primary DC goes down. While Layer 2 redundancy can be thought of as redundancy between Mobility Masters within a data center, layer 3 redundancy can be thought of as redundancy between data centers.

Topologies

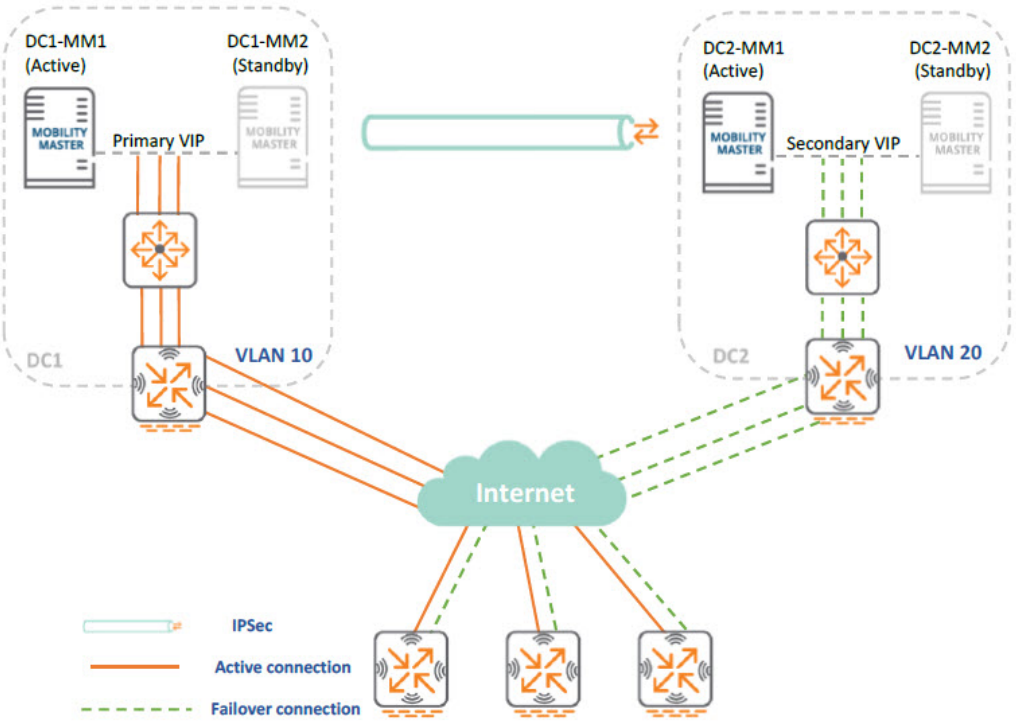
Below are two common examples of topologies that have been configured with layer 3 redundancy between Mobility Masters.

Figure 58 *Layer 3 Redundancy between Two Mobility Masters*



In the topology depicted above DC1 is acting as the primary with DC1-MM while DC2 is the secondary DC with DC2-MM. Layer 3 redundancy has been configured between the primary and secondary DCs. Since MCs are able to detect and initiate the failover, they also need to be configured with the IP address of the secondary Mobility Master.

Figure 59 *Redundancy between Two MM Pairs*



In the figure above, DC1 is the primary DC with DC1-MM1 serving as the active Mobility Master and DC1-MM2 serving as the standby Mobility Master. Layer 2 redundancy is configured between Mobility Masters within each DC. If DC1-MM1 fails, then DC1-MM2 takes over the VIP as the new active MM. The MCs will terminate on the VIP for the VRRP instance between DC1-MM1 and DC1-MM2.

DC2 is the secondary DC with DC2-MM1 as the active MM and DC2-MM2 as the standby Mobility Master. Layer 2 redundancy is configured between them in the same manner as in DC1. If DC2-MM1 fails, then DC2-MM2 takes assumes ownership of the VIP for their shared VRRP instance and becomes the new active MM in DC2.

From the perspective of the mobility controllers, the VIP in DC1 is the primary Mobility Master IP and the VIP in DC2 is the secondary Mobility Master IP address. As with the first layer 3 topology, the mobility controllers need to be configured with the virtual IP addresses for both datacenters.

Synchronization

The entire configuration hierarchy, databases, and associated configurations on the active Mobility Master in DC1 are synchronized with the active Mobility Master in DC2. If Layer 2 redundancy is configured within the DC, then the active Mobility Master in DC2 synchronizes the configuration hierarchy, databases, and associated configurations with its Standby as well.

The configuration sync between MMs does not include configurations under the MM and Device nodes.

Failover

Mobility controllers actively monitor connectivity to both primary and secondary DCs using IP health checks (pings), however active connections are established only with the primary DC. The connection to the secondary DC is built only if the connectivity to all the available Mobility Masters in the primary DC is lost.

If the connectivity to the primary DC is lost, the mobility controllers wait for a 15-minute interval before failing over to the secondary DC. The 15-minute window gives the primary DC a chance to recover and safeguard the Mobility Masters from unwanted failover situations, such as if they have been rebooted. In such instances, the Mobility Master would experience downtime while there was no other intention to fail the mobility controllers over to the secondary DC.

If connectivity to the primary Mobility Master persists after 15 minutes, the mobility controllers will failover to the secondary Mobility Master. The secondary Mobility Master will accept these controllers only if it detects that its own IPsec tunnel with the primary Mobility Master is down. If the primary Mobility Master comes back up at a later time, the mobility controllers will immediately terminate the connection with the secondary Mobility Master and reconnect with the primary Mobility Master.

By default, the secondary Mobility Master remains in the secondary role even after failover. During this time, no configuration changes can be performed on the mobility controllers. This is to prevent a split-brain state when the primary Mobility Master comes back after the secondary Mobility Master had already pushed configuration changes to the mobility controllers resulting in different configurations in each DC. Even in the secondary role, all the services of Mobility Masters will continue to run as usual. Only the configuration capabilities are impacted during a failover of the Mobility Master ; the operational capabilities remain unaffected.

If the primary Mobility Master cannot recover, the secondary Mobility Master can be converted to the primary role and this allows the configuration changes to pushed to the mobility controllers. The process of promoting the secondary Mobility Master to a primary role should be performed manually. This forces network administrators to verify that they are absolutely certain that the primary DC will remain down and this change is both desired and necessary. If the secondary Mobility Master is changed to the role of primary Mobility Master, the failed primary Mobility Master must be reconfigured as the new secondary Mobility Master so that it inherits the new primary Mobility Master's configuration and databases. This prevents the failed primary Mobility Master from assuming its old role when it comes back and also prevents the conflict of having two Mobility Masters in the primary role.

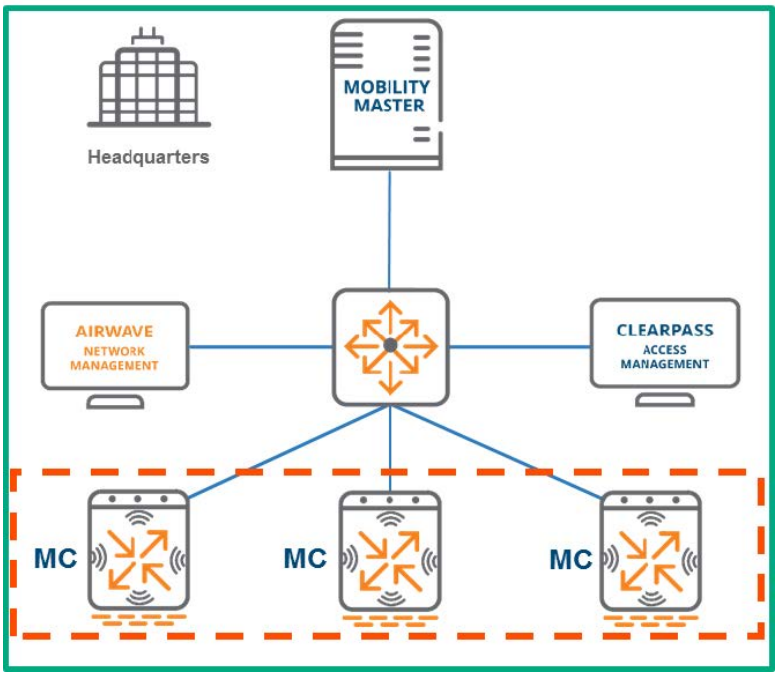
Chapter 8
Clustering

Clustering is one of the key features introduced in ArubaOS 8 and is specifically designed to capitalize on the MM architecture and deliver maximum value for mission-critical networks. Clustering was developed to achieve the following objectives:

- **Seamless Campus Roaming** - Clients in a single large layer 2 domain will associate and stay anchored to a single MC as they roam. Users will retain in the same subnet and have the same IP address even if they roam between APs which are anchored to different controllers. This enables mobility without compromising performance.
- **Stateful Client Failover** - User traffic will remain uninterrupted and high value sessions will be preserved in the event of a cluster member failure. Clients will not be required to re-authenticate and there will be no adverse impact to performance. The impact to performance will be mitigated to such an extent that users will not notice any degradation in their performance and they will have no knowledge that a failure has occurred, regardless of the applications they currently use.
- **Access Point and Client Load Balancing** - APs and users are automatically load balanced across controllers that are members of the cluster. This process ensures an even distribution in order to deliver and maintain optimal network performance and to preserve capacity across all cluster members for new client associations.
- **Live Upgrade** - Aruba allows customers to perform in-service cluster upgrades which allows improvements to be implemented without affecting performance while the network remains fully operational. The Live Upgrade feature allows upgrades to be completely automated. This is a key feature for customers with mission-critical networks that must remain operational 24/7.

Live upgrades can only be performed on MCs in a cluster and the APs attached to them.

Figure 60 *Typical MC Cluster Architecture*



Highlights and Considerations

Clustering is a key feature of ArubaOS 8 yet it cannot be enabled on all devices. Only mobility controllers under the management of a Mobility Master can form a cluster. Mobility Masters cannot become a member of a cluster with another Mobility Master or with mobility controllers. MMs strictly function as management devices for MCs in a cluster. While the redundancy options for an MM environment include both clustering and High Availability (HA) with AP fast failover, these are mutually exclusive features. One or the other must be chosen as the both cannot be concurrently operational.

CAUTION

All MCs in a cluster need to run the same software version so that APs that failover to a new controller will not inadvertently upgrade to a new version.

NOTE

As a best practice, it is recommended to enable CPSec for APs terminating on ArubaOS 8.x Cluster.

It should be noted that clustering is not supported on stand-alone controllers. If stand-alone controllers must be used, then their primary redundancy mechanism is HA. Clustering and all of its constituent features are supported on campus access points, remote access points, and meshed access points and additional licenses are not required. 72xx controlelrs , the 70xx series controllers, and VMCs support cluster.

The cluster capacity for each product line is detailed in the table below:

Table 9: *Cluster Capacity by Product Family*

Product Family	Devices per Cluster
72xx	12
70xx	4
Virtual	4

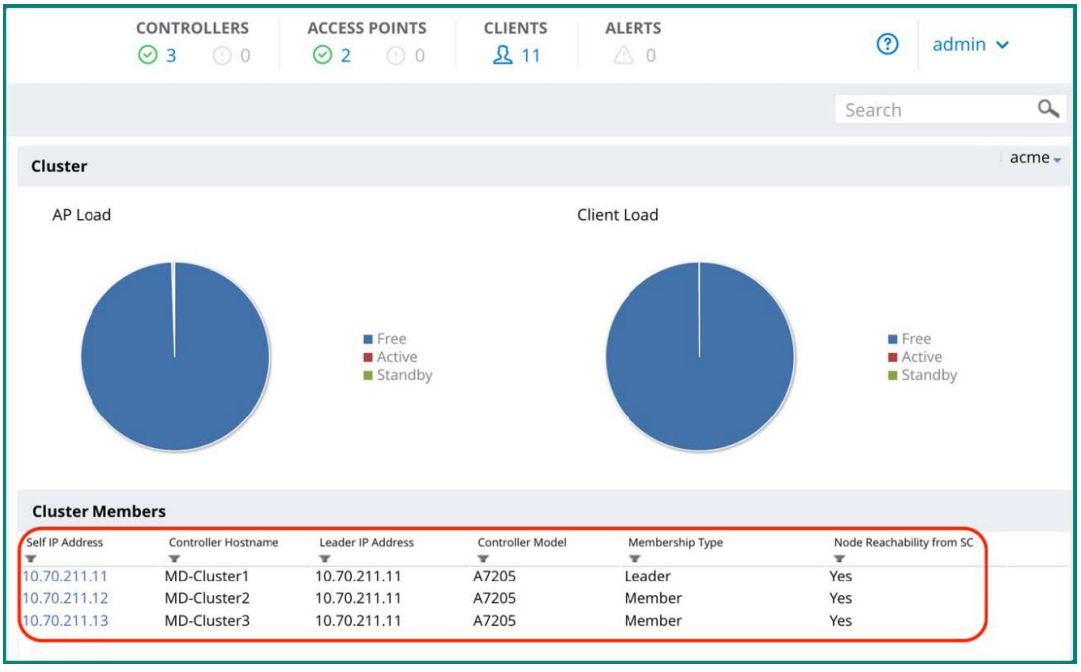
While it is technically possible to combine 72xx and 70xx devices in the same cluster yet it is strongly discouraged as a long term deployment option and is acceptable only as a temporary migration strategy. However as a best practice cluster devices should always be homogeneous. If different controller models are clustered together, the cluster scalability and redundancy limits will be impacted. An Aruba ASE solution provides AP sizing calculation for homogeneous and heterogeneous clusters.

NOTE

Virtual and hardware controllers cannot be combined in a cluster under any circumstances.

If RAPs are terminated on any of the MCs in the cluster, the number of devices allowed in that cluster is limited to 4. However, starting from ArubaOS 8.6, this limit no longer applies to 72xx clusters. The figure below depicts the dashboard view of a cluster:

Figure 61 *MM Cluster Dashboard*



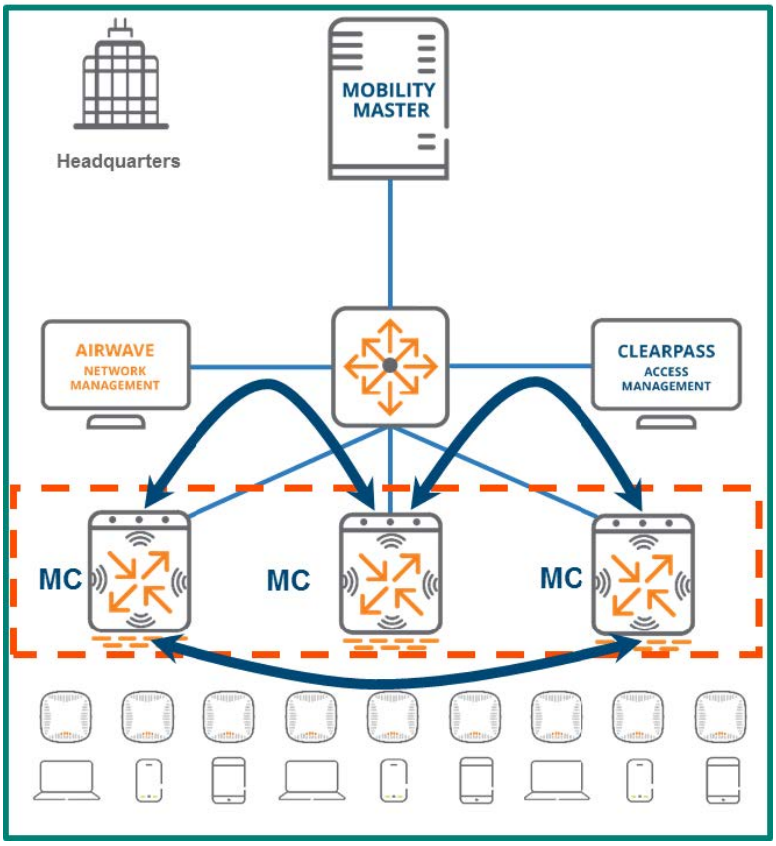
The view above can be accessed through the WebUI by navigating to the **Cluster** tab of the main dashboard. The number of controllers, APs and clients in the cluster managed by the MM and the current AP and client loads of the cluster members can be viewed under this tab. The **Cluster Members** section at the bottom displays statistics pertaining to the MC which are members of the cluster including their IP address, model, and which device is acting as the current cluster leader.

Cluster Formation

Handshake Process

The first step of cluster formation involves a handshake process where messages are exchanged between all potential cluster members. The handshake process occurs using hello messages that are exchanged to verify layer 3 reachability between all cluster members. Information relevant to clustering is exchanged through these messages including build, cluster name, and information about the MC sending the message. After all members have exchanged these messages, they will establish layer 3 IPsec connectivity with each other in a fully-meshed configuration. The figure below depicts cluster members engaging in the hello message exchange process as part of the handshake prior to cluster formation:

Figure 62 *Handshake Process/Hello Messages*



VLAN Probing

After the cluster has entered an L3-Connected state and the cluster members have formed the IPsec connections in a full mush, each member will unicast layer 2 probes on each of its VLANs to the other cluster members. If the probing process is successful, the cluster will transition from an L3-Connected to an L2-Connected state meaning that all cluster members are sharing the same VLANs.

NOTE

Clusters can be formed over a layer 2 or a layer 3 network. Aruba strongly recommends configuring clusters with layer 2 connectivity to enable VRRP. This provides CoA support for the cluster and facilitates controller discovery.

"L2 Connected" and "L3 Connected" are Aruba specific terms which refer to the state of a cluster and indicate whether or not all cluster members share the same VLANs. They are not abbreviations of the traditional networking terms layer 2 and layer 3. The table below provides additional clarification on the topic:

Table 10: *Cluster Connectivity Distinction*

Term	Definition
Layer 2 connectivity	MCs are connected and share the same management VLAN.
Layer 3 connectivity	MCs can reach each other but do not share the same management VLAN.
L2-Connected	A cluster state where all members share all of the same VLANs.
L3-Connected	A cluster state where members do not share all of the same VLANs

MCs in a cluster can be configured in an L2-Connected state even if they do not share all of the same VLANs. This is done by entering a command forcing MCs to exclude certain VLANs from the probing process.

Leader Election

In every cluster one MC will be selected as the cluster leader. The cluster leader has multiple responsibilities including:

- Determining which clients are mapped to each cluster member.
- Dynamically load balancing clients to ensure an even distribution of resources if a cluster member becomes overburdened. When a new member is added to the cluster, the cluster leader will evenly redistribute the load across all members. This is a completely seamless process and users will not experience any performance degradation.
- Identification of the standby MC for each AP and client to ensure stateful failover if a controller goes down.

The cluster election takes place after the initial handshake as a parallel thread to VLAN probing and the heartbeat process. The cluster leader is elected as a result of each cluster member exchanging messages which include their configured priority, platform value, and the MAC address.

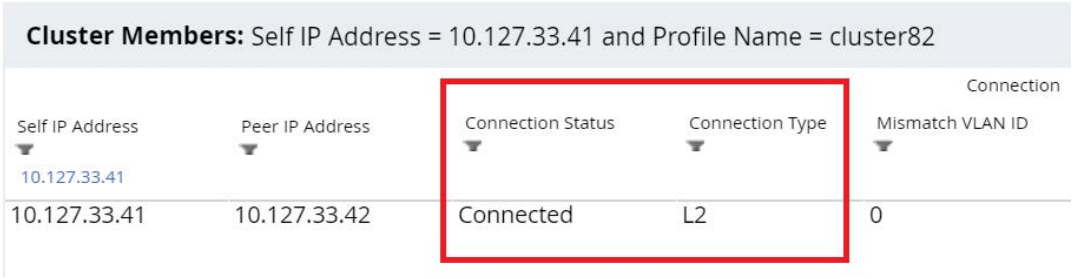
Heartbeats

After the initial handshake, all cluster members will commence sending out heartbeat messages to one another at regular intervals in parallel to the leader election and VLAN probing threads. These heartbeat messages serve as the primary detection mechanism for cluster member failures. Heartbeats are integral to the process the cluster leader uses to determine the role of each cluster member.

Connectivity and Verification

The connectivity of a cluster can be viewed in the WebUI of the MM by navigating to **Dashboard > Cluster > Cluster Members** and then selecting the **IP address** of any cluster member. This view is displayed in the figure below:

Figure 63 *Viewing Cluster Connectivity Status*



Cluster Roles

Apart from being a cluster leader, a mobility controller can have a combination of the following four roles in a cluster:

- AP Anchor Controller (AAC)
- User Anchor Controller (UAC)
- Standby AAC (S-AAC)
- Standby UAC (S-UAC)

AP Anchor Controller

AAC Assignment

Anchoring is a concept that was introduced in ArubaOS 8 as part of the clustering feature . Anchoring and clustering are designed to achieve the following objectives:

- Enhance user mobility through seamless campus roaming.
- Ensure an even distribution of resources across the cluster to maintain the highest achievable performance level.
- Enable redundancy scenarios creating fault tolerance for the cluster and minimizing the impact of an MC failure.

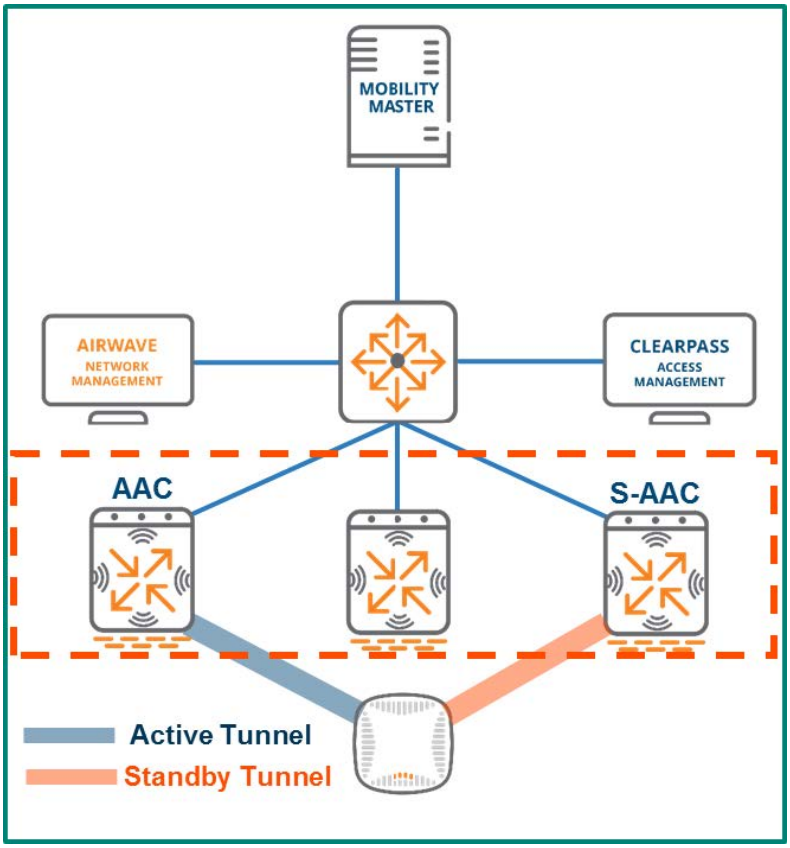
The AP Anchor Controller (AAC) can be thought of as the LMS for any AP that is anchored to it. Each AP receives the IP address of the LMS and once they have been terminated, they will remain anchored until the cluster leader determines that they should be moved to a different cluster member. An AP is anchored to its AAC in a three step process:

1. The AP establishes active tunnels with its AAC.
2. The cluster leader dynamically assigns a standby AP Anchor Controller (S-AAC) for the AP from one of the other cluster members.
3. Once designated the AP established standby tunnels to the S-AAC.

The AAC and S-AAC assignment process works similarly to how HA is configured. However, rather than having to be manually configured the process is completely dynamic. Once the AAC is designated for an AP, the

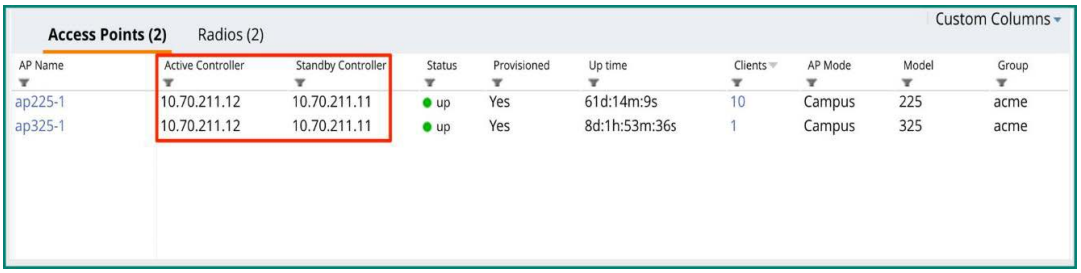
subsequent steps occur automatically. A visual representation of AAC assignment is displayed in the figure below:

Figure 64 *AAC Assignment*



The AAC and S-AAC for an AP can be identified in the WebUI of the MM by navigating to **Dashboard > Access Points:**

Figure 65 *AAC and S-AAC Status*



While the view above indicates that the S-AAC for both APs is the same device (10.70.211.11) it should be noted that the S-AAC is assigned by the cluster leader and not all APs terminated on an AAC will have the same S-AAC. It could be a different cluster member depending on the determination made by the cluster leader based on the conditions in the cluster environment at the time of the assignment.

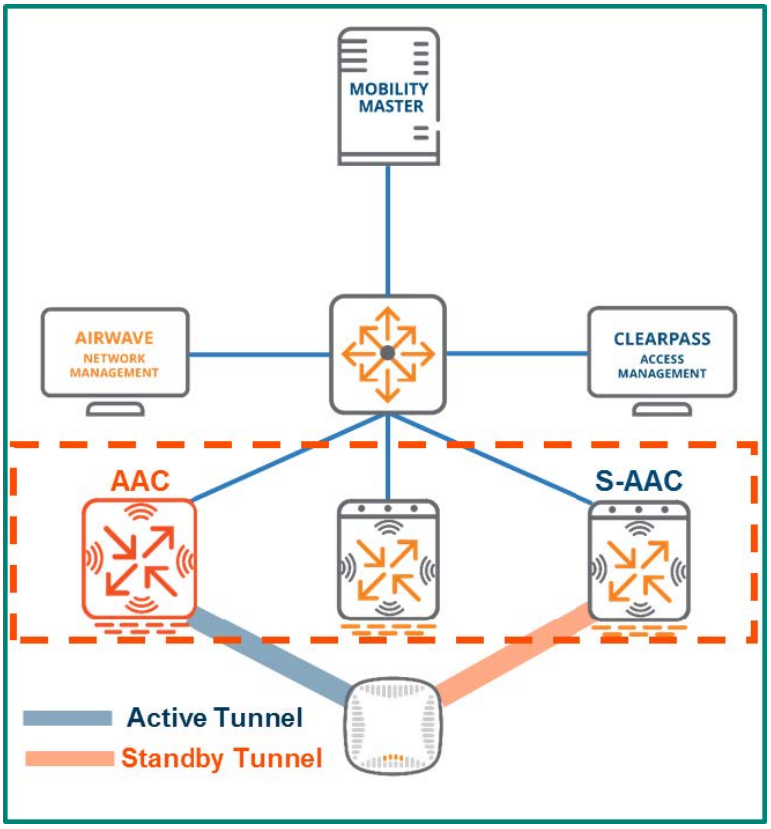
AAC Failover

Every AP is assigned an AAC and S-AAC from the members of the cluster. APs will create tunnels to both MCs in advance to facilitate the failover process. The redundant tunnel to the S-AAC ensures that APs will transition seamlessly in the event of a cluster member failure. When clustering is configured, failover events

have a negligible impact on network performance and users will not be aware of the failure. The failover process occurs as outlined by the steps below:

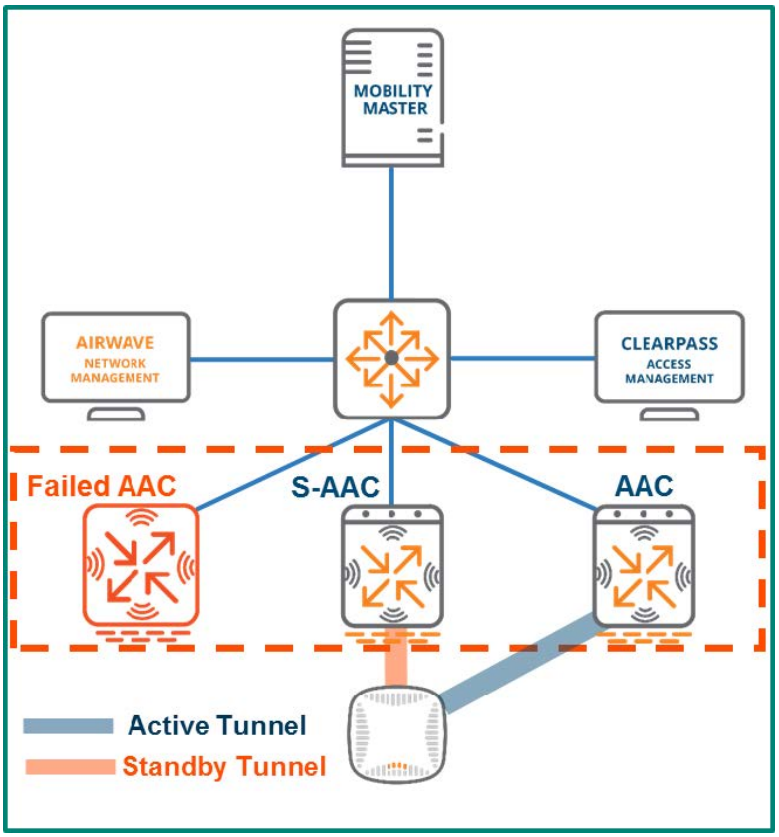
1. An AAC fails. The failure is immediately detected by the S-AAC due to heartbeats.
2. Upon detection of the failure, the S-AAC will instruct the AP to failover.
3. The AP terminates its tunnel to the AAC that has failed and fails over to the S-AAC.
4. The existing AP standby tunnel becomes active with the S-AAC which assumes the role of AAC for that AP.
5. A new S-AAC is dynamically assigned for the AP from the remaining cluster members.
6. The AP establishes standby tunnels to the new S-AAC.

Figure 66 *AAC Fails*



The figure above shows that the AAC the AP was previously connected to has failed. At this point the S-AAC will instruct the AP to failover and tear down its active tunnel to the failed AAC.

Figure 67 *AP Fails Over and New S-AAC Assigned*

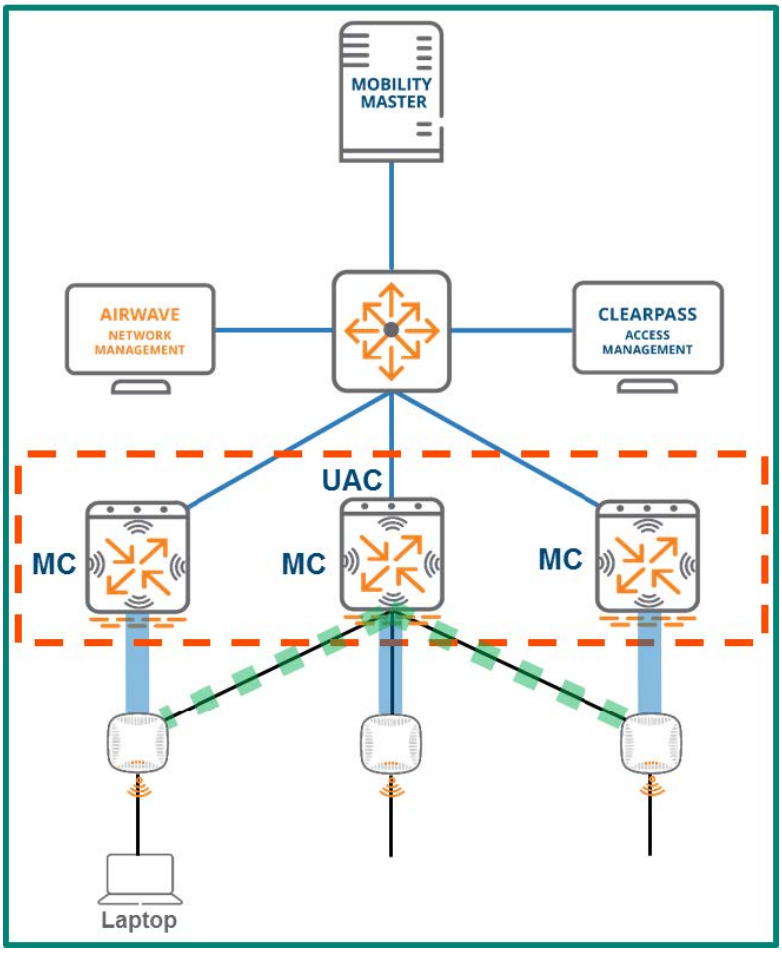


The old S-AAC has now assumed the role of AAC. The old standby tunnel between the AP and the S-AAC has now become an active tunnel. Another member of the cluster was dynamically selected by the cluster leader to serve as the new S-AAC and the AP has built a standby tunnel accordingly. The failover process is now complete and all steps were completely undetectable by the users.

User Anchor Controller

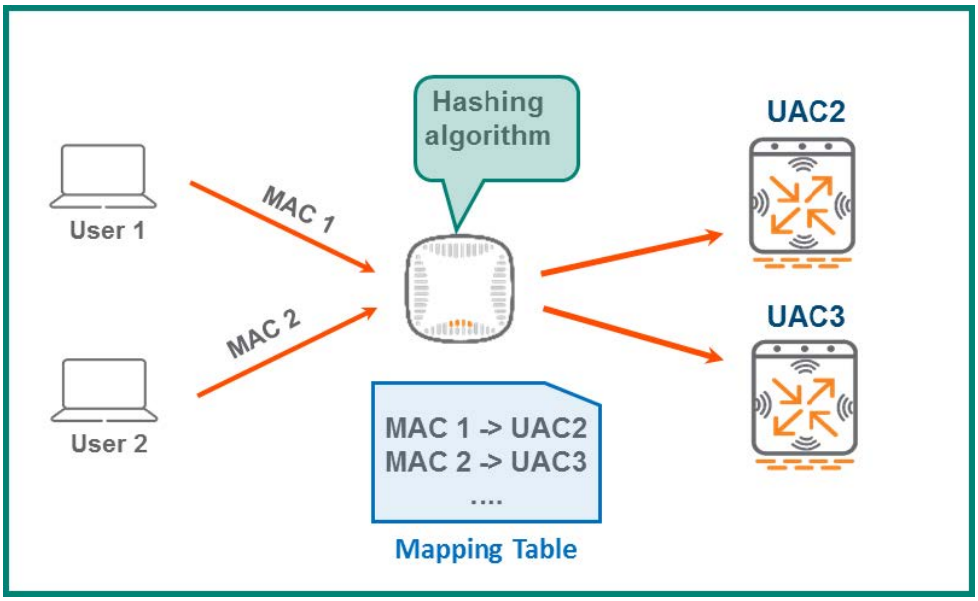
The concept of anchoring users to a controller using a User Anchor Controller (UAC) is new in ArubaOS 8 and was primarily developed to enhance the user roaming experience. When users associate to an AP, they will use the existing tunnel to their UAC if one already exists. If the AP doesn't have tunnel to their UAC established, a dynamic tunnel is created. When the client roams to a new AP, the AP they are roaming away from tears down its dynamic tunnel. User traffic is always tunneled back to their UAC regardless of which AP the client associates to as the user roams, even if that AP has a different AAC.

Figure 68 *Dynamic Tunnel to the Client's UAC*



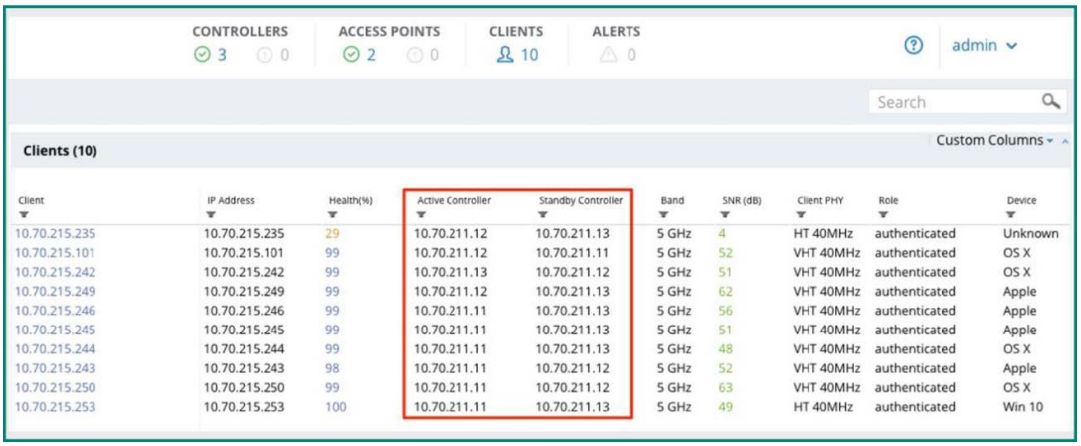
In order to remain anchored, a user must first be mapped to a UAC through a hashing algorithm at the AP level. The MAC address of the client is examined and the hashing algorithm creates an index which is then compared to a mapping table. The same mapping table is pushed to all APs by the cluster leader to ensure UAC mapping consistency across the cluster. In addition, the cluster leader will dynamically select a standby UAC (S-UAC) on a per-user basis for redundancy purposes. An example of the hashing algorithm and UAC assignment process is displayed in the figure below:

Figure 69 *UAC Assignment Process*



The UAC and S-UAC assignments for all associated clients can be identified in the WebUI of the MM by navigating to **Dashboard > Clients:**

Figure 70 *Client UAC and S-UAC Assignments*



NOTE

The Active Controller and Standby Controller columns are not included in the standard view of the Clients page in the WebUI. They can be displayed by adding a customization to the page view.

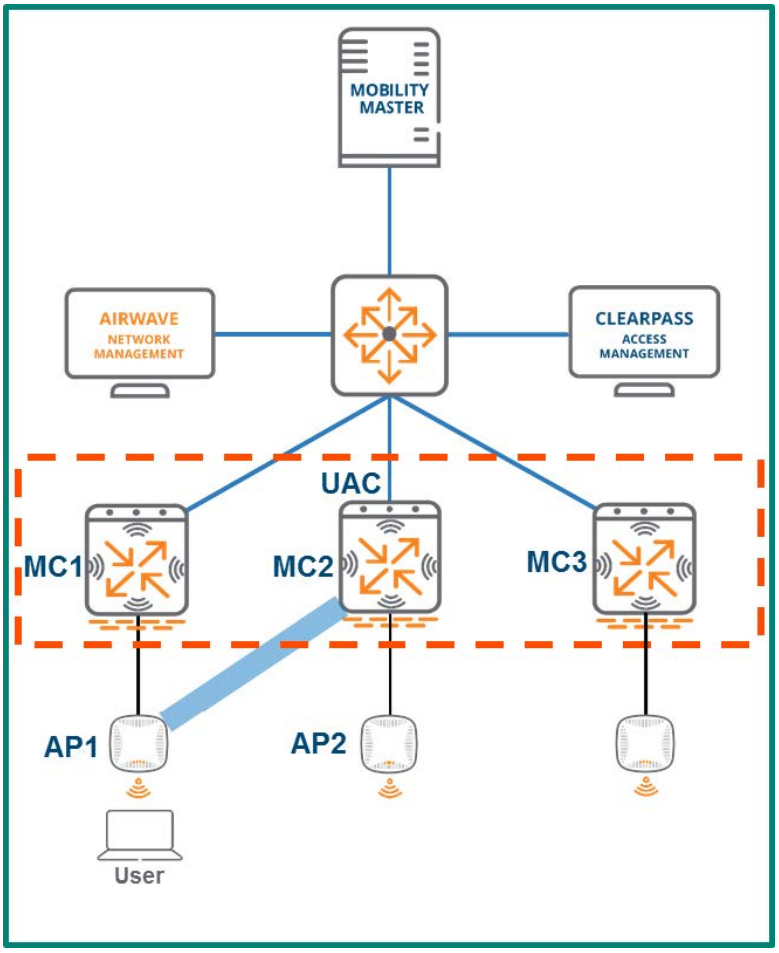
Cluster Features

Seamless Roaming

The advantage of introducing the concept of the UAC is that it significantly enhances the experience for users roaming within a cluster. Once a user associates to an AP, it hashes the client's MAC address and assigns it a UAC. Now the traffic from that user will always be tunneled to their UAC. This remains true regardless of

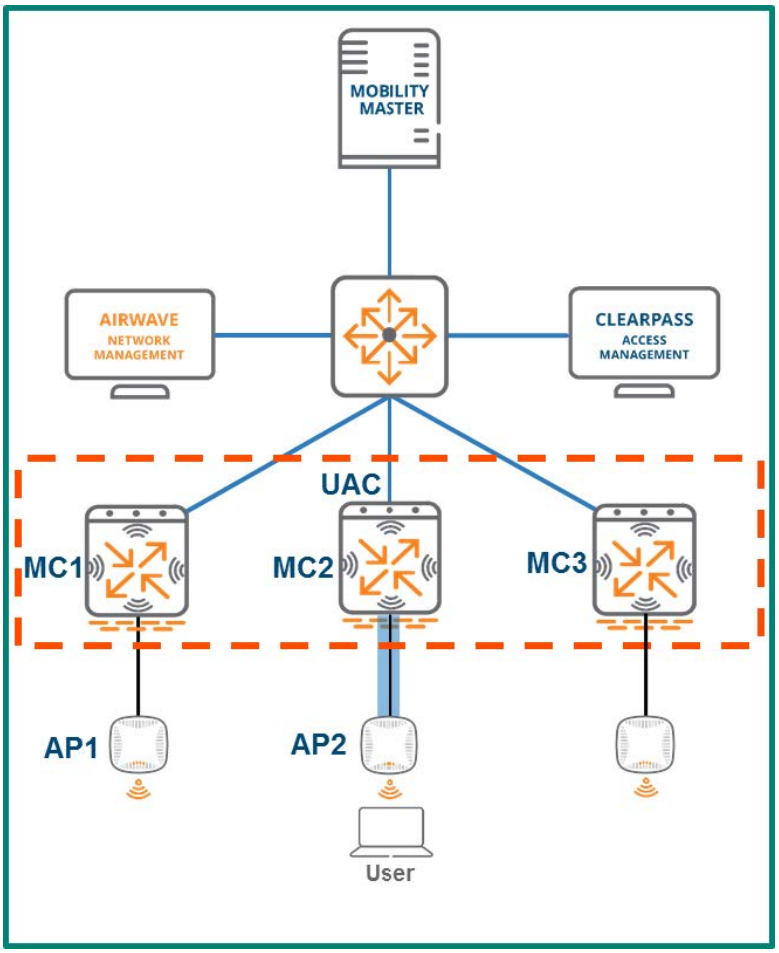
which AP the users associate to as they roam, even if that AP happens to be terminated on a different controller. Any AP the user roams to will automatically forward the traffic to the UAC the user was assigned upon association. If an active or standby tunnel does not exist between the AP where the user has roamed and the UAC, then a dynamic tunnel will be created. A visual representation of the roaming process within a cluster is displayed in the figure below:

Figure 71 *Cluster Seamless Roaming*



In the figure above the user has associated to AP1 which is terminated on MC1, however the traffic is being tunneled to MC2. In this scenario, MC2 has been designated the UAC for the user so as the user roams over to AP2 or any other AP in the cluster the traffic will continue to be tunneled to MC2.

Figure 72 *Cluster Seamless Roaming continued*



Stateful Failover

Stateful failover is a critical aspect of cluster operations that safeguards users from any impacts associated with a controller failure event. The following two key conditions must be met to enable stateful failover functionality for a cluster:

- Redundancy mode must be enabled. It can be disabled however it is enabled by default.
- An L2-Connected state must exist between all cluster members.

If these two conditions have been met, the client state will then be fully synchronized between the UAC and the S-UAC meaning that information such as the station table, the user table, layer 2 user state, layer 3 user state, key cache, and PMK cache will all be shared between the both devices. In addition, high value sessions such as FTP and DPI-qualified sessions are also synced to the S-UAC. Synchronizing all of the client state and high value session information enables the S-UAC to assume the role as the client's new UAC, if the client's current UAC fails. Establishing cluster redundancy in this manner guarantees stateful failover with no client deauthentication when they move from their UAC to their S-UAC. Seamless cluster failover provides a substantial advantage over redundancy enabled with an HA configuration which would require a client to be deauthenticated in the event of a controller failure. The table below outlines the advantages of L2-Connected versus L3-Connected cluster states specifically as they pertain to redundancy, failover, and performance:

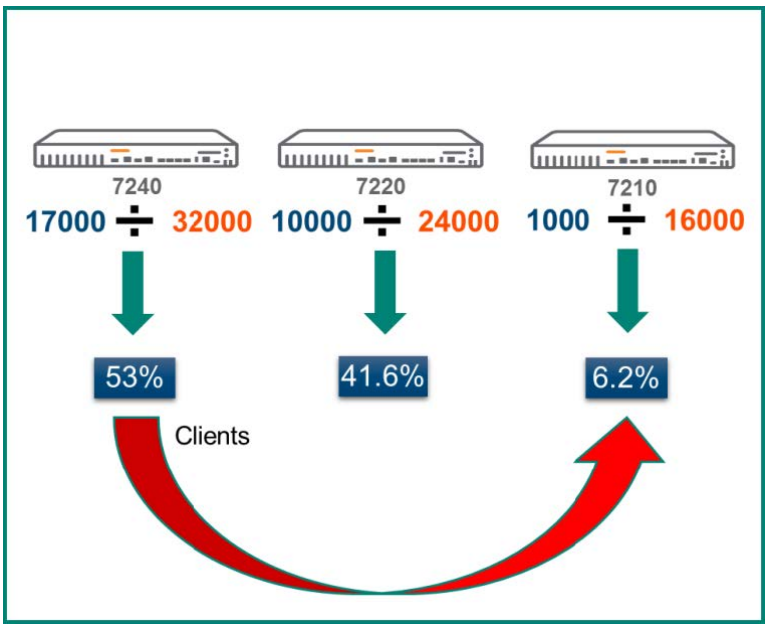
Table 11: *L2-Connected vs. L3-Connected*

L2-Connected	L3-Connected
APs and clients are fully replicated	Only APs fully replicated
Users fully synced between nodes	Users not synced
High value sessions are synced	High value sessions not synced
Users failover with no de-auth	Users are de-authenticated upon failover
Fully redundant	Not fully redundant

Client Load Balancing

Load balancing clients across MCs is another feature that helps maintain cluster performance. While the hashing algorithm applied to clients that associate to an AP for UAC assignment works well for its intended purpose, it can result in a disproportionate distribution of clients across cluster members. This can lead to an inefficient usage of system resources. Load balancing enables the cluster leader to optimally distribute users across the cluster and ensure high performance levels are maintained. The cluster leader load balances clients across the cluster by following a multi-step calculation process where it identifies the model of each controller of the cluster, counts the number of associated clients, and compares the client count against the maximum capacity for each device to calculate its load ratio.

Figure 73 *Cluster Load Calculation Process*



The figure above demonstrates the load calculation process the cluster leader would perform for each member. In this scenario, there are three cluster members each having a different controller model: 7240, 7220, and 7210 controller. The blue numbers below each cluster member indicate the number of associated clients while the orange numbers indicate the maximum capacity for each particular model. The cluster leader compares the client count and checks that against the capacity for each device's model and produces a ratio for each expressed as a percentage of total capacity. The table below presents the specific triggers in place which will result in the cluster leader load balancing clients across the cluster:

Table 12: *Load Balancing Triggers*

Category	Threshold
Active Client Load	50%
Standby Client Load	75%
Unbalance Threshold	5%

The table demonstrates that a rebalancing event will be triggered when the active client load exceeds 50% or the standby client load exceeds 75% on any member of the cluster and while unbalance threshold also exceeds 5%. Unbalance threshold refers to the delta between the member of the cluster with the highest load percentage and the member of the cluster with the lowest load percentage and was put in place to ensure that regardless of how close the cluster members are to approaching a capacity trigger, they will always remain with a evenly distribution of clients.

AP Load Balancing

Just as the cluster leader will load balance clients to ensure an even distribution across cluster members, it will also perform the same function for APs. Dynamic cluster AP load balancing is a configurable feature in ArubaOS 8. It should be enabled whenever there is a need to allow ease of scalability while adding MCs to a cluster or a need to eliminate manual AP distribution.

Before APs can participate in cluster load balancing they must first be assigned an AP Master. The AP Master is the device which owns the IP address that is used in DHCP option 43 and in the DNS record of aruba-master.yourdomain. There are two levels of cluster interconnectivity which have an impact on how new APs will find their AP master when attempting to join a cluster:

- Layer 2 Connectivity – The controller IPs for all cluster nodes are in the same VLAN
- Layer 3 Connectivity – The controller IPs for cluster nodes are in different VLANs

If the cluster members share a layer 2 connection, it signifies that they are a part of the same broadcast domain. A VRRP instance should be created among the cluster members so that its VIP can be used as the AP Master for APs joining the cluster. In a cluster with layer 3 connectivity the members are not in the same broadcast domain therefore creating a VRRP instance is not possible. The IP address of one of the controllers could be designated for discovery through DHCP option 43, however, this would not provide redundancy and would create a single point of failure. The preferred AP Master discovery option for an L3 connected cluster is to use DNS discovery with two Aruba-master records leveraging two controller IP addresses chosen from the cluster members.

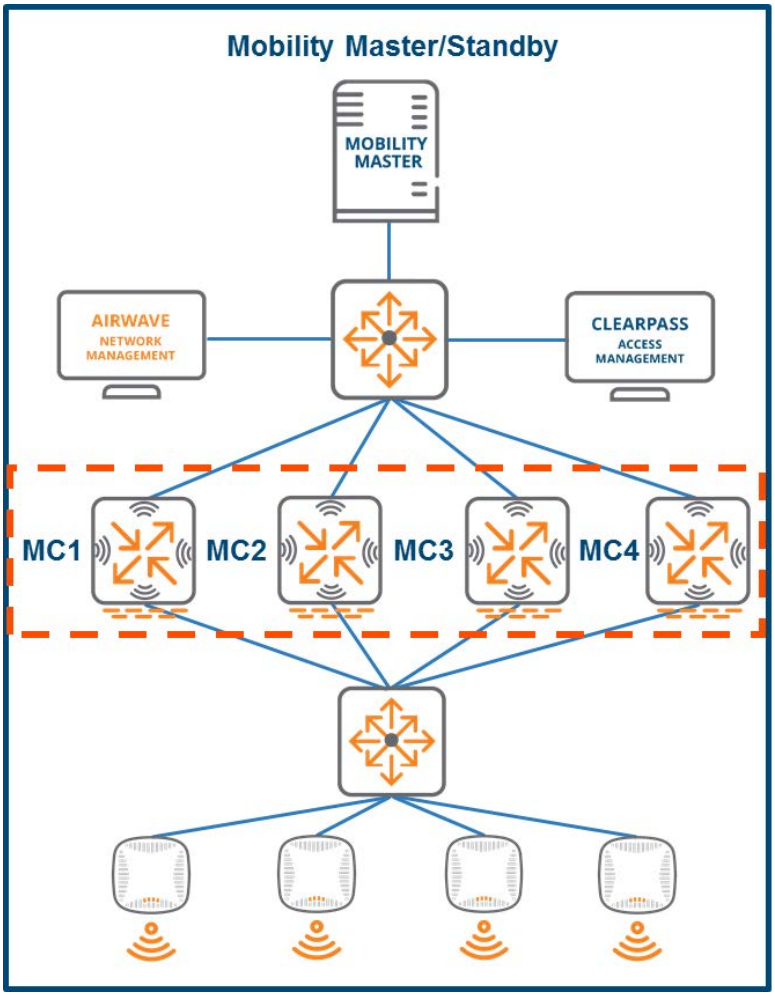
Once an AP joins the cluster, the downloaded node list will have a higher priority than the discovered Master.

Following are two methods for AP distribution among cluster members:

Planned Assignment - This is the traditional method used in ArubaOS 6.x and ArubaOS 8 where the LMS-IP in the AP system profile is leveraged to assign the active AAC within the cluster. It is a deterministic method which requires an administrator to plan AP distribution in advance on a per-AP group basis and configure the appropriate cluster member controller IP address as the LMS-IP in each AP group.

Automated Assignment - This method leverages the AP load balancing feature introduced in ArubaOS 8.1.0.0. AP termination assignment is automated and the cluster leader assigns the active AAC for an AP based on the existing AP load on each cluster member.

Figure 74 *Cluster Architecture*

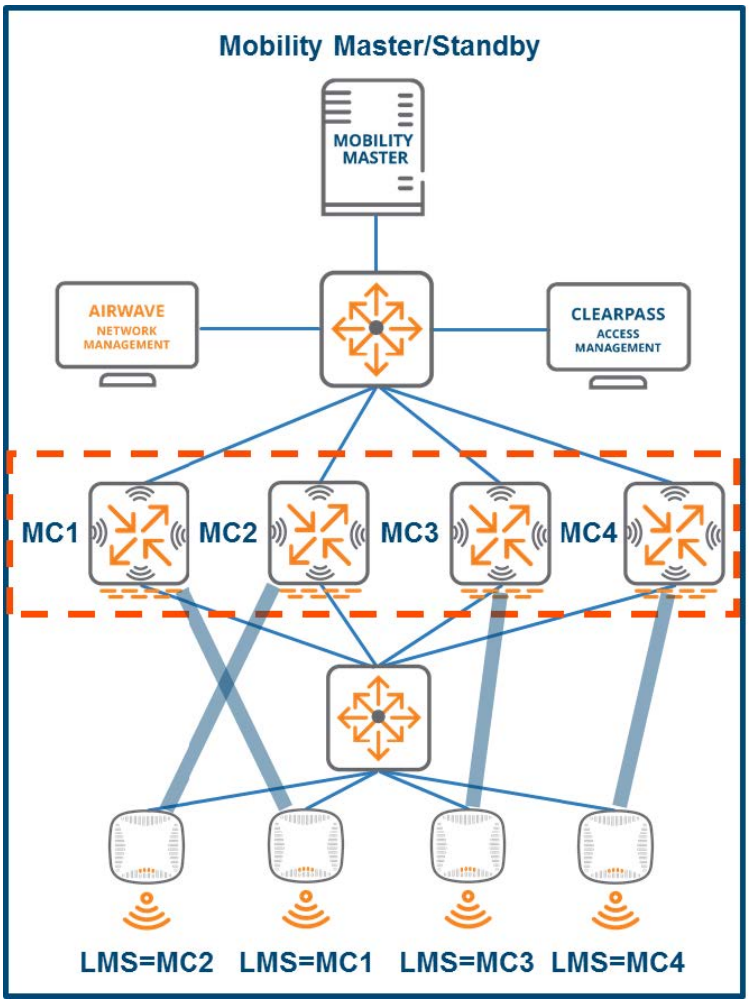


Planned Assignment

Preselecting the AAC for APs allows administrators to have deterministic control over AP load distribution. AP load balancing is enabled by default in ArubaOS 8.3.0.0 and must be disabled if administrators are opting for planned AAC assignment. The LMS-IP in each AP system profile that belongs to each AP group needs to be set to the controller IP address of one of the cluster members. When the planned assignment method is used, APs joining the cluster connect to their AAC using the following steps:

1. The AP downloads its configuration from the discovered AP Master controller, including an LMS-IP address assignment.
2. AP adopts the designated LMS controller as its Active AAC and terminates GRE tunnels.
3. AP receives Standby AAC assignment as determined by the Cluster Leader.

Figure 75 *AAC Tunnel Establishment*



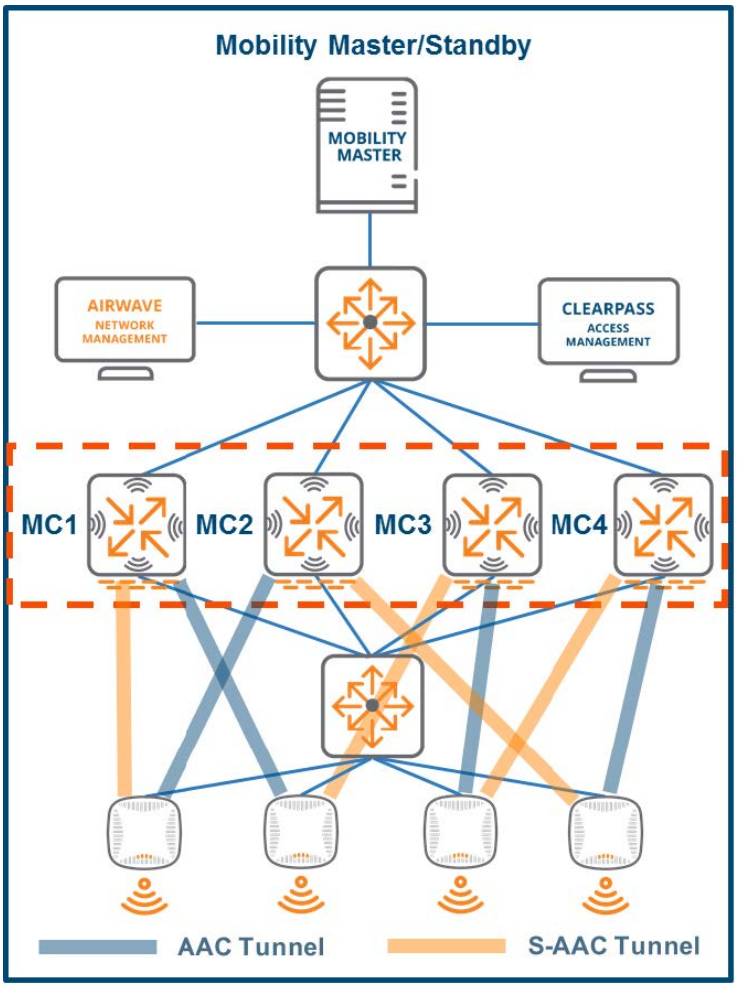
Automated Assignment

In order to utilize the automated AAC assignment method for APs joining the cluster the AP load balancing option within the cluster must be enabled. The following steps will occur:

1. A new AP joining the cluster contacts its AP Master utilizing either the VIP of the VRRP instance if the cluster members are layer 2 connected or designated cluster member if the cluster members are layer 3 connected.
2. The AP master controller checks internally for an AAC for that AP assigned by the cluster leader.
3. Once the AAC assignment for the AP is available to the AP master, it responds to the PAPI hello/handshake of that AP and provides it with its AAC in a few milliseconds.
4. Once the AP has established its GRE tunnels and terminates on its Active AAC, the cluster leader provides it with its Standby AAC assignment.
5. The AP completes the process by establishing its standby tunnel(s) with its designated S-AAC.

AAC and S-AAC assignment are based on existing distribution of the AP load among the cluster members.

Figure 76 *S-AAC Tunnel Establishment*



Load Balancing Metrics

In order to understand the load balancing process it is critical to be familiar with the various metrics related to AP load on the cluster nodes and their definitions:

AP Load Percentage - The ratio of the number of APs on a controller compared to that controller's platform AP capacity. For example, 500 APs on a controller with a 1000 AP capacity is a 50% load. The same 500 APs on a controller with a 2000 AP capacity would be a 25% load.

Active AP Load Percentage – The ratio of the number of APs with active tunnels only on a controller compared to that controller's platform capacity.

Total AP Load Percentage - The ratio of the number of APs on a controller including those with active and standby tunnels compared to that controller's platform capacity.

Prior to ArubaOS 8.3.0.0, the load balancing algorithm used the total AP load ratio. However, the algorithm was enhanced in ArubaOS 8.3 and now only factors in the active AP load percentage when making load balancing decisions.

Load Balancing Algorithm

Load Balancing Prior to ArubaOS 8.3.0.0

In ArubaOS versions prior to 8.3.0.0, the load balancing algorithm works by identifying the MC members that have the highest and lowest total AP load percentage. Load balancing occurs when two thresholds are simultaneously exceeded:

Active AP Rebalance Threshold (Total AP load percentage) exceeds 50%

Active AP Unbalance Threshold (delta between controllers with the highest and lowest Total AP percentage) exceeds 5%

When the algorithm takes effect, the standby AP load is redistributed first to restore the total balance. If load balancing the APs with standby tunnels does not sufficiently rebalance the cluster, the Active AP load is redistributed until the correct balance is achieved.

Load Balancing in ArubaOS 8.3.0.0 and Later Versions

An enhancement was introduced in ArubaOS 8.3.0.0, directing the cluster leader to primarily consider the active AP load percentage on cluster members when making load balancing decisions. In versions prior to ArubaOS 8.3.0.0, the total AP load percentage metric was used which included the standby and the active tunnels from APs to cluster members.

The periodic load balancing algorithm in ArubaOS 8.3.0.0 or later versions works according to the following process:

1. Identify the cluster members with highest and lowest Active AP Load Percentage.
2. Identify the cluster members with highest and lowest Total AP Load Percentage.
3. The load balancing mechanism is triggered when two thresholds are simultaneously exceeded.
4. Active AP Rebalance Threshold (Active AP Load Percentage) exceeds 50% (default).
5. Active AP Unbalance Threshold (delta between the cluster members with the highest and lowest Active AP percentage) exceeds 5%.
6. Active APs are redistributed from the cluster member with the highest load to the cluster member with the lowest load.
7. If Active APs can't be moved to restore the balance, then the standby APs are redistributed from the cluster member with the highest load to the cluster member with the lowest load.

The Load Balancing thresholds are configurable and are controlled using the following additional metrics:

Active AP Rebalance Timer - Controls the load balancing assessment interval.

Active AP Rebalance AP Count – Determines the number of APs that will be moved when load balancing has been triggered by the Active AP Rebalance Timer.

Table 13: *Active AP Rebalancing Defaults*

Metric	Default Prior to ArubaOS 8.3	Default as of ArubaOS 8.3
Active AP Rebalance Timer	1 minute	5 minutes
Active AP Rebalance AP Count	10 APs	30 APs

Load Balancing in ArubaOS 8.5.0.0 and later versions

An enhancement was introduced in ArubaOS 8.5.0.0 to reduce the default load balancing thresholds in order to provide a more aggressive triggering of the load balancing.

Table 14: *Load Balancing Defaults*

Metric	Default Prior to ArubaOS 8.5	Default as of ArubaOS 8.5
Active Client Rebalance Threshold	50%	20%
Standby Client Rebalance Threshold	75%	40%
Unbalance Threshold	5%	5%
Active AP Rebalance Threshold	50%	20%
Active AP Unbalance Threshold	5%	5%
Active AP Rebalance Timer	1 minute	1 minute
Active AP Rebalance AP Count	30 APs	50 APs

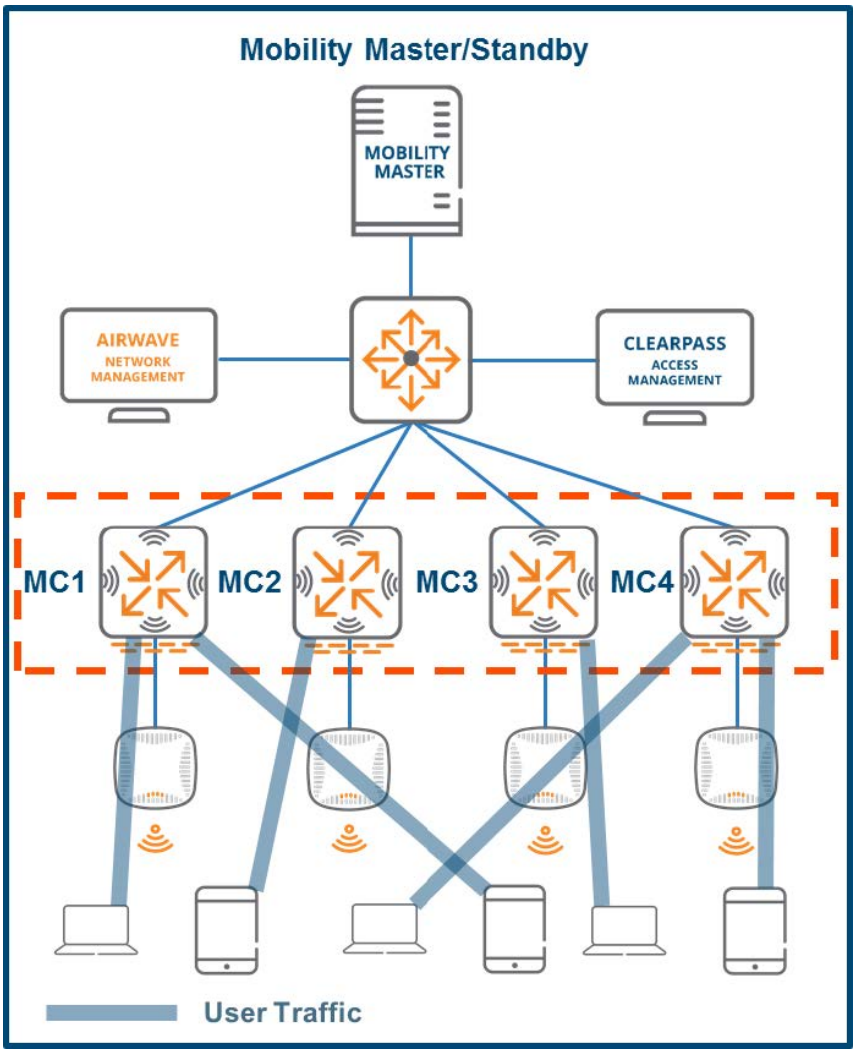
Cluster Grouping

The clustering feature was introduced in ArubaOS 8 as a more powerful redundancy mechanism than the High Availability AP Fast Failover feature in ArubaOS 6. While the HA configuration required configuring controller modes such as Active, Standby, or Dual, clustering automated the failover process by introducing dynamic selection of the standby AP Anchor Controller and standby User Anchor Controller (S-UAC) by the cluster leader.

While the dynamic standby selection offered by clustering is a powerful tool, there are situations in production environments where influencing the selection of the S-AAC and S-UAC is desirable. The following scenarios provide examples of when selecting the standby controllers in a more deterministic manner could be advantageous:

- MCs in a cluster split between different racks in the same datacenter with redundant power supplies.
- Two data centers within the same large campus where it is highly desirable to ensure AAC and UAC redundancy is split between them.

Figure 77 *Typical ArubaOS 8 Cluster Architecture*

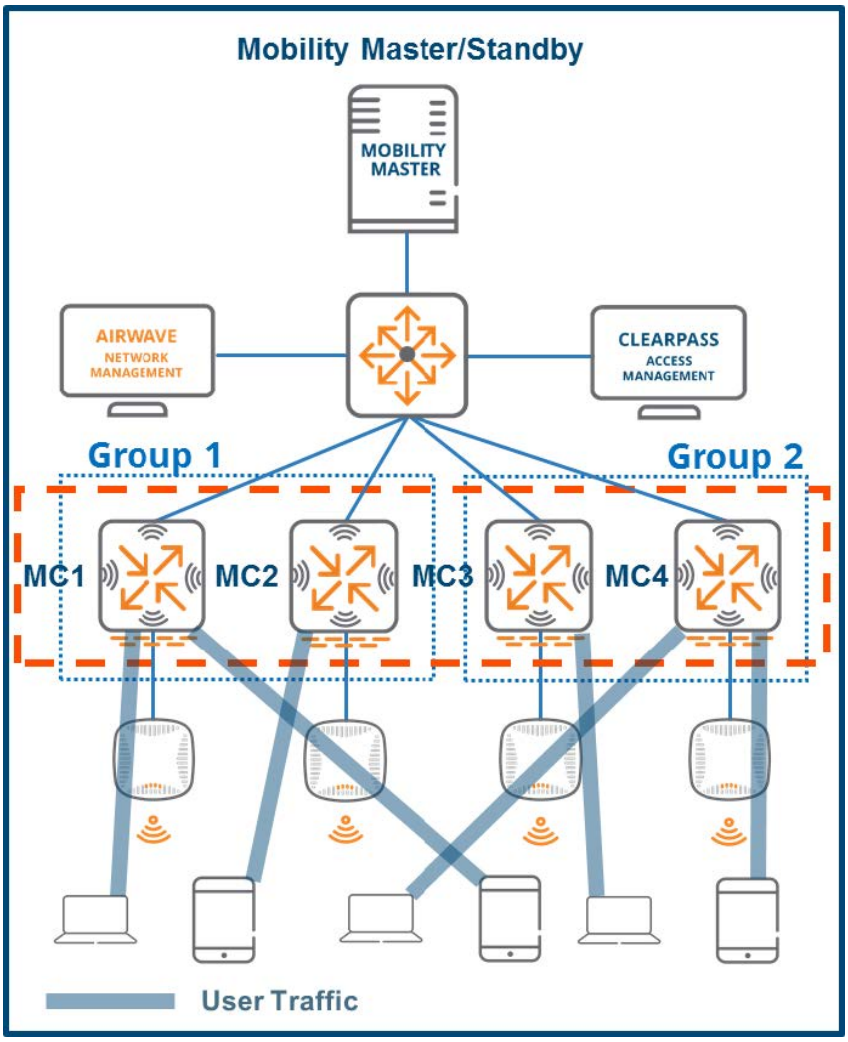


To address this need, Aruba created the group option to group MCs within a cluster into 2 or more groups. When the cluster leader selects a standby controller for an AP or user, it will give preference to a controller that belongs to a different group than the active controller.

In the example provided below, MC1 and MC2 are configured in Group 1, while MC3 and MC4 are configured in Group 2. If an AP has MC1 as its AAC, the Cluster Leader will select either MC3 or MC4 in Group 2 as the S-AAC for that AP. The same selection criteria applies for an AP that terminates on one of the MCs in Group 2; either MC1 or MC2 would be chosen as its S-AAC.

The Cluster Leader follows the same selection process for the Standby User Anchor Controller (S-UAC) as it does for the S-AAC when groups are used.

Figure 78 *Cluster Groups in ArubaOS 8*



NOTE

The grouping feature has no influence on the AAC or UAC selection. Cluster members should always be equally divided between groups.

AP Node List

The AP node list is a repository of IP addresses for each cluster member maintained by each AP. After connecting to the cluster, the AP learns the IP addresses of all cluster members. These addresses are then stored as the AP's node list and saved as an environment variable. After the boot up, the AP will contact the first IP address in its node list. If it does not receive a response, it will try the next IP address in the list to ensure that APs are always able to find a reachable controller within the cluster.

Change of Authorization

Change of Authorization (CoA) is a feature which extends the capabilities of the Remote Authentication Dial-In User Service (RADIUS) protocol and is defined in RFC 5176. CoA request messages are usually sent by a RADIUS server to a Network Access Server (NAS) device for dynamic modification of authorization attributes

for an existing session. If the NAS device is able to successfully implement the requested authorization changes for the user session(s), it will respond to the RADIUS server with a CoA acknowledgement also referred to as a CoA-ACK. Conversely, if the change is unsuccessful, the NAS will respond with a CoA negative-acknowledgement or CoA-NAK.

In the context of an ArubaOS 8 cluster, unsolicited CoA requests for a user with an active session in progress are sent to that user's anchor controller. The UAC will then return an acknowledgement to the RADIUS server upon the successful implementation of the changes or a NAK if the implementation was unsuccessful. However, a user's UAC may change in the course of normal cluster operations due to reasons such as an MC failure or user load-balancing events. Such a scenario would cause CoA requests to be dropped as the intended user would no longer be associated to the MC receiving the request from the RADIUS server and Aruba has implemented cluster redundancy features in order to prevent the scenario.

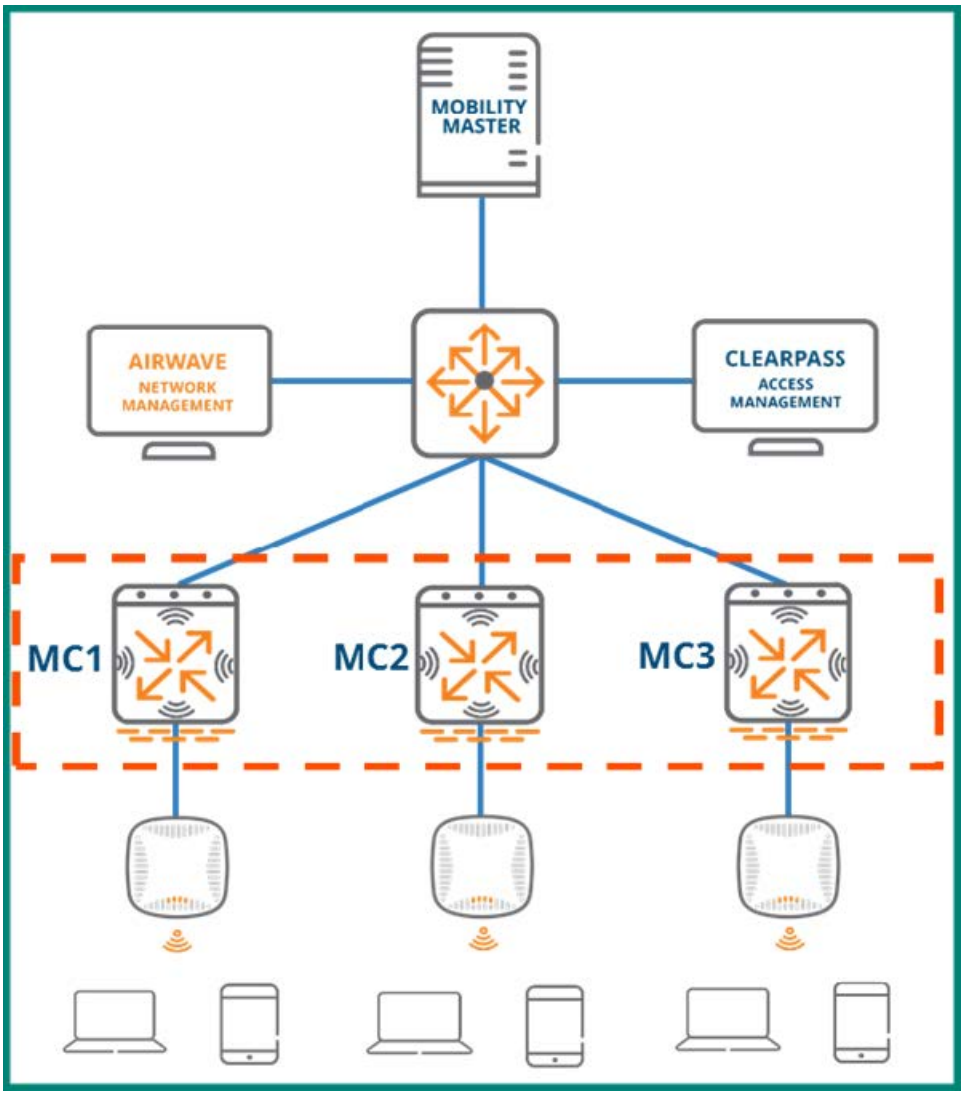
Cluster CoA Support

The primary mechanism Aruba uses to provide CoA support for MC clusters in ArubaOS 8 is VRRP. In every cluster there are the same number of VRRP instances as there are nodes and each MC serves as the master of an instance. For example, a cluster with 5 MCs would have 5 instances of VRRP and 5 virtual IP addresses (VIPs). The master MC receives messages intended for the VIP of its instance while the remaining MCs in the cluster are backups for the all of other instances where they are not acting as the master. This configuration ensures that each cluster is protected by a fault-tolerant and fully redundant design.

This section describes the process of Dynamic Authorization to RADIUS as described in RFC-5176 and how RADIUS communicates with Aruba controllers in a cluster. The Change of Authorization process was selected as a representation of that communication sequence.

ArubaOS reserves VRRP instance IDs in the 220-255 range. When the master of each instance sends RADIUS requests to the RADIUS server, it injects the VIP of its instance into the message as the NAS-IP by default. This ensures that CoA requests from the RADIUS server will always be forwarded correctly regardless of which MC is the acting master for the instance. For example , the RADIUS server sends CoA requests to the current master of the VRRP instance and not to an individual station. From the perspective of the server, it is sending the request to the current holder of the VIP address of the instance. The figure below depicts sample architecture that will be used for the duration of the CoA section:

Figure 79 *Sample Architecture for CoA Demonstration*



This sample network consists of a three-node cluster with three instances of VRRP. The AOS-assigned VRRP ID range falls between 220 and 255, therefore the three instances in this cluster are assigned the VRRP IDs of 220, 221, and 222. The priorities for the MCs in each instance are dynamically assigned so that the master of the instance is assigned a priority of 255, the first backup is assigned a priority of 235, and the second backup is assigned a priority of 215. The table below outlines the priority assignments for each MC and each instance in the example network:

Table 15: *MC Priorities and VIPs for Each VRRP Instance*

VRRP Instance	Virtual IP	MC1 Priority	MC2 Priority	MC3 Priority
ID 220	VIP1	255	235	215
ID 221	VIP2	215	255	235
ID 222	VIP3	235	215	255

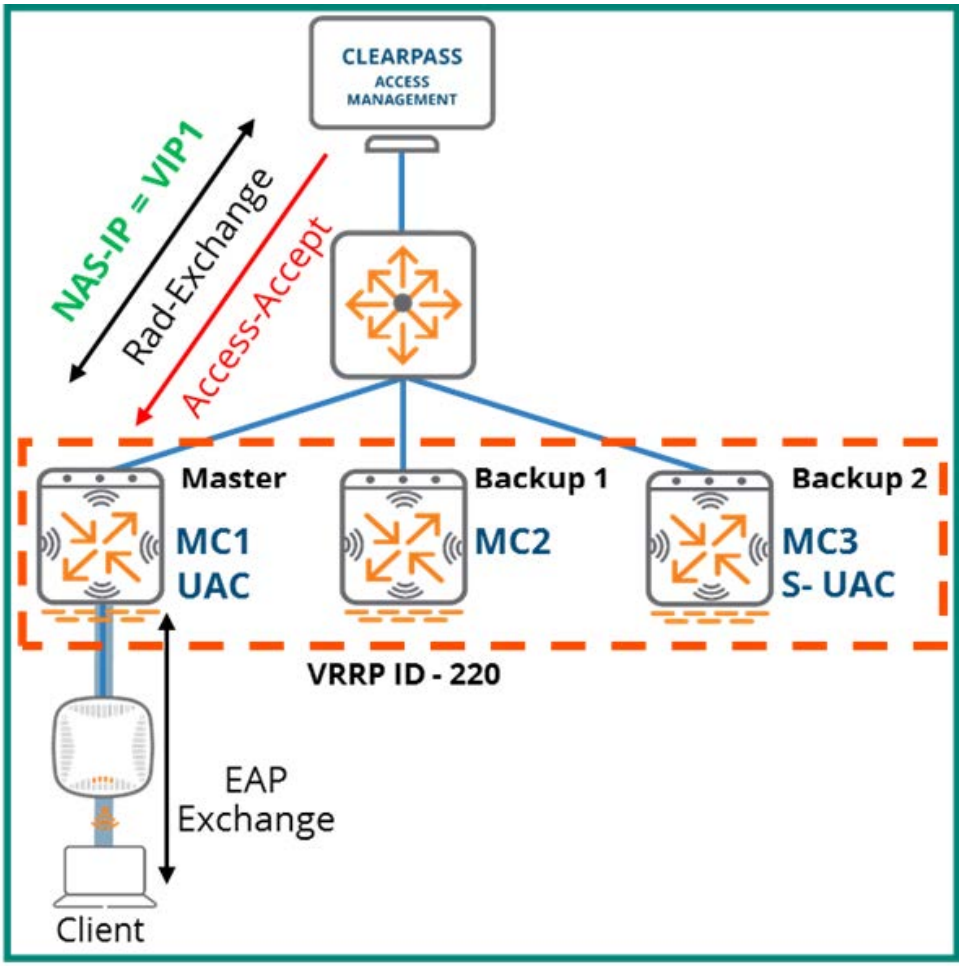
As demonstrated in the table, MC1 is the master of instance 220 with a priority of 255, MC2 is the first backup with a priority of 235, and MC3 is the second backup with a priority of 215. Similarly, MC2 is the master for instance 221 due to having the highest priority of 255, MC3 is the first backup with a priority of 235, and MC1 is the second backup with a priority of 215. Instance 222 follows the same pattern as instances 220 and 221.

CoA with MC Failure

The failure of a cluster node can adversely impact CoA operations if the network doesn't have the appropriate level of fault tolerance. If a user's anchor controller fails, the RADIUS server will push the CoA request to their UAC with the assumption that it will enforce the change and respond with an ACK. However, if a redundancy mechanism such as VRRP hasn't been implemented then the request will go unanswered and will not result in a successful change. In such a scenario, the users associated with the failed node will failover to their standby UAC as usual. However, the UAC will never receive the change request from the RADIUS server since the server is not aware of the cluster operations. VRRP instances must be implemented for each node to prevent such an occurrence and maintain CoA operations in the cluster.

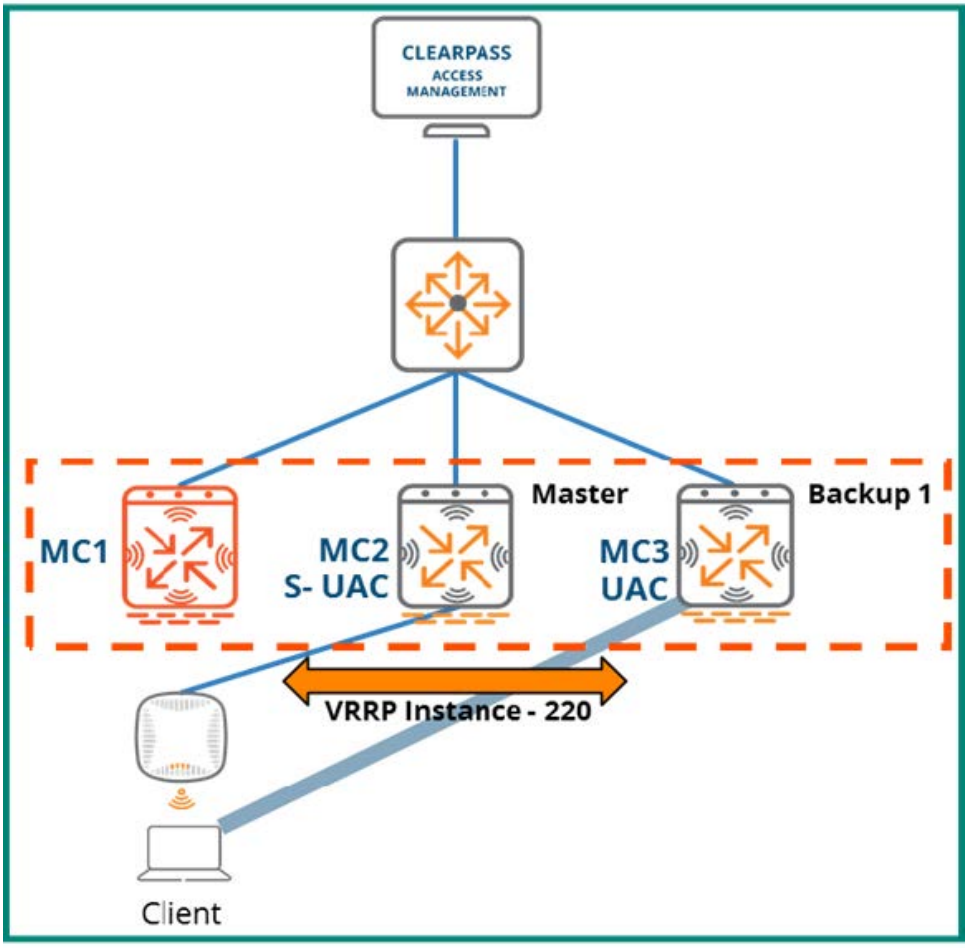
In the figure below, MC1 is the master of instance 220 with MC2 serving as the first backup and MC3 serving as the second backup. A client associated to MC1 has been fully authenticated using 802.1X with MC3 acting as the client's standby UAC. When corresponding with ClearPass, MC1 automatically inserts VIP for instance 220 as the NAS-IP. From the perspective of ClearPass , it is sending CoA requests to the current master of instance 220.

Figure 80 *User Authenticates Against ClearPass*



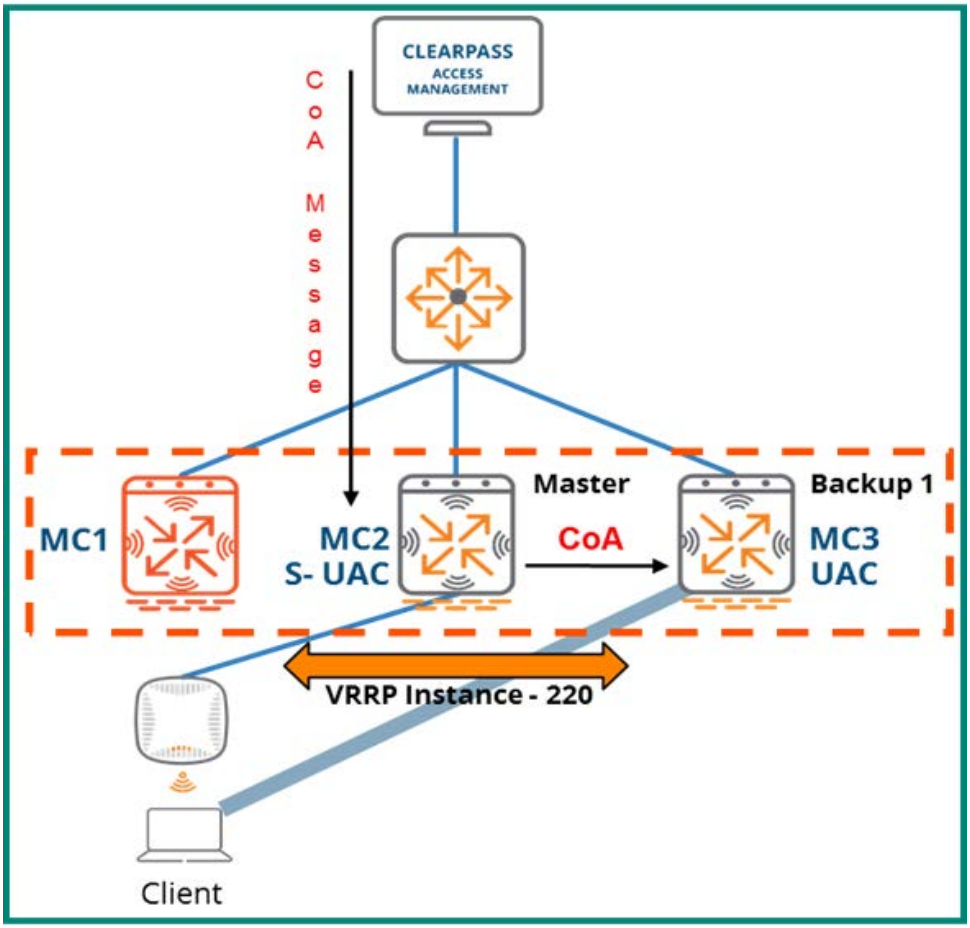
If MC1 fails while the client is in session the AP where the client is associated will failover to MC2. The client's session moves over to MC3 since it was the standby UAC. MC3 then assumes the role of UAC for the client. Since MC2 has a higher priority than MC3 in instance 220 it will assume the role of Master and take ownership of the VIP.

Figure 81 *MC1 Failure*



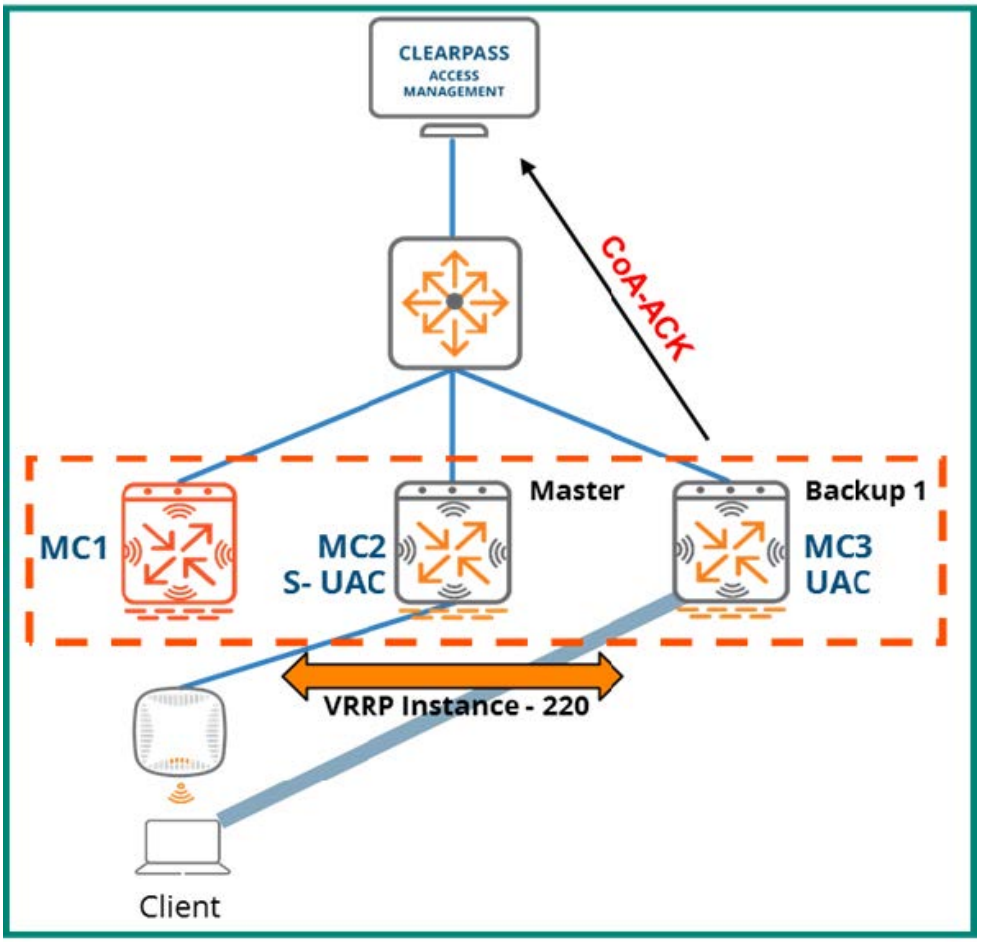
Any CoA requests sent by ClearPass for the client will be addressed to the VIP for instance 220. From the perspective of ClearPass, the VIP of instance 220 is the correct address for any CoA request intended for the client in the example. Since MC1 has failed, MC2 is now the Master of VRRP instance 200 and owns its virtual IP. When ClearPass sends a CoA request for the client, MC2 will receive it and then forward it to all nodes in the cluster. Since the cluster only has three nodes, in this case MC2 forwards the request to MC3.

Figure 82 *CoA message forwarded to MC3*



After the change in the CoA request has been successfully implemented, MC3 will send a CoA-ACK back to ClearPass.

Figure 83 *CoA message forwarded to MC*

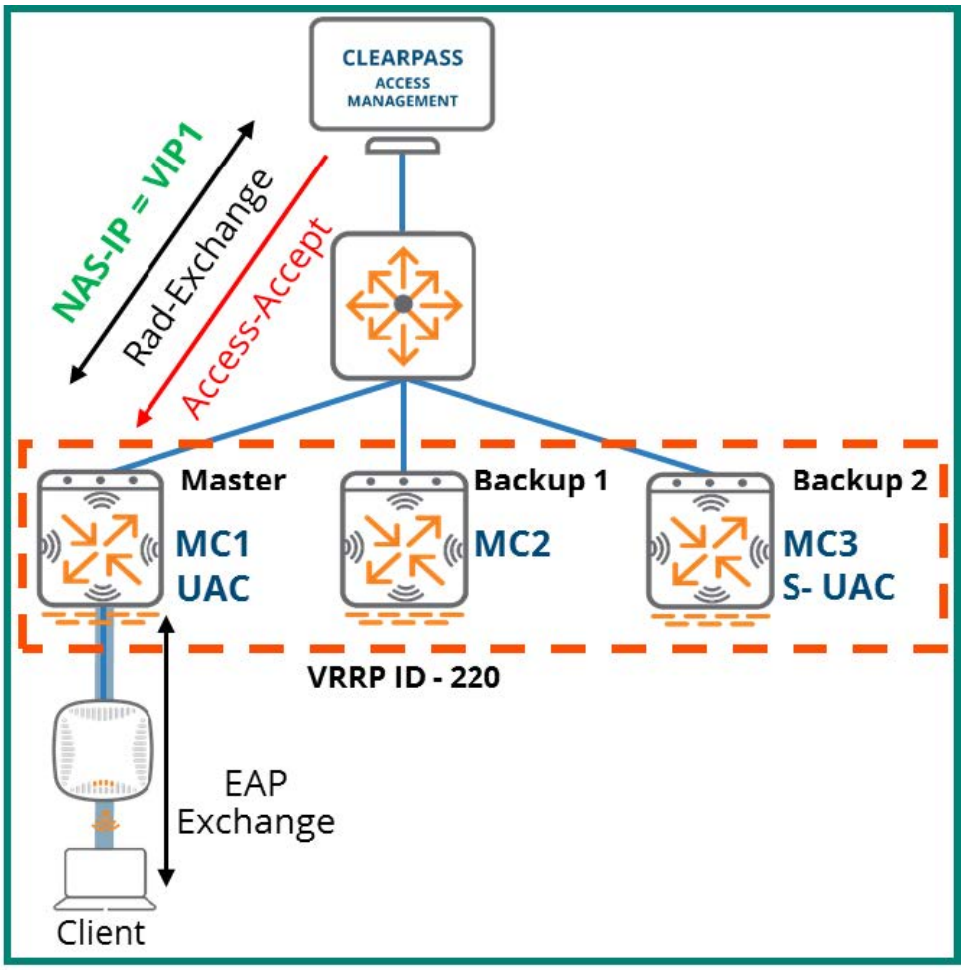


CoA with Load Balancing

If the proper design has not been implemented, load balancing events within a cluster can pose a challenge for CoA operations. To demonstrate Aruba's solution to prevent load-balancing events from impeding CoA functionality, the same architecture will be used for the MC failure example. The example will simulate an event where a client associated to MC1 is load-balanced over to MC3 while still in session.

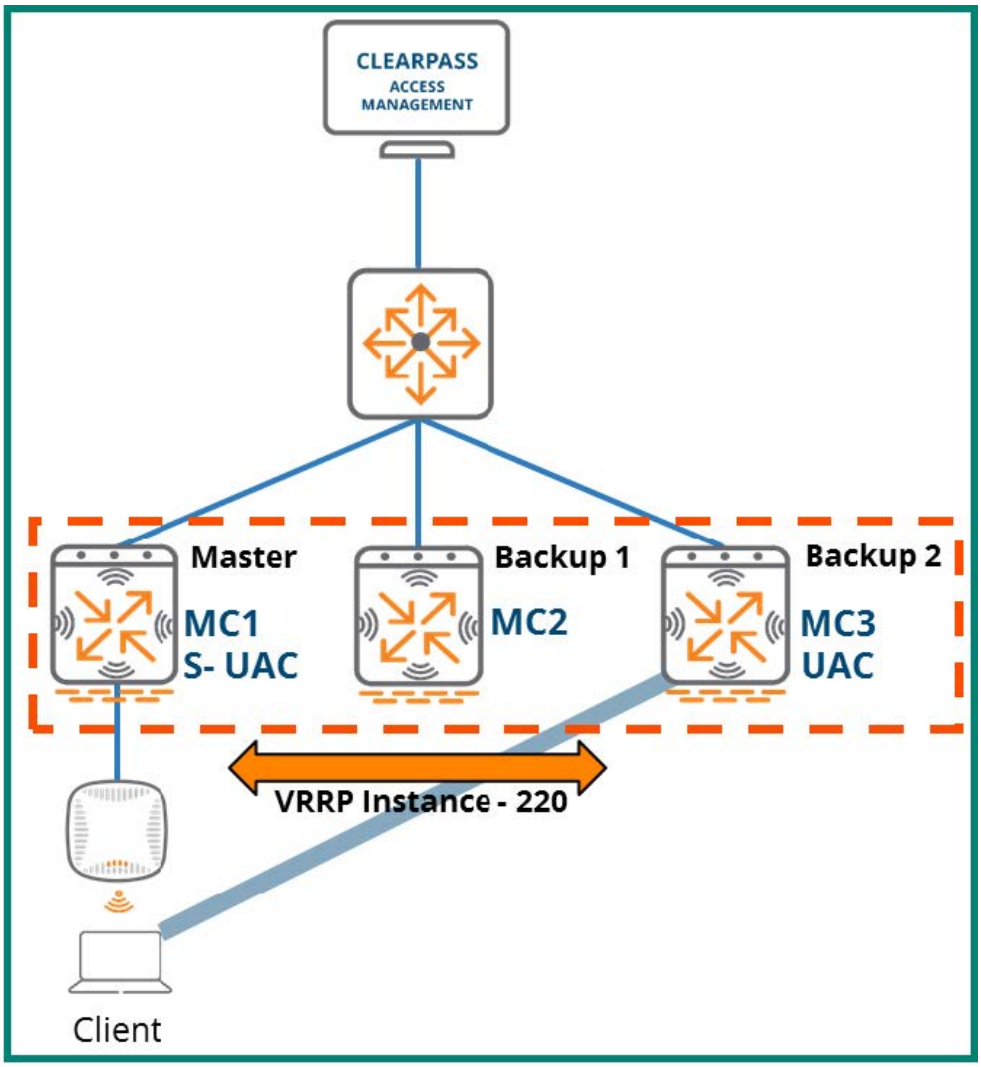
MC1 is operational, master of the VRRP instance 220, and owner of the VIP. As with the previous example, MC1 has inserted VIP1 as the NAS-IP in the RADIUS request which initiated the client authentication so ClearPass will send any CoA requests for the client to the VIP address of VRRP instance 220.

Figure 84 *Client Authenticates Against ClearPass*



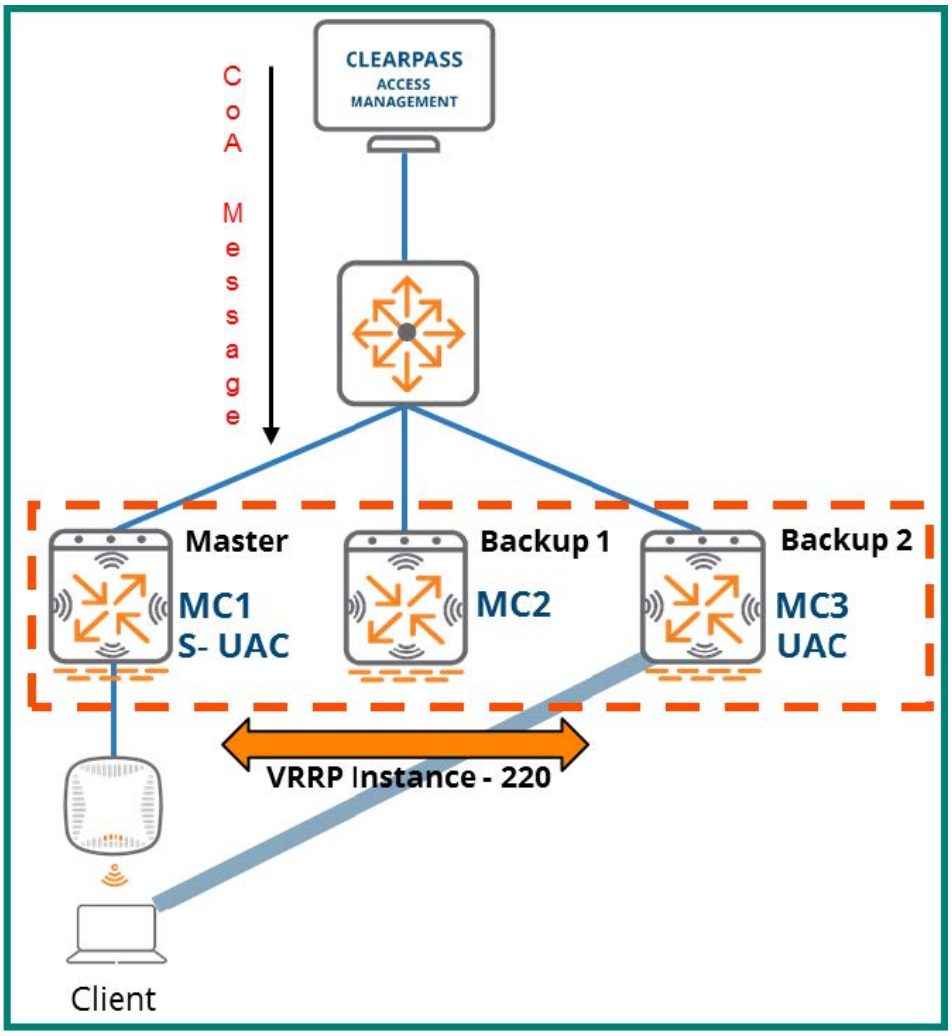
Next, the client is load-balanced over to MC3 which becomes its UAC. MC1 becomes the client's S-UAC but remains Master of VRRP instance 220.

Figure 85 *Client UAC Changes*



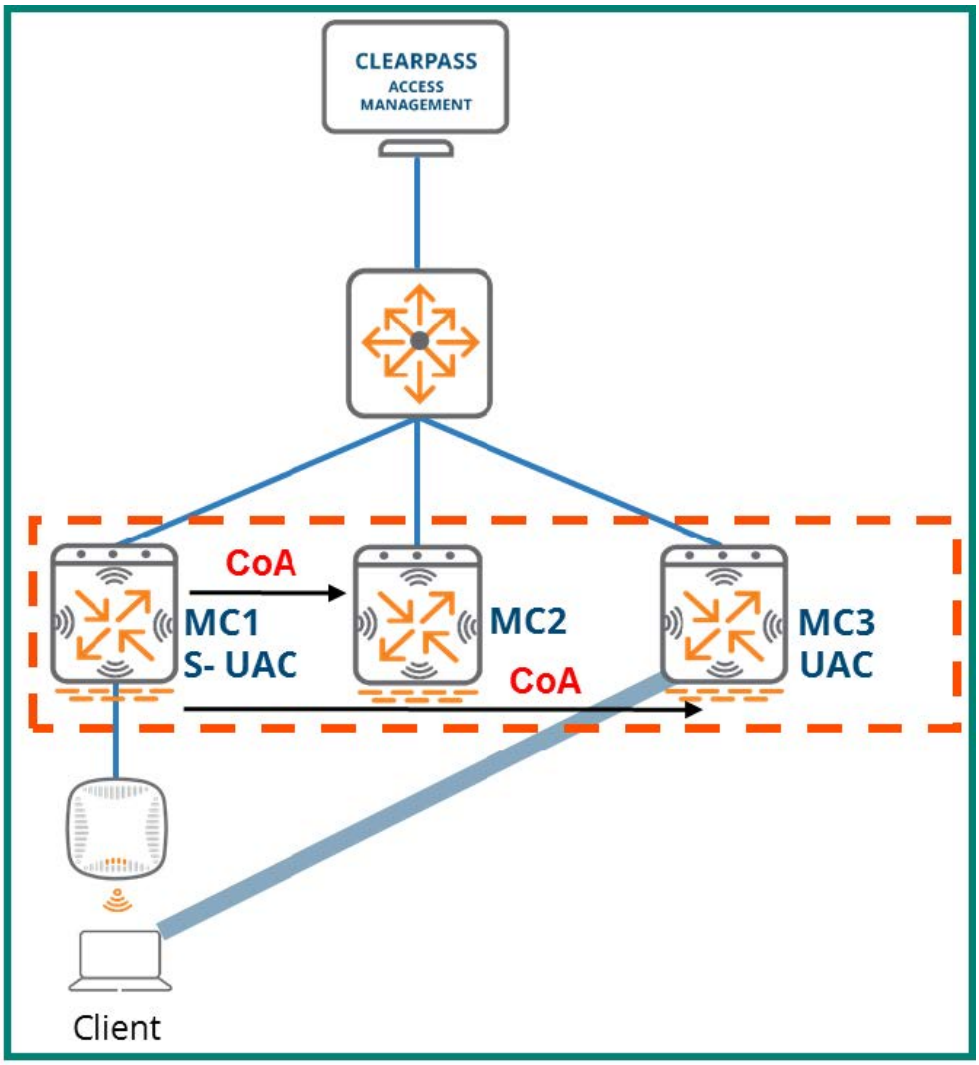
ClearPass sends a CoA message to the owner of the VIP for VRRP ID 220:

Figure 86 *CoA Message sent to VIP1*



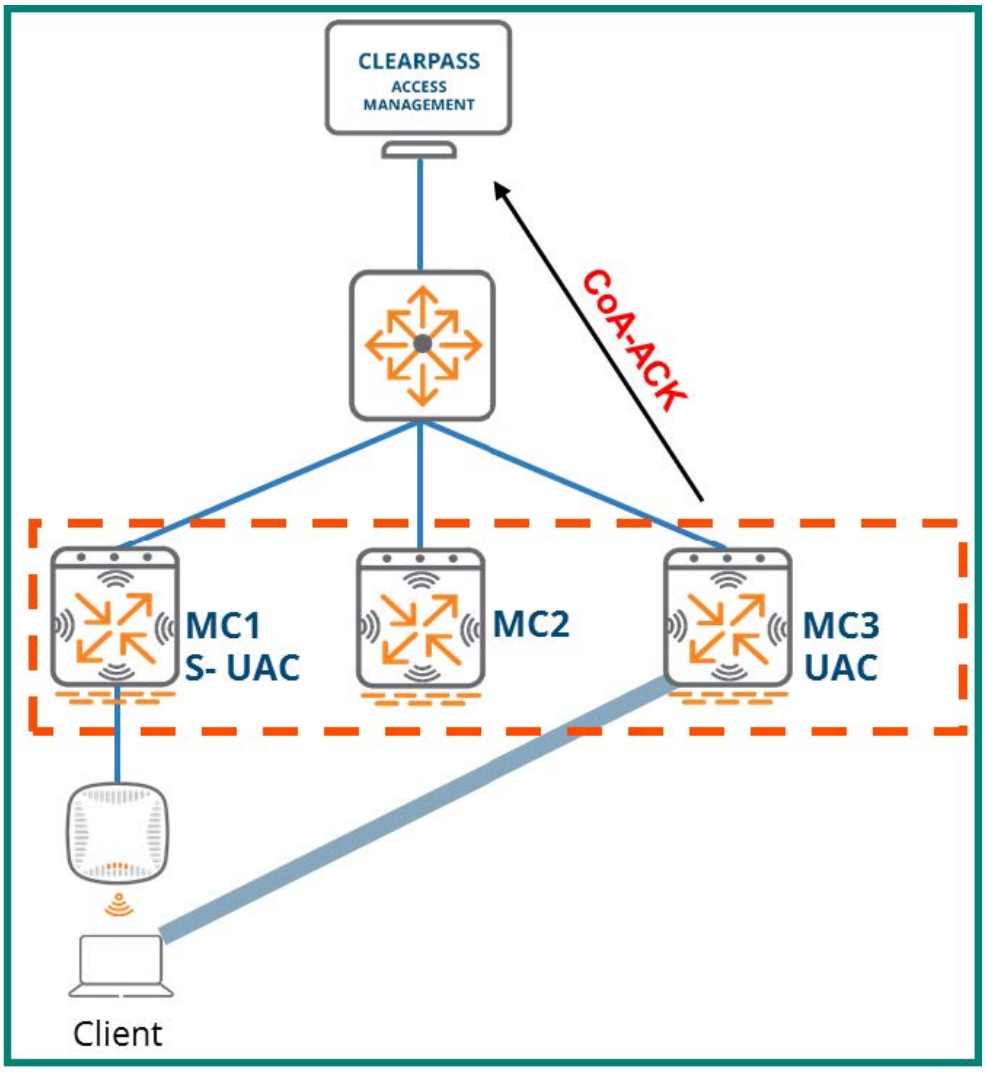
MC1 receives the CoA request as it is the Master for the VRRP instance. It then unicasts the request to the other cluster members.

Figure 87 *MC1 Forwards the Request*



Once MC3 receives the forwarded CoA request from MC1 and successfully implements the change it will respond back to ClearPass with a CoA-ACK. The UAC implementing the change is always the MC responsible for returning the CoA-ACK or CoA-NAK to ClearPass.

Figure 88 *MC3 Returns CoA-ACK to ClearPass*



Live Upgrade

The Live Upgrade feature allows the MCs and APs in a cluster to automatically upgrade their software to a higher ArubaOS version. MCs in a cluster can be upgraded without any adverse impacts to client connectivity and performance. The following points outline the key details of Live Upgrade:

- In-service cluster upgrade
- No manual intervention with minimal RF impact
- Available as of ArubaOS 8.1
- Applicable to a cluster in an MM environment

Prerequisites

The following ArubaOS features are required in order to enable the Live Upgrade feature with minimal RF impact and client disruptions:

- Stateful failover through an L2-Connected cluster with redundancy enabled
- Centralized image upgrade
- AirMatch (schedule enabled)
- Mobility masters must be running an equal or higher version of what is installed on Mobility controllers
- An Upgrade Profile must be configured under the Controller Profile at the same node or higher where the configuration for the cluster receiving the upgrade has been configured

NOTE

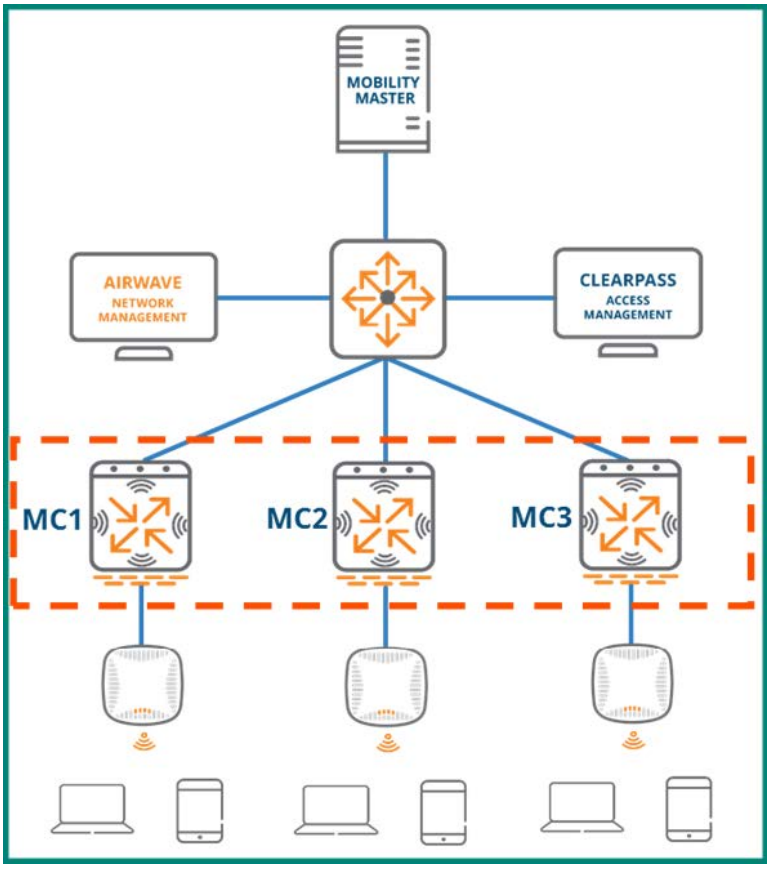
For additional information on how to configure the perquisites listed above refer to the *ArubaOS 8.6.0.0 User Guide*.

Aruba best practices for AP deployment and RF coverage should always be followed to achieve positive results however when performing a Live Upgrade they are a necessity to prevent clients from losing connectivity. APs should be deployed in a capacity-based design so as to guarantee overlapping RF coverage. Doing so ensures that that a client will be always be able to roam to a different AP during the upgrade if the AP where they were previously associated needs to reboot. At a minimum a deployment should be designed so that clients can always see two APs wherever they roam.

CAUTION

In areas without adequate coverage, if the AP a client is connected to reboots during the live upgrade they will lose connectivity until the reboot has finished and the AP comes back up.

Figure 89 *Reference Live Upgrade Architecture*



Live Upgrade Flow

The live upgrade process involves multiple steps to ensure that the upgrade is properly applied and that clients will continue to be served throughout the upgrade. The high level steps required for the upgrade process are as follows and each step will be covered in detail in the subsequent sections:

AP Partition - The APs terminating on the cluster are logically grouped into partitions based on their RF channels.

Target Controller Assignment - Each AP partition is assigned an MC in the cluster which serves as a post-upgrade termination target for the APs in that partition. All cluster members are used as AP partition targets with the exception of one.

New Firmware Pushed to MCs - All of the cluster members download the new ArubaOS firmware through the Centralized Image Upgrade feature using a pre-configured upgrade profile.

Cluster Members Upgrade - The actual upgrade process begins by rebooting one of the cluster members to the new firmware. Once the first controller receiving the upgrade comes back up loaded with its new firmware, the APs in the partitions targeting that controller are pre-loaded with the new firmware. Those APs reboot one partition at a time and come up on their upgraded target controller

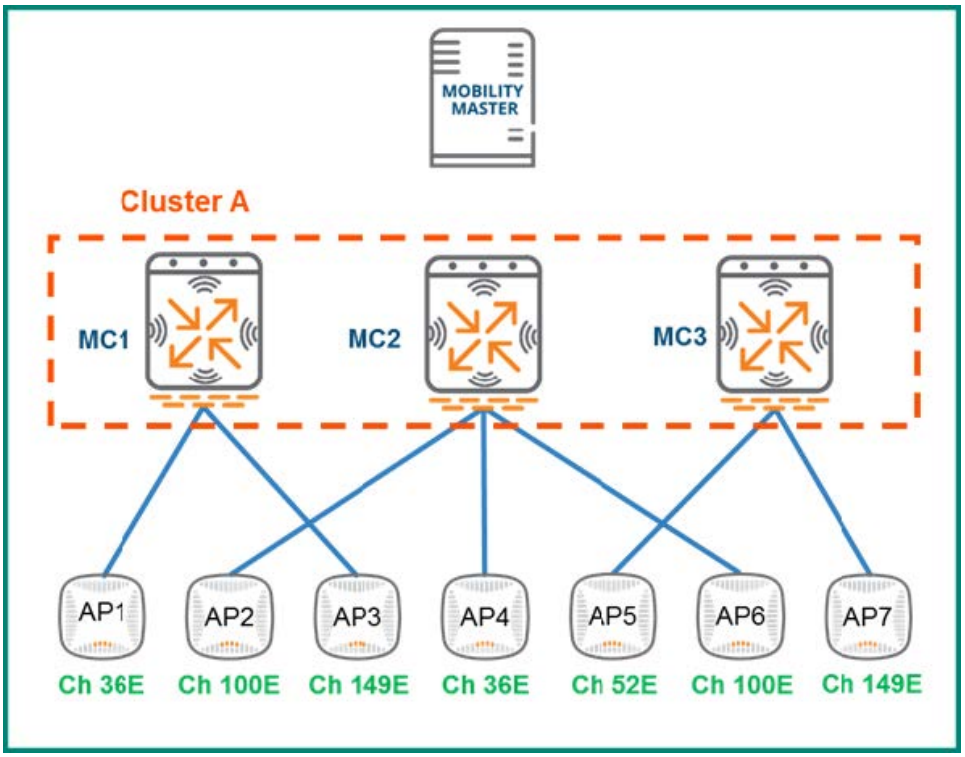
After all APs have rebooted for the first target controller, a second controller in the cluster is rebooted followed by the AP partitions targeting it in the same manner as described above.

After all APs are upgraded and terminated on their upgraded target controllers , then the last controller that has been exempted from targeting is rebooted to come up and join the upgrade cluster.

Initial Lab AP Distribution

The image below depicts the scenario that will be used to demonstrate the key concepts of the live upgrade feature. The selected architecture is a standard ArubaOS 8 design consisting of a fully-redundant MM pair deployed on a virtual appliance. The scenario has three MCs in a single cluster which have been configured in an L2-Connected state with full redundancy enabled between them as specified by the prerequisites. Seven APs are connected to three MCs and the APs operate across a variety of different channels.

Figure 90 *Sample Network for Live Upgrade*



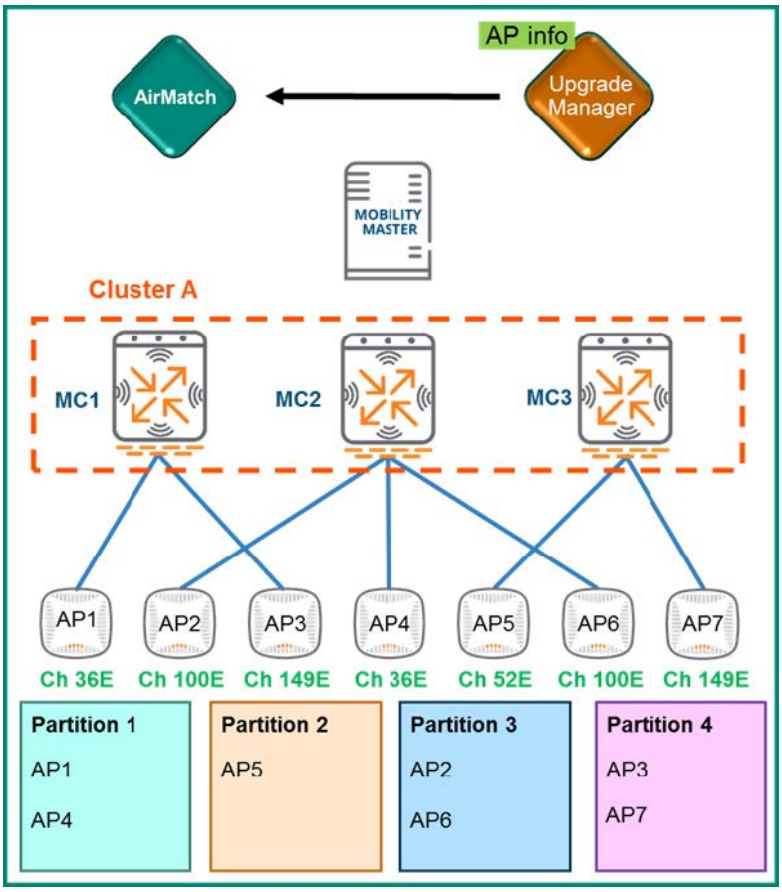
NOTE

The channel assignments for the APs were chosen at random strictly for purposes of demonstrating Live Upgrade operations. They do not represent a best practice recommendation for channel assignment in a production network.

AP Partition

The live upgrade process begins when the upgrade manager for the cluster sends information about all the APs connected to the cluster to AirMatch. This is why it is a prerequisite to leave the default setting of enabling the AirMatch schedule intact to perform live upgrade. Upon receiving the AP information from the upgrade manager, AirMatch will segregate the APs into logical groups and update the upgrade manager with the partition to AP mapping assignments.

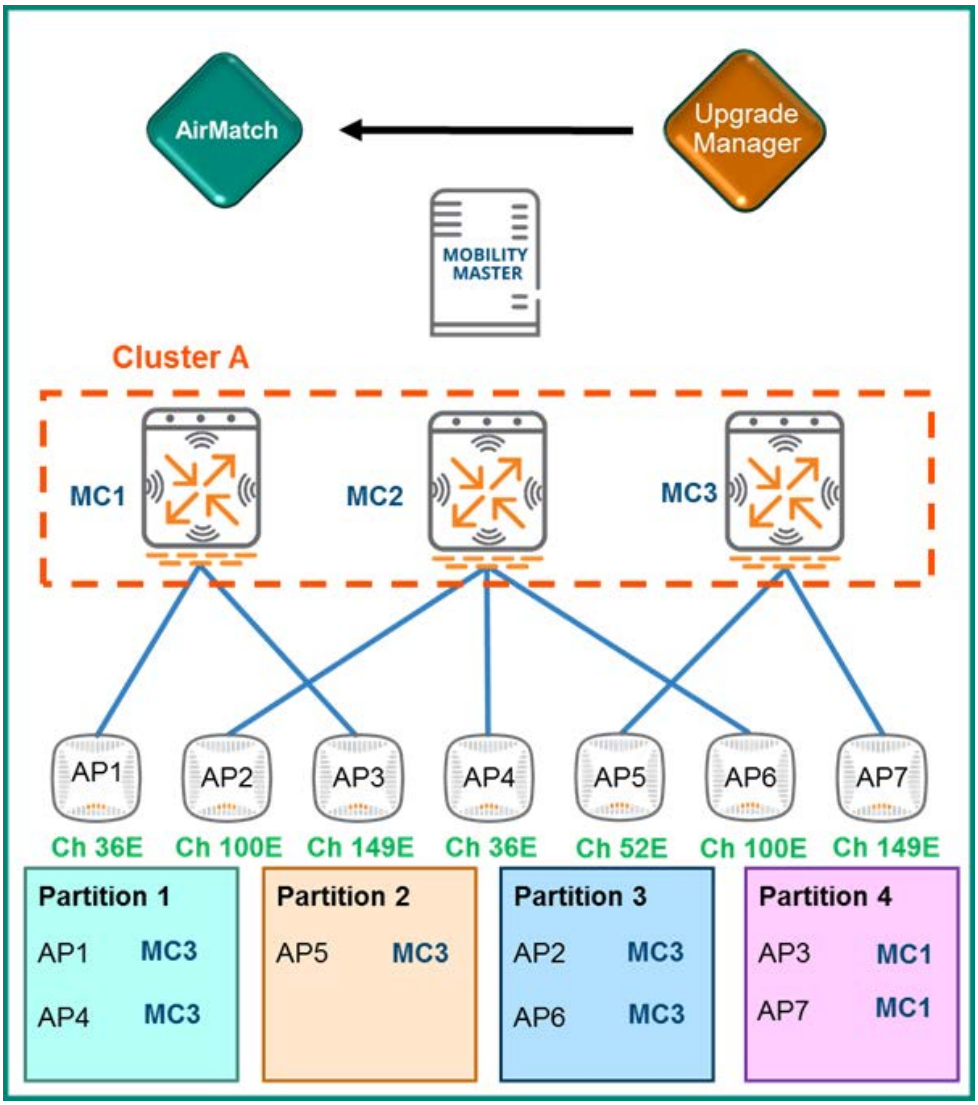
Figure 91 *AP Partitions*



Target Assignment and Firmware Download

After all APs have been logically partitioned by AirMatch based on their information and the upgrade manager has been updated with the assignments, each partition is assigned a target MC. The target represents the MC managing the each partition of APs after they reboot with their new firmware. As the figure below demonstrates, the APs in partitions 1, 2, and 3 have been assigned MC3 as their target while the APs in partition 4 have been assigned MC1:

Figure 92 *Target Assignments*



NOTE

MC2 has not been designated as a target for any partition or APs. It was excluded intentionally and the reasons why will be discussed in the following sections.

Once all partitions have their target assignments the MCs will download the new ArubaOS firmware one at a time. They will continue normal operation while their respective downloads take place.

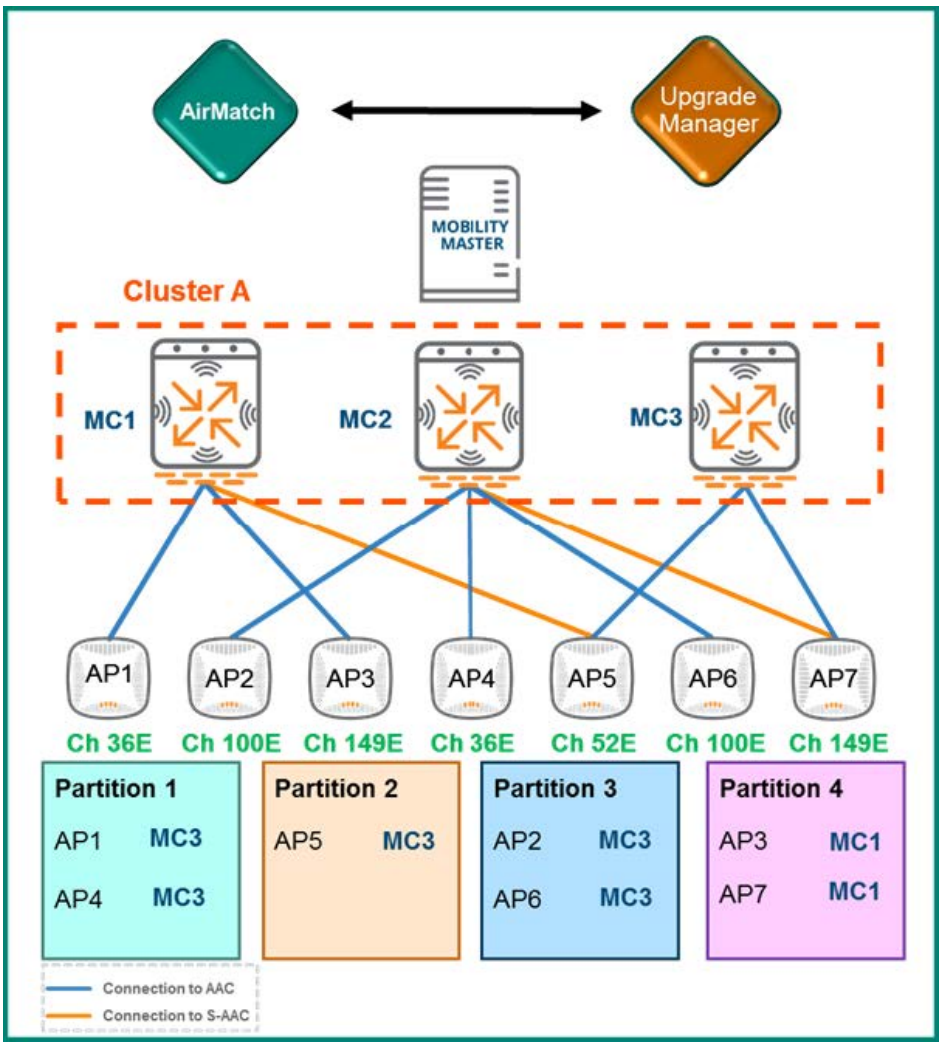
Cluster Members Upgrade

Once all the APs have been partitioned, assigned a target MC, and the MCs have pre-downloaded their new firmware, they are ready to commence the actual upgrade process. The sample cluster has three members, however the process will be identical regardless of how many MCs are present in the cluster. Each cluster member reboots one by one and the final cluster member which was not designated as a target for any APs will be the last one to reboot.

First Member Upgrade

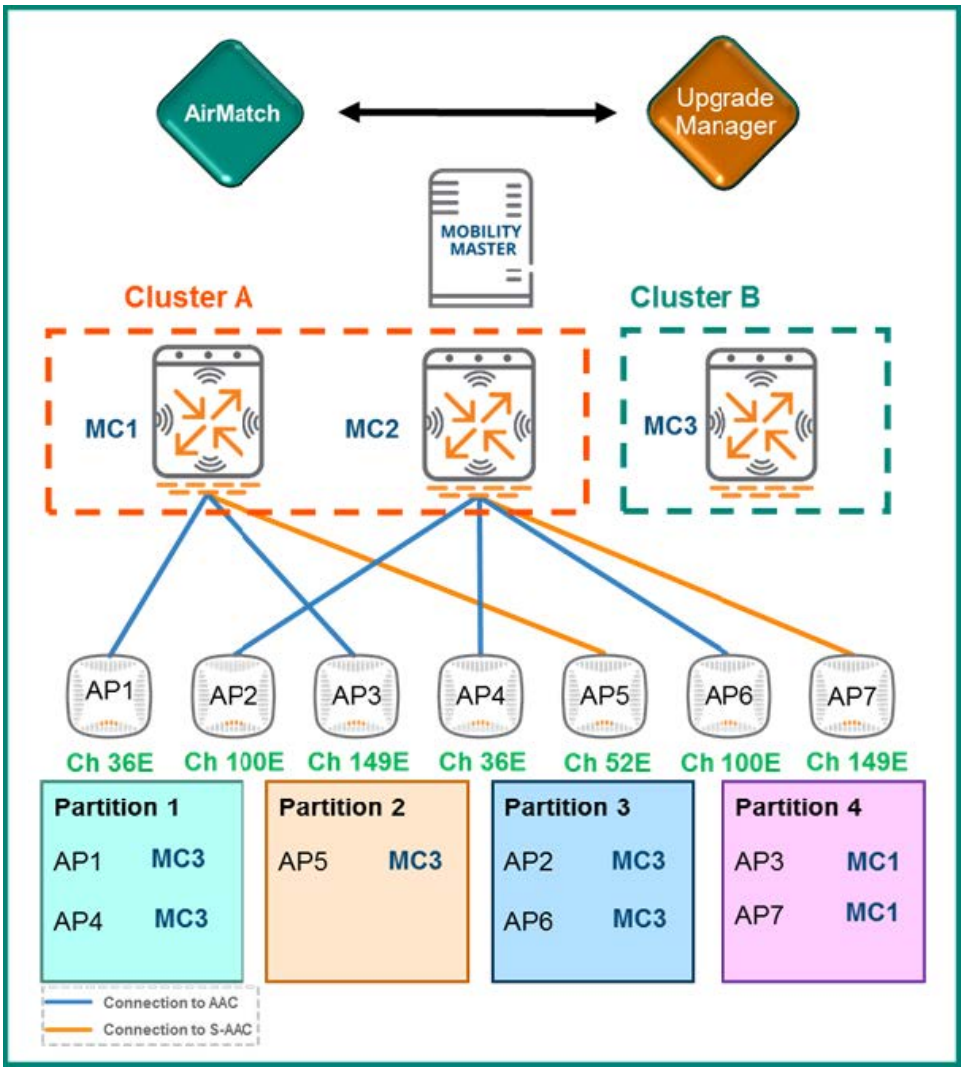
The upgrade process starts when MC3 reboots so that it's pre-downloaded firmware upgrade can take effect. During the reboot process, MC3 will go down and will be unable to continue serving as the AAC for APs 5 and 7 therefore they will need to failover to MC1 and MC2, respectively. Likewise, any clients with MC3 assigned as their UAC will need to failover to MC1 and MC2.

Figure 93 *MC3 begins reboot with APs and clients failing over*



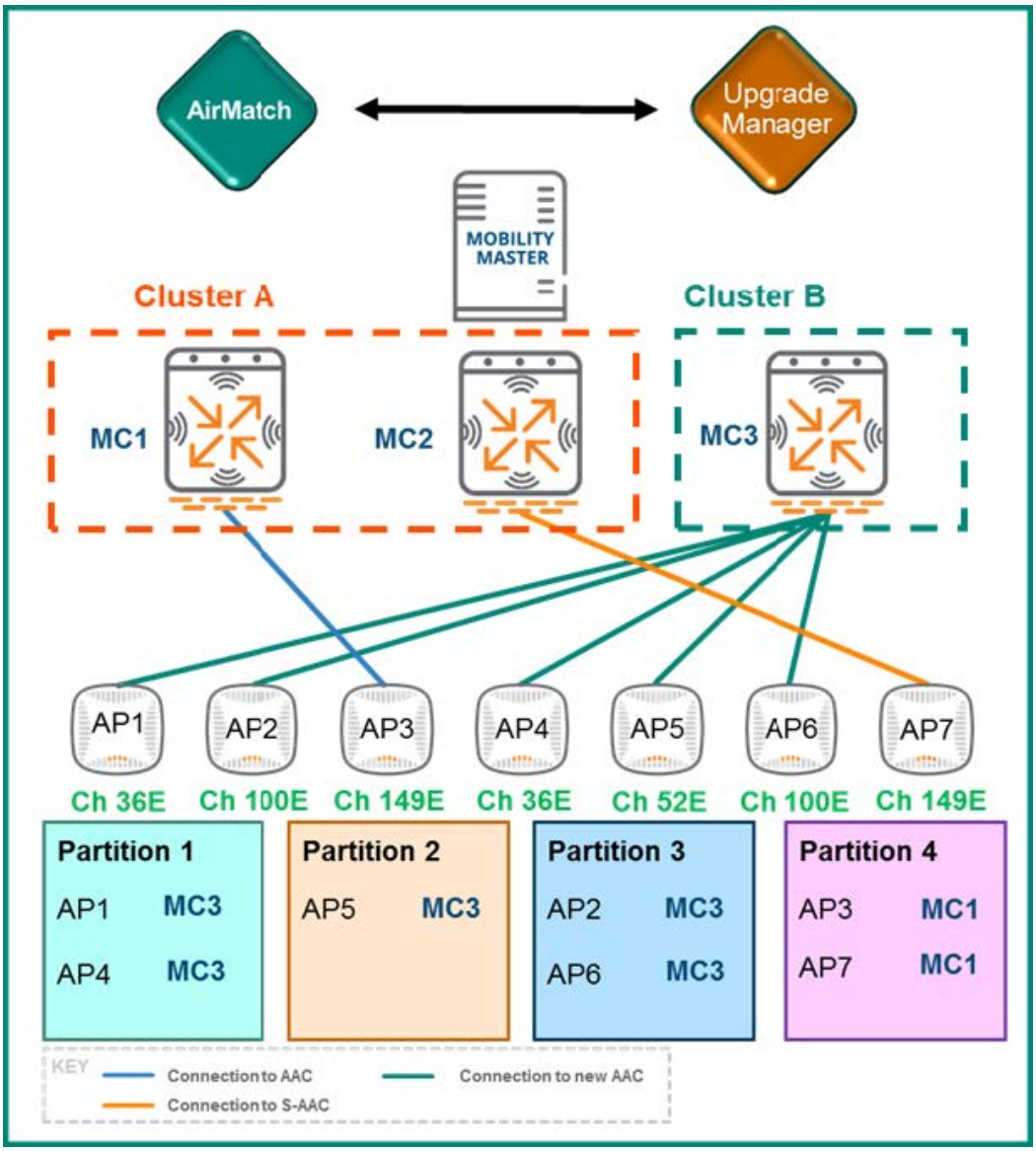
After MC3 finishes rebooting and comes back online running its new firmware, it will form a separate cluster since MCs in the same cluster must run the same firmware version. The new cluster MC3 has formed is represented in the figure below with a green border and will be referred to as Cluster B. At this point MC1 and MC2 along with all associated APs and clients are still in Cluster A running the previous firmware version.

Figure 94 *MC3 Reboots*



Once MC3 is back online, it will assume operation as the AAC for the APs which had it assigned as their target MC. The APs will first preload their new firmware and then reboot. The reboot will occur for one partition at a time to ensure that clients will not be deprived of AP options to maintain connectivity. If all APs were to reboot at once, ARM's coverage hole detection mechanism wouldn't be able to adequately compensate for all the gaps. This could result in clients being forced off the network until the APs had finished rebooting. Clients associated to rebooting APs will roam to APs attached to the red Cluster A. These clients will only need to go through a 4-way 802.1X handshake rather than a full authentication process since they will retain their UAC and it is already a member of the cluster.

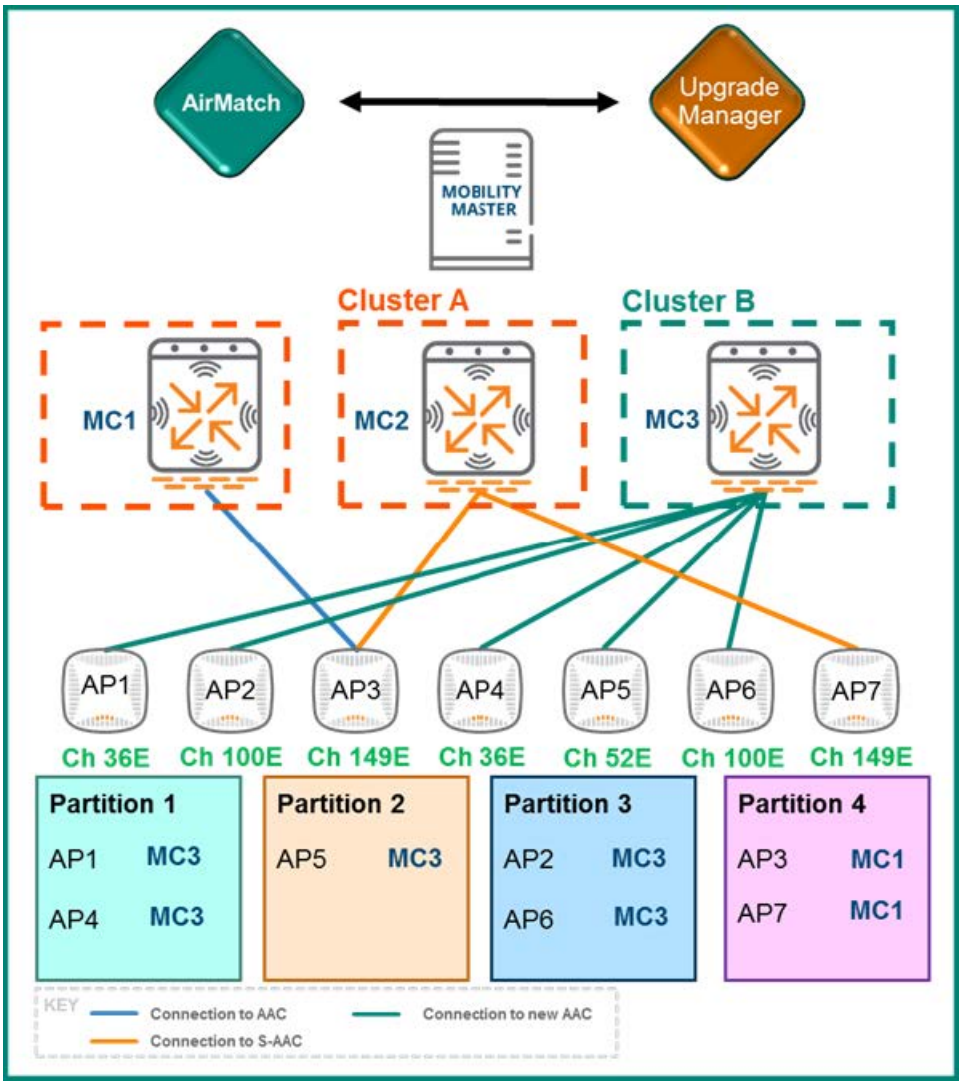
Figure 95 *APs 1-2 and 4-6 connect to Cluster B*



Second Member Upgrade

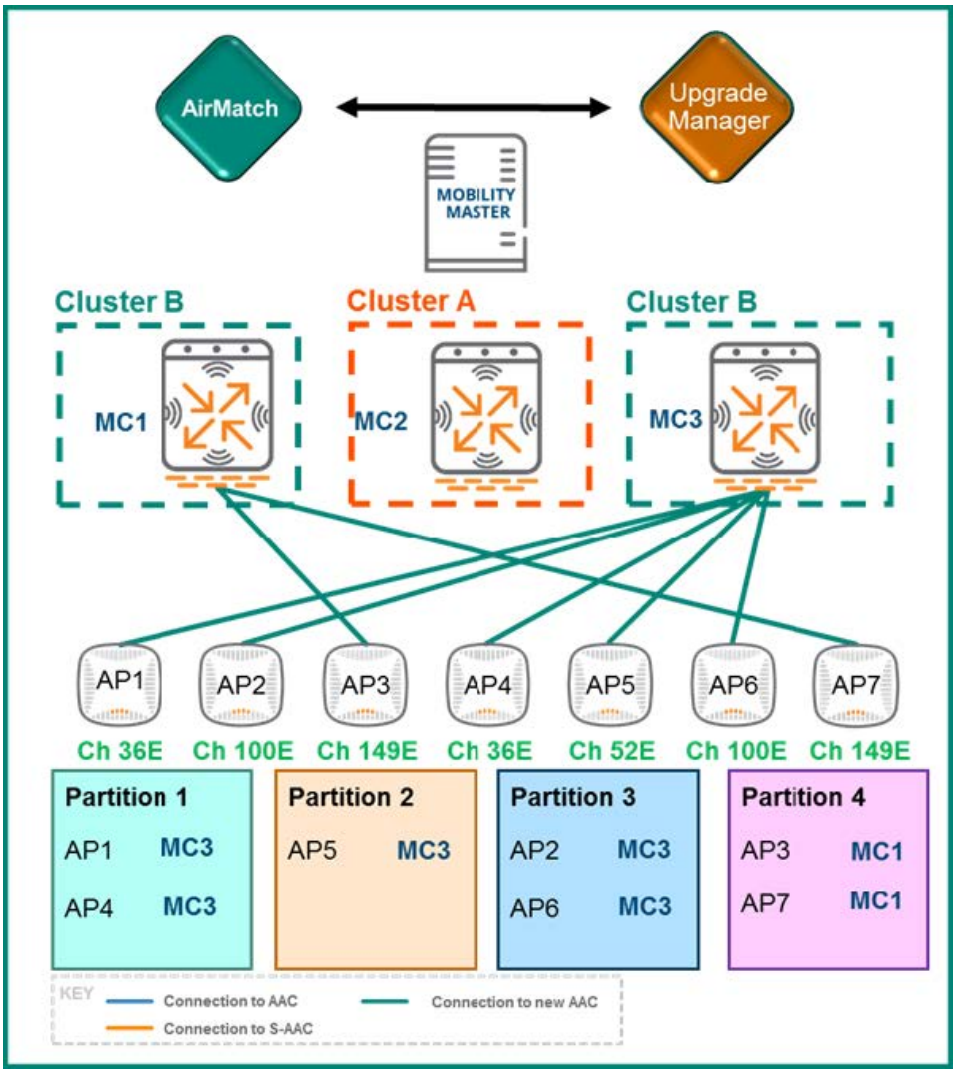
Now that MC3 is operational with its new firmware and its designated APs have rebooted, MC1 will begin its upgrade using an identical process. MC1 will reboot and leave Cluster A making MC2 the last member of the original cluster. After MC1 reboots, any APs which it was serving as AAC will failover to their S-AAC (MC2) and clients will failover to their S-UAC (MC2 as well). In the example, AP3 will failover to MC2 along with any clients whose UAC was MC1.

Figure 96 *APs and Clients failover to MC2 while MC1 reboots*



Once MC1 comes back online, it will immediately join MC3 in Cluster B. AP3 and AP7 in Partition 4 were assigned MC1 as their target and will pre-download the new firmware so that they can reboot and join the new cluster. Once the firmware has been pre-downloaded, the APs reboot causing their associated clients to immediately roam to APs attached to the green Cluster B. Even though the clients were previously connected to MC1 and MC3 the controllers are considered new devices from the client perspective since they upgraded their firmware and formed a new cluster. This will require any 802.1X client to go through the full authorization process just as they would when associating to a new device. Once AP3 and AP7 come back up with their new firmware they will connect to MC1 as their AAC.

Figure 97 *APs 3 and 7 connect to MC1*

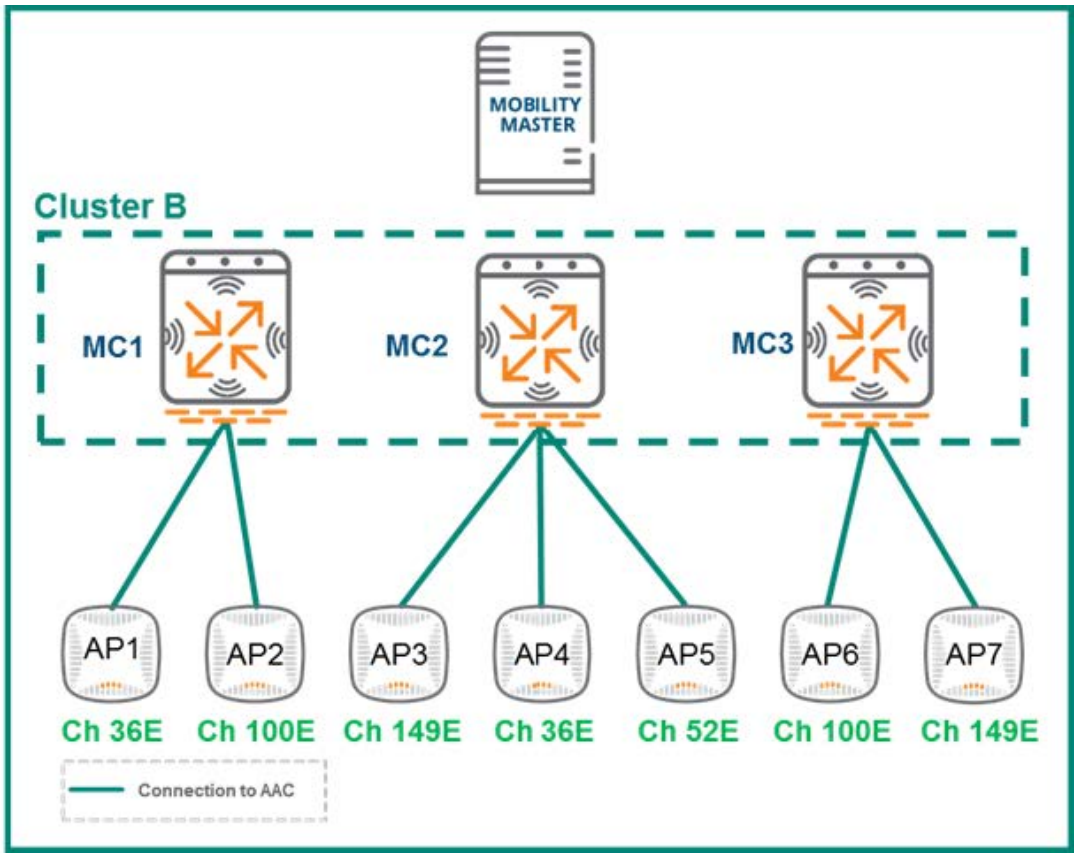


Final Member Upgrade

After all cluster members have received their upgrade and rebooted, the final member (MC2) will begin its upgrade. MC2 will not have any associated clients or APs since it was deliberately excluded as a target controller for the partition and hence neither APs nor clients will have to be redistributed. MC2 can reboot, come back online with its new firmware, and rejoin the other two MCs in Cluster B. After it rejoins the cluster, MC2 will be available for AP and client load balancing as determined by the cluster leader.

For additional information on cluster load balancing please refer to the Client Load Balancing and AP Load Balancing sections.

Figure 98 *Live Upgrade complete*



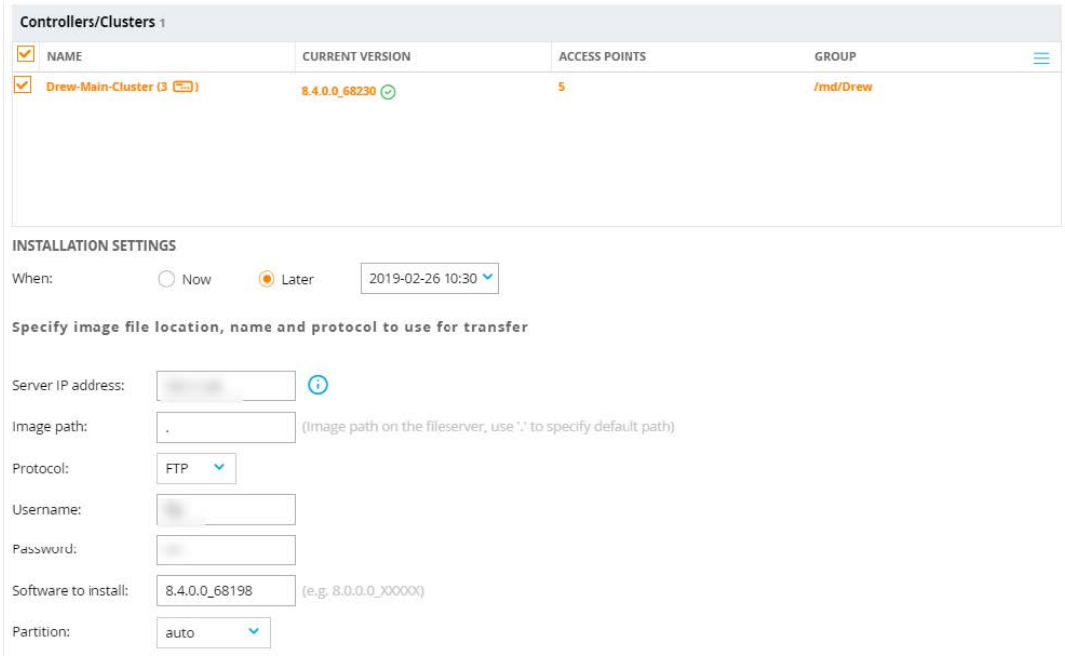
Scheduled Live Upgrades

Starting from ArubaOS 8.4.0.0, the live upgrade feature can be scheduled to occur during a period when there will be a minimal network resource demand . This minimizes the client performance impacts to the greatest possible extent. The process works exactly the same as it would as described above, with the addition of being able to choose when the cluster live upgrade should occur.

NOTE

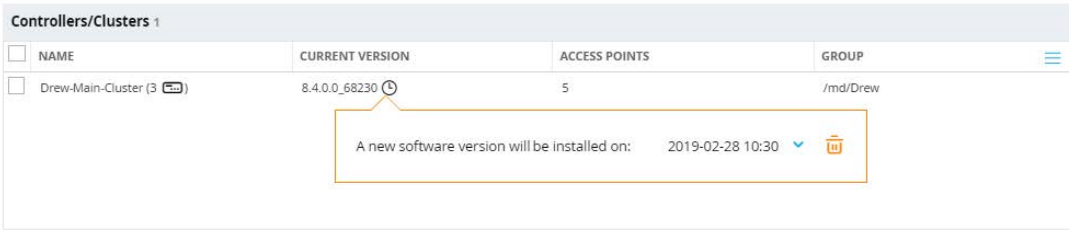
It is vital to ensure that all nodes of the cluster have the same NTP configuration and the same IANA time zone configured, otherwise the MM will not be able to schedule upgrades for a cluster.

Figure 99 *Scheduling a Live Upgrade*



One the live upgrade has been scheduled, a grey clock icon will appear next to the cluster. Clicking on this icon will display a dropdown that displays the exact time the upgrade is scheduled to occur and also gives an option to cancel the upgrade.

Figure 100 *Confirming a Scheduled Live Upgrade*



ArubaOS has supported centralized licensing since ArubaOS 6. Licenses will be installed on one controller and other controllers would subscribe to withdraw licenses from a global license pool as required. However, a significant limitation for this model was that in some customer deployments there was no way to control how many licenses one controller could withdraw from the pool. This limitation led to some situations where license pools would be depleted when one site deployed more APs than there were licenses available in the pool.

With the introduction of ArubaOS 8, the Mobility Master now supports the creation of smaller licensing pools within the global pool. This method of segmentation allows limitation or reservation of licenses that a specific controller or a group of controllers are allowed to withdraw from the global pool.

Licensing Concepts

License Types

Most of the key abilities and features of ArubaOS 8 platform are enabled using licenses. These licenses are generally installed on the Mobility Master but can also be installed on an MCM or a Stand-alone controllers if required. Additionally, centralized licensing allows mobility controllers under the management of the Mobility Master or MCM to subscribe and draw the required number of licenses.

ArubaOS 8 licenses are categorized into three different classes of licenses:

Table 16: *Licenses in ArubaOS 8*

Device Licenses	Feature Licenses	Session Licenses
MM-VA	LIC-PEF	LIC-VIA
MM-HW*	LIC-RFP	LIC-ACR
MC-VA	LIC-PEFV	
LIC-AP	SUBX-WebCC**	
LIC-ENT		

* MM-HW licenses are integrated within the Hardware Mobility Master.

** WebCC is a subscription-based license 'X' equals a 1, 3, 5, 7, or 10 year subscription.

- **Device-Based Licenses** – Licenses that enable device functionality.
  - MM-VA/MM-HW* – Enable controllers and APs to terminate on the Mobility Master. The MM-HW licenses are pre-installed on the Mobility Master Hardware Appliance.

- MC-VA – Enable VMCs to terminate APs. These can be installed on the Mobility Master or directly on any VMC that is not terminated on a Mobility Master.
- LIC-AP – Licenses installed on the MM, MCM, or Stand-alone controller to enable AP termination.

- **Feature-Based Licenses** – Licenses that enable specific software features.
  - LIC-PEF – Enables the Policy Enforcement Firewall (PEF) feature.
  - LIC-RFP – Enables the RF Protect (RFP) features for WIDS/WIPS and Spectrum Analysis support.
  - LIC-PEFV – Enables PEF support on Virtual Internet Access (VIA) client roles as a platform license applied to each controller. Being phased out by LIC-VIA session licenses.
  - SUBX-WebCC – This subscription-based license that enables web filtering support in 1, 2, 3, 5, and 7 year subscriptions.
  - LIC-ENT – This is a bundled combination of the AP, PEF, RFP, and LIC-AW (AirWave) licenses.
- **Session-Based Licenses** – Define a feature based on the number of concurrent sessions allowed across the controller.
  - LIC-VIA – Enables Virtual Internet Access (VIA) clients to connect and establish a tunnel to a controller.
  - LIC-ACR – Advanced Cryptography (ACR) licenses enable the use of Suite B licenses on the controller.

Mobility Master Licensing

The Mobility Master in ArubaOS 8 serves as the centralized licensing server for mobility controllers under its management. APs and controllers will draw from the centralized Mobility Master license pool when the Mobility Master serves as the licensing master. The table below provides a description of the license consumption process on the Mobility Master.

VMM license consumption occurs using a slightly different method because the machines are virtual appliances. Only one MM-VA-XX license needs to be purchased even if multiple VMMs are deployed for redundancy. If a VMM is being used to support up to 5,000 devices, then only one MM-VA-5K license is required and multiple VMMs can be provisioned to manage the WLAN. Additionally, smaller MM-VA licenses can be stacked to support larger numbers of devices on the Mobility Master. However, there is a point where stacking smaller licenses can cost more than a single larger MM-VA license.

Licenses are pre-installed on hardware Mobility Masters because they are hardware appliances and they are not capable of stacking licenses, leading to a higher licensing cost. For example, if a deployment has to support up to 5,000 devices, then two MM-HW-5K appliances will be required, even though together they will still only support up to 5,000 devices.

For all other licenses (AP, PEF, RFP, etc.) the necessary license quantities should be purchased and the licensing database will be shared between the Mobility Masters.

Table 17: *License Consumption in ArubaOS 8*

License Type	Consumption Method
MM-VA/MM-HW	Each controller or AP will consume 1 license.
MC-VA	Each AP terminated on a VMC will consume 1 license.
AP, PEF, RFP	Each AP terminated on a controller will consume 1 license.
LIC-PEFV	Each LIC-PEFV license is applied to each controller.
SUBX-WebCC	Each AP terminated on a controller will consume 1 license.

Table 17: *License Consumption in ArubaOS 8*

License Type	Consumption Method
LIC-VIA	Each "VIA user session" on a controller will consume 1 license.
LIC-ACR	Each "SuiteB" client or tunnel will consume (1) license.

License Model Examples

Sample Deployment 1 – 800 APs with AP, PEF, RFP licenses managed by hardware MCs (MCs) and Virtual MMs (VMMs). With this sample deployment, each of the 800 APs will need an AP, PEF, and RFP license. Having a VMM requires enough MM-VA licenses to cover every AP and MC under its management. The MM-VA-1K license provides a pool of 1000 licenses. 800 of the 1000 licenses in the pool are consumed by APs meaning there are 200 licenses left to cover the MCs as well as any future addition of devices.

Table 18: *License Sample Model 1*

License Type	Quantity
MM-VA-1K	1
LIC-AP	800
LIC-PEF	800
LIC-RFP	800

Sample Deployment 2 – 250 APs with AP and PEF licenses using VMCs and VMMs. In this case, the MM-VA-500 license provides a pool for up to 500 devices on the MM. The MC-VA-250 license will enable up to 250 APs to terminate on any number of VMCs under the MM (could be a single VMC or multiple VMCs).

Table 19: *License Sample Model 2*

License Type	Quantity
MM-VA-500	1
MC-VA-250	1
LIC-AP	250
LIC-PEF	250

Sample Deployment 3 – 6,000 APs with AP, PEF, and RFP licenses using hardware MCs and Hardware MMs (HMM) with redundancy for clustering. The sizing specifications below show two 10k MM appliances, six 7240XM controllers to support all 6,000 APs within a cluster, and 6000 AP licenses for AP, PEF, and RFP respectively.

Table 20: *License Sample Model 3*

License Type	Quantity
MM-HW-10K	2
7240XM MCs	6
LIC-AP	6000
LIC-PEF	6000
LIC-RFP	6000

Sample Deployment 4 – 2000 APs with AP, PEF, and RFP licenses supporting 1,500 clients that require VIA and Suite B cryptography, using Hardware MCs and Hardware MMs. The MM-HW-5k license provides a pool for up to 5,000 devices on the MM.

Table 21: *License Sample Model 4*

License Type	Quantity
MM-HW-5K	2
7240XM MCs	2
LIC-AP	2000
LIC-PEF	2000
LIC-RFP	2000
LIC-VIA	1500
LIC-ACR	1500

Sample Deployment 5 – 2000 APs with AP and PEF licenses using Hardware MCs and HMMs supporting up to 50 clients per AP up to 10,000 total clients. The client count is much higher than average so even though the total AP count is only 2,000 the largest HMM must be able to accommodate all of the clients.

Table 22: *License Sample Model 5*

License Type	Quantity
MM-HW-10K	2
7240XM MCs	2
LIC-AP	2000
LIC-PEF	2000

MCM Licensing

The MC Master (MCM) is similar to the Master-Local controller architecture in ArubaOS 6 where a dedicated hardware controller serves as the central licensing server for all the managed locals and as a central configuration point.

MCM mode is supported only on the 7030 and 7200 series controllers. 7024 and smaller and VMCs cannot serve as an MCM device.

Licenses can be configured and installed on to the MCM controller. The device (except for the MM-VA license), feature, and session based licenses should scale and use the same considerations based on their consumption requirements (similar to the MM).

However, the MC-VA licenses for VMC controllers that will be managed by an MCM will be installed on the individual VMCs and VMCs under an MCM cannot share licenses as the could under a Mobility Master. Additionally, the MC-VA license must be installed on a whole and must match the platform. For example, a single MC-VA-250 license cannot be purchased and then split up across 5 VMCs with 50 licenses each, the MC-VA-250 should be installed on an MC-VA-250 (or smaller) non-MM managed VMC.

Stand-alone Licensing

When licensing a stand-alone controller, all the device, feature, and session based licenses can be installed on a stand-alone controller and are consumed in the same manner.

With MC-VA licenses on stand-alone controllers should be installed on a whole and must match the platform. For example, a single MC-VA-250 license cannot be purchased and then split up across 5 VMCs with 50 licenses each, The MC-VA-250 would need to be installed on an MC-VA-250 (or smaller) non-MM managed VMC.

License Activation and Migration

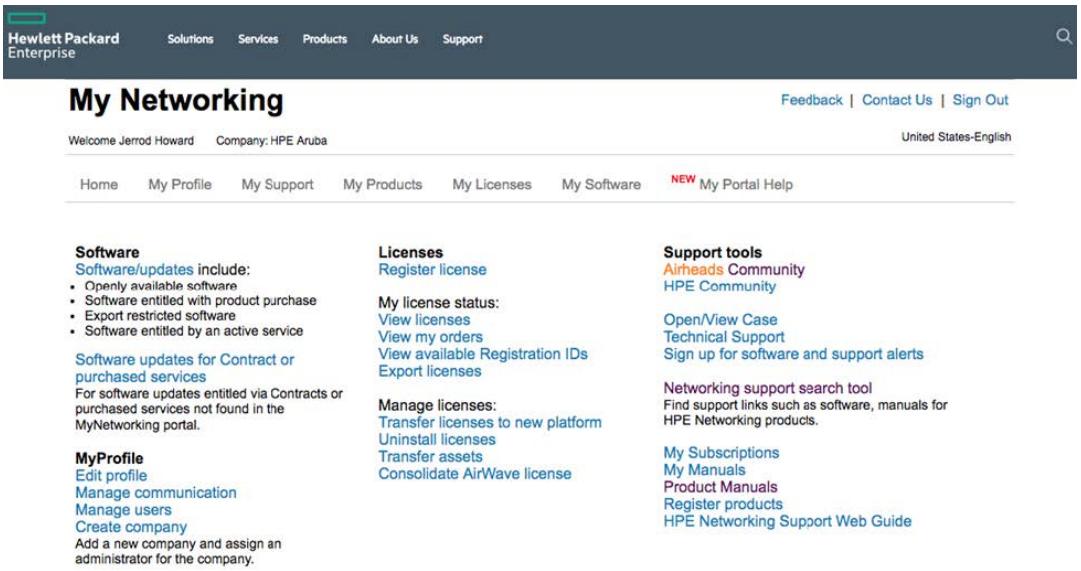
MyNetworking Portal

The MyNetworkingPortal (MNP) is HPE's licensing portal and is used for a variety of support activities including:

- Activation of new licenses from purchases
- Activation of demo and evaluation licenses
- License management (migrate, change ownership, etc.),
- Software and user guides

MNP has a main landing page that is displayed after login and directs users to the appropriate resources they are attempting to locate.

Figure 101 *MyNetworkingPortal Dashboard*



When a new order is placed, a Sales Order is generated and it contains an *associated Registration ID* or *Certificate ID*. Once logged in to MNP, click on **Register License** and enter the same *Registration ID* or *Certificate ID* from the Sales Order. A prompt will then appear asking for the email address corresponding to the order. This email address may belong to an individual or an organization depending on how the order was made, however in either case the appropriate address will appear on the sale invoice. Once entered, a list of all the licenses that are ready for activation are listed. The overall quantity of licenses and the number of licenses that awaits activation will be listed. As licenses are activated from the new sales order the number of available licenses will decrease. MNP can be accessed through the following URL:

https://hpe.com/networking/mynetworking/

Figure 102 *License Registration in MNP*

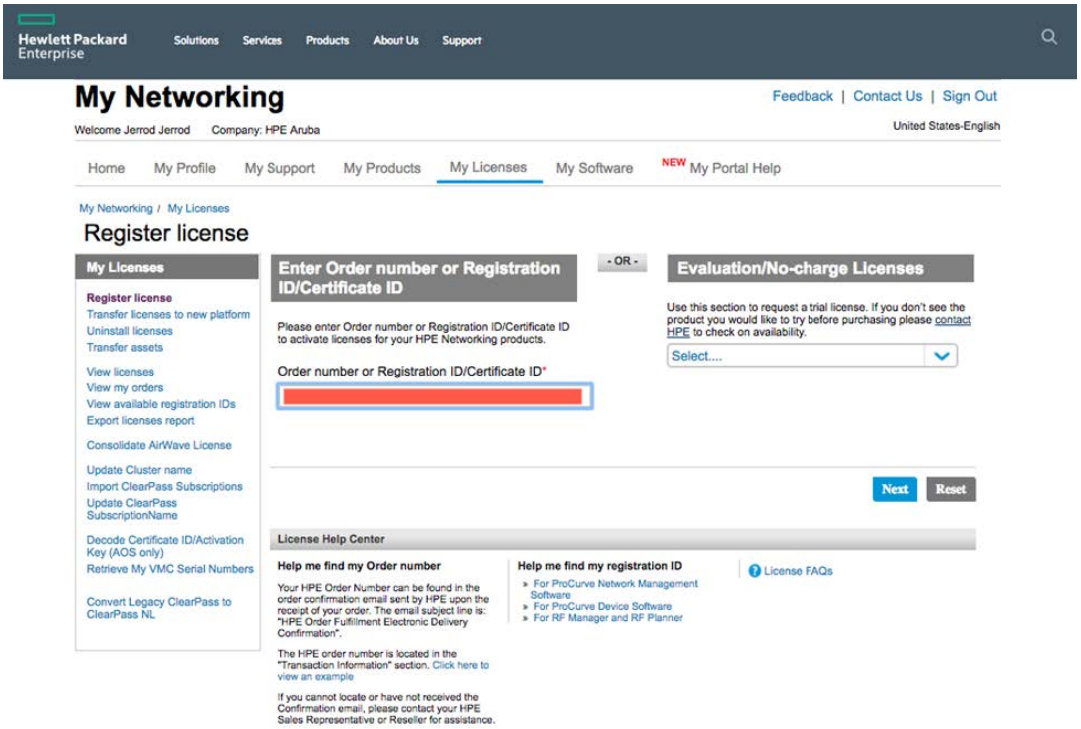
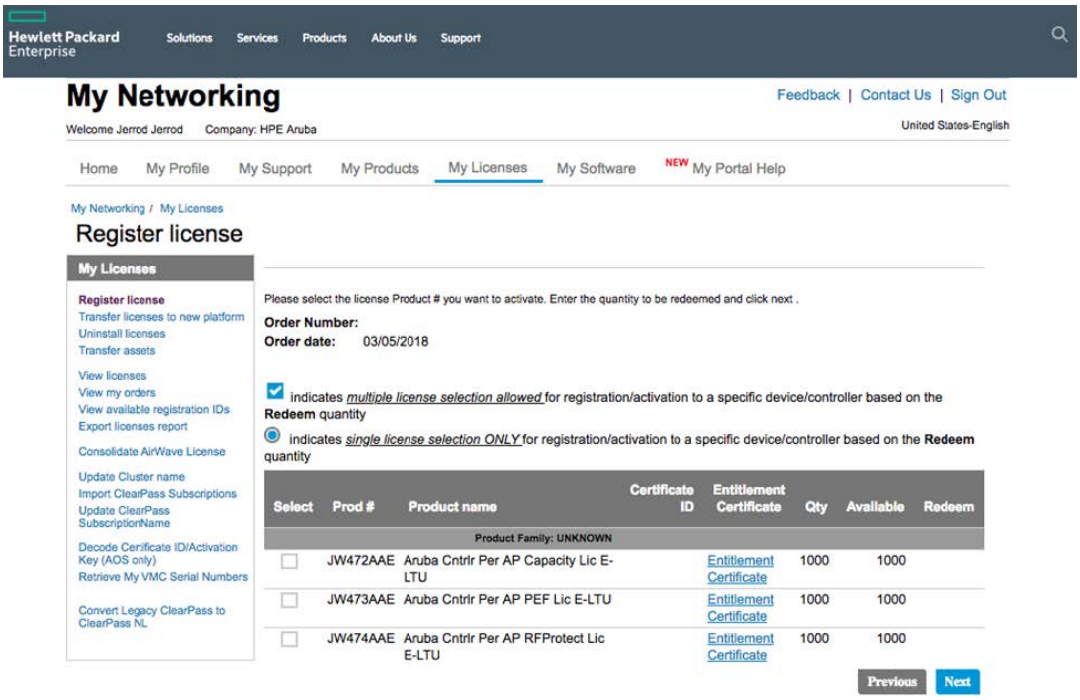
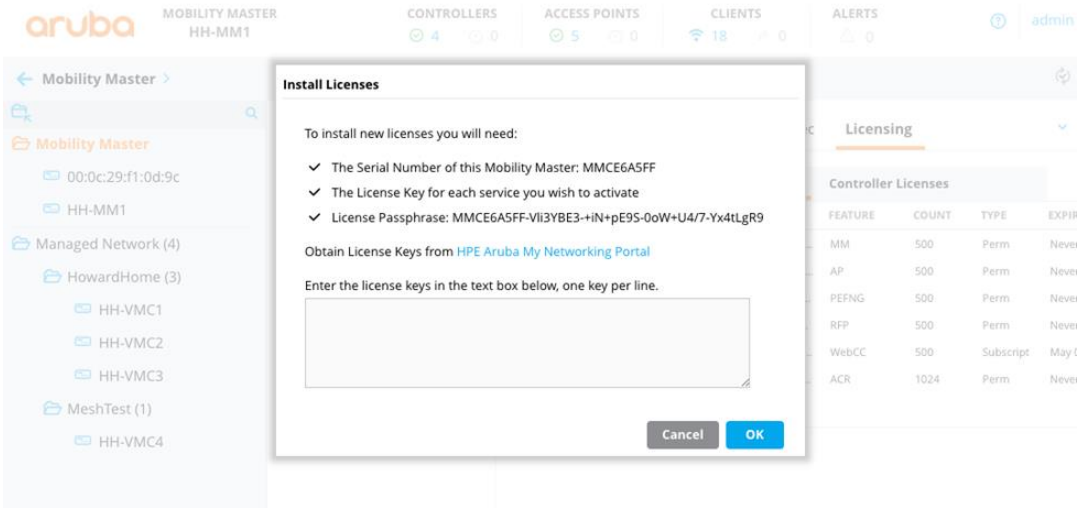


Figure 103 *License Registration in MNP*



All that is required for license activation is the controller serial number in the case of hardware MCs and Mobility Masters or the license passphrase in the case of any virtual appliance or controller. This serial number or license passphrase can be found in the WebUI of the controller by navigating to **System > Licensing > MM/Controller Licensing** and click on the + sign, or from the CLI with the commands **show inventory** for hardware serials or **show licenses passphrase** for virtual appliances or controllers.

Figure 104 *License Activation in MNP*



Follow the procedure given below to migrate a license from ArubaOS 6 to ArubaOS 8 though MNP:

1. Navigate to the MNP portal page and the select **Transfer Licenses to New Platform**. All the serial numbers owned by that account are displayed.
2. Locate the serial number of the device currently holding the licenses and click **Next**.
3. Select the new controller where the licenses will migrate from the dropdown along with the new

ArubaOS 8 serial or passphrase.

4. Click **Transfer**.

MNP will provide new license keys and will update the serial number database within MNP with the new license activation keys. These new licenses keys would be pasted in to the new Mobility Master, MCM, or Stand-alone 8.x controller.

Figure 105 *Transferring Licenses to a New Platform in MNP*

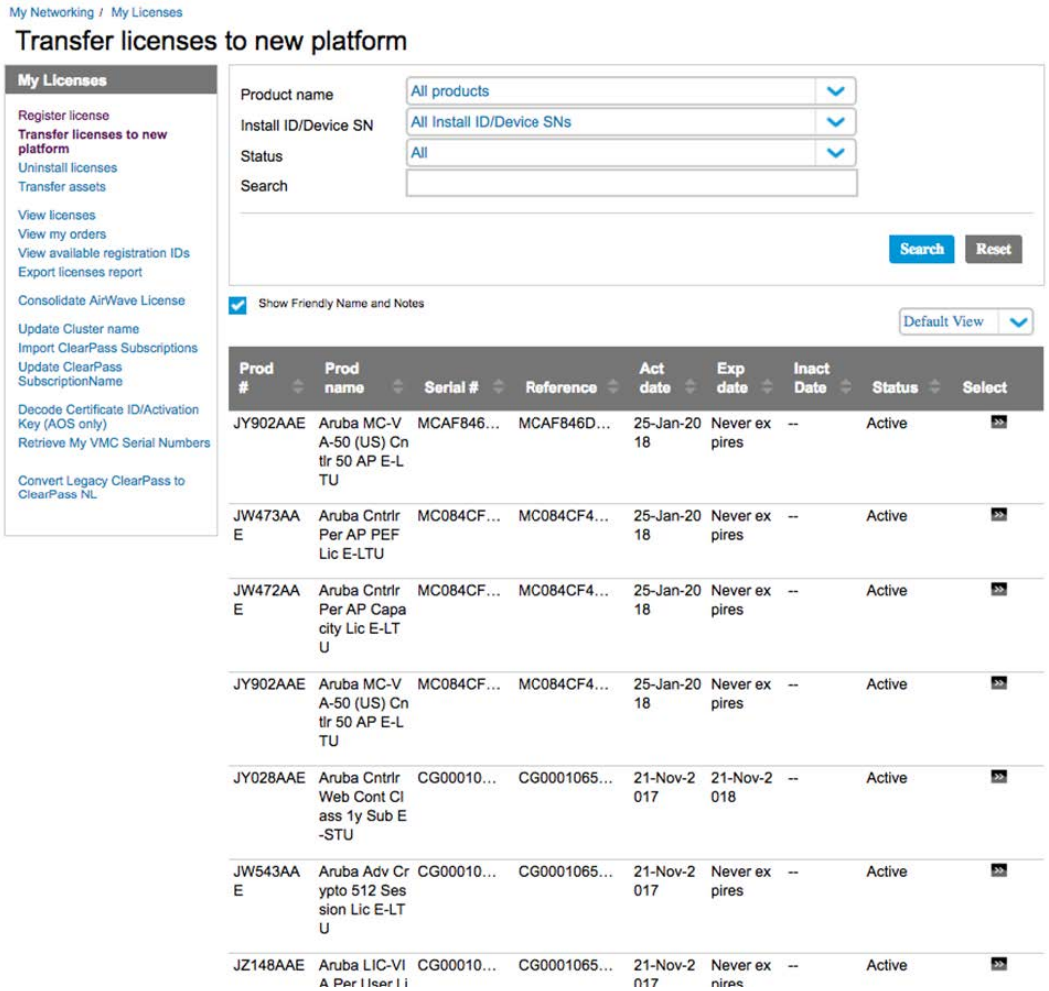
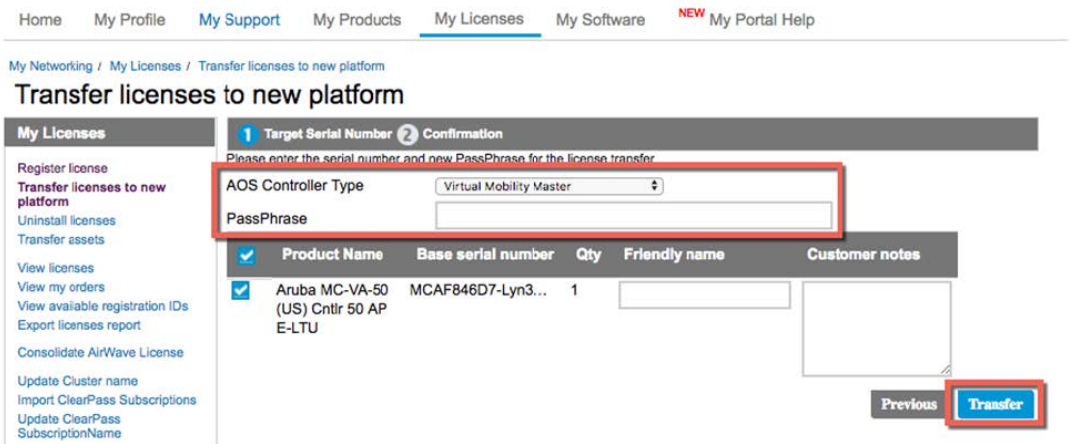


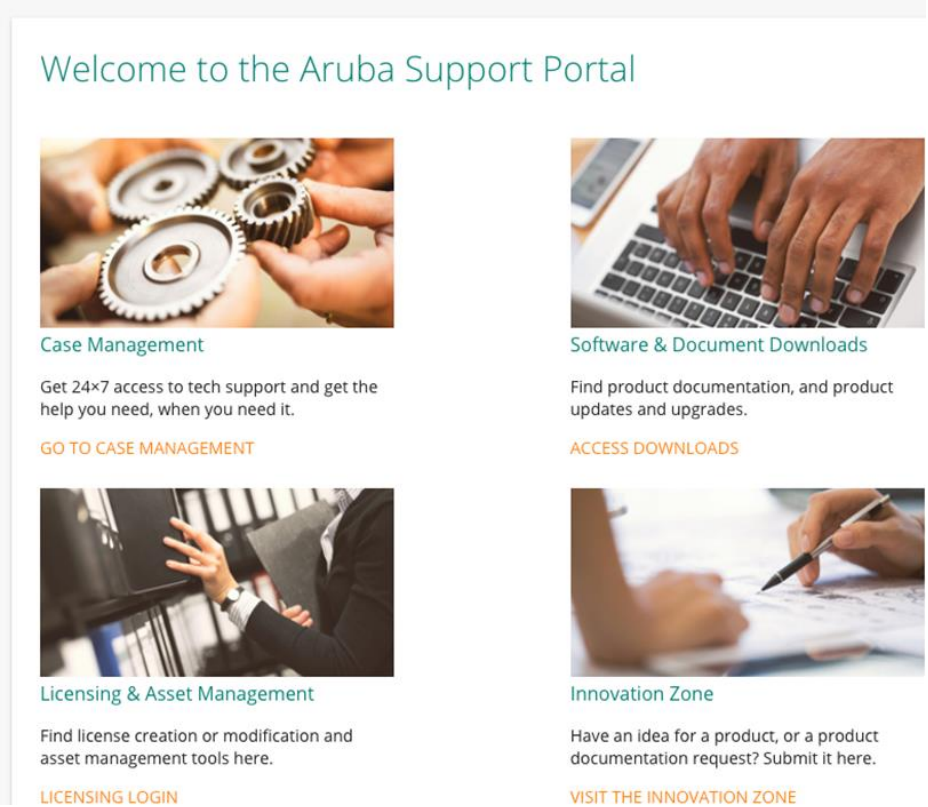
Figure 106 *Transferring Licenses to a New Platform in MNP*



Aruba Support Portal

The Aruba Support Portal (ASP) is Aruba's new support mechanism effective for ArubaOS 8.4.0.0 or later versions. ASP is designed to activate new licenses from purchases, activate demonstration, evaluate licenses, manage licenses (migrate, change ownership, etc.), and access support documentation. ASP is a streamlined and simplified support portal that is easy to use, more advanced in additional capabilities, and will be Aruba's main licensing support portal for all Aruba products.

Figure 107 *Aruba Support Portal*

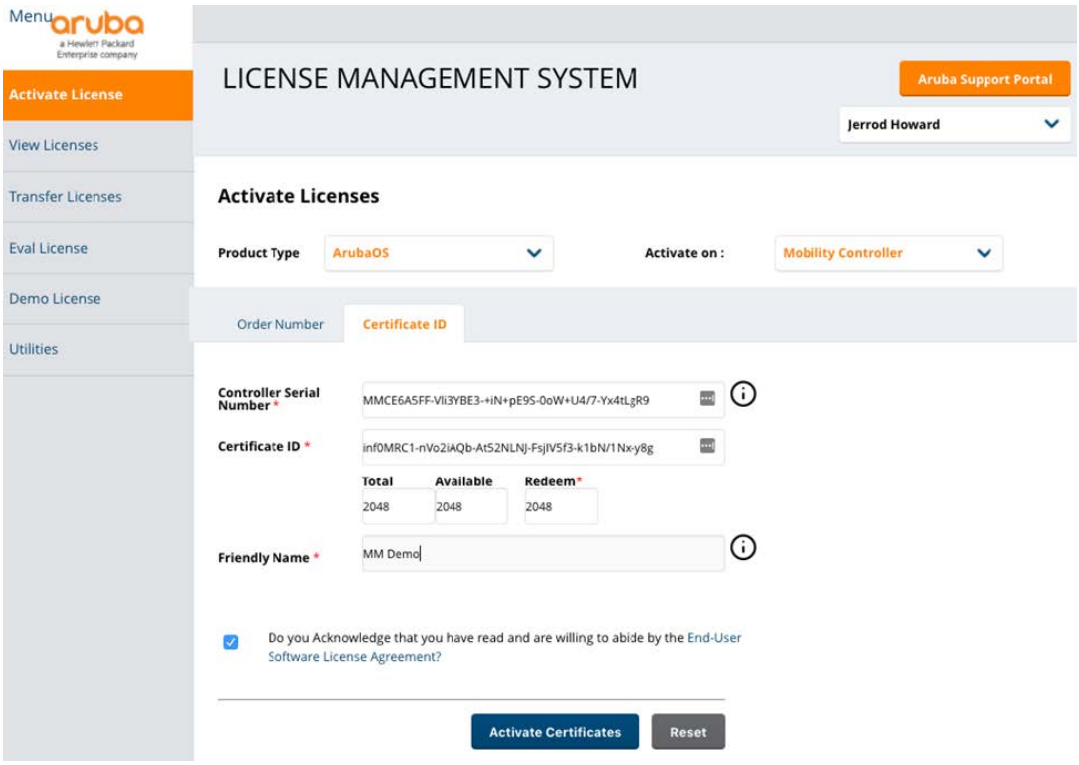


License Activation

ASP works similarly to MNP and new orders have an order number or certificate ID associated with them for license activation.

1. From the **Licensing Login** page, the order number or certificate ID can be entered in to the proper field.
2. Next the controller serial number or passphrase will be entered along with the number of licenses requiring activation.
3. Once all of the requisite information has been entered into the portal, click the **Activate Certificate** button to generate the new license key. ASP can be accessed through the following URL: https://asp.arubanetworks.com

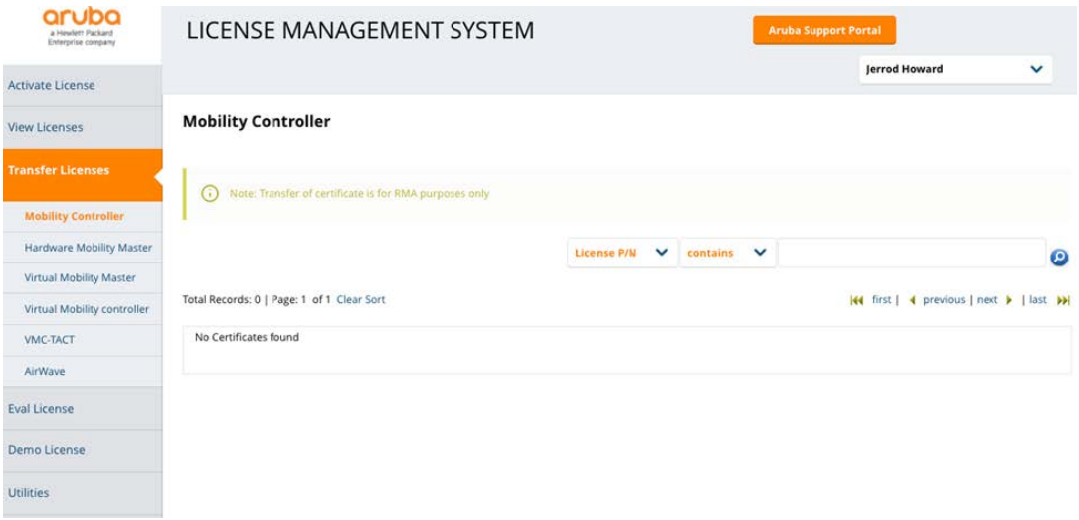
Figure 108 *License Activation in ASP*



License Migration

ASP can also be used to migrate licenses between devices. The portal contains a section dedicated to license migration called **Transfer Licenses** which will reveal the different types of devices which currently hold licenses such as MCs, Hardware MMs, Virtual MMs. After navigating to this section, a page will be displayed for entering the serial of the device where the licenses that will be migrated currently reside. After the serial number has been entered, another window will appear with a prompt asking for the destination for the newly migrated licenses. Once all requisite information has been entered into the tool, ASP will update its database accordingly to display the new ArubaOS 8 license keys associated with the serial number or passphrase of the new device.

Figure 109 *Transferring License in ASP*



License Installation

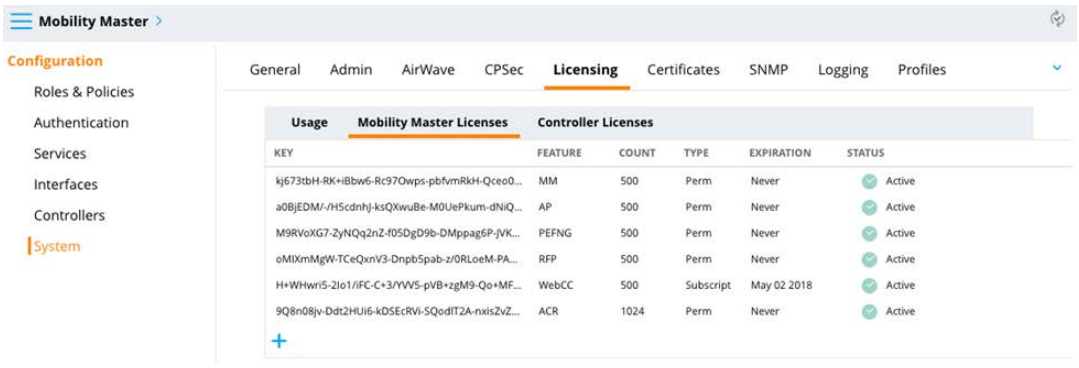
License Components

In order to install licenses on a controller or Mobility Master, the license key generated from the MNP or ASP activation is required. The key generates an alpha-numeric string which enables a specific license type, feature, or subscription. Licenses can be installed on an MM (MM), MM Controller (MCM), or Stand-alone MC (MC) through the WebUI or the CLI.

License Installation via WebUI

The Mobility Master serves as the master licensing server for all controllers and services. Licenses for the devices under a particular Mobility Master are installed at the Mobility Master level. To install licenses on the Mobility Master, access the WebUI and navigate to **Mobility Master > System > Licensing** tab, click **Mobility Master Licenses**, and then click the + sign to add a new license.

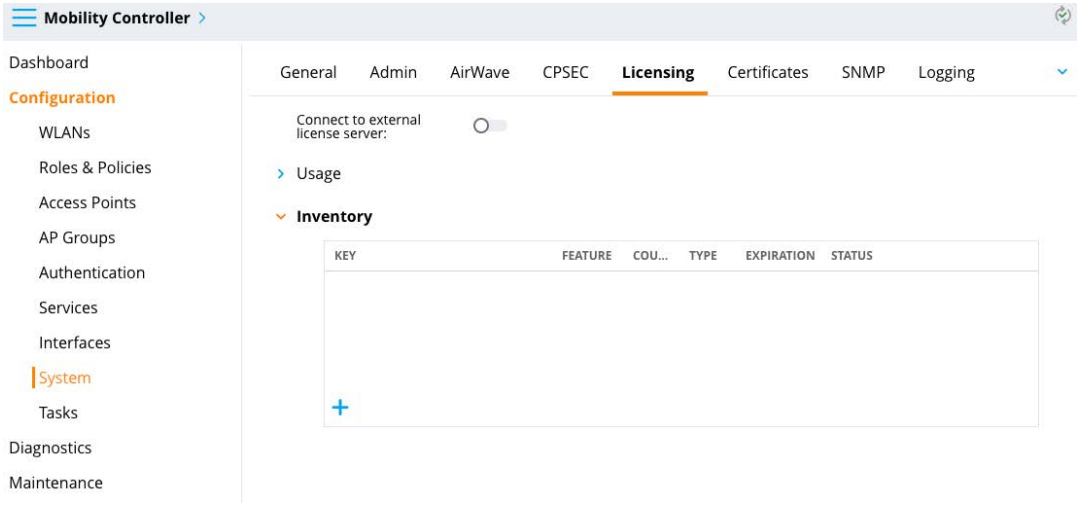
Figure 110 *MM License Installation Using the WebUI*



All installed licenses and their quantities can be viewed using this page. If necessary, licenses can also be deleted using this page. The Mobility Master licensing services are capable of managing all licenses including dynamic provisioning of MC-VA licensing. This functionality is unique to the Mobility Master and allows for a single installed MC-VA license pool to be split up between multiple VMCs under that Mobility Master. For example, a single MC-VA-250 license pool could be spread out over 2 MCs or 20 VMCs under the same Mobility Master so the total number of APs terminated across all controllers does not exceed 250 APs. License allocation under the Mobility Master is completely flexible and can be easily adapted according the needs of a given deployment,

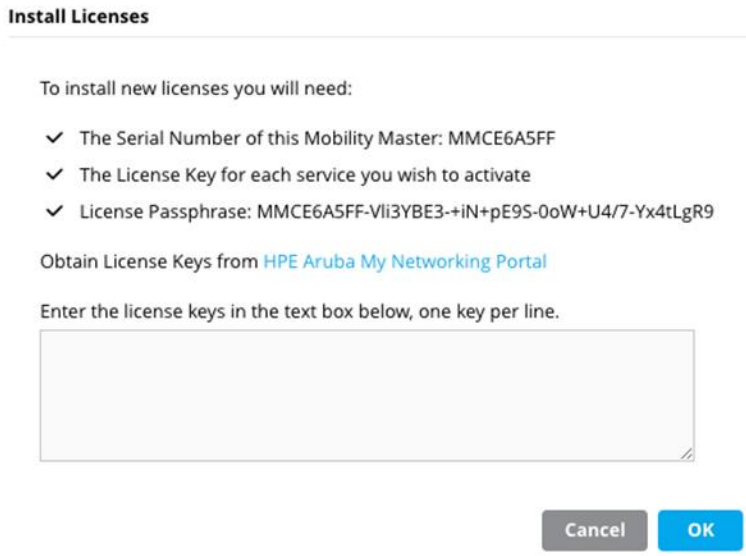
The license installation location and process in the WebUI is the same for MCM and Stand-alone controllers as it is for MCs and VMCs. The main difference is that instead of selecting the Mobility Master section, the **MC > Configuration > System > Licensing** should be selected. Next, choose the **Inventory** drop down screen and click on the **+** sign to add a new license.

Figure 111 *MCM and Stand-alone License Installation Using the WebUI*



In both the cases, a prompt will appear with the serial number, license passphrase (in the case of a virtual appliance or VMC), and a window to paste one or more licenses to apply to the desired controller.

Figure 112 *License Installation Dialog Window*



Once the license keys have been added, select the **OK** button to complete the installation process. In most cases, if the controllers are having licenses installed on them for the first time they will need to be rebooted in order for the licenses to take effect. A reboot is not required for future license additions where additional quantities of existing licenses will be installed. The page indicates whether or not the controllers require a reboot. A license flagged with an "R" designation signifies that a reboot is required.

License Installation via CLI

Install licenses using the CLI by logging in to the MM, MCM, or Stand-alone controller via SSH and execute the following command:

```
#License add <insert-license-key-here>
```

License inventory can be displayed using the following command:

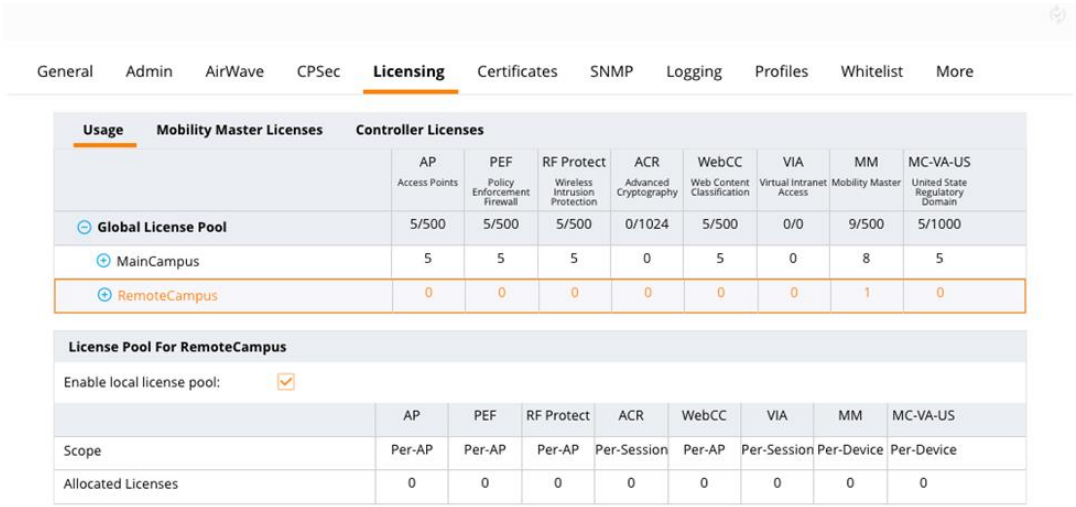
```
#show licensing
```

Mobility Master License Pools

Another feature that is unique to the MM is the ability to create license pools. License pools allow the MM to manage smaller pools of the larger global license pool and also applies licenses to controllers or groups of controllers. Allocating licenses allows for more granular control over how many licenses each controller or group of controllers are allowed to consume. Use cases for this feature include situations where the global network administrator wants to limit how many APs a location can deploy so that their license supply is not exhausted in order to avoid creating issues at other sites.

License Pools are not available in the MCM and Stand-alone Controller Modes.

Figure 113 *Creating License Pools*



License pools are defined by the nodes of the MM. In the example below, there is a Main Campus and a Remote Campus group of controllers. The global license pool consists of 500 licenses for AP, PEF, RF Protect, etc. The network administrators for this example scenario want to create a limit of 50 APs at the Remote Campus.

To set up the desire limit, they would click on the desired node and check the **Enable Local License Pool** box. Next, they would click on each license type to assign the number of licenses that are allowed for the Remote Campus node. This process will need to be repeated for each license type required for the node. In this case there are 50 APs that require licenses and 50 licenses of each type will be deducted from the global license pool. In the example, the RemoteCampus node cannot use more than 50 APs of licensing from the MM global pool. The remaining 450 licenses are available in the global license pool for allocation to other nodes.

Figure 114 *Allocating Licenses to Pools*

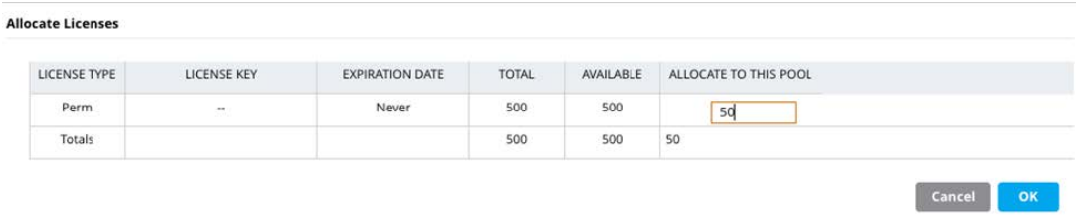
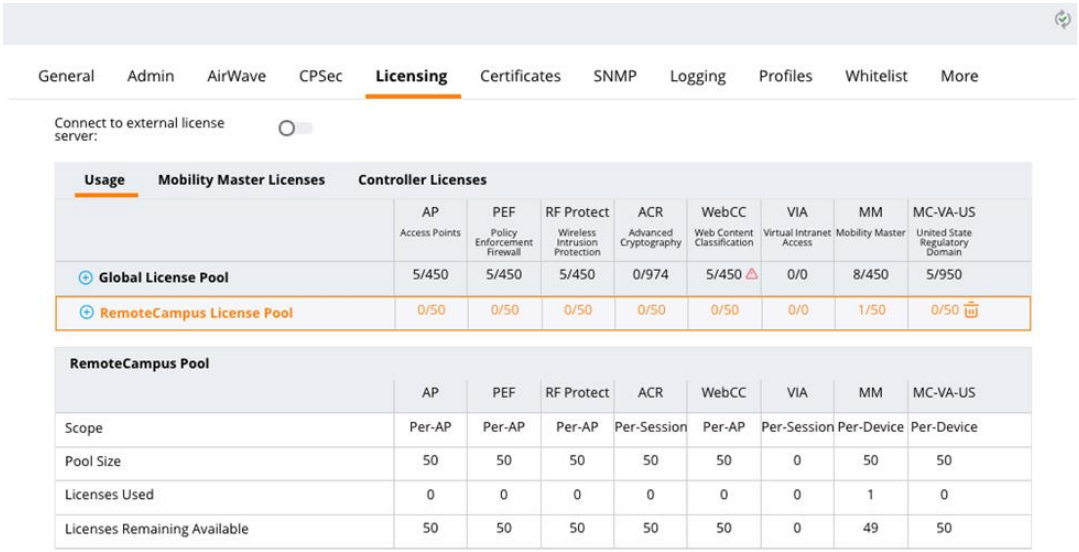


Figure 115 *License Pool Dashboard*

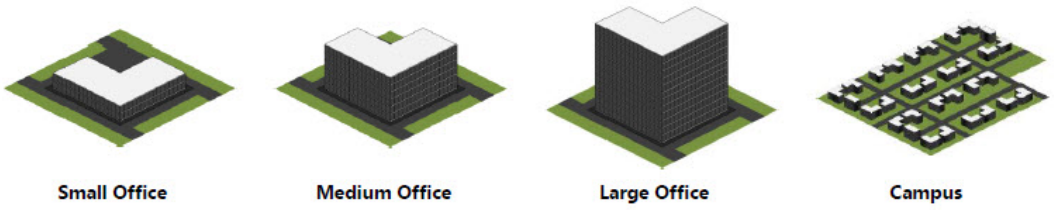


This chapter addresses the design considerations and best practices for implementing an end-to-end Aruba mobile first architecture for a typical enterprise network. This chapter focuses on architecture design recommendations and explains the various configurations and considerations that are needed to build each architecture. Reference architectures are provided for small, medium, and large buildings as well as large campuses. For each architectural model the following topics are discussed:

- Recommended modular local area network (LAN) designs
- MC cluster placement
- Design considerations and best practices
- Suggested switch and wireless platforms

The information provided in this chapter is useful for network architects responsible for greenfield designs, network administrators responsible for optimizing existing networks, and network planners requiring a template that can be followed as their network grows. The scope of this chapter applies to environments from small offices with fewer than 32 APs up to large campuses supporting up to 10,000 APs.

Figure 116 *Scope of Designs*



This chapter does not provide step-by-step configuration examples or vertical specific wireless designs. Detailed configuration examples are provided by Aruba Solutions Exchange (ASE) while vertical specific designs are provided in separate VRD documents.

Design Principles

The foundation of each reference architecture provided in this chapter is the underlying modular LAN design model that separates the network into smaller manageable modular components. A typical LAN consists of a set of common interconnected layers such as the core, distribution, and access layers which form the main network along with additional modules that provide specific functions such as Internet, WAN, Wireless, and server aggregation.

This modular approach simplifies the overall design and management of the LAN while providing the following benefits:

- Modules can be easily replicated which allows for growth and scalability.
- Modules can be added and removed with minimum impact to other layers as network requirements evolve.

- Modules allow the impact of operational changes to be constrained to a smaller subset of the network.
- Modules compartmentalize the network into specific fault domains providing fault tolerance.

The modular design philosophies outlined in this chapter are consistent with industry best practices and can be applied to any size network.

Modular Designs

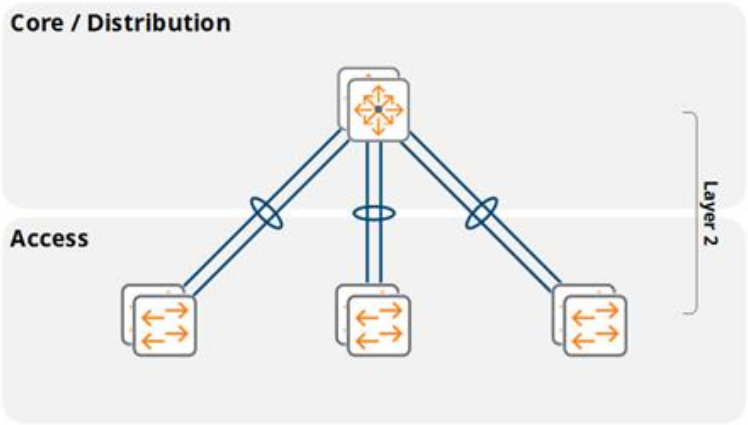
The modular design selected for a specific LAN deployment is dependent on numerous factors. As an industry best practice, networks are built using either a 2-tier or 3-tier modular LAN design which differ from each other by the inclusion or exclusion of a distribution layer. The additional distribution layer resides between the core and access layers to provide aggregation and routing:

2-tier Modular LAN – Collapses the core and distribution layers into a single layer. The switches in the core / distribution layer perform a dual role by providing aggregation to the access layer modules and also performs the IP routing functions

3-tier Modular LAN – Utilizes a dedicated distribution layer between the core and access layers. The distribution layer switches provide aggregation to the access layers and are connected directly to the core. Distribution layer switches are commonly deployed in larger networks and are typically used to connect different modules such as wireless, WAN, internet, and servers.

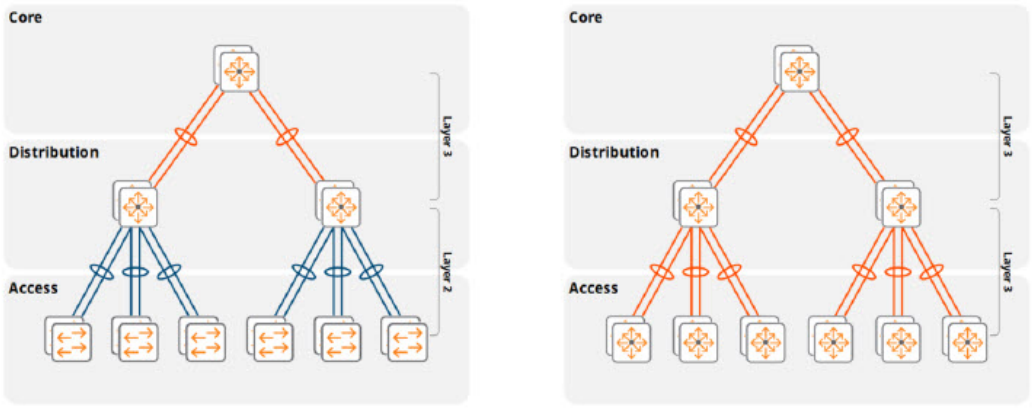
The terms "aggregation layer" and "distribution layer" are interchangeable throughout this chapter.

Figure 117 *2-Tier Modular LAN*



A 2-tier modular LAN is well suited for small buildings with a few wiring closets and access switches. The access layer VLANs are extended between the access layer switches and the core / distribution layer switches using 802.1Q trunking. The core / distribution switches include IP interfaces for each VLAN and operate as the default gateway for the access layer hosts.

Figure 118 *Layer 2 and Routed Access 3-tier LAN Designs*



In a 3-tier modular design, the IP routing functions are distributed between the core and aggregation layers. Depending on the design they may be extended to the access layers as well. All 3-tier LAN designs will implement IP routing between the aggregation and core switches using a dynamic routing protocol such as Open Shortest Path First (OSPF) for reachability and address summarization:

Layer 2 access layer – All VLANs from the access layer are extended to the aggregation layer switches using 802.1Q trunking. The aggregation switches provide layer 3 interfaces (VLAN interfaces or SVIs) for each VLAN and provide reachability to the rest of the IP network

Routed access layer – IP routing is performed between the aggregation and access layer switches (as well as between the aggregation and core layers). In this deployment model, each access layer switch or stack provides reachability to the rest of the IP network

The Aruba Mobile First Architecture supports both the designs allowing the customers to leverage the benefits of Aruba solutions with either network design.

LAN Aggregation Layer

When designing and planning a mobile first network the decision of whether or not to deploy an aggregation layer hinges on several key factors:

- The number of access layer switches that need to be connected. Eventually the number of SFP/ SFP+/QSFP ports required to connect the access layer will exceed the physical port capacity of the core switches. Adding an additional layer between the core and access layers provides aggregation reducing the number physical ports required in the core.
- The structured wiring design of the building. Intermediate distribution frames (IDFs) in larger buildings typically connect to main distribution frames (MDFs) via fiber at strategic locations within the building. Each MDF typically connects to a server room or data center.
  - Aggregation switches are often required in MDFs due to a limited fiber capacity between the MDFs and main server room or data center.
  - When multi-mode fiber is deployed, aggregation switches allow the IDFs to be connected when the combined fiber lengths (IDF + MDF + server room) exceed the distance specifications for fiber optic connections.
- MDFs provide ideal locations for aggregation layer switches as they typically aggregate the fiber connections from the access layer and provide connectivity to the core deployed in the main server room or data center
- Network manageability, stability, and scalability concerns dictate that specific fault domains should be introduced into the network. This is typically achieved by implementing IP routing between the core and

respective aggregation layers. Designing a network in this manner ensures that the core is isolated from layer 2 faults or operational changes originating from other layers or modules.

- Reducing layer 2 and layer 3 processing load on the core. As a network grows the MAC address table sizes and IP protocol processing overhead increases proportionately. The inclusion of an aggregation layer offloads the layer 2 learning and IP protocol processing overhead from the core to the respective aggregation layer switches. The aggregation layer then becomes the layer 2 and layer 3 demarcation points for the clients allowing the core to be dedicated to IP routing functions.

Wireless Module Aggregation Layer

A dedicated aggregation layer will typically be introduced for the wireless module once the number of wireless and dynamically segmented client host addresses exceeds a specific threshold. Wireless and dynamically segmented client traffic is tunneled from the APs or access layer switches to the Mobility Controller (MC) cluster which causes the MAC learning and IP processing overhead to be incurred by the first hop router for those VLANs. In a 2-tier modular network design, this overhead is incurred by the converged core and aggregation layer devices. In a 3-tier modular network design the overhead is incurred by the core. The addition of a dedicated wireless module aggregation layer alleviates the MAC learning and IP processing overhead from the core and shifts it to a dedicated wireless aggregation layer providing stability, fault isolation, and scalability.

As a best practice, Aruba recommends implementing a dedicated wireless aggregation layer when the total number of host addresses from both wireless and dynamically segmented clients exceeds 4,096. This practice safeguards the network from future growth by ensuring that the core layer is not overwhelmed as new classes of devices are added or if IPv6 is introduced which significantly increases the total number of host IP addresses.

The limit to wireless module scalability depends on the scaling capabilities of the aggregation layer switches deployed for the wireless module. Ethernet switches are designed for specific applications and will therefore be optimized for switching or routing operations. Depending on the switch and its recommended usage it will be able to learn, process, and maintain a specific number of data link addresses and network layer bindings. Switches designed for core routing applications will support a lower number of MAC addresses, IPv4 ARP entries, and IPv6 neighbors than switches designed for the aggregation layer or datacenter.

The latest generation of Ethernet switches from Aruba scales to support up to 64,000 host devices depending on the switch model and IP environment. As a best practice the wireless module should be designed so that the total number of IPv4 and IPv6 host addresses does not exceed the capacity of the wireless aggregation switches. The wireless module should also be designed to accommodate future growth. Aruba recommends designing both the MC cluster and aggregation layer to accommodate no more than 80% of their maximum capacity. This approach permits both planned and unplanned growth without needing to redesign the network in the future.

Large deployments that exceed the scaling limits of single the wireless module will require additional wireless modules to be deployed. Each additional wireless module consists of a dedicated wireless aggregation layer and MC cluster. The total number of wireless modules required will vary depending on the size of the deployment and the IP environment. Large deployments that only have IPv4 clients will typically require fewer wireless service modules than deployments supporting native IPv6 or dual-stack clients. This difference is primarily due to how IPv6 is implemented where each host can acquire multiple IPv6 global addresses which consume additional switch resources.

Determining the required capacity for a wireless aggregation layer depends on a number of factors. The two primary considerations are:

- The total number of MAC addresses, IPv4 ARP entries, and IPv6 neighbor entries the aggregation layer switch can support.
- The architecture of the aggregation layer switch.

A strong understanding of the number of users, devices, and the IP environment is critical to successfully determine if a wireless aggregation layer switch can meet the scaling needs of the wireless module.

Most organizations will know how many users the wireless infrastructure needs to supported and a general idea of how many devices each user will need to connect to the wireless network (typically 2-3 devices per user). These requirements will naturally vary by vertical and environment. For example, in higher education environments it is not uncommon for students to connect three or more devices. Assuming 3 devices per user, an organization with 4,000 users should plan on supporting at least 12,000 client devices (14,400 if following best practices allowing 20% room for growth).

Once the total number of client devices is known, an understanding of the IP environment is required to determine how many MAC addresses and network layer bindings (ARP and/or neighbors) need to be supported by the wireless aggregation layer switches:

Table 23: *Aggregation Layer Address Requirements*

IP Environment	MAC Entries	IPv4 ARP Entries	IPv6 Neighbor Entries
Native IPv4	1	1	0
Native IPv6	1	0	3 – 4 (typical)
Dual-Stack	1	1	

Calculating IPv4 scaling is relatively straightforward as each client device will be assigned a single IPv4 address. The wireless aggregation layer switch allocates one MAC and one IPv4 ARP table entry for each IPv4 client. An environment with 14,400 client devices will therefore require a wireless aggregation layer switch that can support 14,400 MAC addresses and 14,400 IPv4 ARP entries.

For native IPv4 deployments, the maximum scaling capacity of a wireless aggregation layer switch is determined by evaluating the total number of MAC addresses and IPv4 ARP entries that can be simultaneously supported. This information is generally provided in product datasheets or documentation. The lowest value of the two will determine the maximum number of IPv4 hosts that can ultimately be supported for each wireless module. For example, the Aruba 8320 series switches can support up to 49,000 MAC addresses (when routing) and 120,000 IPv4 ARP entries. The MAC address table size is the smaller of the two values meaning that the effective limit of the 8320 series switch is 49,000 x IPv4 hosts. Therefore, a wireless module using an 8320 series aggregation layer will be limited to 49,000 IPv4 client devices.

Calculating IPv6 address requirements is a little complex. The process requires an understanding of how many global IPv6 addresses are being allocated for each client device. This number will vary depending on the IPv6 addressing methods that have been deployed, the applications and operating systems. For most IPv6 environments a client device will typically be assigned one Link-Local Address (mandatory) and at least three global addresses.

Calculating scaling requirements for native IPv6 or dual-stack deployments is a more involved process as factors such as the layer 3 switch architecture and number of global IPv6 addresses assigned per host need to be considered. The MAC address table size is not normally a consideration as the total number of IPv6 neighbor entries will typically be reached well before the MAC address limit. Depending on the switch model and vendor, the link-local addresses may also need to be factored into the calculations.

Aruba switches implement different architectures depending on the series and model:

3810/5400R Series – Implements a shared ARP/neighbor table. Scaling calculations must take both link-local and global addresses into account.

8320 Series – Implements a shared ARP/neighbor table where each IPv6 global address consumes two table entries. Scaling calculations do not require inclusion of link-local addresses.

8400 Series – Implements independent ARP/neighbor tables. Scaling calculations do not require inclusion of link-local addresses.

Calculating IPv6 scaling requires an idea of how many global IPv6 addresses each client will be assigned. If the number of global addresses is unknown, then a good starting point is counting on three global addresses per client. Going back to the previous example, an organization with 14,400 client devices will utilize approximately 43,200 IPv6 global addresses. The switch datasheet or documentation can be referenced to determine if the switch is capable of meeting the IPv6 neighbor scaling requirements. The table below provides maximum scaling numbers for both ArubaOS and ArubaOS-CX switches for native IPv4, native IPv6, and dual-stack deployments. These scaling numbers can be referenced to provide the maximum number of client devices (wireless and dynamic segmentation) that can be supported in the wireless module when using an Aruba switch as the wireless module aggregation layer:

Table 24: *Aruba Switch Scalability*

Switch Series	Maximum IPv4 Only Clients	Maximum Native IPv6 Clients*	Maximum Dual Stack Clients*
Aruba 3810 Series (Version 16.04)	25,000	6,250	5,000
Aruba 5400R Series (Version 16.04)	25,000	6,250	5,000
Aruba 8320 Series (Version 10.02)	49,000	20,000	17,000
Aruba 8400 Series (Version 10.02)	82,000	55,000	55,000

*Assumption is each host is assigned 3 x IPv6 global addresses

Please note that the native IPv6 and dual-stack scaling numbers in the table above have been calculated assuming three global IPv6 addresses being assigned per host. If a deployment requires supporting additional global addresses then the table will not apply. As a reminder, Aruba best practices dictate subtracting 20% to accommodate future device growth.

Strategies and architectures for scaling beyond 64,000 host addresses are discussed in the Campus Reference Architecture section. An Aruba mobile first architecture can scale to support up to 100,000 clients per MM by implementing multiple MC clusters each with their own aggregation layer.

Wireless Module Redundancy

One important aspect of an Aruba mobile first redundant design is the connectivity of the wireless module that contains the MCs. The cluster of controllers terminates the AP management and control tunnels, wireless and dynamically segmented client tunnels. To enable redundancy, each cluster consists of a minimum of two

MCs and can potentially scale up to four or twelve cluster members (depending on the controller model). As a best practice, each cluster must contain members of the same model.

Each of the MCs in the cluster connects to a pair of Aruba switches using dynamic port-channels forming a link aggregated connection (LAG). Link Aggregation Control Protocol (LACP) is enabled to verify peer availability and provide layer 2 loop prevention. The MCs are connected to core or wireless aggregation layer switches depending on whether a 2-tier or 3-tier hierarchical network design has been selected for the deployment in addition to the number of wireless and dynamically segmented hosts.

Redundancy within the wireless module is provided at multiple layers:

ArubaOS 8 Clustering – Each AP and client establishes a tunnel to a primary and secondary MC within the cluster. This ensures that a network path is available to APs and clients in the event of a live upgrade or MC outage.

Device and Link Redundancy – Each MC is connected to two Aruba switches that support network virtualization functionality (NVF) if they are core switches or LAG if they are wireless aggregation switches. This ensures that a network path is always available to the MCs, APs, and clients in the event of a switch outage or link failure.

Path Redundancy – Link Aggregation Control Protocol (LACP) is part of the IEEE 802.3ad standard and ensures that all paths are fully redundant. LACP is an active protocol that allows switch peers to detect the operational status of peers devices and their connected ports.

First Hop Router Redundancy – The network must ensure that packets will continue to be forwarded in the event of a default gateway failure. First hop router redundancy is natively provided by Aruba Switches supporting NVF without the need for implementing first-hop routing redundancy protocols such as VRRP.

MC ports in the LAG are distributed between pairs of Aruba switches implementing NVF for all mobile first reference architectures. The model chosen for the switches that the MCs connect to will be depend on the 2-tier or 3-tier hierarchical network design selected for the deployment and the number of wireless clients that are supported. Switches supporting the wireless module can be stack of Aruba 3810Ms, a pair of Aruba 5400Rs configured for virtual switching framework (VSF), or a pair of Aruba 8320s/8400s configured for MC-LAG.

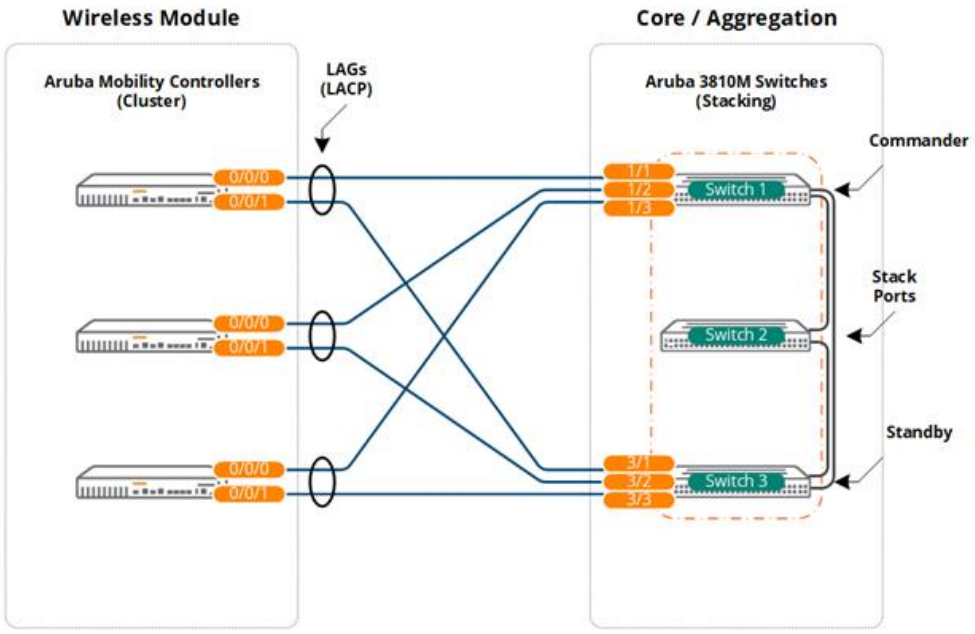
Aruba 3810M Switches

The figure below demonstrates how a cluster of MCs is connected to a stack of Aruba 3810M switches deployed in the core, core/aggregation, or wireless aggregation layer. The Aruba stacking architecture virtualizes both the control and data planes allowing the 3810M stack of switches to forward traffic as well as be configured and managed as a single virtual switch.

In this example, two or more 1 Gigabit or 10 Gigabit Ethernet ports from each MC are configured as a LAG and are distributed between the Aruba 3810M switches in the stack. The switch ports are configured as a dynamic port-channel on the Aruba MCs and LACP trunks on the Aruba 3810M switches.

First-hop router redundancy for the cluster management and client VLANs is natively provided by the stack of Aruba 3810M switches that provide the default gateway for each VLAN. One Aruba 3810M switch in the stack operates in a commander role while a second switch operates as a standby. The switch roles can be automatically or manually assigned. The commander switch provides IP forwarding during normal operation and the standby switch provides backup when the commander switch fails.

Figure 119 *Core/Aggregation using Stacking*



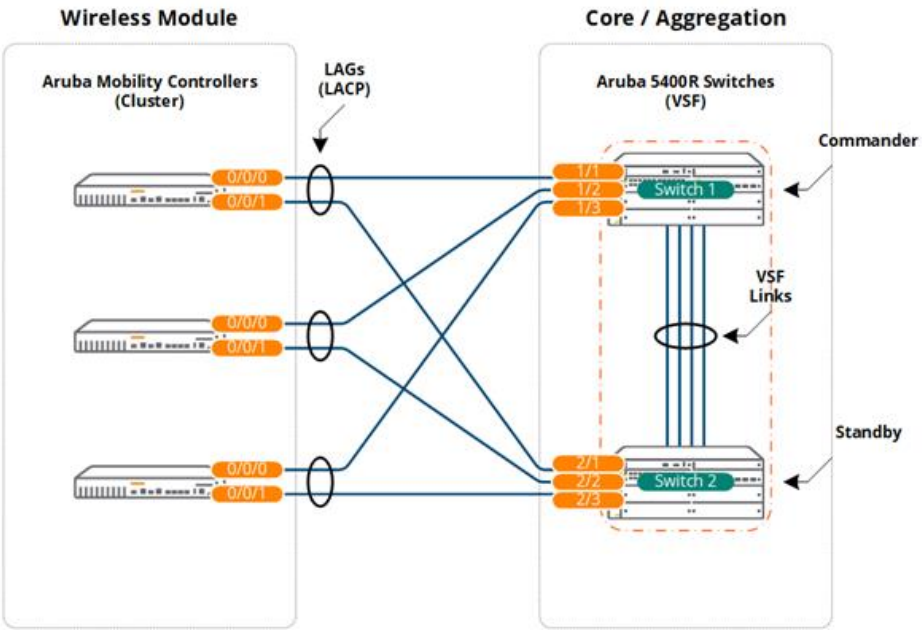
Aruba 5400R Switches

The following figure demonstrates how a cluster of MCs is connected to a pair of Aruba 5400R switches configured for VSF that have been deployed in either the core or wireless aggregation layer. The Aruba VSF architecture virtualizes both the control and data planes allowing all the pair of 5400R switches to forward traffic and be configured and be managed as a single virtual switch.

In this example, two or more 1 Gigabit, 10 Gigabit, or 40 Gigabit Ethernet ports from each MC are configured as a LAG and are distributed between the pair of Aruba 5400R switches. The switch ports are configured as a dynamic port-channel on the Aruba MCs and LACP trunks on the Aruba 5400R switches.

First-hop router redundancy for the cluster management and client VLANs is natively provided by the VSF pair of Aruba 5400R switches that provide the default gateway for each VLAN. One Aruba 5400R switch operates in a commander role while the second switch operates as a standby. The switch roles can be automatically or manually assigned. The commander switch provides IP forwarding during normal operation while the standby switch provides backup when the commander switch fails.

Figure 120 *Core/Aggregation using Virtual Switching Framework*



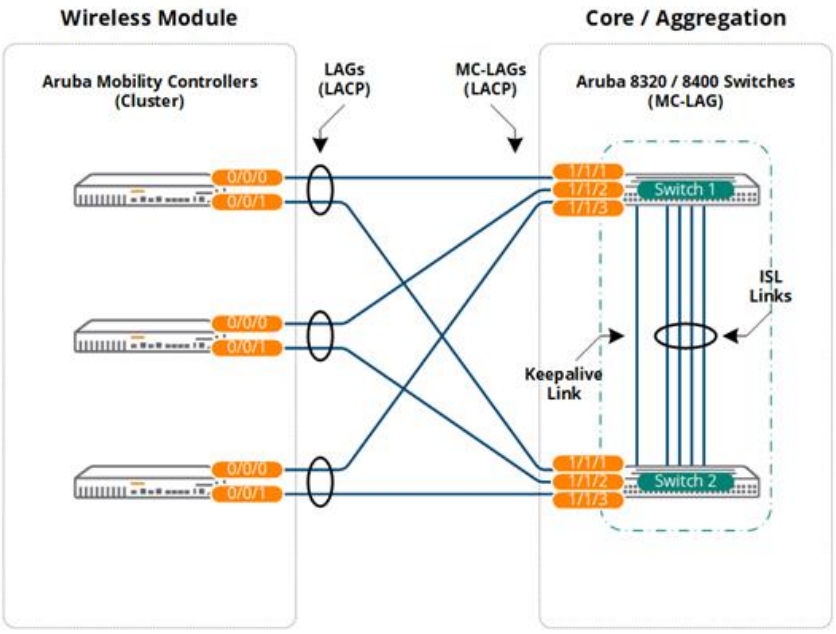
Aruba 8320/8400 Switches

The figure below demonstrates how a cluster of MCs is connected to a pair of Aruba 8320 or 8400 switches that have been configured for Multi-Channel LAG and are deployed in the core or wireless aggregation layer. The Aruba MC-LAG architecture virtualizes data planes allowing all the pair of 8320/8400 switches to forward traffic as a single virtual switch. Unlike the Aruba stacking or VSF architectures, each 8230/8400 is configured and managed independently.

In this example, two or more 1 Gigabit, 10 Gigabit, or 40 Gigabit Ethernet ports from each MC are configured as a LAG and are distributed between the pair of Aruba 8320/8400 switches. The switch ports are configured as a dynamic port-channel on the Aruba MCs and MC-LAG on the Aruba 8320/8400 switches.

First-hop router redundancy for the cluster management and client VLANs is natively provided by the MC-LAG pair of Aruba 8320/8400 switches which provide the default gateway for each VLAN. The active gateway feature is enabled for each VLAN providing IP forwarding and failover on both switches.

Figure 121 *Core/Aggregation using Multi-Chassis LAG*



Reference Architectures

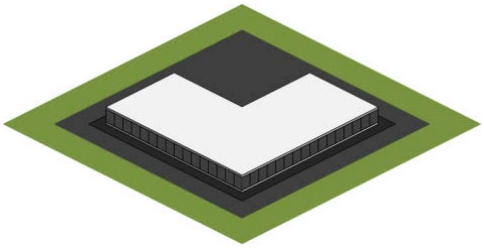
This section includes mobile first reference architectures for small, medium, and large buildings as well as campuses consisting of multiple buildings of varying size. A scenario is provided for each architecture which provides a foundation on the modular network and wireless module design. Each architecture also builds upon the previous design adding additional layers as the access layer and client counts are increased.

Small Office

Scenario

The following reference design is for a small office consisting of a single floor. The building includes one MDF/server room and one IDF that connects to the MDF using multi-mode fiber. The building supports up to 150 employees and requires 15 802.11ac Wave 2 Access Points to provide full 2.4GHz and 5GHz coverage.

Figure 122 *Small Office Characteristics*



Building Characteristics:

- 1 Floor / 20,000 sq. ft. Total Size
- 150 x Employees / 300 x Concurrent IPv4 Clients
- 15 x 802.11ac Wave 2 Access Points

- 1 x Combined Server Room / Wiring Closet (MDF)
- 1 x Wiring Closet (IDF)

The building only has two wiring closets and therefore does not require an aggregation layer between the core and access layer. This building will implement a 2-tier modular network design where the access layer switches and modules connect directly to a collapsed core/aggregation layer. This 2-tier modular network design can also accommodate small buildings with a larger square footage and additional floors if required.

The following is a summary of the modular network architecture and design:

LAN Core/Aggregation:

- Cluster or stack of switches with mixed ports:
  - SFP/SFP+ (Access Layer Interconnects)
  - 10/100/1000BASE-T Ports (Module Connectivity)
- IP routing
- Layer 2 Link Aggregation to Access layer devices and Module Connectivity

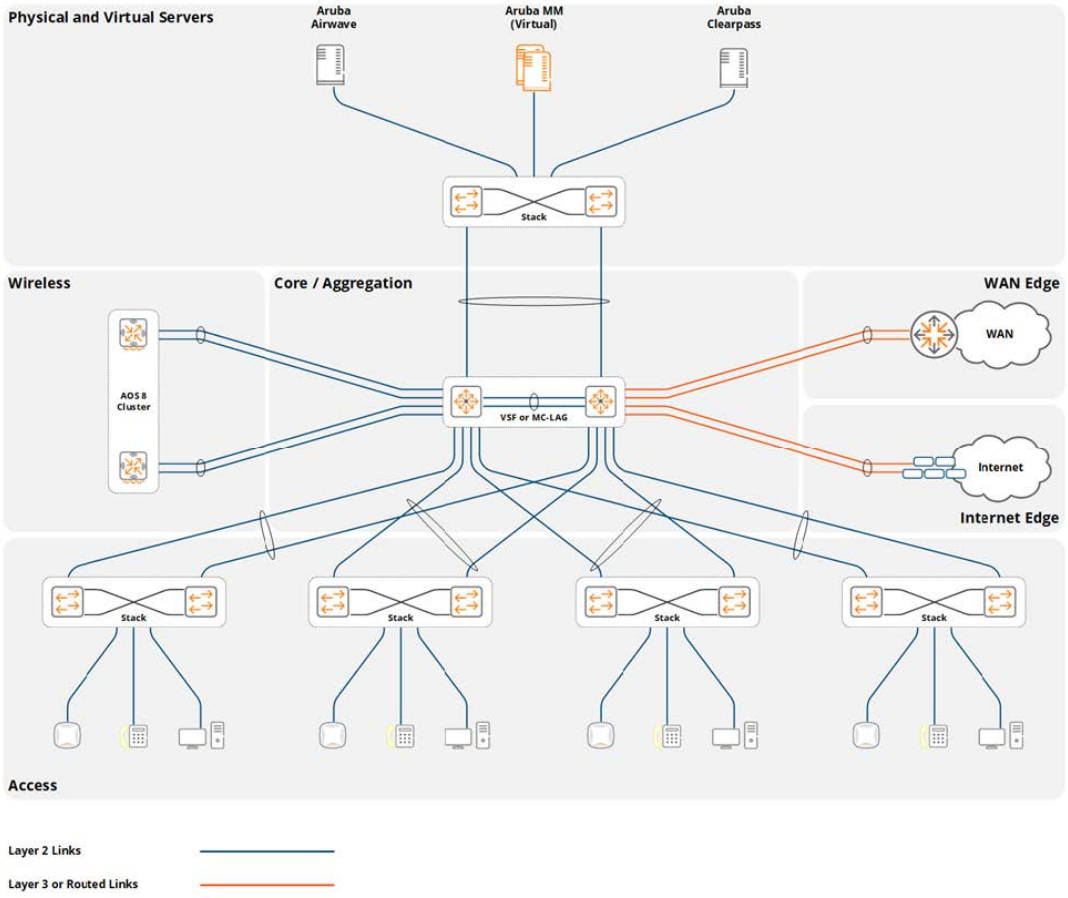
LAN Access:

- A stack of two or more switches per wiring closet
  - SFP/SFP+ (core/aggregation layer interconnects)
  - 10/100/1000BASE-T with PoE+ (Edge Ports)
- Layer 2 link aggregation to core/aggregation layer devices
- 802.11ac Wave 2 APs

The number of APs required for this hypothetical scenario was calculated based on the buildings square footage along with the wireless density and capacity requirements. It was determined that 15 APs would be appropriate assuming that each AP provides 1,200 square feet of coverage. Each AP in this scenario is supporting 20 clients.

The actual number of APs and their placement for a production environment should be determined using a site survey that accounts for the density requirements for each individual coverage area.

Figure 123 *Small Office 2-Tier Modular Network Design*



Considerations and Best Practices

Wireless LAN Components

Aruba offers both controller-less and controller-based deployment options for small deployments. A controller-less architecture is provided using Aruba Instant Access Points (IAPs) while a controller-based architecture is provided using MCs and Campus APs. Both deployment options are valid for this reference design, however this guide focuses specifically on a controller-based architecture.

The small building in this scenario includes various wireless components which are either deployed in the wireless module or server room. A MM and a single cluster of MCs are required to accommodate the AP and client counts. The exact number of cluster members is determined by the hardware or Virtual MC model that has been selected. For redundancy purposes, the MC cluster consists of a minimum of two MCs. Each cluster member needs to provide adequate capacity and performance to operate the wireless network in the event of a single MC failure.

Table below provides a summary of these components:

Table 25: *Small Building Wireless LAN Components*

Component	Description	Notes
Aruba MM (MM)	Virtual Appliance	1 Required, 2 Recommended
Aruba MCs	Hardware or Virtual Appliances	2 Minimum (Clustered)
Aruba Access Points	802.11ac Wave 2 Access Points	15 Required
Aruba ClearPass	Virtual Appliance	Recommended

While the number of 802.11ac Wave 2 APs required for this design is relatively small, Aruba recommends implementing a MM to take advantage of specific features that are required to provide mission-critical wireless services when wireless is the primary access medium. The addition of a MM to the design provides centralized configuration and monitoring, supports features including clustering, AirMatch, and Live Upgrades, and provides centralized application support (UCC and AppRF).

While a controller-based solution can be deployed without a MM, it is not a recommended best practice. If it is not feasible to deploy a MM the MCs can optionally be deployed as a pair of standalone devices and be configured for master redundancy. However, a deployment model implemented in such a fashion will not support clustering and therefore will lack specific features such as fast failover, live upgrades, AirMatch, and centralized application support.

Redundancy

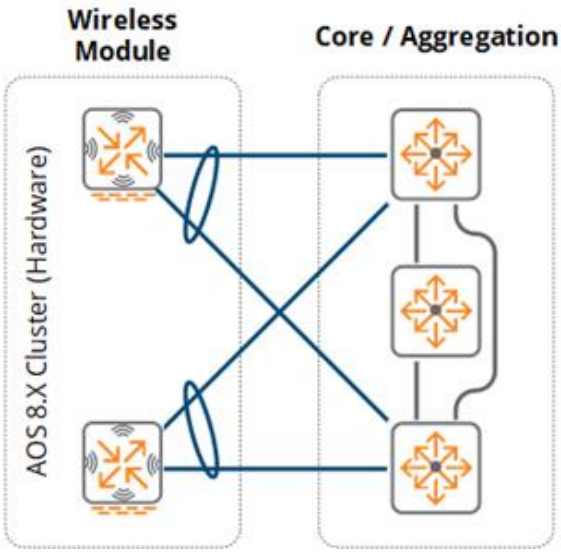
Redundancy for a small building reference architecture is provided across all layers. The redundancy built into the 2-tier modular network design that establishes the foundation network is what determines the level of redundancy that is provided to the modules. Often the cost of an outage is the key driver in implementing to provide network redundancy. Most small networks use dual power supplies and often use a stack of switches as their primary redundancy mechanism.

For this scenario the MM and MC cluster members are deployed within a server room and are directly connected to the core/aggregation switches. To provide full redundancy, two virtual MMs and one cluster of hardware or virtual MCs is required:

- Aruba MM (MM):
  - Two virtual MMs
  - L2 master redundancy (Active / Standby)
- Hardware MCs (MCs):
  - Single cluster of hardware MCs
  - Minimum of two cluster members
- Virtual MCs (MCs):
  - Single cluster of virtual MCs
  - Minimum of two cluster members
  - Separate virtual server hosts
- Access Points
  - AP Master pointing to the cluster's VRRP VIP
  - Fast failover using cluster's redundancy functionality

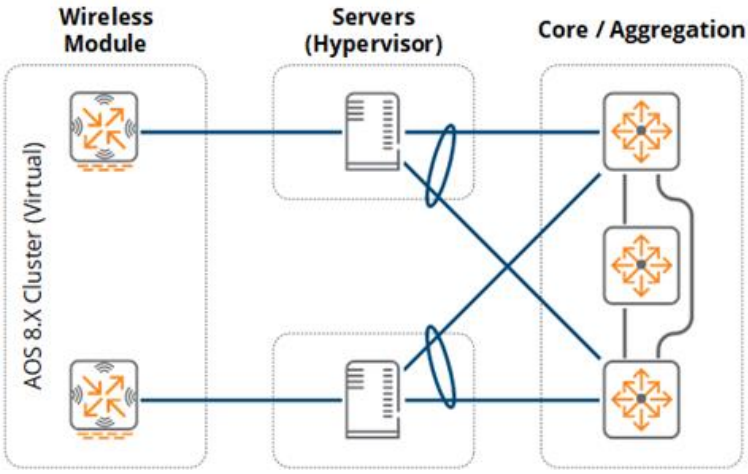
The figures below provide detailed examples of how the virtual and hardware cluster members are connected to the core / aggregation layer. Hardware MCs are directly connected to the core / aggregation layer switches via two or more 1 Gigabit Ethernet ports configured in a LAG group. The LAG port members are distributed between core/aggregation layer stack members.

Figure 124 *Hardware MC Cluster – Core/Aggregation Layer*



VMCs are logically connected to a virtual switch within the virtual server host. The virtual host server is directly connected to the core/aggregation switches via two or more 1 Gigabit or 10 Gigabit Ethernet ports implementing 802.3ad link aggregation or a proprietary load-balancing/failover mechanism. Each port is distributed between core/aggregation layer switch stack members.

Figure 125 *Virtual MC Cluster – Core/Aggregation Layer*



The MMs are deployed in a similar manner to the VMC clusters. Each virtual server host supports one VMM operating in active/standby mode. While a single MM can be implemented for a small building there are no additional licenses required to implement a standby. The only network overhead for such a model would be the additional CPU, memory, and storage utilization on the virtual server host.

NOTE

Redundancy for virtual servers is hypervisor-dependent. To safeguard the network against link, path, and node failures, the hypervisor may implement 802.3ad link aggregation or a proprietary load-balancing/failover mechanism.

Virtual MCs

Virtual MCs can optionally be deployed for a small building environments. If VMCs are deployed then the virtual server infrastructure must be scaled accordingly to provide the necessary CPU and memory resources to each VMC in the cluster:

- Each VMC should be deployed across different virtual server hosts. This design requires two virtual server hosts.
- Uplinks between the virtual server host and the core/aggregation layer must be scaled accordingly to support the wireless and dynamically segmented client throughput requirements. The throughput of cluster will be limited by the Ethernet PHYs installed on the virtual server host.

Redundancy between the virtual server host and its peer switches can use standard 802.3ad link aggregation or a proprietary hypervisor specific load-balancing and failover mechanism. Each hypervisor supports specific load-balancing and failover mechanisms such as active / standby, round-robin load-balancing, or link aggregation. The appropriate redundancy mechanism should be selected to support the specific implementation requirements.

Scalability

For this scenario there are no specific LAN scalability considerations that need to be taken into account. The core / aggregation and access layers can easily accommodate the APs and client counts without modification or derivation from the base design. A wireless aggregation layer can be added in the future if necessary to accommodate additional APs and clients that are added to the network.

Wireless module scalability is not a concern as the MMs can be expanded and additional cluster members can be added over time to accommodate additional APs, clients, and switching capacity as the network increases in size.

As a best practice, Aruba recommends implementing the MM-VA-50 MM and a cluster of two hardware or virtual MCs for such a small building design per the platform suggestions. The MM selected for this design can scale to support 50 APs, 500 clients, and 5 MCs.

Virtual LANS

For this design the core / aggregation layer provides layer 2 transport (VLAN extension via 802.1q trunking) and terminates all the VLANs from the access layer and wireless module with layer three interfaces. Aruba recommends using tagged VLANs throughout the network.

The wireless module consists of one or more client VLANs depending on the security and policy model. For a single VLAN design, all wireless and dynamically segmented clients are assigned a common VLAN with roles and policies determining the appropriate level of network access for each client. The single VLAN is extended from the core / aggregation layer switches to each physical or virtual MC cluster member. Additional VLANs can be added and extended as required. For example, the mobile first design may require separate VLANs to be assigned to wireless and dynamically segmented clients for policy compliance purposes.

A minimum of two VLANs are required between the core / aggregation layer and each MC cluster member. One VLAN is dedicated for management and MM communications while the second VLAN is used for client traffic. All VLANs are common between cluster members to permit seamless mobility. The core / aggregation layer switches are configured with layer three interfaces and addressing to operate as the default gateway for each VLAN. First-hop router redundancy is natively provided by the Aruba stacking architecture.

Figure 126 *Hardware MC Cluster – VLANs*

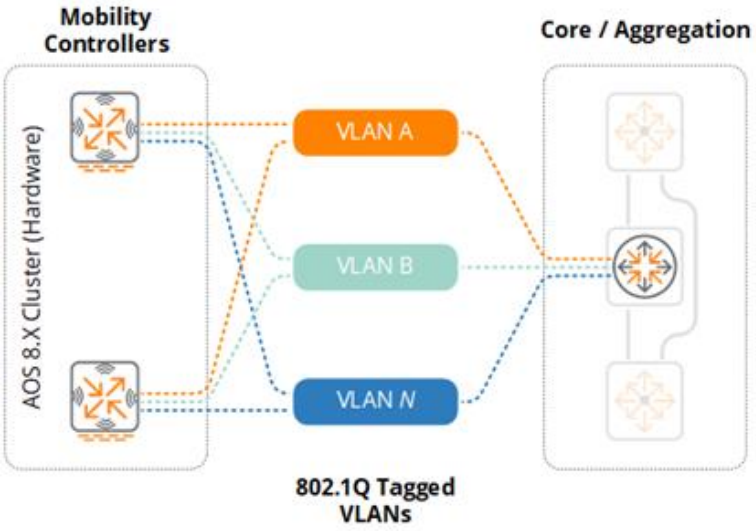
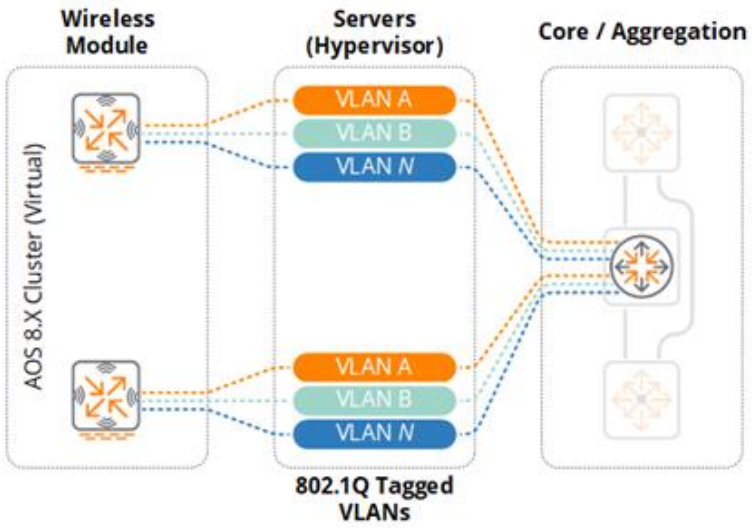


Figure 127 *Virtual MC Cluster – VLANs*



As a best practice Aruba recommends implementing unique VLAN IDs within the wireless module. This allows an aggregation layer to be introduced in the future without disrupting the other layers within the network. It also facilitates the creation of smaller layer 2 domains which is critical to reducing layer 2 instability. Operational changes, loops, or misconfigurations originating from other layers or modules in the network can adversely impact the wireless module unless the network has been properly segmented with appropriately sized layer 2 domains.

Platform Suggestions

The figure below provides platform suggestions for a small building scenario supporting 15 APs and 300 concurrent clients. A "good, better, and best suggestion" is made based on feature, performance, and scaling capabilities. These are suggestions are scenario-specific and may be substituted at your own discretion.

Figure 128 *Small Building Platform Suggestions*

		Good	Better	Best
Switching	Core / Aggregation Layer	2930	3810	3810
	Access Layer	2930	2930	2930
Wireless	MMs	MM-VA-50		
	Virtual MC Cluster	MC-VA-50		
	MC Cluster	7024	7030	
	802.11ac Wave 2 Access Points	300 Series	310 Series	330/340 Series

Features, Performance & Scaling

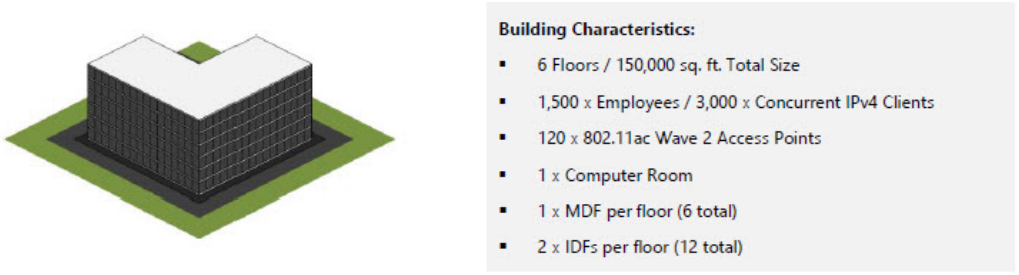
Medium Office

Scenario

The following reference design is for a medium office building with six floors. The building includes a data center which is connected to an MDF on each floor through single-mode fiber. Each floor includes three IDFs

which connect to the MDF through multi-mode fiber. The building supports up to 1,500 employees and requires 120 802.11ac Wave 2 APs to provide full 2.4 and 5GHz coverage.

Figure 129 *Medium Office Characteristics*



As this design implements a structured wiring design using MDFs and IDFs, an aggregation layer is required to connect the access layer. This building will also implement a 3-tier modular network design where the access layer switches connect to aggregation layer switches in each MDF which in turn connect directly to the core. This modular network design also includes an additional aggregation layers for the computer room which facilitates scalability, aggregation, and fault domain isolation.

The list below provides an outline of the modular network architecture and design:

- LAN Core: A cluster of switches with fiber ports:
- SFP/SFP+ (module connectivity)
- IP routing to aggregation layer devices and modules

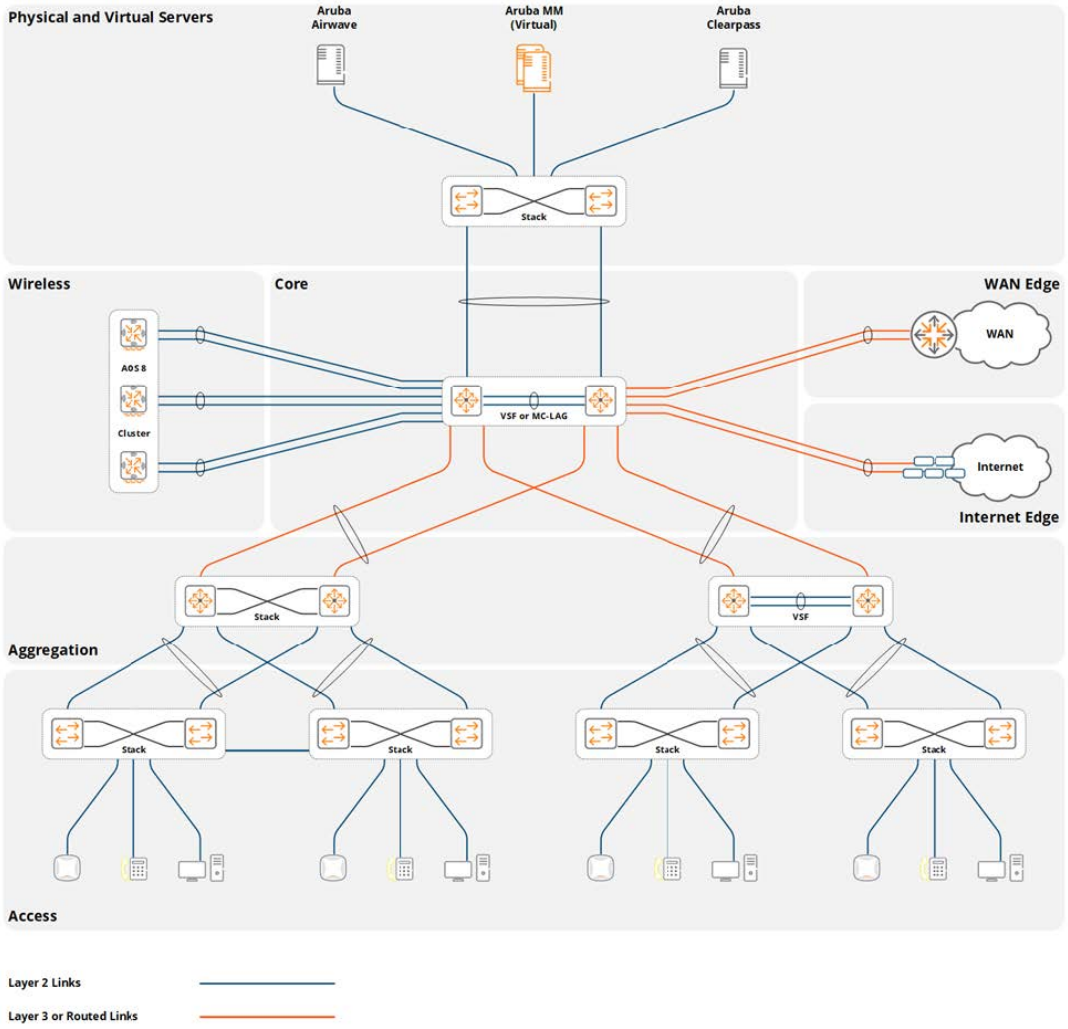
LAN Aggregation:

- A stack of two switches with fiber ports for each MDF:
  - FP/SFP+/QSFP+ (core and access layer interconnects)
- IP routing to core layer devices
- Layer 2 link aggregation to access layer devices

LAN Access:

- A stack of two or more switches for each MDF and IDF:
  - SFP/SFP+ (aggregation layer interconnects)
  - 10/100/1000BASE-T with PoE+ (edge ports)
- Layer 2 link aggregation to aggregation layer devices
- 802.11ac Wave 2 APs

Figure 130 *Medium Office – 3-Tier Modular Network Design*



The number of APs required for this hypothetical scenario was calculated based on the building's square footage, wireless density, and capacity requirements. It was determined that 120 APs would be required based on the assumption that each AP will provide coverage for 1,200 square feet and support 25 clients.

The actual number of APs and their placement for a production environment should be determined using a site survey that accounts for the density requirements for each individual coverage area.

Considerations and Best Practices

Wireless LAN Components

The medium building in this scenario includes various wireless components which are either deployed in the wireless module or the server room. To accommodate the AP and client counts, an MM and a single cluster of MCs is required. The number of cluster members is determined by the MC (either hardware or virtual) model that is selected. The MC cluster consists of a minimum of two MCs for redundancy purposes. Each member provides adequate capacity and performance to allow the wireless network to continue to function in the event of a single MC failure.

Table 25 provides a summary of these components:

Table 26: *Medium Building Wireless LAN Components*

Component	Description	Notes
Aruba MM (MM)	Virtual Appliance	1 MM is required, 2 are recommended
Aruba MCs	Hardware or Virtual Appliances	2 Minimum (Clustered)
Aruba Access Points	802.11ac Wave 2 Access Points	120 APs Required
Aruba ClearPass	Virtual Appliance	Recommended

Redundancy

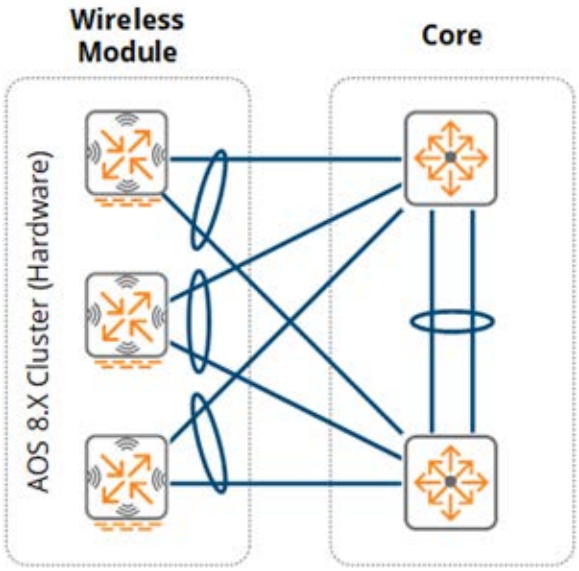
Redundancy for a medium building reference architecture is provided across all layers. The redundancy built into the 3-tier modular network design that establishes the foundation network determines the level of redundancy that is provided to the modules. Aruba recommends using NVF functions (stacking or MC LAG) to provide network and link redundancy and redundant power supplies to maximize network availability and resiliency.

For this scenario the MM and cluster members are deployed within a computer room and connect directly to the core or computer room aggregation switches. Two VMMs and one cluster of hardware or virtual MCs is required to fully enable redundancy:

- Aruba MM (MM):
  - Two virtual MMs
  - L2 master redundancy (active/standby)
- Hardware MCs (MCs):
  - Single cluster of hardware MCs
  - Minimum of two cluster members
- Virtual MCs (VMCs):
  - Single cluster of virtual MCs
  - Minimum of two cluster members
  - Separate virtual server hosts
- Access Points
  - AP Master pointing to the cluster's VRRP VIP address
  - Fast failover using built in cluster redundancy

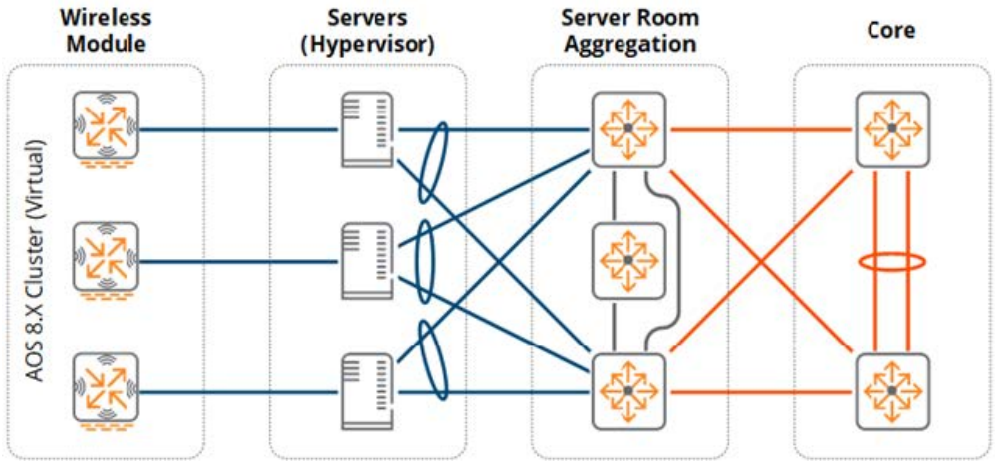
The following figures provide detailed examples for how the virtual and hardware cluster members are connected to their respective layers. Hardware MCs are directly connected to the core layer switches via two or more 1 Gigabit or 10 Gigabit Ethernet ports configured in a LAG group. The LAG port members being distributed between redundant core/aggregation switches.

Figure 131 *Hardware MC Cluster – Core Layer*



VMCs are logically connected to a virtual switch within the virtual server host. The virtual host server is directly connected to the computer room aggregation switches via two or more 1 Gigabit or 10 Gigabit Ethernet ports implementing 802.3ad link aggregation or a proprietary load-balancing and failover mechanism. Each port is distributed between redundant computer room aggregation switches.

Figure 132 *Virtual MC Cluster – Computer Room Aggregation Layer*



The MM(s) are deployed in a similar manner to the cluster of VMCs. Each virtual server host supports one virtual MM operating in an active/standby mode.

NOTE

Redundancy for virtual servers is dependent on the hypervisor. To provide against link, path and node failures, the hypervisor may implement 802.3ad link aggregation or a proprietary load-balancing and failover mechanism.

Virtual MCs

For medium building deployments VMCs may also be deployed as an alternative to hardware MCs. If VMCs are deployed, the virtual server infrastructure must be scaled accordingly to provide the necessary CPU and memory resources to support each virtual MC in the cluster:

- Each VMC in the cluster should be deployed across different virtual server hosts. For this design two virtual server hosts are required.
- Uplinks between the virtual server host and the computer room aggregation layer must be scaled accordingly to support the wireless and dynamically segmented client throughput requirements. The throughput of cluster will be limited by the Ethernet PHYs installed on the virtual server host.

Redundancy between the virtual server host and its peer switches can use either standard 802.3ad link aggregation or a proprietary hypervisor specific load-balancing and failover mechanism. Each hypervisor supports specific load-balancing and failover mechanisms such as active / standby, round-robin load-balancing, or link aggregation. The appropriate redundancy mechanism should be selected to support the specific implementation requirements for each site.

Scalability

For this scenario there are no specific LAN scalability considerations that need to be taken into account. The core, aggregation, and access layers can easily accommodate the APs and client counts without modification or derivation from the design. A wireless aggregation layer can be added in the future as additional APs and clients are added to the network.

Wireless module scaling is also not a concern as the MMs can be expanded and additional cluster members can be added over time to accommodate additional APs, clients, and switching capacity as the network scales.

For this medium building design Aruba recommends implementing the MM-VA-500 MM and a cluster of two or more hardware or virtual MCs per the platform suggestions. The MM selected for this design can scale to support 500 APs, 5,000 clients, and 50 MCs.

Virtual LANs

In the medium office design the core or computer room aggregation layer terminates all VLANs from the MCs. The VLANs are extended from the MCs to the core or computer room aggregation layer using 802.1Q trunking. Aruba recommends using tagged VLANs wherever possible to provide additional loop prevention. The wireless module consists of one or more user VLANs depending on the security and policy model. For a single VLAN design, all wireless and dynamically segmented clients are assigned to a common VLAN ID. Roles and policies determine the level of access each user is provided on the network. The single VLAN is extended from the core or computer room aggregation layer switches to each physical or virtual MC cluster member. Additional VLANs can be added and extended as required. For example, the mobile first design may require separate VLANs to be assigned to wireless and dynamically segmented clients for policy compliance reasons.

A minimum of two VLANs are required between the core or computer room aggregation layer and each MC cluster member. One VLAN is dedicated for management and MM communications while the second VLAN is mapped to clients. All VLANs are common between cluster members to permit seamless mobility. The core or computer room aggregation layer switches have VLAN-based IP interfaces defined and operate as the default gateway for each VLAN. First-hop router redundancy is natively provided by the Aruba stacking architecture.

Figure 133 *Hardware MC Cluster – VLANs*

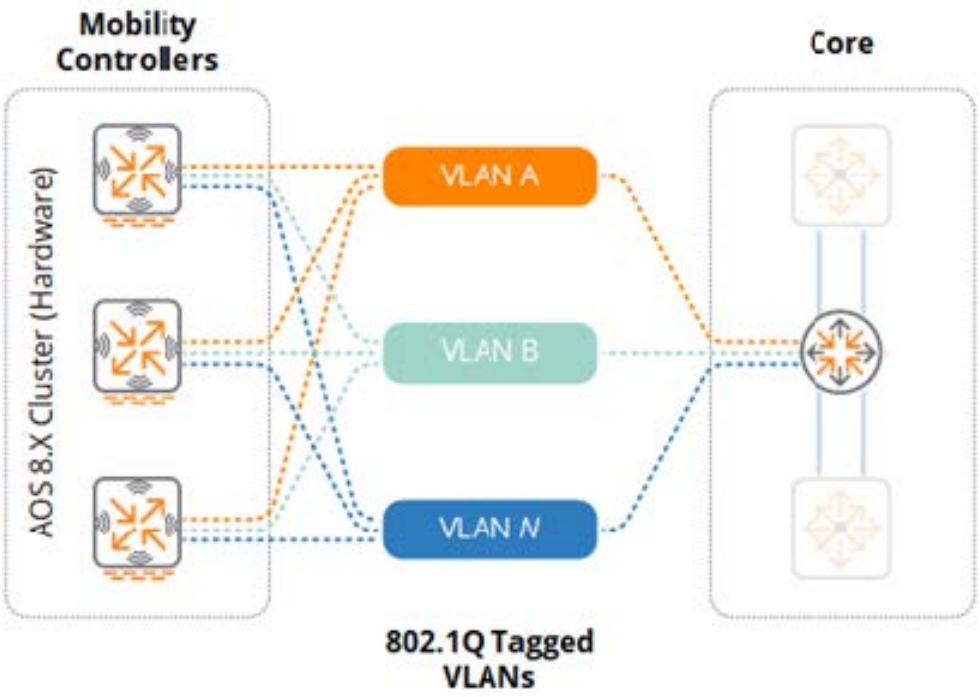
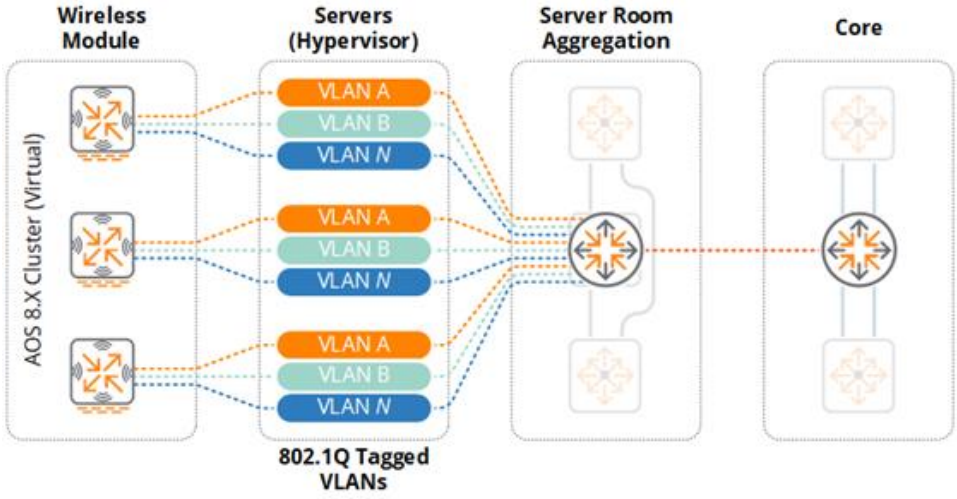


Figure 134 *Virtual MC Cluster – VLANs*



As a best practice, Aruba recommends implementing unique VLAN IDs within the wireless module. This allows for an aggregation layer to be introduced in the future without disrupting the other layers within the network. This also allows for the creation of smaller layer 2 domains. Segmenting the network in this manner reduces layer 2 instability and protects the wireless module from operational changes, loops, or misconfigurations originating from other layers or network modules.

Platform Suggestions

The figure below provides platform suggestions for the medium building scenario supporting 120 APs and 3,000 concurrent clients. A good, better, and best suggestion is made based on features, performance, and scalability. These are suggestions based on the described scenario and may be altered according to the discretion of network administrators.

Figure 135 *Medium Building Platform Suggestions*

		Good	Better	Best
Switching	Core Layer	3810	5400R	8230
	Aggregation Layer	3810	5400R	8320
	Access Layer	2930	3810	5400R
	Wireless Module	3810	5400R	8320
Wireless	Mobility Masters	MM-VA-500		
	Virtual Mobility Controller Cluster	MC-VA-250		
	Mobility Controller Cluster	7205	7210	
	802.11ac Wave 2 Access Points	300 Series	310 Series	330/340 Series

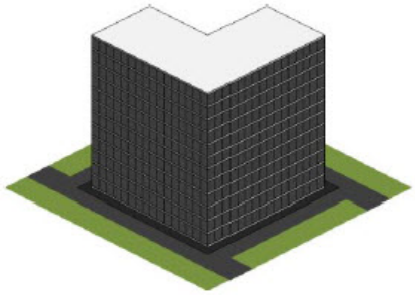
Features, Performance & Scaling

Large Office

Scenario

The following reference design is for a large office consisting of 12 floors. The building includes a data center which connects via single-mode fiber to an MDF on each floor. Each floor also includes three IDFs which connect to the MDF via multi-mode fiber. The building supports up to 3,000 employees and requires 300 802.11ac Wave 2 APs to provide full 2.4 and 5GHz coverage.

Figure 136 *Large Office Characteristics*



Building Characteristics:

- 12 Floors / 360,000 sq. ft. Total Size
- 3,000 x Employees / 6,000 x Concurrent IPv4 Clients
- 300 x 802.11ac Wave 2 Access Points
- 1 x Computer Room
- 1 x MDF per floor (12 total)
- 2 x IDFs per floor (24 total)

The large building design implements a structured wiring design using MDFs and IDFs which requires an aggregation layer to connect the access layer. The building implements a 3-tier modular network design where the access layer switches connect via aggregation layer switches in each MDF which in turn connect directly to the core. The modular network design also includes additional aggregation layers for the computer room and wireless modules for scalability, aggregation, and fault domain isolation.

The list below provides an outline of the modular network architecture and design:

LAN Core:

- A pair of redundant switches with a mix of 10G and 40G fiber ports:
  - SFP/SFP+/QSFP+ (aggregation layer interconnects)
- IP routing to aggregation layer devices and modules
- Optional NVF Functions (MC LAG)

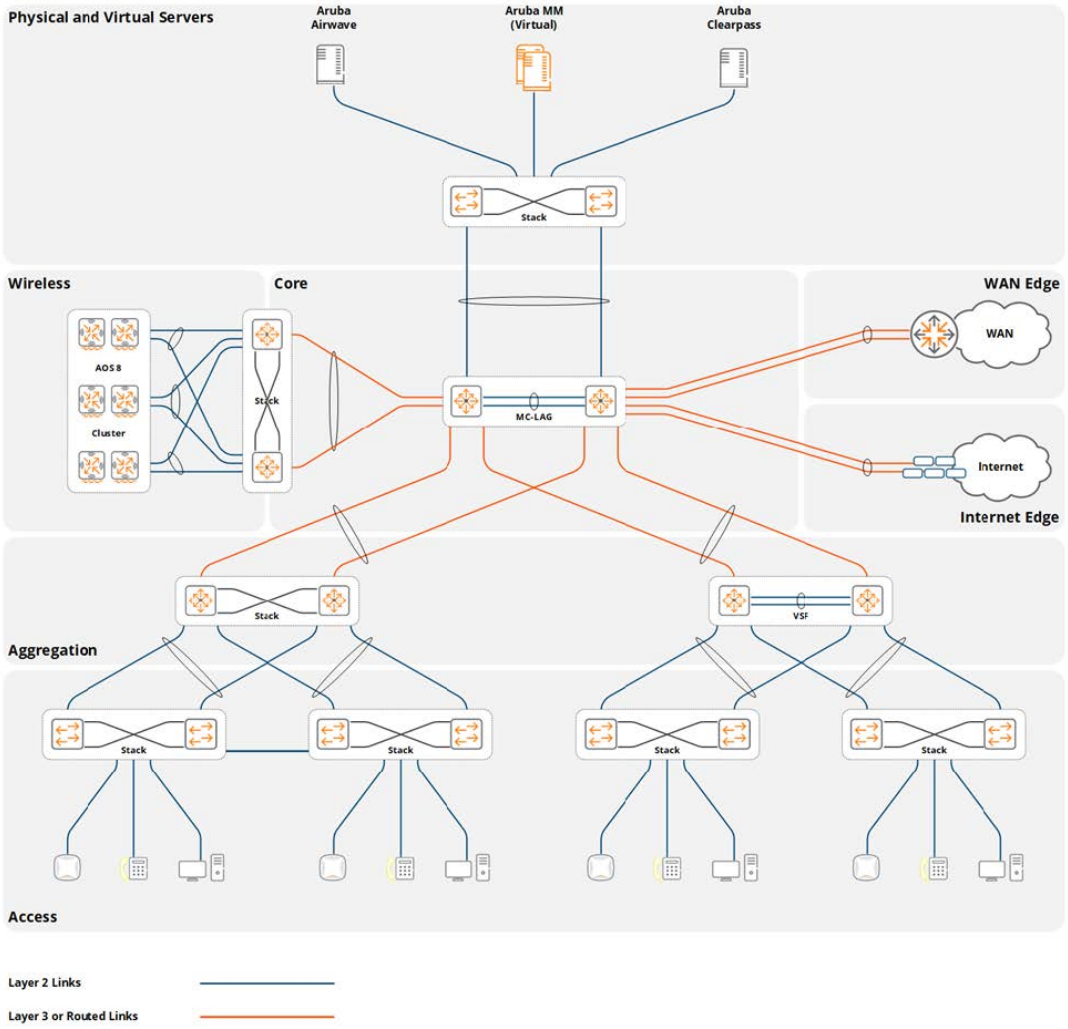
LAN Aggregation:

- A stack of two switches with fiber ports per MDF:
  - SFP/SFP+/QSFP+ (core and access layer interconnects)
- NVF Functions (MCLAG/VSX)
- IP routing to core layer devices

LAN Access:

- A stack of two or more switches per MDF and IDF:
  - SFP/SFP+ (aggregation layer interconnects)
  - 10/100/1000BASE-T with PoE+ (edge ports)
- Layer 2 link aggregation to access layer devices
- 802.11ac Wave 2 APs

Figure 137 *Large Office – 3-Tier Modular Network Design*



The number of APs required for this hypothetical scenario was calculated based on the square footage, wireless density, and capacity requirements for the building. It was determined that 300 APs would be required based on an assumption of each AP providing 1200 square feet of coverage and supporting 20 clients.

The actual number of APs and their placement for a production deployment should be determined using a site survey which takes into account the density requirements for each coverage area.

Considerations and Best Practices

Wireless LAN Components

The large building in this scenario includes various wireless components which are either deployed in the wireless module or the server room. To accommodate the AP and client counts for this scenario an MM and a single cluster of MCs is required. The number of cluster members is determined by the hardware or virtual MC model that is selected. The MC cluster consists of a minimum of two MCs for redundancy purposes. Each member provides adequate capacity and performance to allow the wireless network to continue to function in the event of a single MC failure.

The following table provides a summary of these components:

Table 27: *Medium Building Wireless LAN Components*

Component	Description	Notes
Aruba MM (MM)	Hardware or Virtual Appliances	2 are required
Aruba MCs	Hardware or Virtual Appliances	2 Minimum (Clustered)
Aruba Access Points	802.11ac Wave 2 Access Points	300 Required
Aruba AirWave	Hardware or Virtual Appliance	Recommended
Aruba ClearPass	Hardware or Virtual Appliance	Recommended

Redundancy

Redundancy for a large building architecture is provided across all layers. The redundancy built into the 3-tier modular network design that establishes the foundation network determines the level of redundancy that is provided to the modules. Aruba recommends using NVF functions (stacking or MC LAG) to provide network redundancy as well as using redundant links and power supplies to maximize network availability and resiliency. The Aruba 8400 provides the maximum redundancy capabilities of any Aruba Switch and is recommended for use in the Core, Aggregation, and Wireless Aggregation layers.

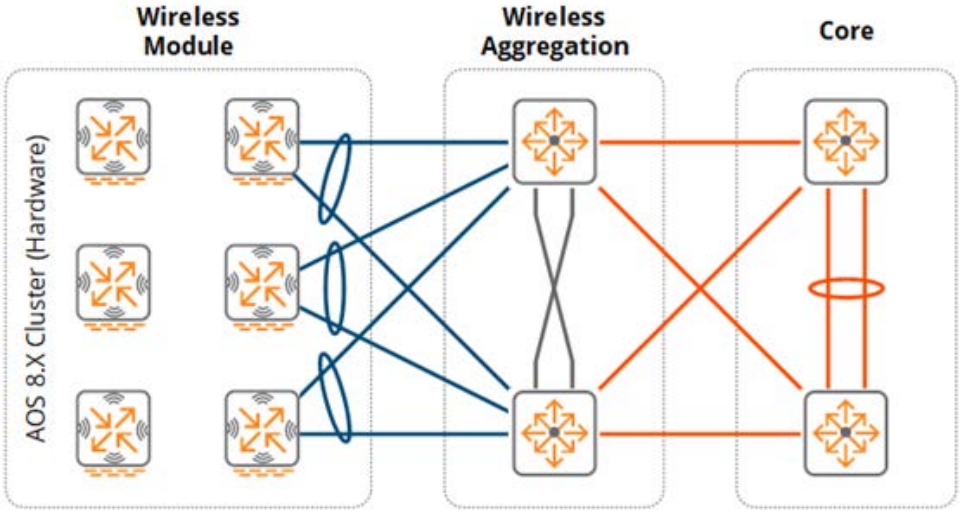
For this scenario the MM and mobility cluster members are deployed within a computer room and are directly connected to the wireless aggregation or computer room aggregation switches. Two hardware or virtual MMs and one cluster of hardware or virtual MCs is required to fully enable redundancy:

- Aruba MM (MM):
  - Two hardware or virtual MMs
  - L2 master redundancy (active/standby)
- Hardware MCs (MCs):
  - Single cluster of hardware MCs
  - Minimum of two cluster members

- Virtual MCs (MCs):
  - Single cluster of virtual MCs
  - Minimum of two cluster members
  - Separate virtual server hosts
- Access Points
  - AP Master pointing to the cluster's VRRP VIP
  - Fast failover using built in cluster redundancy

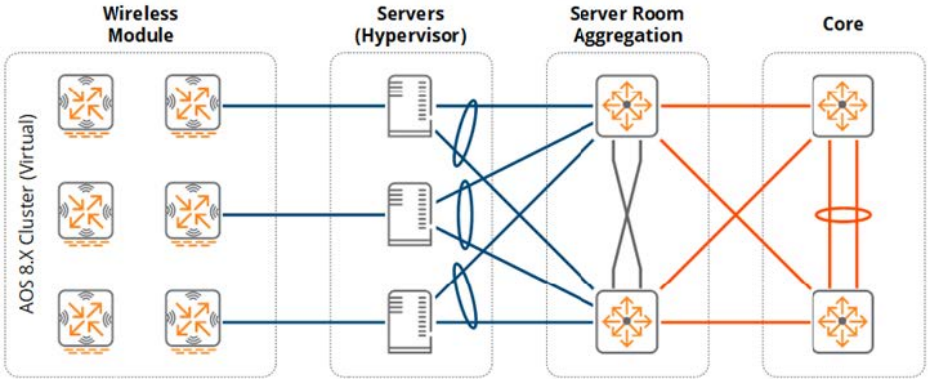
The figures below provide detailed examples for how the virtual and hardware cluster members are connected to their respective layers. Hardware-based MCs are directly connected to the core layer switches via two or more 10 gigabit Ethernet ports configured in a LAG. The LAG port members are distributed between redundant wireless aggregation switches.

Figure 138 *Hardware MC Cluster – Wireless Aggregation Layer*



VMCs are logically connected to a virtual switch within the virtual server host. The virtual host server is directly connected to the computer room aggregation switches via two or more 10 gigabit Ethernet ports implementing 802.3ad link aggregation or a proprietary load-balancing and failover mechanism. Each port is distributed between redundant computer room aggregation switches.

Figure 139 *Virtual MC Cluster – Computer Room Aggregation Layer*



The MM(s) are deployed in a similar manner as the cluster of VMCs. Each virtual server host supports one virtual MM operating in an active/standby mode.

Redundancy for virtual servers is hypervisor-dependent. To provide against link, path, and node failures, the hypervisor may implement either 802.3ad link aggregation or a proprietary load-balancing and failover mechanism.

Virtual MCs

VMCs may be optionally deployed for large building deployments. If VMCs are deployed the virtual server infrastructure must be scaled accordingly to provide the necessary CPU and memory resources for each VMC in the cluster:

- Each VMC should be deployed across different virtual server hosts. Two virtual server hosts are required for the large office design.
- Uplinks between the virtual server host and the computer room aggregation layer must be scaled accordingly to support the wireless and dynamically segmented client throughput requirements. The throughput of cluster will be limited by the Ethernet PHYs installed on the virtual server host.

Redundancy between the virtual server host and its peer switches can use standard 802.3ad link aggregation or a proprietary hypervisor specific load-balancing and failover mechanism. Each hypervisor supports specific load-balancing and failover mechanisms such as active/standby, round-robin load-balancing, and link aggregation. The appropriate redundancy mechanism should be selected to support the specific implementation requirements of the deployment.

Scalability

The large office design includes a wireless aggregation layer to accommodate 6,000 wireless IPv4 hosts on the network. As a general best practice Aruba recommends considering a wireless aggregation layer once the combined IPv4 and IPv6 host count exceeds 4,094. The wireless aggregation layer is needed if hardware MCs are deployed and are connected directly to the core layer. If VMCs are deployed then the computer room aggregation switches provide the aggregation functionality.

Future growth is not a concern as the MMs can be easily expanded and additional cluster members can be added over time to accommodate additional APs, clients, and switching capacity. For this large building design, Aruba recommends implementing the MM-HW-5K or MM-VA-5K MM and a cluster of two or more hardware or virtual MCs. The MM selected for this design can scale to support 5,000 APs, 50,000 clients, and 500 MCs.

Virtual LANs

In the large office design the wireless module aggregation layer terminates all layer 2 VLANs from the MCs. The VLANs are extended from the MCs to their respective aggregation layer switches using 802.1Q trunking. Aruba recommends using tagged VLANs wherever possible to provide additional loop prevention.

The wireless module consists of one or more user VLANs depending on the security and policy model that has been implemented. For a single VLAN design, all wireless and dynamically segmented clients are assigned to a common VLAN ID with roles and policies determining the level of access each user is provided on the network. The single VLAN is extended from the respective aggregation layer switches to each physical or virtual MC cluster member. Additional VLANs can be added and extended as required. For example, a mobile first design may require separate VLANs to be assigned to wireless and dynamically segmented clients for policy compliance reasons.

A minimum of two VLANs are required between each aggregation layer switch and the respective MC cluster members. One VLAN is dedicated for management and MM communications while the second VLAN is

mapped to clients. All VLANs are common between cluster members to enable seamless roaming functionality for clients. The aggregation layer switches have defined VLAN-based IP interfaces and operate as the default gateway for each VLAN. First-hop router redundancy is natively provided by the Aruba clustering and stacking architecture.

Figure 140 *Hardware MC Cluster – VLANs*

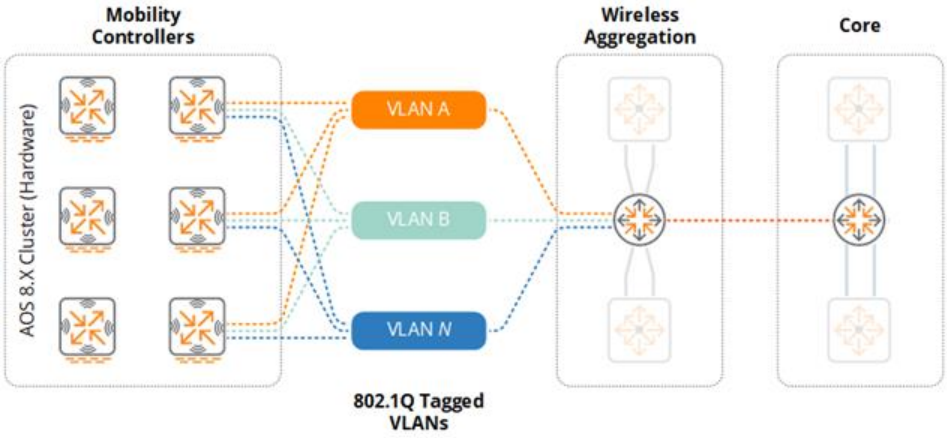
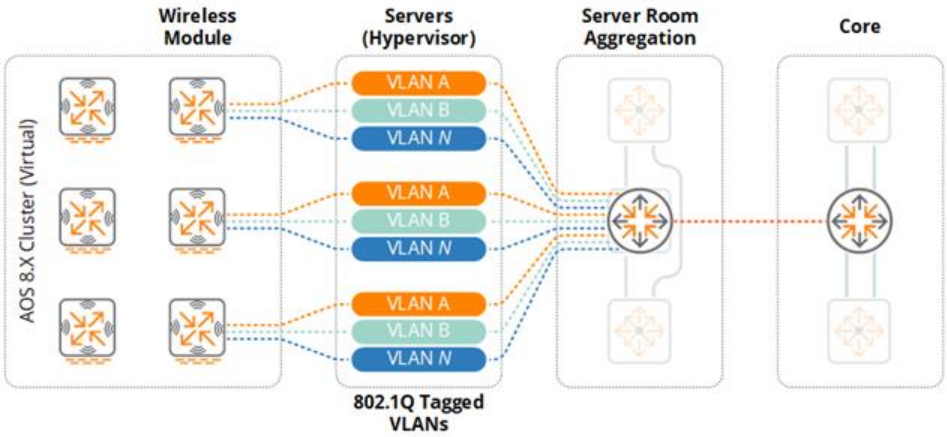


Figure 141 *Virtual MC Cluster – VLANs*

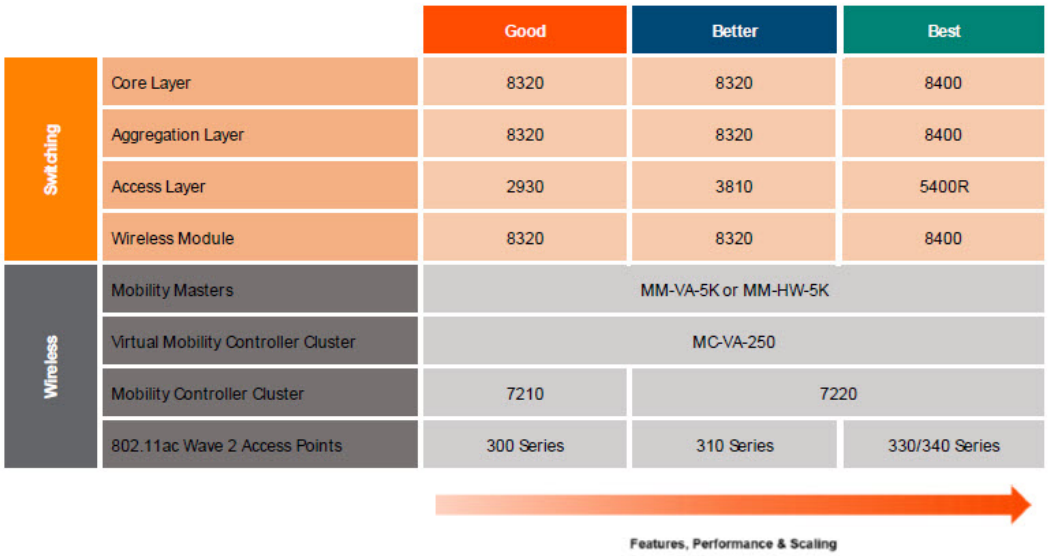


As a best practice Aruba recommends implementing unique VLAN IDs within the wireless module. This allows for the introduction of an aggregation layer in the future without disrupting the other layers within the network. This also allows for the creation of smaller layer 2 domains. Segmenting the network in this manner reduces layer 2 instability and protects the wireless module from operational changes, loops, or misconfigurations originating from other layers or network modules.

Platform Suggestions

Figure 143 provides platform suggestions for the large building scenario based on the assumption of supporting 300 APs and 6,000 concurrent clients. A good, better, and best suggestion is made based on features, performance, and scalability. These are suggestions based on the described scenario and may be altered according to the discretion of network administrators.

Figure 142 *Large Building Platform Suggestions*



Campus

The following reference design is intended for a campus deployment which consists of multiple buildings of varying size and two datacenters. Each building in the campus implements its own 2-tier or 3-tier modular network which connects to a campus backbone. The campus in this scenario needs to support 64,000 concurrent dual-stack clients and requires 6,000 802.11ac Wave 2 APs.

A key decision that needs to be taken into account for a campus deployment is where to place the MC clusters (wireless module). Due to the challenging scalability requirements, a campus of this size will generally require multiple clusters of MCs which can either be centralized in the datacenters or strategically distributed between the buildings. The clusters in both cases are managed by hardware or virtual MMs deployed across the datacenters.

Both centralized and distributed MC deployment models are valid for campus deployments with each model supporting different mobility needs. As seamless mobility can only be provided between APs managed by a common cluster, the mobility requirements are usually the determining factor influencing the cluster deployment model that is selected.

Traffic flows are another factor that needs to be taken into account when determining cluster placement. If user applications are primarily hosted in the datacenter, then a centralized cluster is an appropriate choice as the wireless and dynamically segmented client sessions are terminated within the cluster. Placing the cluster closer to the applications optimizes the traffic flows. If the primary applications are distributed between buildings in the campus, a distributed MC model may be a more efficient design.

Centralized Clusters

- Permits a larger mobility domain when ubiquitous indoor and outdoor coverage is required.
- Efficient when the primary applications are hosted in the cloud or datacenter.

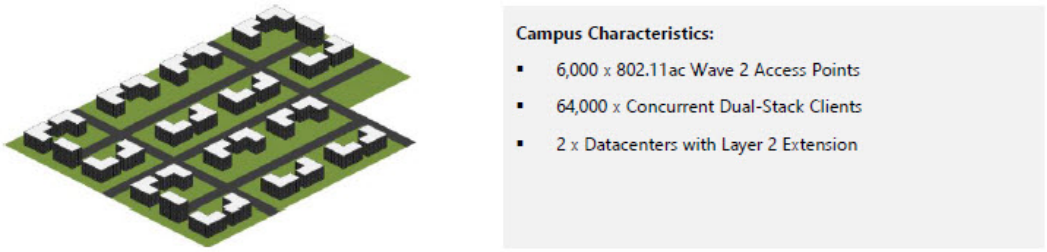
Distributed Clusters

- Permits smaller mobility domains such as within buildings or between co-located buildings.
- Efficient when the primary applications are distributed or workgroup based.

Scenario 1 – Centralized Clusters

The Centralized Clusters reference design is appropriate for a campus such as a corporate headquarters with two datacenters implementing centralized clusters. The campus LAN implements a high-speed layer 3 backbone that interconnects each building to both datacenters. The campus needs to support 64,000 concurrent dual-stack wireless clients across 6,000 802.11ac Wave 2 APs. Each host in this example is assigned a single global IPv6 address from a stateful DHCPv6 server (1 x global IPv6 address per client). To enable roaming between large groups of buildings indoor and outdoor APs with overlapping coverage will be assigned to the same MC cluster.

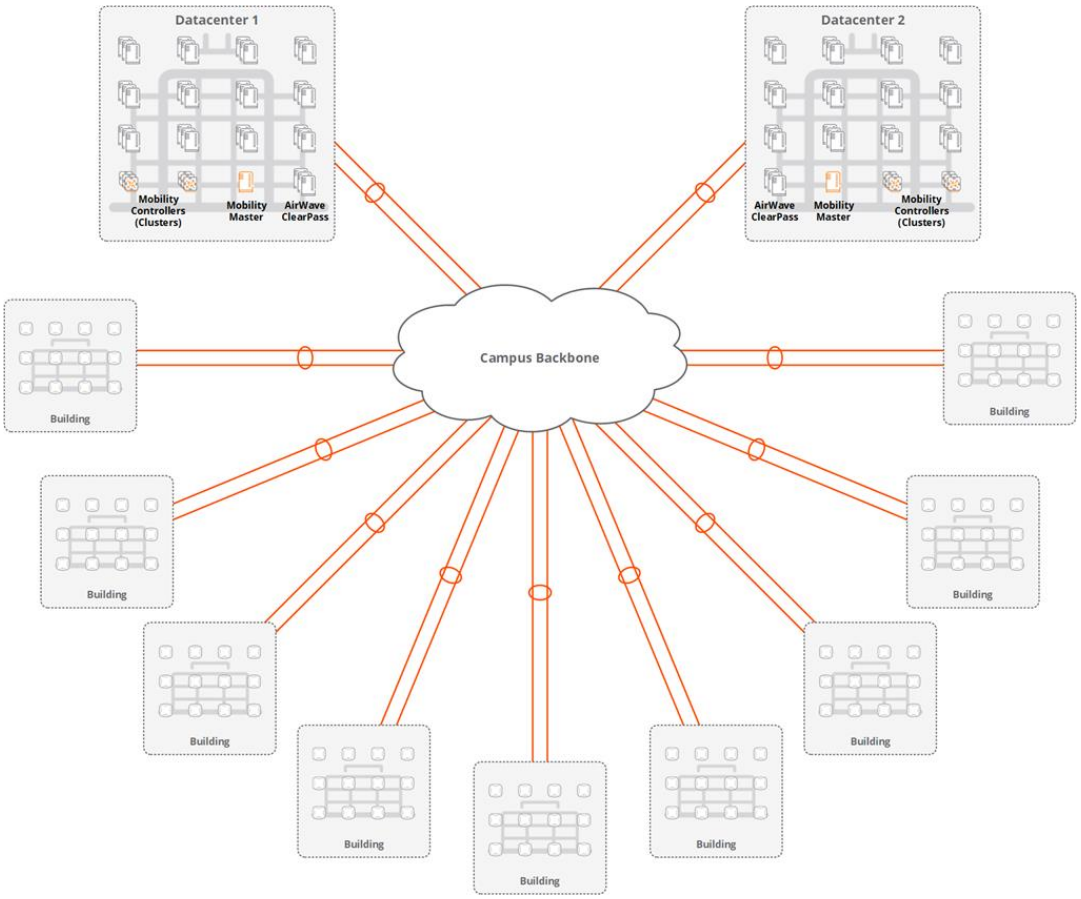
Figure 143 *Scenario 1 Campus Characteristics*



NOTE

For this scenario it is assumed that stateful DHCPv6 is implemented where each client receives a 1 x global IPv6 address. If SLAAC is utilized for addressing, each client could potentially consume 3 – 4 x global IPv6 addresses which would not be supported by this design without deploying additional clusters and wireless aggregation layer switches. If you are planning an IPv6 deployment for a large campus environment, please engage your Aruba account team for design assistance.

Figure 144 *Campus Modular Network Design – Centralized MC Clusters*



Wireless LAN Components

The campus in this scenario includes the MMs and clusters of MCs which are distributed across two datacenters. The number of MMs and MC clusters required to enable full redundancy will be influenced by the datacenter design. The datacenters can either support Layer 2 VLAN extensions or be separated at layer 3:

- Layer 2 Extensions – VLANs and their associated broadcast domains are common between datacenters.
- Layer 3 Separation – VLANs and their associated broadcast domains are unique for each datacenter.

When VLANs are extended between the datacenters, the MMs and MC cluster members can be split between the datacenters. Each datacenter hosts 1 MM and half of the MCs. Two MMs and two clusters of MCs are required to accommodate the AP and client counts for this scenario. To enable aggregation layer scalability as well as fault domain isolation, each cluster of mobility MCs is connected to separate Aruba 8400 series aggregation layer switches. Each aggregation layer can accommodate up to 32,000 IPv4 and 64,000 IPv6 host addresses.

Table 28: *Wireless LAN Components – Layer 2 Extension*

Component	Description	Notes
Aruba MM (MM)	Hardware or Virtual Appliances	2 required

Table 28: *Wireless LAN Components – Layer 2 Extension*

Component	Description	Notes
Aruba MCs	Hardware or Virtual Appliances	2 Clusters
Aruba Access Points	802.11ac Wave 2 Access Points	6000 Required
Aruba AirWave	Hardware or Virtual Appliance	Recommended
Aruba ClearPass	Hardware or Virtual Appliance	Recommended

A different approach is required when datacenters are separated at layer 3. To support the AP and client counts and maintain full redundancy an active/standby model is implemented. In such a design each datacenter hosts an equal quantity of MMs and MCs:

MMs – Two MMs are hosted per datacenter implementing layer 2 and layer 3 master redundancy. Layer 2 master redundancy is provided between MMs within each datacenter while layer 3 master redundancy provides redundancy between datacenters.

MC Clusters – Two clusters of MCs are hosted per datacenter. The APs are configured with a primary LMS and backup LMS to determine their primary and secondary cluster assignments. Fast failover is provided within the primary cluster while a full bootstrap is required to failover between the primary and secondary clusters.

Each cluster of MCs is connected to separate Aruba 8400 series aggregation layer switches for aggregation layer scaling and fault domain isolation. Each aggregation layer switch can accommodate up to 32,000 IPv4 and 64,000 IPv6 host addresses. Each datacenter is separated at layer 3 requiring four wireless modules and wireless aggregation layers to accommodate an individual datacenter failure.

Table 29: *Wireless LAN Components – Layer 3 Separation*

Component	Description	Notes
Aruba MM (MM)	Hardware or Virtual Appliances	4 required (L3 redundancy
Aruba MCs	Hardware or Virtual Appliances	4 clusters (2 per datacenter)
Aruba Access Points	802.11ac Wave 2 Access Points	6000 Required
Aruba AirWave	Hardware or Virtual Appliance	Recommended
Aruba ClearPass	Hardware or Virtual Appliance	Recommended

Roaming Domains

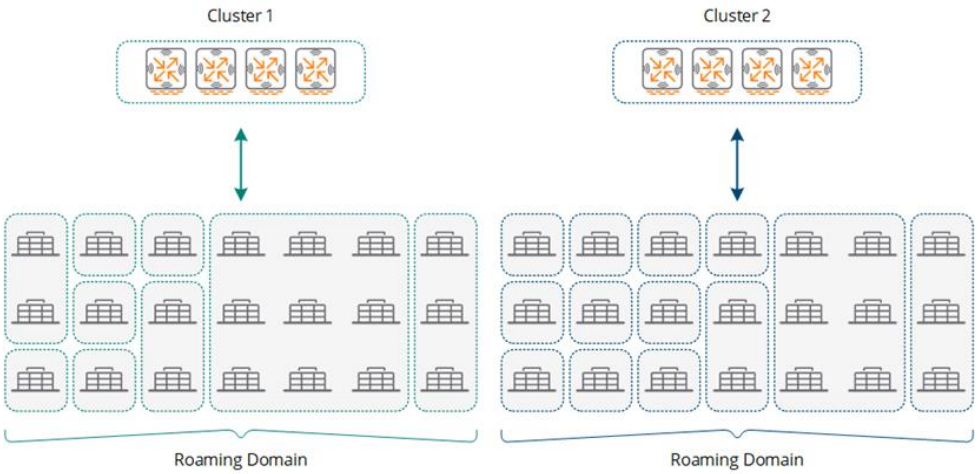
In an ArubaOS 8 architecture, seamless mobility is provided between APs managed by a common cluster. Each wireless and dynamically segmented client is assigned a primary UAC and S-UAC cluster member to provide fast failover in the event of a cluster member failure or live upgrade. Two clusters of MCs are required in order to ensure adequate scalability.

It is important to take into account that seamless roaming can only occur between APs managed by the same cluster. The following considerations need to be made:

- APs in the same building must be managed by the same cluster. This ensures wireless client sessions are not interrupted as the clients roam within the building.
- Indoor and outdoor APs in co-located buildings with overlapping coverage must be managed by the same cluster. This ensures client sessions are not interrupted as the clients roam within a building or between buildings.

APs in buildings that are geographically separated and do not have overlapping coverage can be distributed between clusters as required with attention being made to ensure AP and client capacity is evenly distributed as possible:

Figure 145 *Roaming Domains*



NOTE

If the campus deployment supports both wireless and dynamically segmented clients it may be beneficial to deploy separate clusters.

Redundancy

In the Centralized Clusters scenario the datacenters are located in separate buildings which are connected to the campus backbone. The datacenters are interconnected using high-speed links ensuring there is adequate bandwidth capacity available to support the hosted applications and services that are hosted in each datacenter.

For a dual datacenter design, the MMs and MC clusters are distributed between both datacenters. The wireless components can be deployed using several strategies to achieve redundancy which is depend on the datacenter design:

- Layer 2 Extension – If VLANs are extended between datacenters, the MMs and MC cluster members can be split between the datacenters. Each datacenter will host 1 MM and half of the cluster members.
- Layer 3 Separation – The MMs and MC cluster members are duplicated in each datacenter.

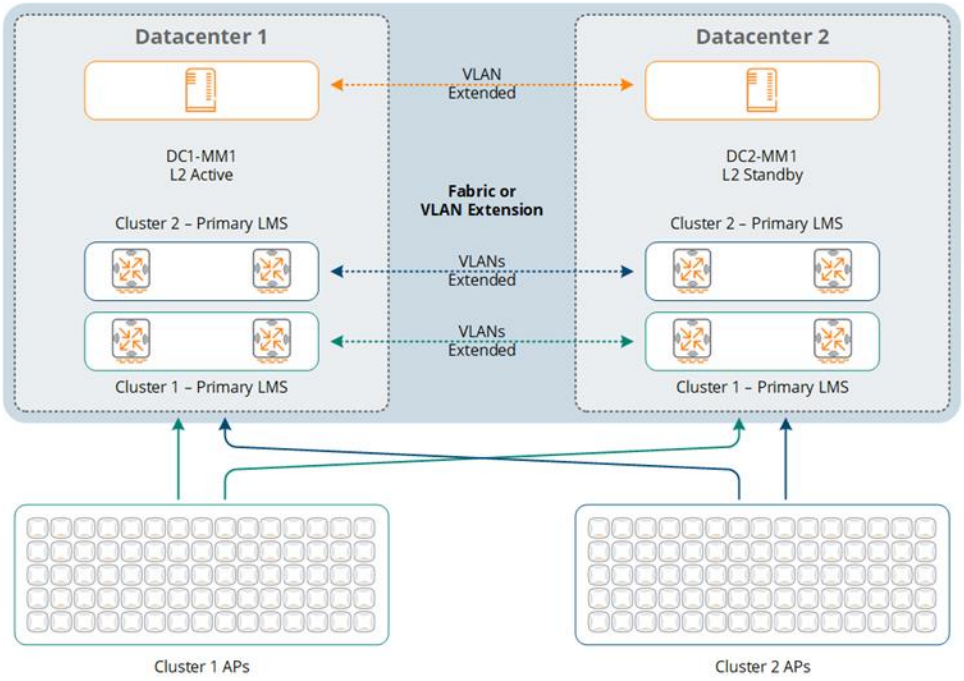
Layer 2 Extension

The layer 2 datacenter redundancy model is relatively straightforward as it operates in the same manner as a single datacenter deployment model. Each datacenter hosts a MM and half of the MCs of each cluster. The MMs are configured for L2 redundancy while AP and client load-balancing as well as fast failover functionality is provided by each cluster:

- Aruba MM (MM):
  - Two hardware or virtual MMs (one per datacenter)
  - L2 master redundancy (active/standby)
- Hardware MCs (MCs):
  - Two clusters of hardware MCs
  - Cluster members equally distributed between datacenters
- Access Points
  - AP Master pointing to the cluster's VRRP VIP address
  - Fast failover using cluster built-in redundancy
  - AP cluster assignment based on roaming requirements for each building

APs and clients will be load-balanced and distributed between cluster members residing in each datacenter by default. With the Centralized Cluster Campus design it is possible that APs and clients within a building will be assigned to cluster members in different datacenters.

Figure 146 *Redundancy – Layer 2 Extension*



Layer 3 Separated

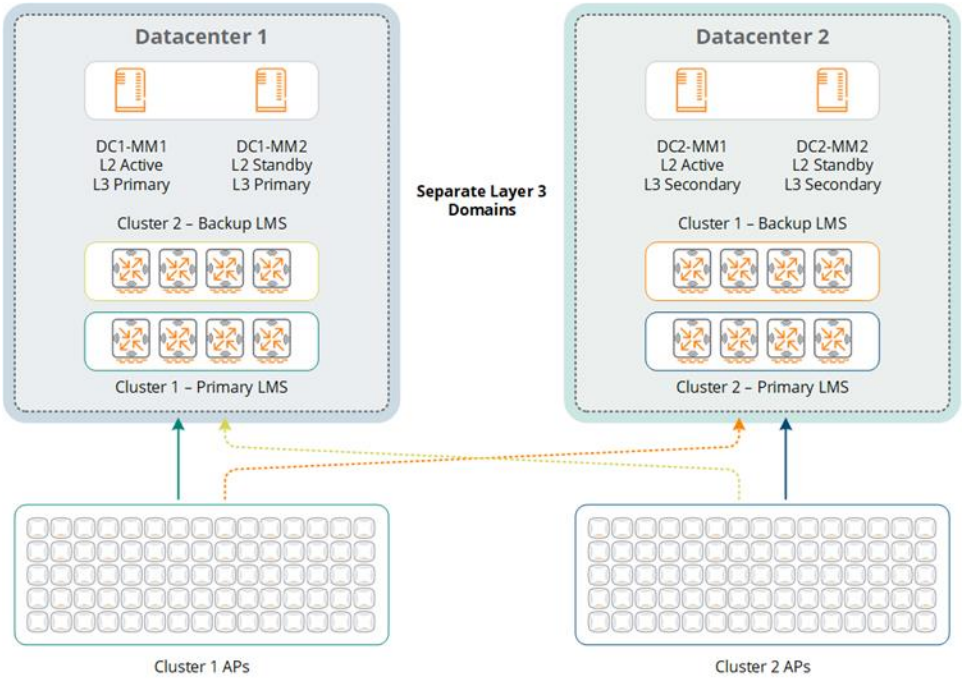
The layer 3 Separated datacenter redundancy model differs from Layer 2 Extension by duplicating the MMs and clusters within each datacenter. Each datacenter hosts two MMs and two clusters of MCs. The MMs are configured for L2 redundancy within the datacenter and L3 redundancy between datacenters. The APs within each building are assigned a primary and backup cluster using the primary and backup LMS. AP and client fast failover functionality is provided within each cluster while a full bootstrap is required to provide failover between clusters:

- Aruba MM (MM):

- Four hardware or virtual MMs (two per datacenter)
- L2 master redundancy (Active/Standby)
- L3 master redundancy (Primary/Secondary)

- Hardware MCs (MCs):
  - Four clusters of hardware MCs (Primary/Secondary)
  - Cluster members duplicated between datacenters
  - Primary clusters alternating between datacenters
- Access Points
  - Primary and Backup LMS using the primary and secondary cluster VRRP VIP addresses
  - Fast failover using cluster built-in redundancy
  - Bootstrap failover between primary and secondary clusters
  - AP cluster assignment based on roaming requirements for each building

Figure 147 *Redundancy – Layer 3 Separation*



Scalability

Scalability is the primary concern for this campus scenario and the inclusion of a secondary datacenter with the datacenter deployment model can pose a challenge. Considerations had to be made for both the datacenter aggregation layer and the MC cluster design to accommodate the network growth and redundancy requirements.

Datacenter Aggregation Layer

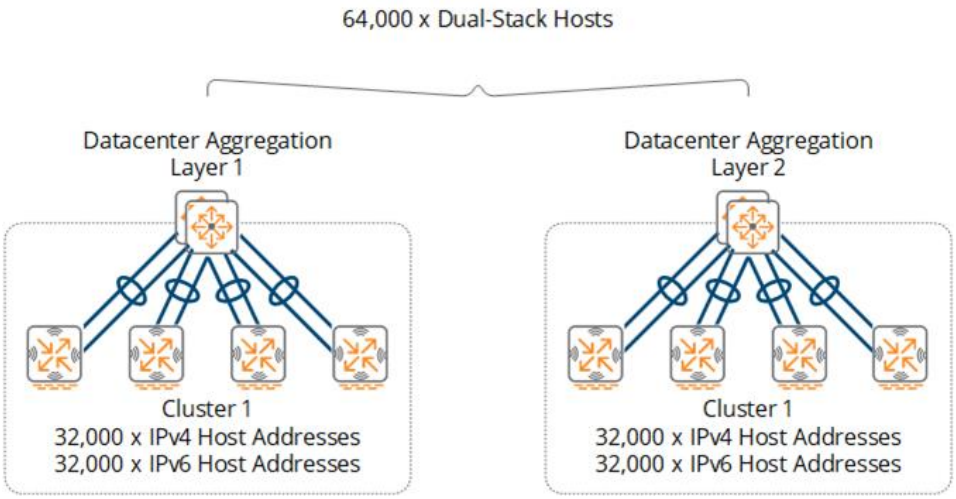
Both datacenter deployment models require clusters of MCs that are connected to their respective datacenter aggregation layers. Two clusters of MCs are required to accommodate 64,000 concurrent dual-stack hosts with each supporting up to 32,000. Each IPv6 host in this example is assigned a single global IPv6 address.

Each cluster is connected to a separate Aruba 8400 series wireless aggregation layer switch due to the high number of clients that must be supported. This recommendation applies to both layer 2 extended and layer 3 separated datacenter designs:

- Layer 2 Extension – Requires two datacenter aggregation layers which are split between datacenters. Each wireless aggregation layer supports one cluster of MCs.
- Layer 3 Separated – Requires two datacenter aggregation layers per datacenter. Each wireless aggregation layer is connected to a primary or secondary cluster of MCs.

This datacenter aggregation layer design ensures that a single aggregation layer never exceeds more than 64,000 IPv4 or IPv6 host addresses during normal operation as well as provides sufficient capacity to continue normal operations in the event of a datacenter failure:

Figure 148 *Datacenter Wireless Aggregation Layer 3 Separated Design*



MC Clusters

Scalability for each cluster is provided by selecting the appropriate controller model and determining the correct number members per cluster. The throughput capabilities of the chosen MC model are also a factor as each model has different switching capacities and physical interfaces. For this campus scenario the 7200 series controllers are recommended with each cluster consisting of four MCs.

While the VMCs can be selected for a campus deployment, Aruba recommends hardware MCs be deployed for throughput and performance reasons. The fact that the hardware is dedicated guarantees that a specific level of performance can be provided.

MM

For the Centralized Cluster Campus design, Aruba recommends implementing the MM-HW-10K or MM-VA-10K MM. Data switching throughput is not a a big concern as with the MC clusters so either hardware or virtual MMs can be deployed.

The MM selected for this design should scale to support 10,000 APs, 100,000 clients, and 1,000 MCs. Implementing this level of capacity will ensure adequate support for the AP, client, and MCs while providing additional room for future growth. Additional clients and APs can be added as the campus grows by adding additional aggregation layers and MC clusters.

Scaling beyond 64,000 dual-stack clients for a centralized deployment model can be achieved by deploying additional MC clusters within the datacenter. In an ArubaOS 8 deployment a MM can scale to support up to

100,000 clients, 10,000 APs, 1,000 MCs. Additional scalability can be achieved by deploying additional MMs and MC clusters.

Virtual LANs

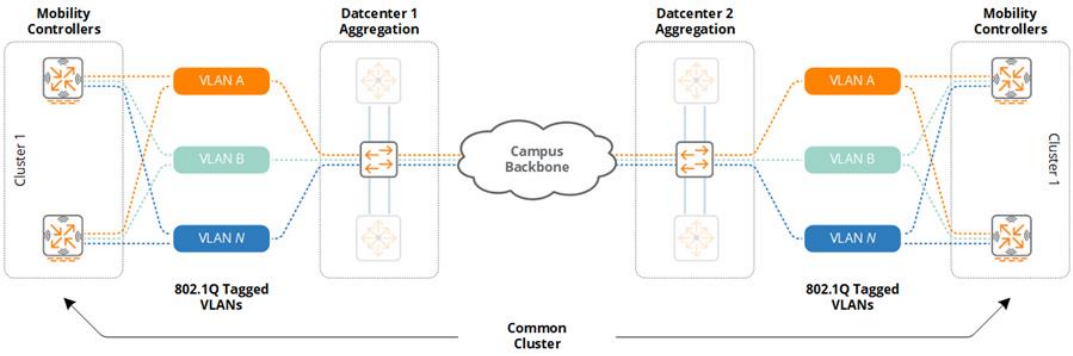
In a centralized cluster design the datacenter aggregation layer terminates all the VLANs from the MC cluster members. The datacenter architecture is what determines the VLAN design. In both designs the VLANs are extended from the MCs to their respective datacenter aggregation layer switches using 802.1Q trunking. The primary difference between the designs being the number of VLANs that are required.

Layer 2 Extension

When VLANs are extended between datacenters, each cluster implements its own unique VLAN IDs and broadcast domains. Each cluster consists of one or more user VLANs depending on the VLAN model that has been implemented. For a single VLAN design, all wireless and dynamically segmented clients are assigned to a common VLAN ID with roles and policies determining the level of access each user is provided on the network. Each cluster implements unique VLAN IDs.

The user VLANs are extended from the aggregation layer switches to each MC cluster member. A minimum of two VLANs are required between the datacenter aggregation layers and each MC cluster member. One VLAN is dedicated for management, cluster, and MM communications while the additional VLANs are mapped to clients. The VLANs are common between cluster members split between the datacenters to enable seamless mobility. The datacenter aggregation layer switches have VLAN based IP interfaces defined and operate as the default gateway for each VLAN. First-hop router redundancy is natively provided by VRRP or the Aruba clustering architecture.

Figure 149 *Wireless and Dynamically Segmented Client VLANs – Layer 2 Extension*

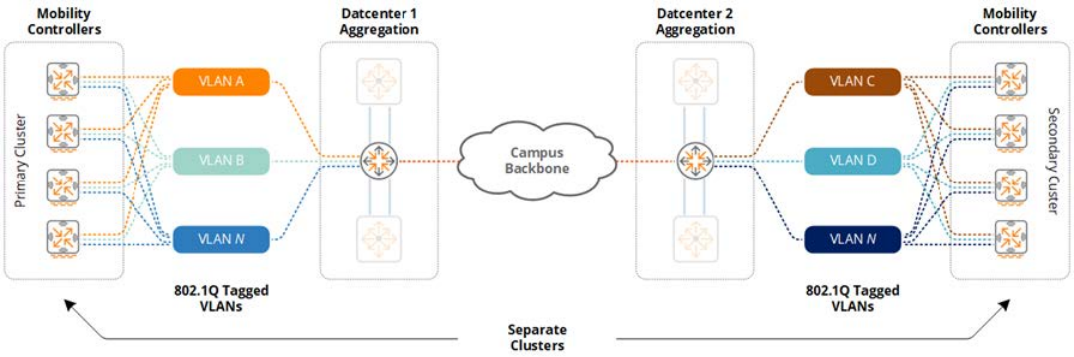


Layer 3 Separation

When the datacenters are separated at layer 3, the VLANs are unique for each datacenter. The primary and secondary clusters in each datacenter each requiring their own unique VLAN IDs and broadcast domains. Each cluster consists of one or more user VLANs depending on the VLAN model that has been implemented. For a single VLAN design, all wireless and dynamically segmented clients are assigned to a common VLAN ID with roles and policies determining the level of access each user is provided on the network. Each cluster implements unique VLAN IDs.

The user VLANs are extended from the aggregation layer switches to each MC cluster member. A minimum of two VLANs are required between the datacenter aggregation layers and each MC cluster member. One VLAN is dedicated for management, cluster, and MM communications while the additional VLANs are mapped to clients. The VLANs are common between cluster members in each datacenter to permit seamless mobility. The datacenter aggregation layer switches have VLAN based IP interfaces defined and operate as the default gateway for each VLAN. First-hop router redundancy is natively provided by VRRP or the Aruba clustering architecture.

Figure 150 *Wireless and Dynamically Segmented Client VLANs – Layer 3 Separation*



One key difference between the two datacenter designs is client VLAN assignment and broadcast domain membership during a datacenter failure. While both models offer full redundancy, only the layer 2 VLAN extension model offers fast failover in the event of a datacenter outage:

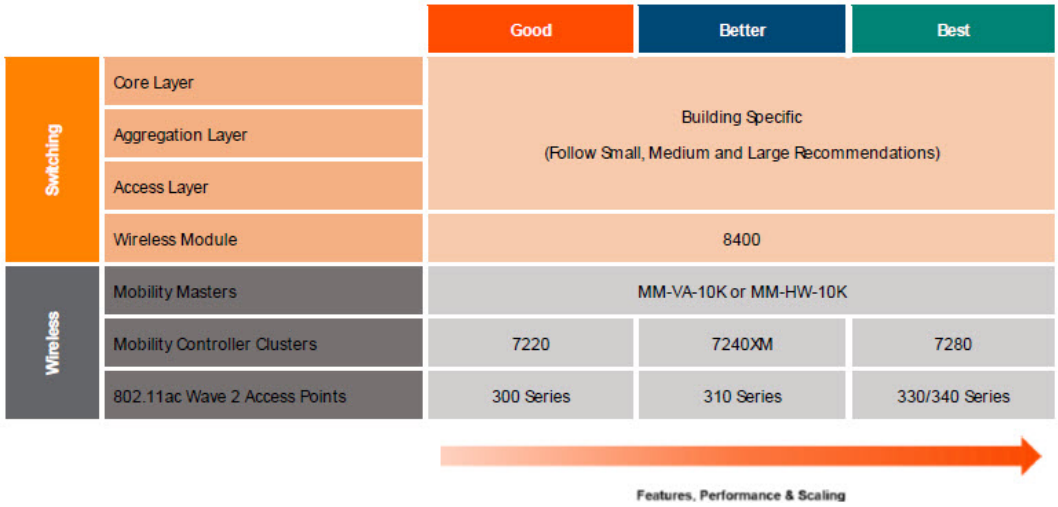
Layer 2 Extension – Impacted clients maintain their VLAN ID and IP addressing after a datacenter failover. The APs, Aruba switches, and clients are assigned to a new cluster member in their existing cluster in the remaining datacenter.

Layer 3 Separated – Impacted clients are assigned a new VLAN ID and IP addressing after a datacenter failover. The APs, Aruba switches, and clients will be assigned to a secondary cluster member in the remaining datacenter.

Platform Suggestions

The following figure provides platform suggestions for the centralized cluster campus deployment scenario that supports 6,000 APs and 64,000 concurrent clients. Where appropriate a good, better, and best suggestion is made based for feature, performance, and scalability requirements. These are suggestions based on the described scenario and may be altered according to the discretion of network administrators.

Figure 151 *Centralized Cluster Campus Building Platform Suggestions*



As each building in the campus can vary in size, each one will require its own 2-tier or 3-tier hierarchical network design. Hence, switching suggestions for core, aggregation, and access layers are not provided as these selections will be unique for each building. The individual building selections should be made following the small, medium, and large suggestions highlighted in the previous sections.

Scenario 2 – Distributed Clusters

The following reference design is for a large campus such as a university with 285 buildings distributed over a 900 acre site. Each building will implement its own 2-tier or 3-tier modular network design that connects to a common campus backbone. The university has 20,000 faculty, staff, and students with IPv4 and IPv6 clients. The university has deployed 3,500 802.11ac Wave 2 APs to provide adequate coverage.

Figure 152 *Scenario 2 Campus Characteristics*

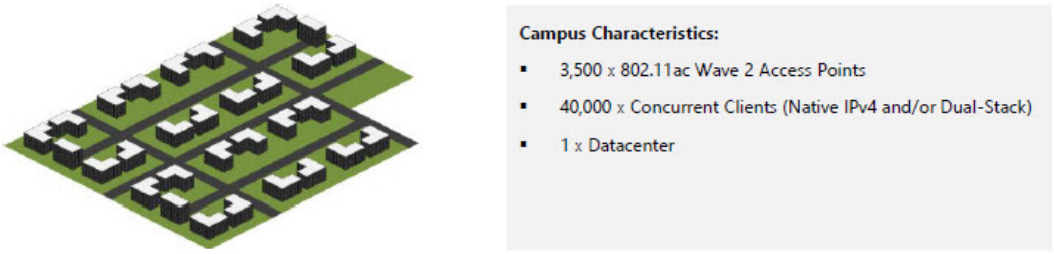
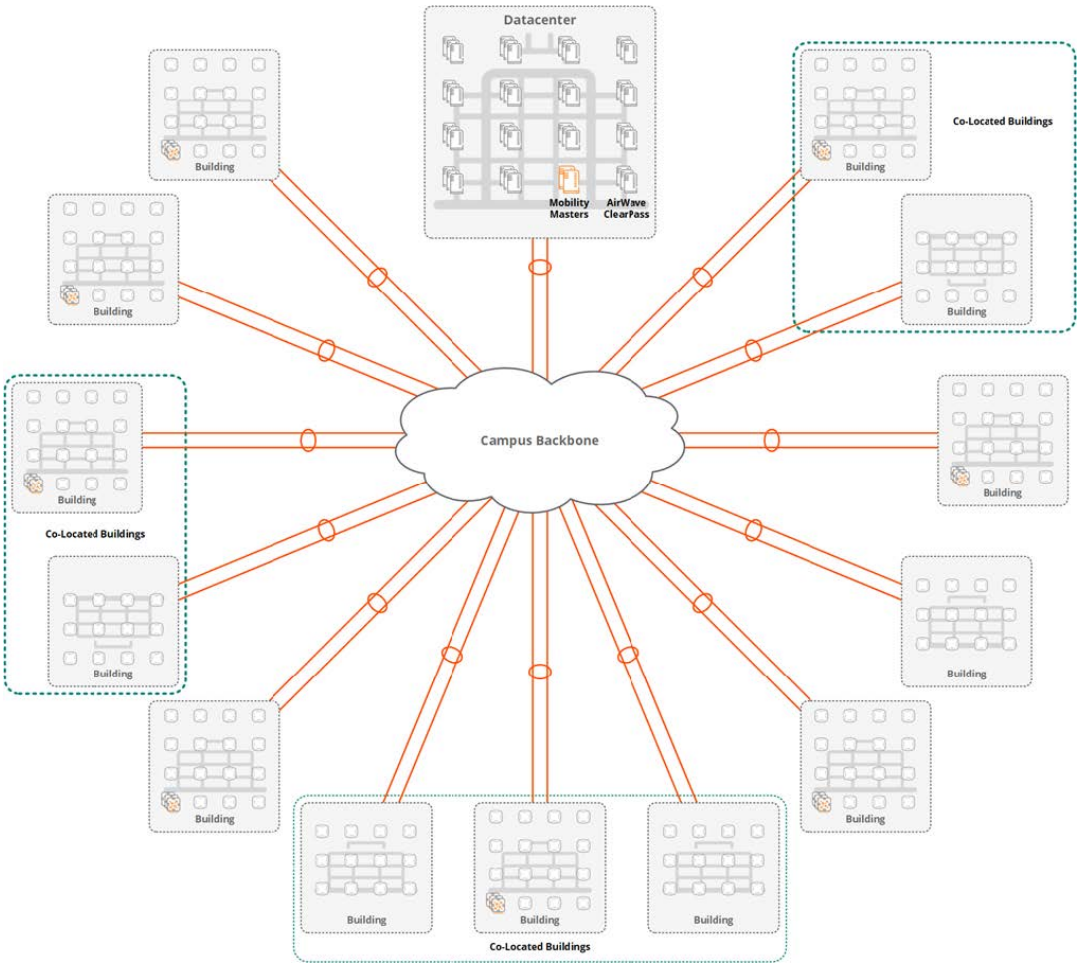


Figure 153 *Distributed Clusters Campus Architecture*



Wireless LAN Components

The campus in this scenario includes the MMs deployed in a datacenter and clusters of MCs that are distributed between buildings. The campus in this scenario includes a single datacenter, however multiple datacenters may exist in production deployments. If multiple datacenters exist, then the campus reference

architecture detailed in previous chapters provides details for the MM deployments options that can be selected for layer 2 and layer 3 datacenter deployment models.

Unlike the previous campus example, the MC clusters described in this section are distributed between individual buildings rather than deployed in the datacenter. This means that wireless and dynamically segmented traffic is terminated within the buildings rather than the datacenter. Roaming can occur only within a cluster of MCs, therefore APs in co-located buildings require overlapping coverage and are serviced by a cluster of MCs strategically deployed in one of the buildings. APs and clients in isolated buildings need to be serviced by their own cluster of MCs.

The modular network design and MC cluster placement recommendations for each building in the campus follow the same recommendations provided for the small, medium, and large office reference designs. The MC clusters connect to their respective layers depending on the size of the building. As with the previous recommendations, a wireless aggregation layer is recommended when the wireless and dynamically segmented client count exceeds 4,096.

As the building grows in size the number of APs and hosts will vary. The MC clusters are customized for each building or co-located buildings to meet the specific AP, client, and throughput requirements. For ease of deployment, troubleshooting, and repair it is recommended to standardize common models of MCs for small, medium, and large buildings. A design may include specifying two or three different controller models depending on the range of building sizes requiring support.

Table 30: *Wireless LAN Components*

Component	Description	Notes
Aruba MM (MM)	Hardware or Virtual Appliances	2 required
Aruba MCs	Hardware or Virtual Appliances	Varies
Aruba Access Points	802.11ac Wave 2 Access Points	3,500 required (distributed)
Aruba AirWave	Hardware or Virtual Appliance	Recommended
Aruba ClearPass	Hardware or Virtual Appliance	Recommended

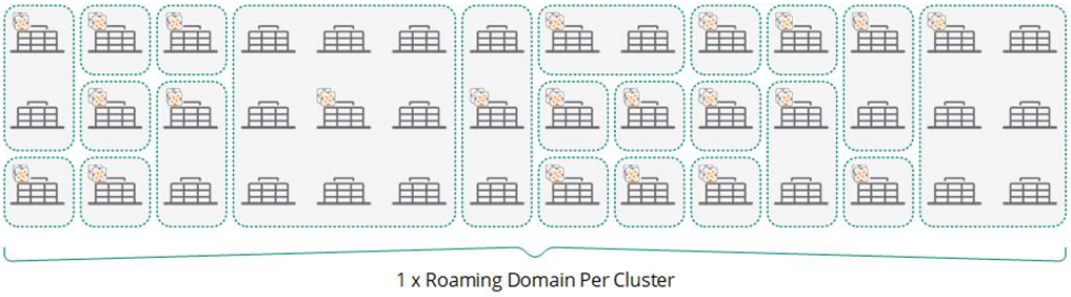
Roaming Domains

Seamless mobility is provided between APs managed by a common cluster in an ArubaOS 8 architecture. Each wireless and dynamically segmented client is assigned a primary UAC and secondary S-UAC cluster member to provide fast failover in the event of a cluster member failure or live upgrade.

This campus design includes both standalone and co-located buildings. Roaming is provided within each building as well as strategically between co-located buildings where overlapping coverage is provided. Co-located buildings provide indoor as well as outdoor coverage and enable roaming as faculty and students move between the buildings:

- Standalone Buildings – Serviced by a cluster of MCs deployed within each building. When necessary APs in small buildings are serviced by an MC cluster in a neighboring building.
- Co-Located Buildings – Serviced by a cluster of MCs strategically deployed in one of the co-located buildings. Each cluster services APs across two or more buildings.

Figure 154 *Roaming Domains*



Redundancy

For this scenario, the MMs are deployed within the datacenter and connect directly to separate datacenter aggregation switches. Redundancy within each building is provided by the modular network design and clusters of MCs. The MCs are deployed following the same recommendations provided for the small, medium, and large office reference designs:

- Aruba MM (MM):
  - Two hardware or virtual MMs
  - L2 master redundancy (Active/Standby)
- Hardware MCs (MCs):
  - Multiple clusters of hardware MCs
  - Minimum of two cluster members
- Virtual MCs (MCs):
  - Multiple clusters of virtual MCs
  - Minimum of two cluster members
- Access Points
  - AP Master pointing to the cluster's VRRP VIP address
  - Fast failover using cluster built-in redundancy

If required, additional redundancy between clusters can be achieved by implementing the backup LMS option. This will allow APs in a building to failover to an alternative designated cluster in the event of a cluster or wireless aggregation layer failure. If such an event was to occur, the APs will perform a full bootstrap to failover to the alternate cluster which will impact users. The alternate cluster and aggregation layer must also be scaled accordingly to accommodate the AP and client counts.

Scalability

The primary scalability concern for Distributed Cluster Campus scenario is MM scaling. For this campus design, the total number of APs and clients need to be accommodated in addition to the total number of MCs which are distributed between buildings. The 285 buildings in this scenario will be serviced by 180 clusters which each have a minimum of two members. Clusters in some of the larger buildings may contain three or four cluster members as required.

For this campus design, Aruba recommends implementing the MM-HW-5K or MM-VA-5K MM. Either hardware or virtual MMs can be deployed since the number of distributed MCs is a key concern. The MM selected for this design needs to scale to support 5,000 APs, 50,000 clients, and 500 MCs. This will provide adequate capacity to support the AP, client, and MC counts while providing additional room for future growth. If a specific campus design requires additional MCs, then the MM-HW-10K or MM-VA-10K MM can be selected. These MMs support up to 1,000 MCs each.

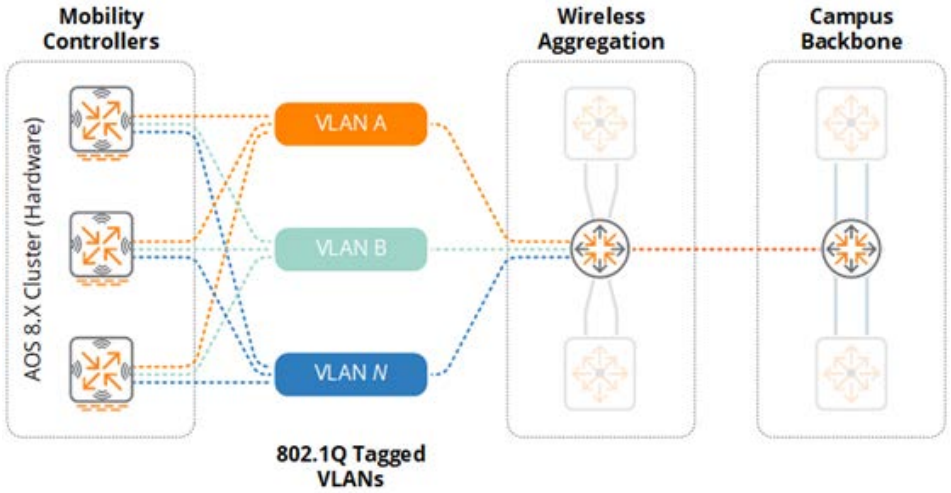
Virtual LANs

For a distributed cluster design, the building core or wireless aggregation layer terminates all the VLANs from each building's wireless module. The wireless and dynamically segmented client VLANs are extended from the MCs to their respective building switches using 802.1Q trunking.

The wireless module consists of one or more user VLANs depending on the architectural model that is implemented. For a single VLAN design, all wireless and dynamically segmented clients are assigned to a common VLAN ID with roles and policies determining the level of access each user is provided on the network. The single VLAN is extended from the respective aggregation layer switches to each physical or virtual MC cluster member. Additional VLANs can be added and extended as required. For example, a particular first design may require separate VLANs to be assigned to wireless and dynamically segmented clients for policy compliance purposes.

A minimum of two VLANs are required between the core or wireless aggregation layer switches in each building and each MC cluster member. One VLAN is dedicated for management and MM communications while the additional VLANs are mapped to clients. The VLANs are common between cluster members to permit seamless mobility within each building.

Figure 155 *Hardware MC Cluster – VLANs*



Each building may implement common VLAN IDs or unique VLAN IDs as required. Each building is layer 3 separated from the other buildings in the campus. This means that the VLAN IDs can be reused which simplifies the WLAN and dynamically segmented client deployment. However, each VLAN will require its own IPv4 and IPv6 subnet assignments.

Platform Suggestions

The distributed campus scenario requires switching and wireless components to be selected based on the specific requirements for each building. The component selection for each building should be based on the small, medium, and large suggestions highlighted in the previous sections. Each building in the campus will implement a 2-tier or 3-tier hierarchical network design with appropriate selections to meet each building's wired and wireless connectivity, performance, and redundancy requirements.

As previously mentioned, Aruba recommends standardizing on common models of MCs for the small, medium, and large buildings to simplify deployment, troubleshooting, and repair. A specific campus design may standardize on a common model of MC for all buildings or one model for each building size. The number of cluster members for each building should be adjusted to meet each building's redundancy and performance needs.

To support this distributed campus scenario, Aruba recommends the MM-VA-5K or MM-HW-5K which can scale to accommodate 5,000 Aps, 50,000 clients, and 500 MCs. The suggested MM models can meet the initial requirements to support 3,500 APs and 40,000 concurrent clients while allowing for future network scalability. If required, larger MMs such as the MM-VA-10K or MM-HW-10K are available to support larger distributed campuses. MM-VA-10K or MM-HW-10K are capable of supporting 10,000 APs, 100,000 clients, and 1,000 MCs.

Chapter 11
Migration to ArubaOS 8

Migration of Aruba deployments from ArubaOS 6 to ArubaOS 8 requires a few precautions to be taken and it is not as simple as performing a controller image upgrade. This chapter covers topics including migration methods, best practices and recommendations on when to choose a particular method over another, and also outlines how a typical ArubaOS 6 network topology can be migrated to an ArubaOS 8 topology.

There is no automatic migration from 8.x stand-alone or MC Master to ArubaOS 8 MM.

Migration Strategies

Manual Migration

Manual migration involves taking a backup from all controllers, rebuilding them by individually upgrading each one to ArubaOS 8, and performing the initial setup to convert them to MM-managed controllers or stand-alone controllers. Conversion to an MM-managed controller requires having the MM installed, configured, and ready to accept controller connections. A manual migration may also be performed by standing up an MM in parallel, building the configuration, and then moving one controller at a time.

Benefits

- ArubaOS 8 requirex new configuration elements post migration. In such cases, it may be more effective to bring up an MM in parallel to your existing ArubaOS 6 deployment and manually reconfigure elements of your WLAN to accommodate the new features.
- Manual migration allows for small, incremental changes to be performed and tested, while allowing the existing network to keep running during the migration process.
- Existing topologies may contain obsolete or deprecated features and manual migration allows for alternatives to be planned and configured accordingly.
- If the existing configuration is very complex (For example, numerous static GRE/IPsec tunnels, large mesh deployments, complex static channel plans, AP-specific settings, etc.), it may be more effective to migrate manually.

Supported Topologies

Since manual migration involves individually preparing each controller for migration, a number of migration topologies are possible. Following are the examples of topologies that can be migrated manually:

- Master-Local to MM or MC Master (MCM)
- All-Masters to MM
- Master-Branch (BOC) to MM
- Master/standby-master to stand-alone/standby-stand-alone
- Stand-alone to MM, MC Master, or stand-alone
- Migrating to a stand-alone controller

Migration Best Practice Recommendations

The following practices are recommended before the migration:

- Always backup everything in your existing topology prior to migration.
- Always test the desired migration approach in a lab environment prior to migrating the production deployments.
- While lab testing, exercise caution when testing license migration via the “My Networking Portal” (MNP). There is a limitation of three license migration.
- If Activate is used, make sure to update the ZTP settings if required, prior to migration

Migration Caveats

- Migration to ArubaOS 8 is not supported on 6000/M3, 3000, or 600 controller platforms. The prerequisite for migration is having 7000 and / or 7200 series controllers.
- The 7000 / 7200 controllers requirement for the master still applies for scenarios where only the local controllers need to be migrated and not the master. If the deployment has a master that is not from the 7000/7200 series, then either the master will need to be temporarily replaced with a 7000/7200 series controller and the devices require manual migration.
- All controllers that are being migrated should have their licenses in the same My Networking Portal account, otherwise license migration will not work.
- All controllers that are being migrated must have a controller-IP and default gateway configured.
- Deployments using custom captive portal web pages and images may have to be rebuilt after migration.
- Only the 7030 and greater controller models can run as a MC Master in MC Master mode.
- The 7024 and lower models can only be converted to MM managed, stand-alone, or MC Master managed controllers.
- In scenarios where existing master-local deployments need to be migrated to a MC Master managed deployment, the MC Master cannot terminate APs. If APs were previously terminating on the master, they will need to be accommodated either on the locals that moved under the MC Master or on a new controller.
- ArubaOS 8 does not currently have a migration path to take a stand-alone or MC Master managed controller and bring it under the MM.
- If a controller is repeatedly upgraded or downgraded between ArubaOS 6 and ArubaOS 8, subsequent migrations may fail due to temp files being created on the controller and this might cause a pre-migration check failure. If repeated upgrades or downgrades are required, the best solution is to capture a flash backup before the upgrade, then restore the backup before second or subsequent upgrades.

General Migration Requirements

Controllers

The table below provides recommendations on the minimum controller model required for ArubaOS 8 migration:

Table 31: *ArubaOS 8 Recommended Controllers*

Legacy ArubaOS 6 Controllers	APs	Clients	Minimum 7000/7200 Platform for ArubaOS 8 Migration	APs	Clients
6000/M3	512	8K	7210-7240	512-2K	16K-32K
3600	128	8K	7205	256	8K
3400	64	4K	7030	64	4K
3200	32	2K	7010	32	2K
651	16	512	7005/7008	16	1K
650	16	512	7005/7008	16	1K
620	8	256	7005/7008	16	1K

Virtual Private Network Concentrators

MCs can be configured as VPNCs to function as an IPsec termination point in the data center for controllers located in different geographical locations.

- From a topology standpoint, a VPNC is the hub with branch controllers as spokes.
- From a configuration standpoint, the VPNC acts as another MC that is managed by the MM. VPNCs are placed under their own hierarchical node on the MM containing VPNC-specific configuration.
- A VPNC may be backed up by a standby VPNC for redundancy.
- Though MCs could terminate their IPsec connections directly on the MM, (provided that the MM is built according to SKU-mandated hardware specifications) it is highly recommended to terminate the controllers on a VPNC if user traffic from any branch site needs to be routed to the data center.

Unsupported Access Points

The following APs are not supported under ArubaOS 8, as of ArubaOS 8.2.0.1:

- AP-60
- AP-65
- AP-68
- AP-70
- AP-85
- AP-120/121
- AP-124/125
- AP-92/93 (supported up to ArubaOS 8.2.00.)

Refer the latest ArubaOS release notes for the supported hardware platform list.

ArubaOS 6 Topology Migrations

This section describes common ArubaOS 6 topologies being used in production environments and provides corresponding ArubaOS 8 topology migration recommendations.

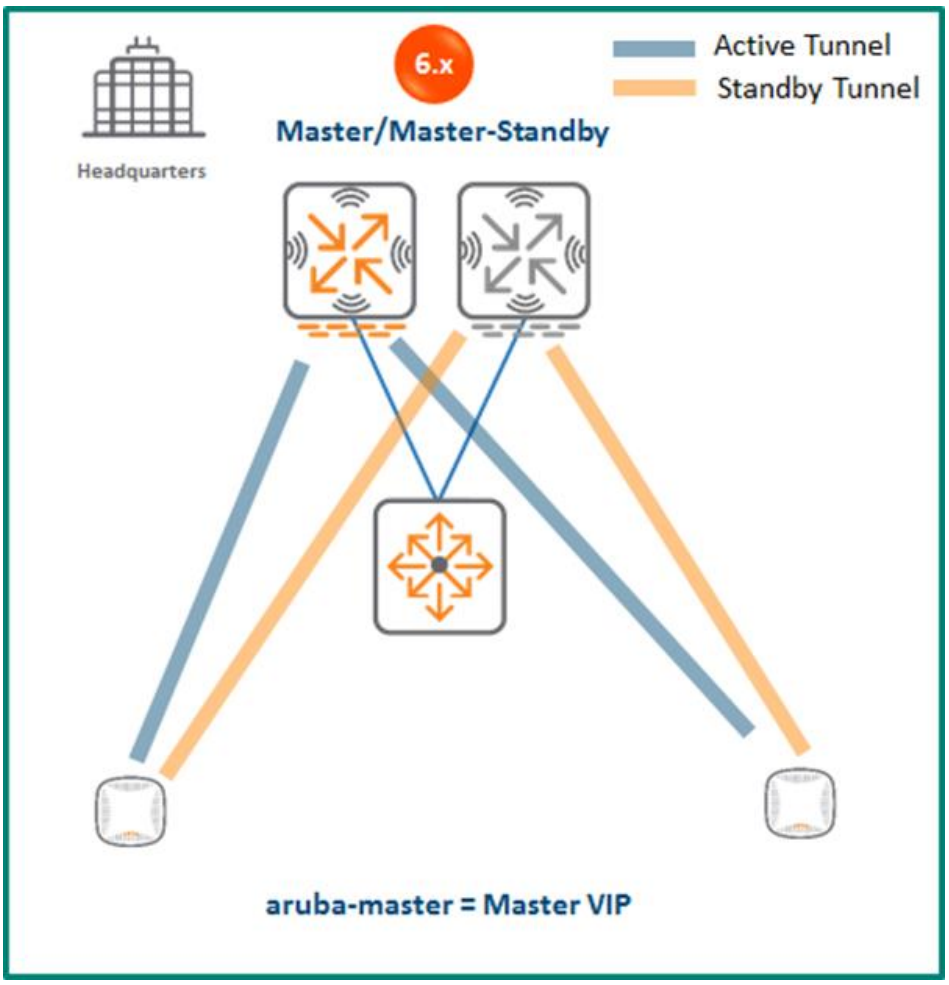
For each topology recommendation, the following details are included:

- Description
- Advantages and disadvantages
- Migration requirements
- Migration procedure (manual)

Master and Standby Master

In this ArubaOS 6 design, a master controller terminates all APs in the network. This active master is supported by a standby master using Virtual Router Redundancy Protocol (VRRP) for redundancy. High Availability (AP Fast Failover) is configured on the master and hence APs terminate their active tunnels with the active master in addition to establishing standby tunnels with the standby master.

Figure 156 *ArubaOS 6 Master/Standby Architecture*



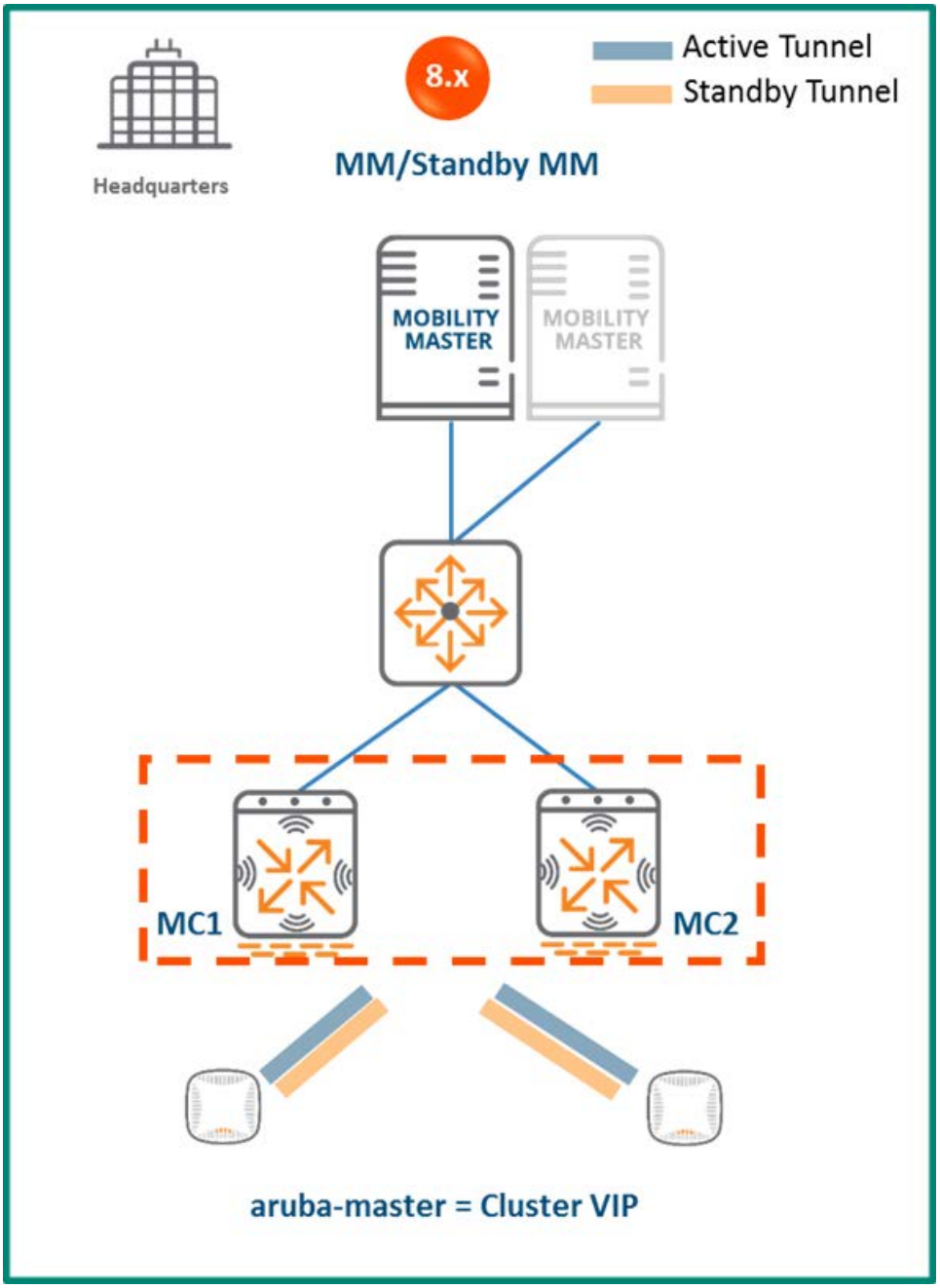
Since VRRP is used for master failure detection and the master-standby master design does not support the inter-controller heartbeat feature of AP Fast Failover, failure detection will not be sub-second. APs will wait for three missed VRRP heartbeats before being instructed by the standby master to fail over. However, the failover process will be instant and simultaneous for all APs unlike traditional VRRP failover which requires APs to re-bootstrap upon failover.

MM Terminating MCs

Topology

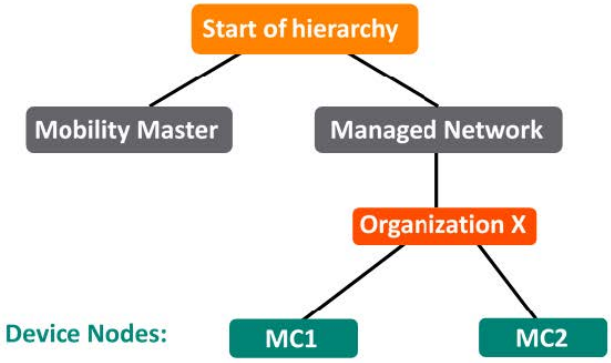
To implement this ArubaOS 8 design, first the MM must be deployed and configured. The ArubaOS 6 master and standby master controllers become MCs managed by the MM. The controllers can form a cluster for redundancy and AP and client load balancing. The controller that is elected as the cluster leader will determine how APs and clients are load balanced in the cluster.

Figure 157 *MM Terminating MCs*



Configuration Hierarchy

Figure 158 *MM Terminating MCs Configuration Hierarchy*



Design Benefits

- **Maximize benefits** - The MM terminating MCs design is ideal for fully leveraging the capabilities of ArubaOS 8.
- **Scalability** - New controllers can be easily added and managed by the MM.
- **Ease of migration** - If an existing deployment has multiple topologies, they can be migrated under the MM into their own nodes in the hierarchy.
- **Management** - Centralized configuration and management of controllers.
- **Hierarchical configuration model** - Configuration is performed on nodes (logical folders such as USA, West Coast, California, Santa Clara, etc.) and each controller is assigned to a particular node depending on location and context.
- **Clustering** - Having controllers in a cluster enables seamless client failover between controllers with no impact to user experience. The clustering feature also facilitates client roaming as well as AP and client load balancing. Clustering is required to support live upgrades.
- **Live Upgrade** - Upgrade a cluster of controllers in real time without end users experiencing any loss of connectivity or performance. There is no need for scheduling maintenance cycles for network upgrade.
- **AirMatch** - RF intelligence is centralized on the MM which significantly improves the RF management and interference mitigation capabilities of the WLAN.
- **REST API support**
- **Multi-version support** - Flexibility of upgrading individual controllers to test out new features or bug fixes. Controllers in a cluster need to run the same ArubaOS software version and may be upgraded together.
- **In-service software module upgrades** - Loadable Service Modules (LSMs) such as UCC, AirGroup, AppRF can be updated during runtime removing the need to schedule any maintenance cycles.

Design Caveats

The MM does not terminate APs. APs can only be terminated on a MC.

Migration Requirements

- Migration requires purchase of virtual MM capacity licenses or a hardware MM (and optionally a backup hardware MM).
- If a backup MM is available, then the licenses on each MM will be aggregated and synchronized across the network.
- Other licenses such as AP and PEF need to be migrated manually or via the My Networking Portal

Migration Options

- Manual migration steps are detailed below.

Migration Strategy

Existing ArubaOS 6 Deployment

- Active and standby master
- APs terminating on the active master with standby master as backup

New ArubaOS 8 Deployment

- MM managing controllers MC1 and MC2
- APs terminating on MC1 and MC2

Migration Procedure

Manual migration requires a complete rebuild of the existing ArubaOS 6 topology from by going through the following steps:

1. Deploy the MM and perform initial setup.
2. Configure licensing on the MM.
3. Create a configuration hierarchy on MM and whitelist the active and standby master MAC addresses.
4. Repeat step 1 if a backup MM is being installed as well.
5. Configure MM redundancy if a backup MM has been installed. The MM VIP will be used for configuration management.
6. Configure clustering between the controllers and enable AP load balancing.
7. Create a VIP between the cluster member IPs and optionally create VIPs for RADIUS COA.
8. Create an AP group by navigating to **Managed Network > (select node) > AP Groups.**
9. Create a new SSID by navigating to **Managed Network > (select node) > Tasks > Create a new WLAN.**
10. Whitelist the APs on the MM by populating the CPSec whitelist table (including mapping the APs to the appropriate AP group) by navigating to **Managed Network > (select node) > Configuration > Access Points > Whitelist.**
11. Back up the existing configuration on the ArubaOS 6 master controllers by navigating to **Maintenance > Backup Flash.**
12. Upgrade the image on the active master to ArubaOS 8 and reboot it by navigating to **Maintenance > Image Management.**
13. Provision the master to be managed by MM via the CLI setup dialog. The master will now become MC1.
14. Repeat steps 11-12 to convert the standby master to ArubaOS 8 as MC2.
15. Change **aruba-master** to point to the cluster VIP.

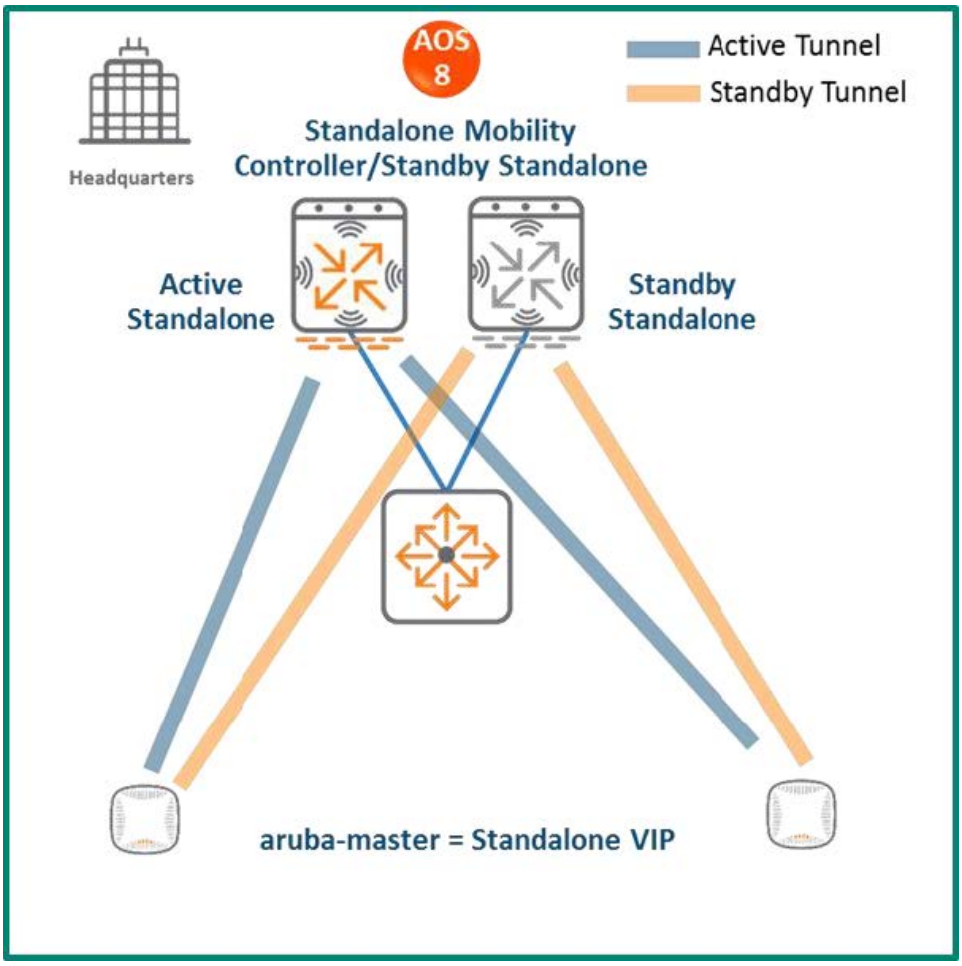
16. The APs that were previously terminating on the master will find the cluster VIP, upgrade their images, terminate on MC1 or MC2 (depending on how the cluster leader load balances the APs), and broadcast the configured SSID.
17. Connect a wireless client to the SSID to test connectivity.
18. Optionally, test seamless client failover by running a voice/video application and disconnecting the user's active controller.

Stand-alone MC and Standby Stand-alone

Topology

This ArubaOS 8 design consists of a stand-alone MC backed up by another stand-alone MC. As in the Master and Standby Master ArubaOS 6 design, VRRP is used between the two stand-alone controllers in an active-standby configuration. Similarly, High Availability (AP Fast Failover) is configured between the controllers so that APs terminate their tunnels on the active stand-alone controller in addition to setting up a standby tunnel to the standby stand-alone controller.

Figure 159 *Stand-alone MC and Standby Stand-alone Topology*



In this topology, there is no configuration or database synchronization between the two stand-alone controllers. The VRRP VIP is used for master discovery. However, the AP Fast Failover detection is sub-second (HA standby detects the failure and instructs the AP to fail over). The HA standby stand-alone becomes the HA active controller.

Design Benefits

- No additional hardware is required for migration
- Multi-threaded CLI
- Auto-completion of profile names

Design Caveats

- Identical WLAN configuration across the two stand-alone controllers (roles, ACLs, SSID, VAP and AAA profiles), as well as VLANs
- Identical CPSec whitelists across the two stand-alone controllers

Migration Requirements

Licenses such as AP and PEF need to be migrated manually or via the My Networking Portal

Migration Options

Migration can only be performed manually.

Migration Strategy

Existing ArubaOS 6 Deployment

- Active and standby master
- APs terminating on the active master with standby master as backup

New ArubaOS 8 Deployment

- Active stand-alone and standby stand-alone controllers
- APs with the active and standby tunnels terminating on the active and standby controllers respectively

Migration Procedure

Manual migration requires a complete rebuild of the existing ArubaOS 6 topology.

1. Backup the existing configuration on the ArubaOS 6 masters.
2. Upgrade the image on the active master to ArubaOS 8 and reboot the controller.
3. Provision the active master as an ArubaOS 8 stand-alone controller via the CLI setup dialog. The master will now become an ArubaOS 8 stand-alone controller.
4. Repeat steps 2-3 to convert the standby master into an ArubaOS 8 stand-alone controller.
5. Configure licensing on the active and standby stand-alone controllers, as there is no database synchronization between the two stand-alone controllers. The use of a centralized licensing server is recommended.
6. Configure VRRP between the two stand-alone controllers. A VIP will be created between MC1 and MC2 as a result of the VRRP configuration and after which the VIP is used for master discovery.
7. Create identical WLAN configuration on each stand-alone controller.
8. Ensure that CPSec whitelists are identical on both stand-alone controllers.
9. Configure AP Fast Failover for both stand-alone controllers under /mm/mynode.
10. Change **aruba-master** to point to the stand-alone VIP
11. The APs will then find the VIP (i.e. active stand-alone controller), upgrade their images, terminate their tunnels on the active stand-alone, and broadcast the configured SSID.
12. Connect a wireless client to the SSID and test connectivity.
13. Optionally, test client failover by disconnecting the active stand-alone controller.

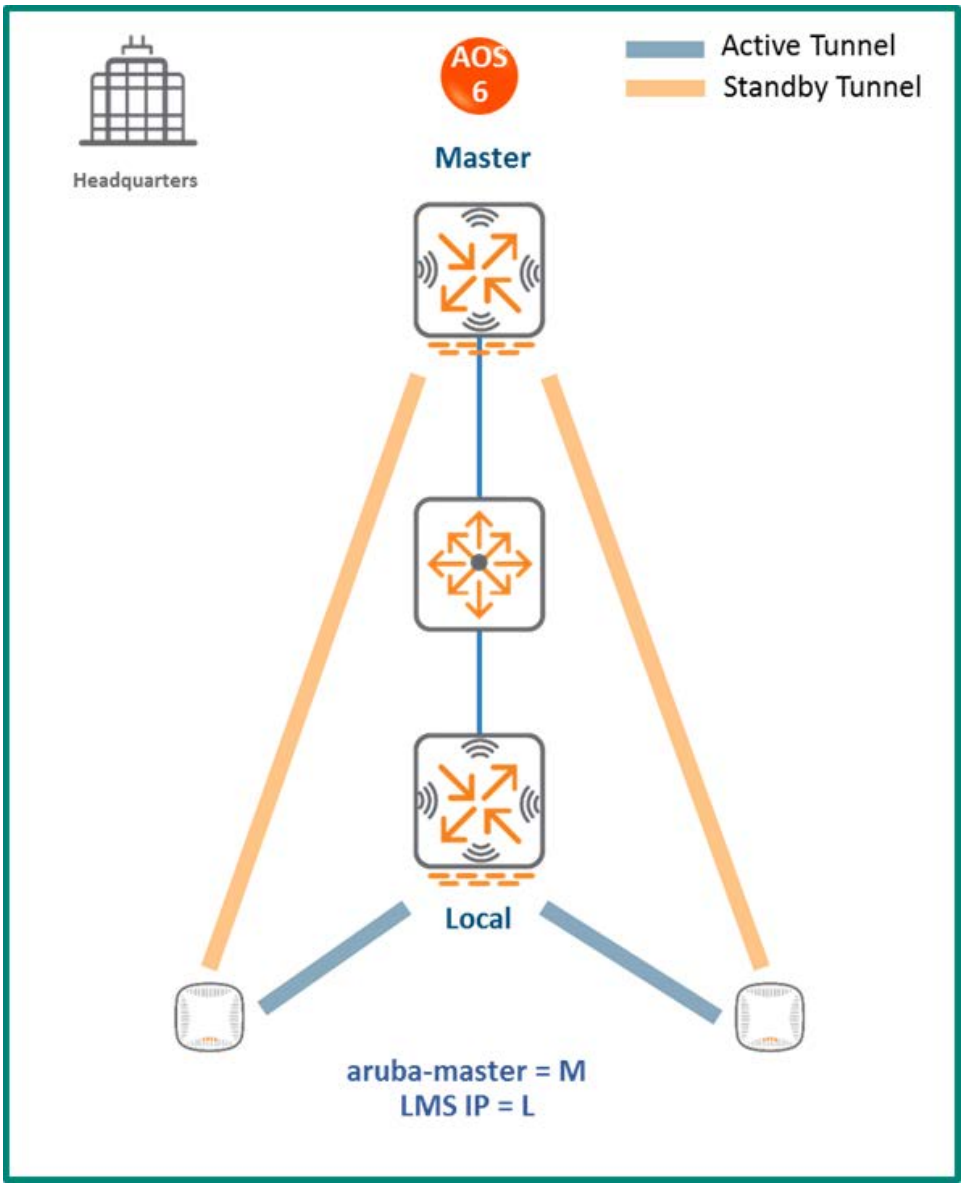
Master and Single Local

In this ArubaOS 6 design, a master controller managed the local controller. The same controller models are recommended for the master and local. Following are the two variations of this design:

Redundancy Model (also known as an Active-Standby model) - APs terminate on the local controller and the master provides redundancy for the local. High Availability (AP Fast Failover) is configured between the controllers so that when the APs lose connectivity to the local controller, they can instantly failover to the master.

Capacity Model (also known as an Active-Active model) - This is an alternative single-master, single-local design where the master, in addition to managing the local, also shares the AP load with the local. High Availability (AP Fast Failover) is configured between the controllers such that when one controller goes down, its APs can seamlessly failover to the other controller.

Figure 160 *Master and Single Local*



In both designs:

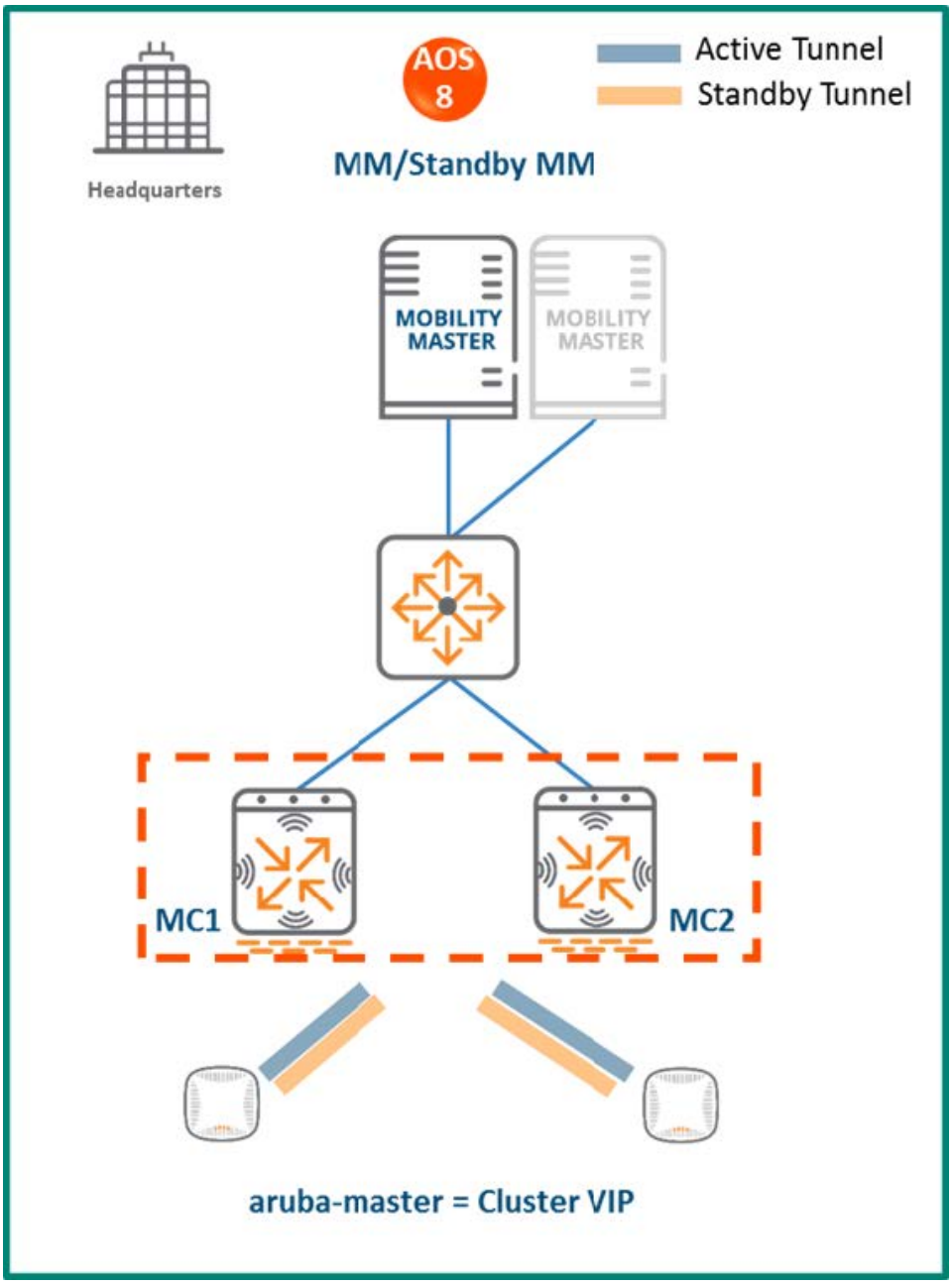
- Each controller needs to have enough capacity to accommodate the number of APs that could potentially failover from the second controller. In the redundancy model, each controller typically terminates APs at up to 80% of the controller capacity. In the capacity model, each controller typically terminates APs at up to 40% of the controller capacity.
- The AP Fast Failover detection is not sub-second (APs will wait for eight missed heartbeats to the master) however the failover itself occurs quickly since all the APs already have standby tunnels built to the standby stand-alone controller. The standby stand-alone controller becomes the new active controller upon failover.

MM Terminating MCs

Topology

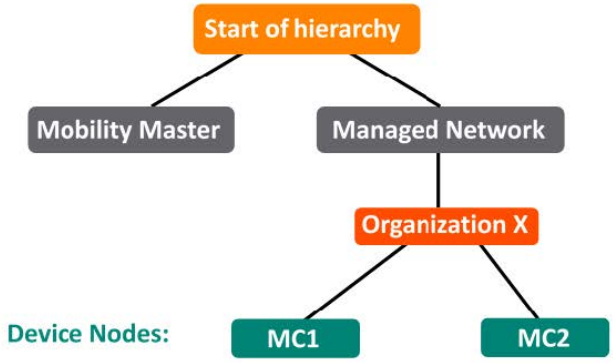
In this ArubaOS 8 design, an MM is initially deployed and configured. The ArubaOS 6 master and local controllers become MCs managed by the MM. The controllers can form a cluster for redundancy and AP/client load balancing purposes. The controller that is elected as the cluster leader will decide how APs and clients are load balanced in the cluster.

Figure 161 *MM Terminating MCs Topology*



Configuration Hierarchy

Figure 162 *MM Terminating MCs Configuration Hierarchy*



Design Benefits

- **Maximize benefits** - The MM terminating MCs design is ideal for fully leveraging the capabilities of ArubaOS 8.
- **Scalability** - New controllers can be easily added and managed by the MM.
- **Ease of migration** - If an existing deployment has multiple topologies, they can be migrated under the MM into their own nodes in the hierarchy.
- **Management** - Centralized configuration and management of controllers.
- **Hierarchical configuration model** - Configuration is performed on nodes (logical folders such as USA, West Coast, California, Santa Clara, etc.) and each controller is assigned to a particular node depending on location and context.
- **Clustering** - Having controllers in a cluster enables seamless client failover between controllers with no impact to user experience. The clustering feature also facilitates client roaming as well as AP and client load balancing. Clustering is required to support live upgrades.
- **Live Upgrade** - Upgrade a cluster of controllers in real time without end users experiencing any loss of connectivity or performance. There is no need for scheduling maintenance cycles for network upgrade.
- **AirMatch** - RF intelligence is centralized on the MM which significantly improves the RF management and interference mitigation capabilities of the WLAN.
- **REST API support**
- **Multi-version support** - Flexibility of upgrading individual controllers to test out new features or bug fixes. Controllers in a cluster need to run the same ArubaOS software version and may be upgraded together.
- **In-service software module upgrades** - Loadable Service Modules (LSMs) such as UCC, AirGroup, AppRF can be updated during runtime removing the need to schedule any maintenance cycles.

Design Caveats

The MM does not terminate APs. APs can only be terminated on a MC.

Migration Requirements

- Migration requires the purchase of virtual MM capacity licenses or the purchase of a hardware MM (and optionally a backup hardware MM)
- If a backup MM is available, then the licenses on each MM will be aggregated and synchronized across both the MMs.
- Other licenses such as AP and PEF need to be migrated manually or via the My Networking Portal

Migration Options

- Manual migration steps are detailed below.

Migration Strategy

Existing ArubaOS 6 Deployment

- Master and local
- APs terminating on the local with master as backup

New ArubaOS 8 Deployment

- MM backed up by a standby MM
- MM managing controllers MC1 and MC2
- APs terminating on MC1 and MC2

Migration Procedure

Manual migration requires a complete rebuild of the existing ArubaOS 6 topology from by going through the following steps:

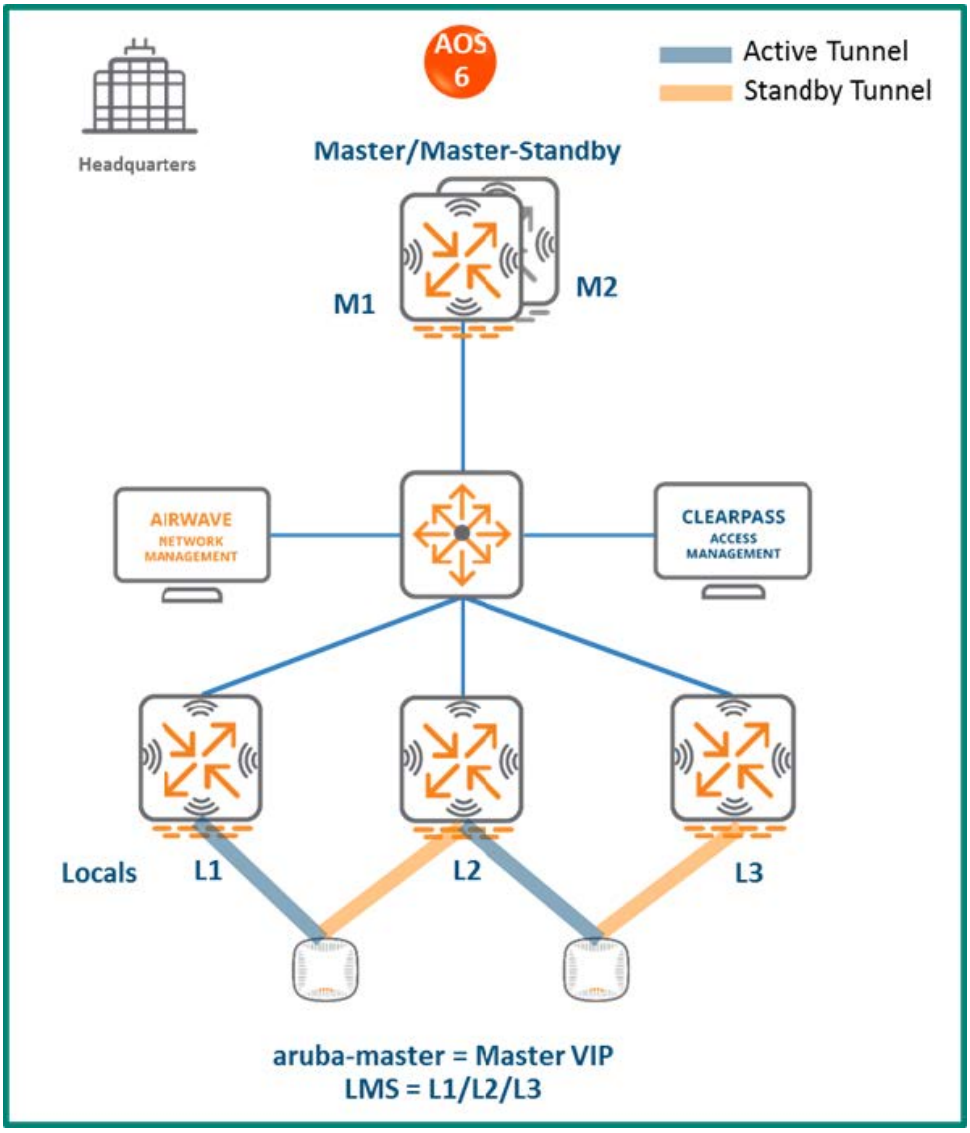
1. Deploy the MM and perform initial setup
2. Configure licensing on the MM.
3. Create a configuration hierarchy on MM and whitelist the active and standby master MAC addresses.
4. Repeat step 1 if a backup MM is being installed.
5. Configure MM redundancy if a backup MM has been installed and the MM VIP will be used for configuration management.
6. Configure clustering between the controllers and enable AP load balancing.
7. Create a VIP between the cluster member IPs and optionally create VIPs for RADIUS COA.
8. Create an AP group by navigating to **Managed Network > (select node) > AP Groups.**
9. Create a new SSID by navigating to **Managed Network > (select node) > Tasks > Create a new WLAN.**
10. Whitelist the APs on the MM by populating the CPSec whitelist table (including mapping the APs to the appropriate AP group) by navigating to **Managed Network > (select node) > Configuration > Access Points > Whitelist.**
11. Back up the existing configuration on the ArubaOS 6 master controllers by navigating to **Maintenance > Backup Flash.**
12. Upgrade the image on the active master to ArubaOS 8 and reboot it by navigating to **Maintenance > Image Management.**
13. Provision the master to be managed by MM via the CLI setup dialog. The master will now become MC1.
14. Repeat steps 11-12 to convert the standby master to ArubaOS 8 as MC2.
15. Change aruba-master to point to the cluster VIP.
16. The APs that were previously terminating on the master will find the cluster VIP, upgrade their images, terminate on MC1 or MC2 (depending on how the cluster leader load balances the APs), and broadcast the configured SSID.

17. Connect a wireless client to the SSID to test connectivity.
18. Optionally, test seamless client failover by running a voice/video application and disconnecting the user's active controller.

Master and Multiple Locals (Single Campus)

In this ArubaOS 6 design, a master (backed up by a standby master) controller manages a group of local controllers. APs terminate on one of the local controllers with the other locals acting as backup controllers. AP Fast Failover is configured to provide sub-second failover for the APs when connectivity to their primary controller is lost.

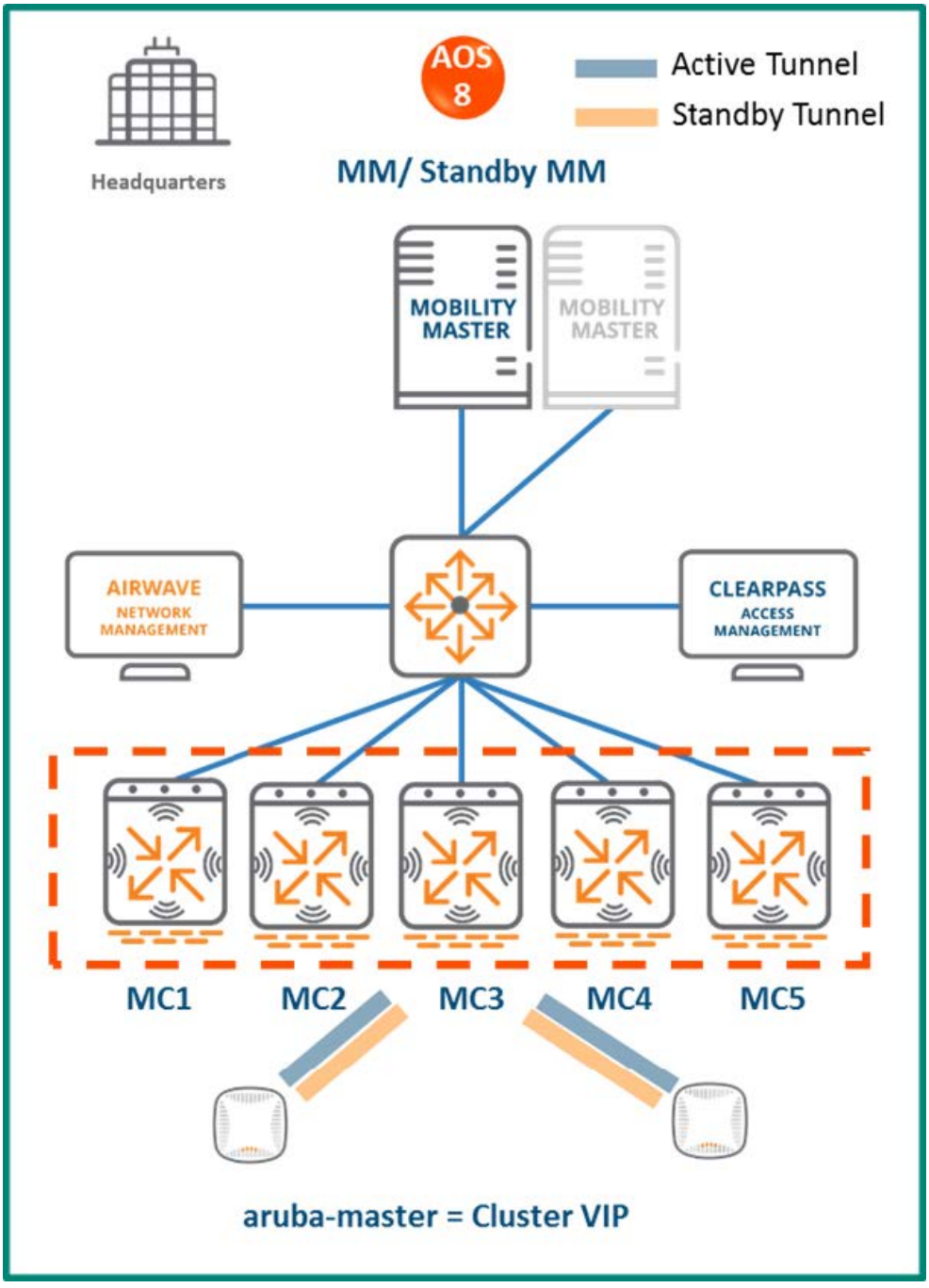
Figure 163 *Master Controller and Multiple Locals*



MM Terminating MCs

Topology

Figure 164 *MM Terminating MCs Topology*



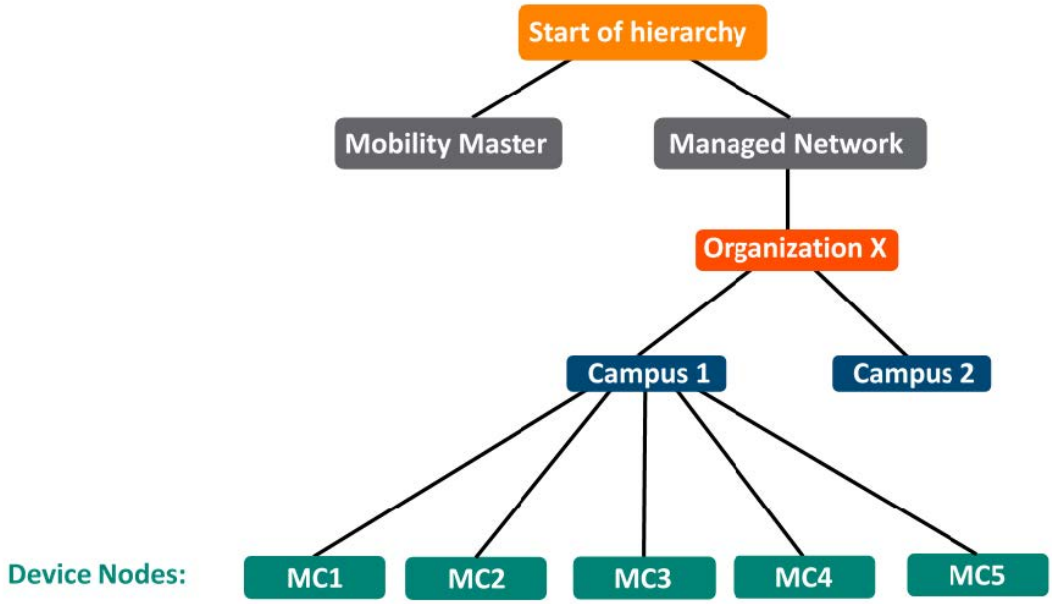
In this ArubaOS 8 design:

- An MM (either virtual or hardware) is deployed and configured along with a backup MM.
- Each ArubaOS 6 local controller (L1, L2, and L3) becomes an ArubaOS 8 MC (MC1, MC2, MC3).
- The ArubaOS 6 master (M1) and standby master (M2) become two additional ArubaOS 8 MCs (MC4 and MC5).

- The MCs can be part of a cluster and share the AP and client load.
- If the locals were geographically separated from each other, then post migration the APs terminating on L1, L2, and L3 will now terminate on MC1, MC2 and MC3 respectively.
- If all the locals were part of a large campus, then the cluster leader will distribute the AP and client load among MC1-MC5.

Configuration Hierarchy

Figure 165 *MM Terminating MCs Configuration Hierarchy*



Design Benefits

- **Maximize benefits** - The MM terminating MCs design is ideal for fully leveraging the capabilities of ArubaOS 8.
- **Scalability** - New controllers can be easily added and managed by the MM.
- **Ease of migration** - If an existing deployment has multiple topologies, they can be migrated under the MM into their own nodes in the hierarchy.
- **Management** - Centralized configuration and management of controllers.
- **Hierarchical configuration model** - Configuration is performed on nodes (logical folders such as USA, West Coast, California, Santa Clara, etc.) and each controller is assigned to a particular node depending on location and context.
- **Clustering** - Having controllers in a cluster enables seamless client failover between controllers with no impact to user experience. The clustering feature also facilitates client roaming as well as AP and client load balancing. Clustering is required to support live upgrades.
- **Live Upgrade** - Upgrade a cluster of controllers in real time without end users experiencing any loss of connectivity or performance. There is no need for scheduling maintenance cycles for network upgrade.
- **AirMatch** - RF intelligence is centralized on the MM which significantly improves the RF management and interference mitigation capabilities of the WLAN.
- **REST API support**

- **Multi-version support** - Flexibility of upgrading individual controllers to test out new features or bug fixes. Controllers in a cluster need to run the same ArubaOS software version and may be upgraded together.
- **In-service software module upgrades** - Loadable Service Modules (LSMs) such as UCC, AirGroup, AppRF can be updated during runtime removing the need to schedule any maintenance cycles.

Migration Requirements

- Requires purchase of virtual MM capacity licenses or a hardware MM (and optionally a backup hardware MM).
- If you have a backup MM, then the licenses on each MM will be aggregated and synchronized across both MMs.
- Other licenses such as AP and PEF need to be migrated manually or via the My Networking Portal

Migration Options

- Manual migration steps are detailed below.

Migration Strategy

Existing ArubaOS 6 Deployment

- Locals L1, L2, and L3 and masters M1and M2
- 3 AP groups are configured to have groups of APs terminate on each of L1, L2 and L3.

New ArubaOS 8 Deployment

- MM backed up by a standby MM
- MM managing MC1, MC2, MC3, MC4, and MC5
- APs terminating on:
  - MC1, MC2, MC3 for a multi-site campus, with a controller in each site
  - The cluster VIP for a large campus

Migration Procedure

Manual migration requires a complete rebuild of the existing ArubaOS 6 topology by performing the steps listed below. These steps cover termination of APs on a cluster VIP. In case of a multi-site campus, the APs could terminate on one of three local management switch (LMS) IPs (MC1, MC2, or MC3).

1. Deploy the MM and perform initial setup.
2. Configure licensing on the MM.
3. Create a configuration hierarchy on MM and whitelist the active and standby master MAC addresses.
4. Repeat step 1 if a backup MM is being installed.
5. Configure MM redundancy if a backup MM has been installed. Going forward, the MM VIP will be used for configuration management.
6. Configure clustering between the controllers and enable AP load balancing.
7. Create a VIP between the cluster member IPs and optionally create VIPs for RADIUS COA.
8. Create an AP group by navigating to **Managed Network > (select node) > AP Groups.**
9. Create a new SSID by navigating to **Managed Network > (select node) > Tasks > Create a new WLAN.**
10. Whitelist the APs on the MM by populating the CPSec whitelist table (including mapping the APs to the appropriate AP group) by navigating to **Managed Network > (select node) > Configuration > Access Points > Whitelist.**

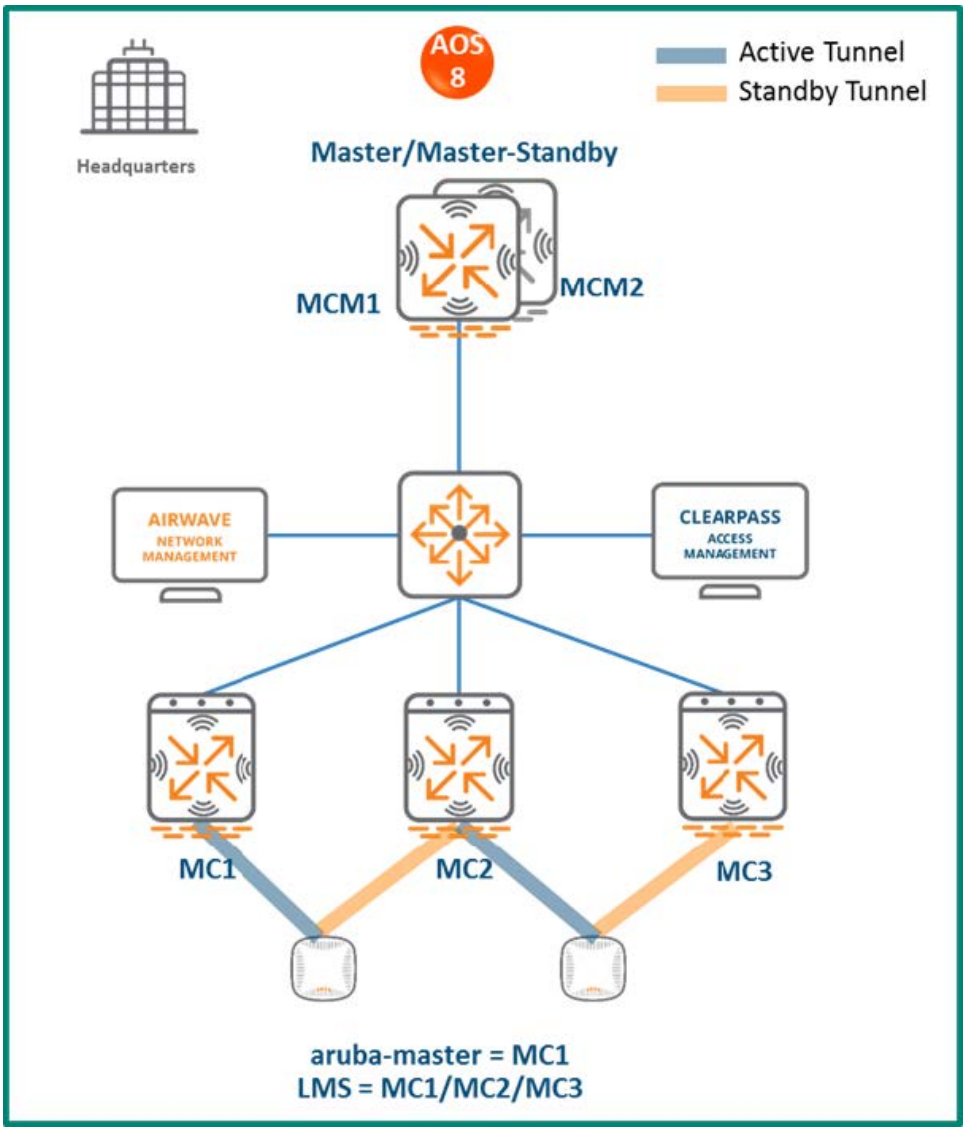
11. Back up the existing configuration on the ArubaOS 6 master controllers. by navigating to **Maintenance > Backup Flash.**
12. Upgrade the image on the active master to ArubaOS 8 and reboot it by navigating to **Maintenance > Image Management.**
13. Provision Local L1 master to be managed by MM via the CLI setup dialog. The master will now become MC1.
14. Repeat steps 11-12 to convert the standby master to ArubaOS 8 as MC2.
15. Repeat steps 11-12 to convert M1 and M2 to MC4 and MC5. These controllers can be added to the cluster to share the AP and client load between cluster members
16. Change **aruba-master** to point to the cluster VIP.
17. The APs that were previously terminating on the master will find the cluster VIP, upgrade their images, terminate on MC1 or MC2 (depending on how the cluster leader load balances the APs), and broadcast the configured SSID.
18. Connect a wireless client to the SSID to test connectivity.
19. Optionally, test seamless client failover by running a voice/video application and disconnecting the user's active controller.

MC Master Terminating MCs

Topology

This ArubaOS 8 design consists of a hardware controller deployed as a MC Master (optionally backed up by another MC Master) that manages a group of MCs.

Figure 166 *MC Master Terminating MCs Topology*



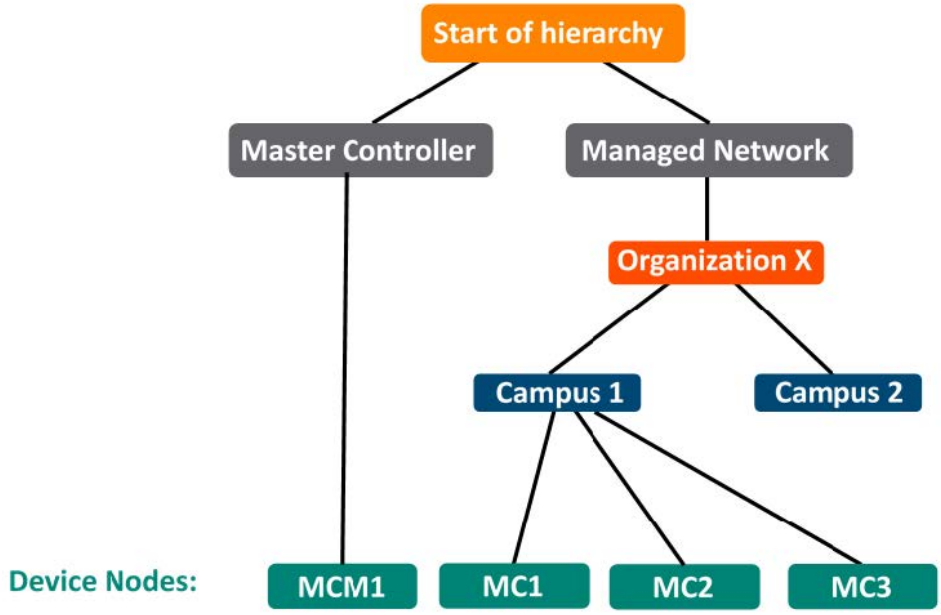
This design helps transitioning deployments to ArubaOS 8 that are unable to deploy an MM. This MC Master topology should eventually be migrated to an MM topology in order to take full advantage of the capabilities offered by ArubaOS 8.

In this design:

- The ArubaOS 6 master (M1) and standby master (M2) become ArubaOS 8 MC Masters (MCM1 and MCM2).
- The ArubaOS 6 local controllers (L1, L2 and L3) become ArubaOS 8 MCs (MC1, MC2 and MC3).
- APs terminating on L1, L2, and L3 will now terminate on MC1, MC2, and MC3 respectively.

Configuration Hierarchy

Figure 167 *MC Master Terminating Mobility Configuration Hierarchy*



Design Benefits

- A similar topology is maintained in which the MC Master manages the MCs and no additional hardware is required as long as the MC Master is an Aruba 7030 or larger controller.
- The hierarchical configuration model offers fully centralized configuration and management of the WLAN.
- Additional controllers could be added later and managed by the MC Master.

Design Caveats

- Requires purchase of an Aruba 7030 or larger controller to serve as the MC Master and a backup MCM if one is not already present.
- AP termination on the MC Master is not supported. This has the following impact on AP termination options:
  - Any APs that are terminating on the master in ArubaOS 6 would need to be redistributed among the locals prior to migration. The locals should have enough capacity to accommodate the additional APs
  - APs can failover between MCs but cannot failover to the MC Master.
- The clustering feature is not supported in a MC Master deployment. AP Fast Failover between MCs is the only controller redundancy option.
- AirMatch is not supported.
- All controllers in the topology must run the same ArubaOS version.
- No centralized monitoring

Migration Requirements

- Verify that the ArubaOS 6 master controller meets the MC Master hardware requirements (Aruba 7030 or any Aruba 7200 series controller).
- Ensure that the ArubaOS 6 master is not terminating any APs as an ArubaOS 8 MC Master does not support

AP termination.

- Ensure that AP, PEF, and all other licenses have been migrated manually or via the My Networking Portal.

Migration Options

- Manual migration steps are detailed below.

Migration Strategy

Existing ArubaOS 6 Deployment

- Locals L1, L2, L3 and masters M1 and M2
- 3 AP groups are configured for termination on L1, L2, and L3

New ArubaOS 8 Deployment

- MCM1 backed up by MCM2
- MCM1 managing MC1, MC2, and MC3

Migration Procedure

Manual migration requires a complete rebuild of the existing ArubaOS 6 topology by performing the steps listed below:

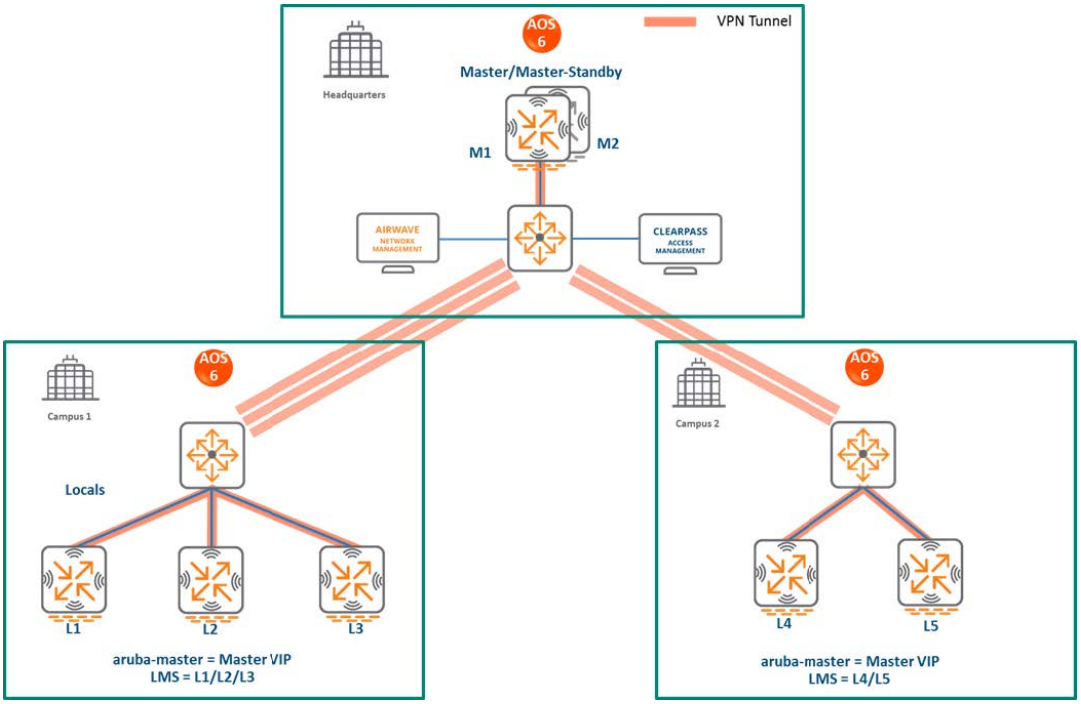
1. Back up the existing configuration on the ArubaOS 6 masters and locals by navigating to **Maintenance > Backup Flash.**
2. Upgrade the image on master M1 to ArubaOS 8 and reboot the controller.
3. Provision M1 as a MC Master through the CLI setup dialog. M1 will now become MCM1.
4. Repeat steps 2 and 3 to convert M2 to MCM2.
5. Configure master redundancy between MCM1 and MCM2. The MC Master VIP will be used for configuration.
6. Configure licensing on the MC Master.
7. Create a configuration hierarchy on the MC Master and whitelist the MAC addresses of controllers L1-L3.
8. Create three AP groups under **/md** (or a child node), each with the LMS IP of MC1, MC2, and MC3 respectively by navigating to **Managed Network > (select node) > AP Groups.**
9. Create an SSID for each AP group by navigating to **Managed Network > (select node) > Tasks > Create a new WLAN.**
10. Whitelist the APs on the MC Master. This includes mapping them to their respective AP groups by navigating to **Managed Network > (select node) > Configuration > Access Points > Whitelist.**
11. Upgrade the image on local L1 to ArubaOS 8 and reboot it by navigating to **Maintenance > Image Management.**
12. Provision local L1 to be managed by the MC Master via the CLI setup dialog. L1 will become MC1
13. Now repeat steps 11-12 for L2 and L3 to convert them to ArubaOS 8 MC2 and MC3
14. Change **aruba-master** to MC1's IP.
15. Once MC1 is visible on the MC Master, the APs that were terminating on L1 will find MC1, upgrade their images, download the LMS-IP for MC1, terminate their tunnels on MC1, and broadcast the configured SSID.
16. Similarly, the APs on L2 and L3 will show up on MC2 and MC3, respectively.
17. Connect a wireless client to the SSID and test connectivity.
18. Optionally, configure AP Fast Failover via the MC Master to enable sub-second AP failover between the MCs.

Master and Multiple Locals (Multiple Campuses)

In this ArubaOS 6 design, a master controller backed up by a standby master manages a group of local controllers. APs terminate on one of the local controllers with the other locals acting as backups. AP Fast

Failover is configured to provide sub-second failover for the APs when connectivity to their primary controller is lost.

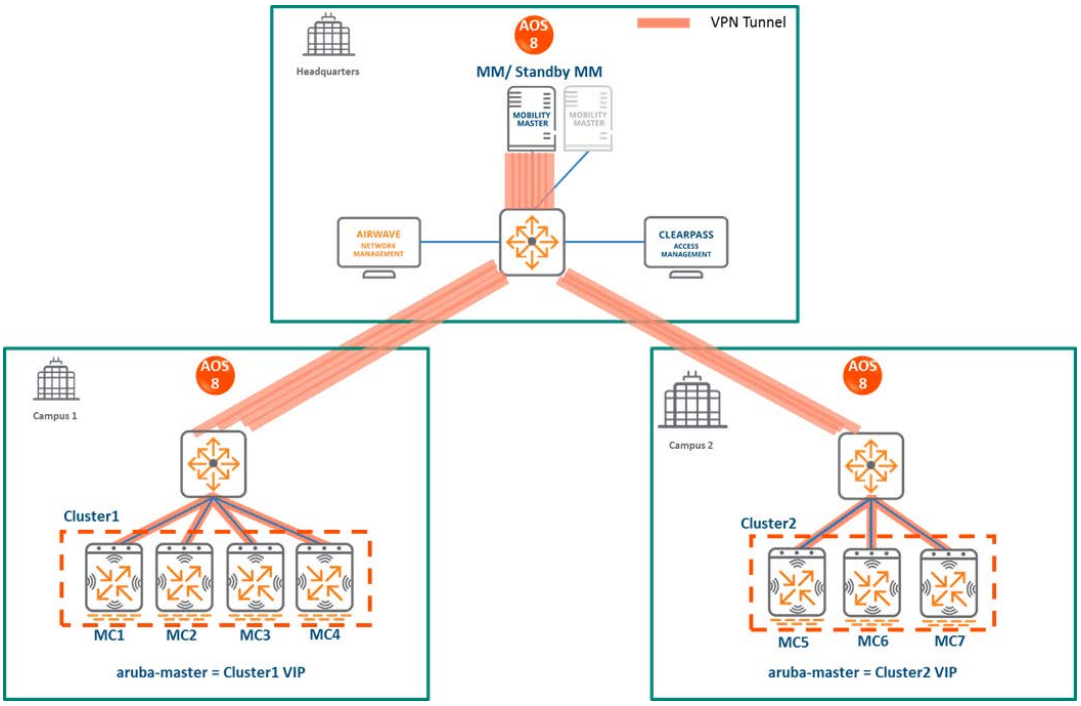
Figure 168 *Master and Multiple Locals (Multiple Campuses)*



MM Terminating MCs

Topology

Figure 169 *MM Terminating MCs Topology*

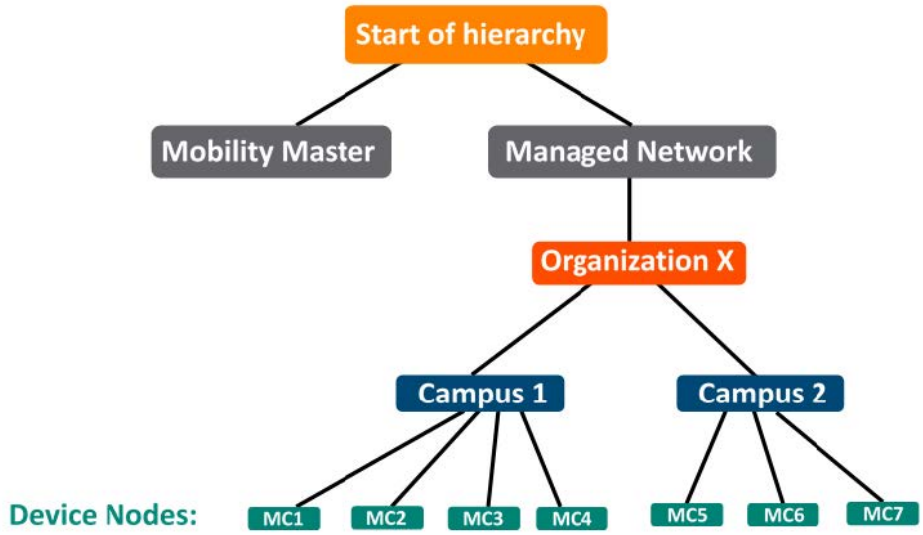


In this ArubaOS 8 design:

- The MM (either virtual or hardware) is deployed and configured along with a backup MM.
- In Campus 1, each ArubaOS 6 local controller (L1, L2, and L3) becomes an ArubaOS 8 MC (MC1, MC2, MC3).
- In Campus 2, each ArubaOS 6 local controller (L4 and L5) becomes an ArubaOS 8 MC (MC5 and MC6).
- The MCs in each campus are configured as a cluster and will share the AP and client load.
- All MCs terminate their IPsec tunnels on the MM.
- If the locals were geographically separated from each other, then the migration is performed so that APs terminating on L1, L2, and L3 will now terminate on MC1, MC2 and MC3 respectively.
- If all the locals in each campus are co-located, then post migration the cluster leader will distribute the AP and client load among the cluster members.
- The ArubaOS 6 master (M1) and standby master (M2) become two additional ArubaOS 8 MCs (MC4 and MC7) which can be repurposed to become cluster members in each campus.
- For remote sites that are separated from the MM via MPLS and/or internet links, if user traffic needs to be routed to access HQ resources then it is recommended to deploy a hardware VPNC at HQ to terminate IPsec connections from the controllers in each site.

Configuration Hierarchy

Figure 170 *MM Terminating MCs Configuration Hierarchy*



Design Benefits

- **Maximize benefits** - The MM terminating MCs design is ideal for fully leveraging the capabilities of ArubaOS 8.
- **Scalability** - New controllers can be easily added and managed by the MM.
- **Ease of migration** - If an existing deployment has multiple topologies, they can be migrated under the MM into their own nodes in the hierarchy.
- **Management** - Centralized configuration and management of controllers.
- **Hierarchical configuration model** - Configuration is performed on nodes (logical folders such as USA, West Coast, California, Santa Clara, etc.) and each controller is assigned to a particular node depending on location and context.

- **Clustering** - Having controllers in a cluster enables seamless client failover between controllers with no impact to user experience. The clustering feature also facilitates client roaming as well as AP and client load balancing. Clustering is required to support live upgrades.
- **Live Upgrade** - Upgrade a cluster of controllers in real time without end users experiencing any loss of connectivity or performance. There is no need for scheduling maintenance cycles for network upgrade.
- **AirMatch** - RF intelligence is centralized on the MM which significantly improves the RF management and interference mitigation capabilities of the WLAN.
- **REST API support**
- **Multi-version support** - Flexibility of upgrading individual controllers to test out new features or bug fixes. Controllers in a cluster need to run the same ArubaOS software version and may be upgraded together.
- **In-service software module upgrades** - Loadable Service Modules (LSMs) such as UCC, AirGroup, AppRF can be updated during runtime removing the need to schedule any maintenance cycles.

Design Caveats

- The MM does not terminate APs. APs can only be terminated on a MC.
- If the existing ArubaOS 6 deployment has more than 1000 controllers and/or 10,000 APs, then migration to an ArubaOS 8 MM deployment requires the deployment of multiple MMs

Migration Requirements

- Requires purchase of virtual MM capacity licenses or a hardware MM.
- A backup hardware MM may also be deployed in which case the licenses on each MM will be aggregated and synchronized across both MMs.
- Other licenses such as AP and PEF need to be migrated manually or via the My Networking Portal.

Migration Options

- Manual migration steps are detailed below.

Migration Strategy

Existing ArubaOS 6 Deployment

- HQ: Master controllers M1 and M2
- Campus1: L1, L2, and L3. Three AP groups are configured for termination on each of the local controllers
- Campus2: L4 and L5. Two AP groups are configured for termination on each of the local controllers

New ArubaOS 8 Deployment

- MM backed up by a standby MM
- The MM will manage MC1, MC2, MC3, MC4 in Campus1 in addition to MC5, MC6 and MC7 in Campus2
- APs terminate on one of the cluster members in each campus

Migration Procedure

Manual migration requires a complete rebuild of the existing ArubaOS 6 topology by performing the steps listed below. These steps cover termination of APs on a cluster VIP. For a multi-site campus, the APs could terminate on any of the three LMS IPs (MC1, MC2, or MC3)

MM Specific

1. Deploy the MM and perform initial setup
2. Configure licensing on the MM
3. Create a configuration hierarchy and whitelist the MAC addresses of M1, M2, L1-L5 on the MM. Whitelist each device under the following configuration hierarchies:
   - L1, L2, L3, and M1 whitelisted under **Managed Network > Campus1**
   - L4, L5, and M2 whitelisted under **Managed Network > Campus2.**
4. Repeat step 1 if a backup MM has to be installed.
5. Configure MM redundancy if a backup MM is being installed. The MM VIP will be used for configuration management.

Campus1

1. Configure clustering between MC1-MC4. Also enable AP load balancing by navigating to **Managed Network > Campus1 > Services > Cluster**
2. Create a VIP (now referred to as "Cluster1 VIP") between the cluster members MC1-MC4 by navigating to **Managed Network > Campus1 > Services > Redundancy > Virtual Router Table**. Optionally create VIPs for RADIUS COA.
3. Create an AP group by navigating to **Managed Network > Campus1 > AP Groups**.
4. Create a new SSID bu navigating to **Managed Network > Campus1 > Tasks > Create a new WLAN.**
5. Whitelist the Campus1 APs on the MM. This includes mapping them to the appropriate AP group by navigating to **Managed Network > Campus1 > Configuration > Access Points > Whitelist.**
6. Back up the existing configuration on ArubaOS 6 controllers L1-L3 and M1 by navigating to **Maintenance > Backup Flash.**
7. Upgrade the image on local L1 to ArubaOS 8 and reboot it by navigating to **Maintenance > Image Management.**
8. Provision local L1 to be managed by the MM via the CLI setup dialog. L1 will now become MC1.
9. Repeat steps 6-7 to convert L2, L3, and M1 to MC2, MC3, and MC4 respectively.
10. In the Campus1 network, point aruba-master towards the Cluster1 VIP.
11. The APs that were terminating on the L1-L3 will find the cluster VIP, upgrade their images, terminate on one of controllers in the MC1-MC4 range (depending on how the cluster leader load balances the APs), and broadcast the configured SSID for Campus1.
12. Connect a wireless client to the SSID and test connectivity.
13. Optionally, test seamless client failover by running a voice/video application and disconnecting the user's active controller.

Campus2

1. Configure clustering between MC5, MC6, MC7. Also enable AP load balancing by navigating to **Managed Network > Campus2 > Services > Cluster.**
2. Create a VIP (now referred to as "Cluster1 VIP") between the cluster members MC5, MC6, and MC7 by navigating to **Managed Network > Campus2 > Services > Redundancy > Virtual Router Table**. Optionally create VIPs for RADIUS COA.
3. Create an AP group by navigating to **Managed Network > Campus2 > AP Groups**.
4. Create a new SSID by navigating to **Managed Network > Campus2 > Tasks > Create a new WLAN.**
5. Whitelist the Campus2 APs on the MM. This includes mapping them to the appropriate AP group by navigating to **Managed Network > Campus2 > Configuration > Access Points > Whitelist.**
6. Back up the existing configuration on ArubaOS 6 controllers L4 , L5 and M2 by navigating to **Maintenance > Backup Flash.**

7. Upgrade the image on local L4 to ArubaOS 8 and reboot it by navigating to **Maintenance > Image Management.**
8. Provision local L1 to be managed by the MM via the CLI setup dialog. L4 will now become MC5.
9. Repeat steps 6-7 to convert L5 to MC6 and M2 to MC7.
10. In the Campus2 network, point aruba-master towards the Cluster2 VIP.
11. The APs that were terminating on the L1-L3 will find the cluster VIP, upgrade their images, terminate on one of controllers in the MC1-MC4 range (depending on how the cluster leader load balances the APs), and broadcast the configured SSID for Campus2.
12. Connect a wireless client to the SSID and test connectivity.
13. Optionally, test seamless client failover by running a voice/video application and disconnecting the user's active controller.

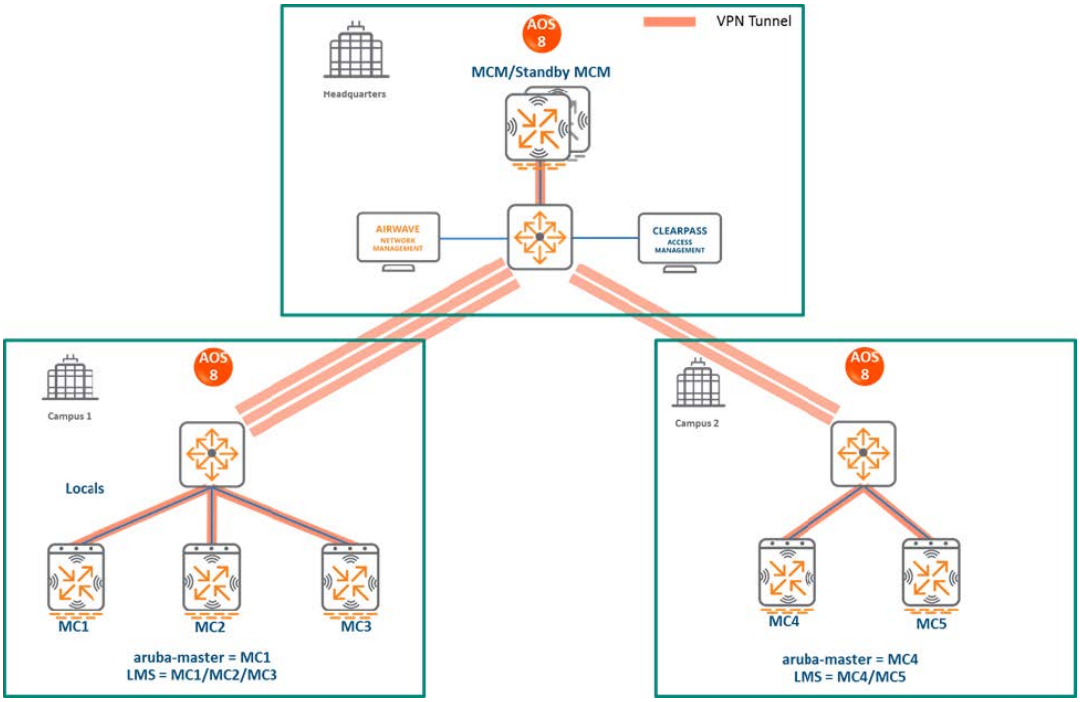
MC Master Terminating MCs

Topology

This ArubaOS 8 design consists of a hardware controller deployed as a MC Master (optionally backed up by another MC Master) that manages a group of MCs in different campuses.

This design helps transitioning deployments to ArubaOS 8 that are unable to deploy an MM. This MC Master topology should eventually be migrated to the MM topology in order to take full advantage of the capabilities offered by ArubaOS 8.

Figure 171 *MC Master Terminating MCs Topology*



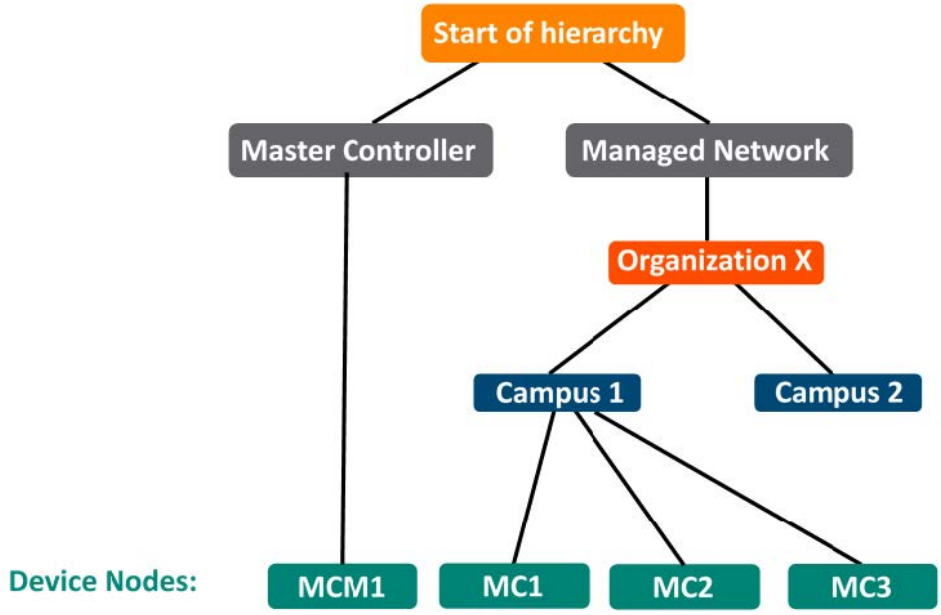
In this design:

- The ArubaOS 6 master (M1) and standby master (M2) become ArubaOS 8 MC Masters (MCM1 and MCM2).
- In Campus1, the ArubaOS 6 local controllers (L1, L2, and L3) become ArubaOS 8 MCs (MC1, MC2, and MC3).
- In Campus2, the ArubaOS 6 local controllers (L4 and L5) become ArubaOS 8 MCs (MC4 and MC5).
- All MCs terminate their IPsec tunnels on the MC Master MCM1.

- APs terminating on L1, L2, and L3 will now terminate on MC1, MC2, and MC3 respectively.
- APs terminating on L4 and L5 will now terminate on MC4 and MC5 respectively.

Configuration Hierarchy

Figure 172 *MC Master Terminating Mobility Configuration Hierarchy*



Design Benefits

- A similar topology is maintained in which the MC Master manages the MCs and no additional hardware is required as long as the MC Master is an Aruba 7030 or larger controller.
- The hierarchical configuration model offers fully centralized configuration and management of the WLAN.
- Additional controllers could be added later and managed by the MC Master

Design Caveats

- Requires purchase of an Aruba 7030 or larger controller to serve as the MC Master as well as the backup MCM if one is not already present
- AP termination on the MC Master is not supported. This has the following impact on AP termination options:
  - Any APs that terminate on the master in ArubaOS 6 would need to be redistributed among the locals prior to migration. The locals should have enough capacity to accommodate the additional APs.
  - APs can failover between MCs but cannot failover to the MC Master.
- The clustering feature is not supported in a MC Master deployment. AP Fast Failover between MCs is the only controller redundancy option.
- AirMatch is not supported
- All controllers in the topology must run the same ArubaOS version
- No centralized monitoring

Migration Requirements

- Verify that the ArubaOS 6 master controller meets the MC Master hardware requirements (Aruba 7030 or any Aruba 7200 series controller).
- Ensure that the ArubaOS 6 master is not terminating any APs as an ArubaOS 8 MC Master does not support

AP termination.

- Ensure that AP, PEF, and all other licenses have been migrated manually or via the My Networking Portal.

Migration Options

- Manual migration steps are detailed below.

Migration Strategy

Existing ArubaOS 6 Deployment

- HQ: M1 and M2
- Campus1: L1, L2 and L3
- Campus2: L4 and L5
- In Campus1, three AP groups are configured for termination on L1, L2, and L3
- In Campus2, two AP groups are configured for termination onL4 and L5

New ArubaOS 8 Deployment

- MCM1 backed up by MCM2
- MCM1 managing MC1, MC2, and MC3 in Campus1 and MC4 and MC5 in Campus2

Migration Procedure

Manual migration requires a complete rebuild of the existing ArubaOS 6 topology by performing the steps listed below:

MC Master Specific

1. Backup the existing configuration on the ArubaOS 6 masters and locals by navigating to **Maintenance > Backup Flash.**
2. Upgrade master M1 to ArubaOS 8 and reboot the controller by navigating to **Maintenance > Image Management.**
3. Provision M1 as a MC Master through the CLI setup dialog. M1 will become MCM1.
4. Repeat steps 2 and 3 to convert M2 to MCM2.
5. Configure master redundancy between MCM1 and MCM2. The MC Master VIP will be used for configuration management.
6. Configure licensing on the MC Master
7. Create a configuration hierarchy on the MC Master and whitelist the MAC addresses of controllers L1-L5. Whitelist each device under the following configuration hierarchies:

- L1-L3 whitelisted under **Managed Network > Campus1**
- L4 and L5 whitelisted under **Managed Network > Campus2**

Campus1

1. Create three AP groups, each with the LMS IP of MC1, MC2, and MC3 respectively by navigating to **Managed Network > Campus1 > AP Groups.**
2. Create a common SSID or one for each AP group by navigating to **Managed Network > Campus1 > Tasks > Create a new WLAN.**
3. Whitelist the APs on the MC Master. This includes mapping them to the appropriate AP group by navigating to **Managed Network > Campus1 > Configuration > Access Points > Whitelist.**
4. Upgrade the image on local L1 to ArubaOS 8 and reboot it by navigating to **Maintenance > Image Management.**
5. Provision local L1 to be managed by the MC Master via the CLI setup dialog. L1 will become MC1.
6. Repeat steps 4-5 for L2 and L3 to convert them to ArubaOS 8 MC2 and MC3.

7. Change **aruba-master** to point towards MC1's IP.
8. Once MC1 is visible on the MC Master, the APs that were terminating on L1 will find MC1, upgrade their images, download the LMS-IP for MC1, terminate their tunnels on MC1, and broadcast the configured SSID.
9. Similarly, the APs on L2 and L3 will be displayed on MC2 and MC3 respectively.
10. Connect a wireless client to the SSID and test connectivity.
11. Optionally, configure AP Fast Failover via the MC Master to enable AP failover between the MCs.

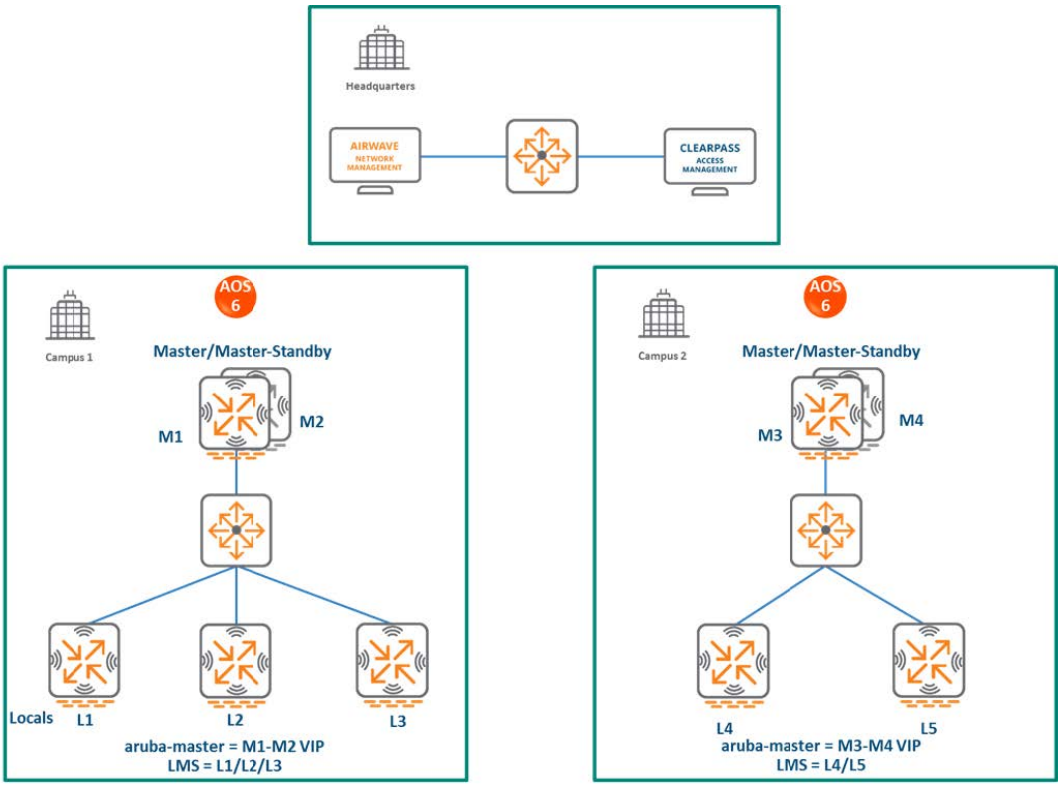
Campus2

1. Create two AP groups, each with the LMS IP of MC1 and MC2 respectively by navigating to **Managed Network > Campus2 > AP Groups.**
2. Create a common SSID or one for each AP group by navigating to **Managed Network > Campus2 > Tasks > Create a new WLAN.**
3. Whitelist the APs on the MC Master. This includes mapping them to the appropriate AP group by navigating to **Managed Network > Campus2 > Configuration > Access Points > Whitelist.**
4. Upgrade the image on local L4 to ArubaOS 8 and reboot it by navigating to **Maintenance > Image Management.**
5. Provision local L1 to be managed by the MC Master via the CLI setup dialog. L4 will become MC4.
6. Repeat steps 4-5 to convert L5 into MC5.
7. Change aruba-master to point towards MC4's IP.
8. The APs that were terminating on L4 will find MC4, upgrade their images, download their LMS IP (i.e. MC4), terminate their tunnels on MC4, and broadcast the configured SSID.
9. Similarly, the APs on L5 will be displayed on MC5.
10. Connect a wireless client to the SSID and test connectivity.
11. Optionally, configure AP Fast Failover via the MC Master to enable AP failover between the MCs.

Multiple Master-Locals

This ArubaOS 6 design consists of multiple sites, with the master at each site (typically backed up by a standby master) managing a group of local controllers.

Figure 173 *Multiple Master-Locals*



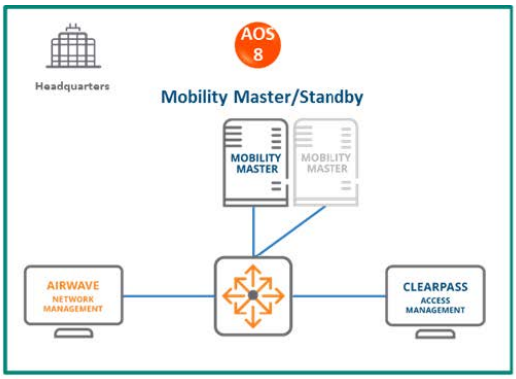
In this design:

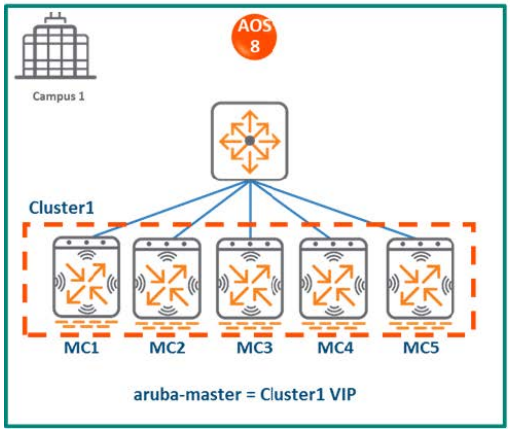
- Each site has its own configuration that is defined on the master and pushed to the respective locals. There is no central point of configuration for multiple sites.
- The APs at each site terminate on one of the local controllers with other locals acting as backups. For example, some APs in Campus 1 could terminate on L1, with L2 and L3 providing backup for L1.
- AP Fast Failover is configured to provide sub-second failover for the APs when connectivity to their primary controller is lost.

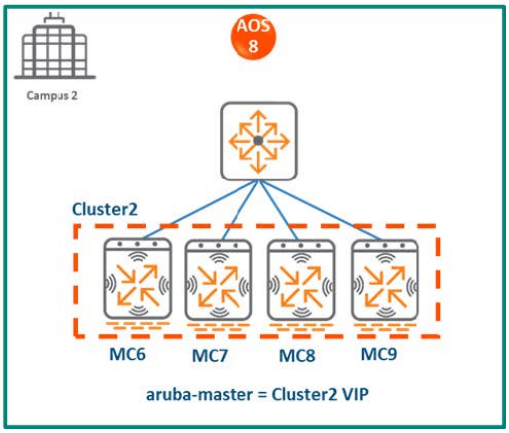
MM Terminating MCs

Topology

Figure 174 *MM Terminating MCs Topology*







HQ/DC

- The MM (either hardware or virtual) is deployed and configured in the HQ/DC along with a backup MM.
- Both campuses are centrally managed by the MM.

Campus1

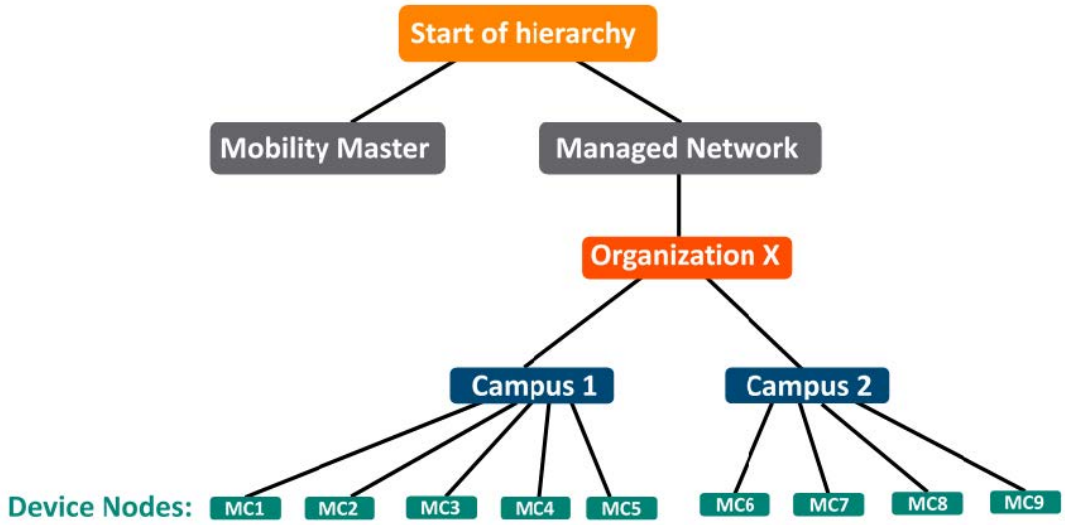
- ArubaOS 6 local controllers L1, L2, and L3 become ArubaOS 8 MC1, MC2, and MC3 respectively.
- A cluster is formed between MC1, MC2, and MC3 for controller redundancy, load balancing, and failover of APs and clients.
- The ArubaOS 6 masters M1 and M2 become ArubaOS 8 MC4 and MC5.
- APs that were terminating on L1, L2 and L3 will now terminate on MC1, MC2, and MC3 respectively.
- MC4 and MC5 can be included in the cluster for added redundancy and client and AP load balancing.

Campus2

- Similarly, ArubaOS 6 locals L4 and L5 become ArubaOS 8 MC6 and MC7 respectively.
- A cluster is formed between MC6 and MC7 for controller redundancy and to load balance and failover APs and clients.
- The ArubaOS 6 masters M3 and M4 become ArubaOS 8 MC8 and MC9.
- APs that were terminating on L4 and L5 will now terminate on MC6 and MC7 respectively.
- MC8 and MC9 can be included in the cluster for added redundancy as well as client and AP load balancing.

Configuration Hierarchy

Figure 175 *MM Terminating MCs Configuration Hierarchy*



Design Benefits

- **Maximize benefits** - The MM terminating MCs design is ideal for fully leveraging the capabilities of ArubaOS 8.
- **Scalability** - New controllers can be easily added and managed by the MM.
- **Ease of migration** - If an existing deployment has multiple topologies, they can be migrated under the MM into their own nodes in the hierarchy.
- **Management** - Centralized configuration and management of controllers.
- **Hierarchical configuration model** - Configuration is performed on nodes (logical folders such as USA, West Coast, California, Santa Clara, etc.) and each controller is assigned to a particular node depending on location and context.
- **Clustering** - Having controllers in a cluster enables seamless client failover between controllers with no impact to user experience. The clustering feature also facilitates client roaming as well as AP and client load balancing. Clustering is required to support live upgrades.
- **Live Upgrade** - Upgrade a cluster of controllers in real time without end users experiencing any loss of connectivity or performance. There is no need for scheduling maintenance cycles for network upgrade.
- **AirMatch** - RF intelligence is centralized on the MM which significantly improves the RF management and interference mitigation capabilities of the WLAN.
- **REST API support**
- **Multi-version support** - Flexibility of upgrading individual controllers to test out new features or bug fixes. Controllers in a cluster need to run the same ArubaOS software version and may be upgraded together.
- **In-service software module upgrades** - Loadable Service Modules (LSMs) such as UCC, AirGroup, AppRF can be updated during runtime removing the need to schedule any maintenance cycles.

Design Caveats

- The MM does not terminate APs. APs can only be terminated on a MC.
- If the existing ArubaOS 6 deployment has more than 1000 controllers and/or 10,000 APs, then migration to an ArubaOS 8 MM deployment requires the deployment of multiple MMs.

Migration Requirements

- Requires purchase of virtual MM capacity licenses or the purchase of a hardware MM.
- A backup hardware MM may also be deployed in which case the licenses on each MM will be aggregated and synchronized across both MMs.
- Other licenses such as AP and PEF need to be migrated manually or via the My Networking Portal.

Migration Options

- Manual migration steps are detailed below.

Migration Strategy

Existing ArubaOS 6 Deployment

Campus1:

- Locals L1, L2, L3
- Masters M1 and M2
- 3 AP groups are configured to have APs terminate among L1, L2, and L3

Campus2

- Locals L4 and L5
- Masters M3 and M4
- 2 AP groups are configured to have APs terminate among L4 and L5

New ArubaOS 8 Deployment

- MM backed up by a standby MM
- MM managing MC1-MC5 in Campus1 and M6-M9 in Campus2

Migration Procedure

Manual migration requires a complete rebuild of the existing ArubaOS 6 topology by performing the steps listed below:

MM Specific

1. Deploy the MM and perform the initial setup.
2. Configure licensing on the MM.
3. Create a configuration hierarchy and whitelist the MAC addresses of M1-M4 and L1-L5 on the MM. Whitelist each device under the following configuration hierarchies:
   - M1, M2, L1-L3 whitelisted under Managed Network > Campus1
   - M3, M4, L4 and L5 whitelisted under Managed Network > Campus2
4. Repeat step 1 if a backup MM is being installed.

5. Configure MM redundancy if a backup MM has been installed. The MM VIP will be used for configuration management moving forward.

Campus1

1. Configure clustering between MC1-MC5 IPs. Also enable AP load balancing by navigating to **Managed Network > Campus1 > Services > Cluster**
2. Create a VIP between the cluster members MC1-MC5 by navigating to **Managed Network > Campus1 > Services > Redundancy > Virtual Router** Table. Optionally create VIPs for RADIUS COA.
3. Create an AP group by navigating to **Managed Network > Campus1 > AP Groups.**
4. Create a new SSID by navigating to **Managed Network > (select node) > Tasks > Create a new WLAN.**
5. Whitelist the Campus1 APs on the MM. This includes mapping them to the appropriate AP group by navigating to **Managed Network > Campus1 > Configuration > Access Points > Whitelist.**
6. Back up the existing configuration on the ArubaOS 6 masters M1, M2 and locals L1-L3 by navigating to **Maintenance > Backup Flash.**
7. Upgrade the image on local L1 to ArubaOS 8 and reboot it by navigating to **Maintenance > Image Management.**
8. Provision local L1 to be managed by the MM, via the CLI setup dialog. L1 will now become MC1.
9. Repeat steps 6-7 to convert L2, L3, M1, and M2 to MC2, MC3, MC4, and MC5 respectively.
10. In the Campus1 network point aruba-master towards the cluster VIP for MC1-MC5.
11. The APs that were terminating on the L1-L3 will find the cluster VIP, upgrade their images, terminate on one of MC1-MC5 (depending on how the cluster leader load balances the APs), and broadcast the configured SSID for Campus1.
12. Connect a wireless client to the SSID and test connectivity.
13. Optionally, test seamless client failover by running a voice/video application and disconnecting the user's active controller.

Campus 2

1. Configure clustering between MC1-MC5 IPs. Also enable AP load balancing by navigating to **Managed Network > Campus2 > Services > Cluster.**
2. Create a VIP between the cluster members MC1-MC5 by navigating to **Managed Network > Campus2 > Services > Redundancy > Virtual Router** Table. Optionally create VIPs for RADIUS COA.
3. Create an AP group by navigating to **Managed Network > Campus2 > AP Groups.**
4. Create a new SSID by navigating to **Managed Network > (select node) > Tasks > Create a new WLAN.**
5. Whitelist the Campus2 APs on the MM. This includes mapping them to the appropriate AP group by navigating to **Managed Network > Campus2 > Configuration > Access Points > Whitelist.**
6. Back up the existing configuration on the ArubaOS 6 masters M3 and M4 as well as locals L4 and L5 by navigating to **Maintenance > Backup Flash.**
7. Upgrade the image on local L4 to ArubaOS 8 and reboot the device by navigating to **Maintenance > Image Management.**
8. Provision local L1 to be managed by the MM, via the CLI setup dialog. L4 will now become MC6.
9. Repeat steps 6-7 to convert L5, M3, and M4 to MC7, MC8, and MC9 respectively.
10. In the Campus1 network point aruba-master towards the cluster VIP for MC6-MC9.
11. The APs that were terminating on the L4 and L5 will find the cluster VIP, upgrade their images, terminate on one of MC6-MC9 (depending on how the cluster leader load balances the APs), and broadcast the configured SSID for Campus2
12. Connect a wireless client to the SSID and test connectivity.
13. Optionally, test seamless client failover by running a voice/video application and disconnecting the user's active controller.

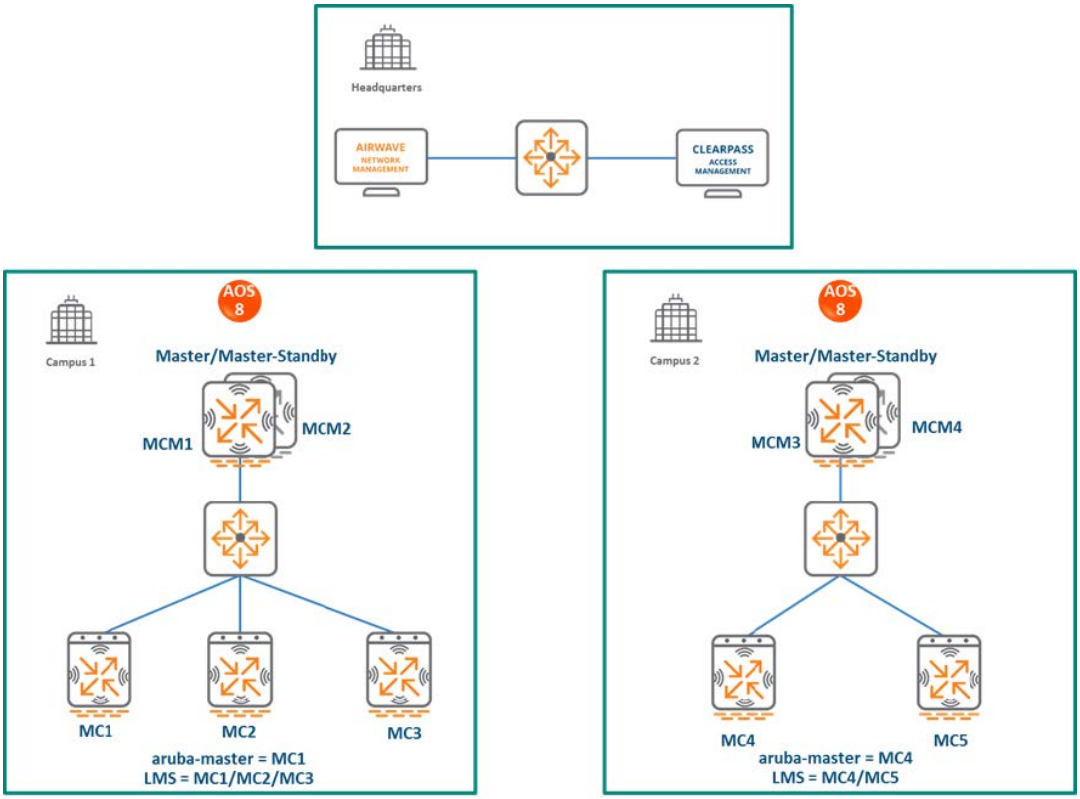
MC Master Terminating MCs

Topology

In this ArubaOS 8 design, each site consists of a hardware controller deployed as a MC Master (optionally backed up by another MC Master) that manages a group of MCs.

This design helps transition deployments to ArubaOS 8 that are unable to deploy an MM. This MC Master topology should eventually be migrated to an MM topology in order to take full advantage of the capabilities offered by ArubaOS 8.

Figure 176 *MC Master Terminating MCs Topology*



In this design, each campus is still managed by its own MC Master.

Campus1

- ArubaOS 6 locals L1, L2, and L3 become ArubaOS 8 MC1, MC2, and MC3 respectively.
- The ArubaOS 6 masters M1 and M2 become ArubaOS 8 MCM1 and MCM2.
- APs that were terminating on L1, L2, and L3 will now terminate on MC1, MC2 and MC3 respectively.

Campus2

- ArubaOS 6 locals L4 and L5 become ArubaOS 8 MC4 and MC5 respectively.
- The ArubaOS 6 masters M3 and M4 become ArubaOS 8 MCM3 and MCM4.
- APs that were terminating on L4 and L5 will now terminate on MC4 and MC5 respectively.

Figure 177 *MC Master Terminating Mobility Configuration Hierarchy Campus 1*

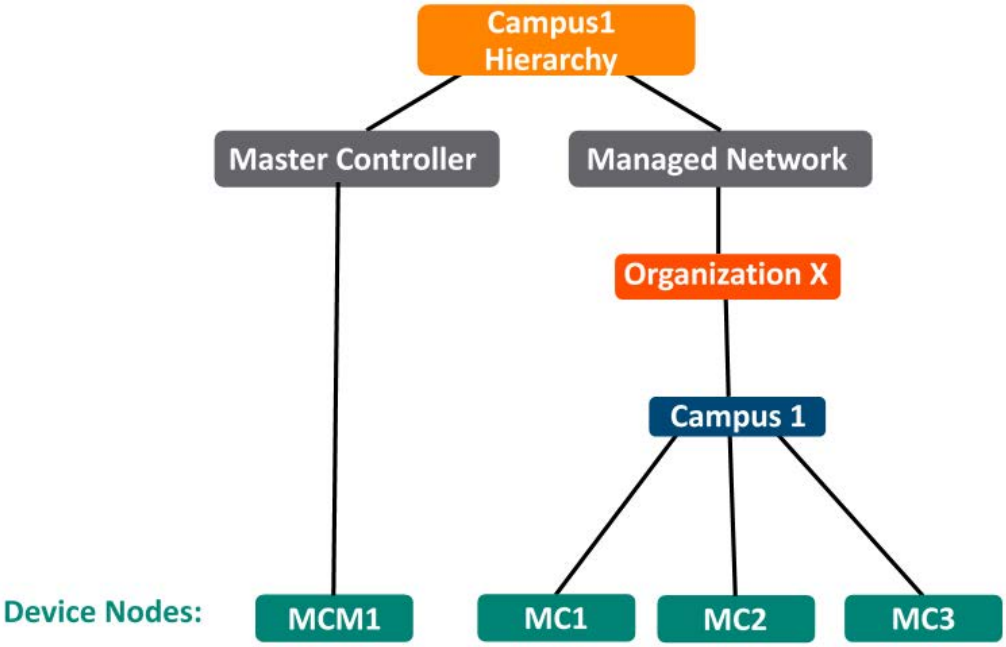
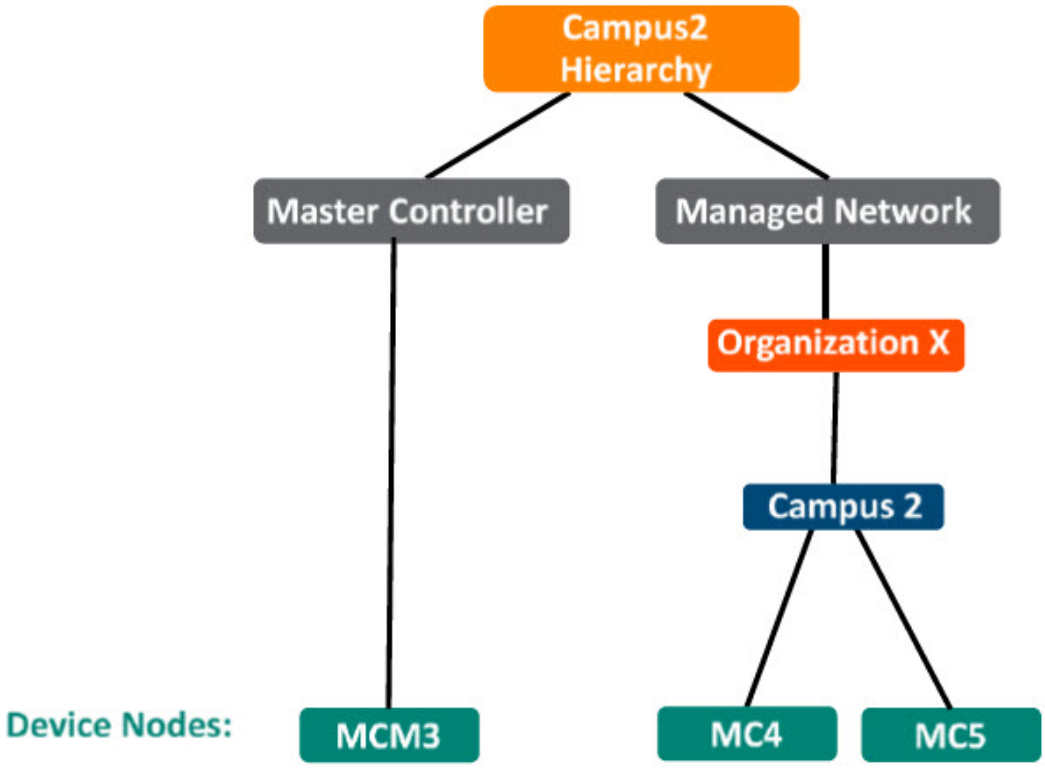


Figure 178 *MC Master Terminating Mobility Configuration Hierarchy Campus 2*



Design Benefits

- A similar topology is maintained in which the MC Master manages the MCs and no additional hardware is required as long as the MC Master is an Aruba 7030 or larger controller.

- The hierarchical configuration model offers fully centralized configuration and management of the WLAN.
- Additional controllers could be added later and managed by the MC Master.

Design Caveats

- Requires purchase of an Aruba 7030 or larger controller to serve as the MC Master as well as the backup MCM if one is not already present.
- AP termination on the MC Master is not supported. This has the following impact on AP termination options:
  - Any APs that are terminating on the master in ArubaOS 6 would need to be redistributed among the locals prior to migration. The locals should have enough capacity to accommodate the additional APs
  - APs can failover between MCs but cannot failover to the MC Master.
- The clustering feature is not supported in a MC Master deployment. AP Fast Failover between MCs is the only controller redundancy option.
- AirMatch is not supported.
- All controllers in the topology must run the same ArubaOS version.
- No centralized monitoring.

Migration Requirements

- Verify that the ArubaOS 6 master controller meets the MC Master hardware requirements (Aruba 7030 or any Aruba 7200 series controller).
- Ensure that the ArubaOS 6 master is not terminating any APs as an ArubaOS 8 MC Master does not support AP termination.
- Ensure that AP, PEF, and all other licenses have been migrated manually or via the My Networking Portal.

Migration Options

- Manual migration steps are detailed below.

Migration Strategy

Existing ArubaOS 6 Deployment

- Locals L1, L2, L3
- Masters M1 and M2
- 3 AP groups are configured to have groups of APs terminate among L1, L2, and L3

New ArubaOS 8 Deployment

Campus1

- MCM1 backed up by MC2
- MCM1 managing MC1, MC2, and MC3

Campus2

- MCM3 backed up by MCM4
- MCM3 managing MC4 and MC5

Migration Procedure

Manual migration requires a complete rebuild of the existing ArubaOS 6 topology by performing the steps listed below:

1. Back up the existing configuration on the ArubaOS 6 masters and locals by navigating to **Maintenance > Backup Flash.**
2. Upgrade the image on master M1 to ArubaOS 8 and reboot the controller.
3. Provision M1 as a MC Master through the CLI setup dialog. M1 will now become MCM1.
4. Repeat steps 2 and 3 to convert M2 to MCM2.
5. Configure master redundancy between MCM1 and MCM2. The MC Master VIP will be used for configuration management.
6. Configure licensing on the MC Master.
7. Create a configuration hierarchy on the MC Master and whitelist the MAC addresses of controllers L1-L3
   - L1-L3 will be whitelisted under Managed Network > Campus1.
8. Create three AP groups with LMS IP of MC1, MC2, and MC3 respectively by navigating to **Managed Network > Campus1 > AP Groups.**
9. Create an SSID for each AP group by navigating to **Managed Network > (select node) > Tasks > Create a new WLAN.**
10. Whitelist the APs on the MC Master. This includes mapping them to their respective AP groups by navigating to **Managed Network > (select node) > Configuration > Access Points > Whitelist.**
11. Upgrade the image on local L1 to ArubaOS 8 and reboot it by navigating to **Maintenance > Image Management.**
12. Provision local L1 to be managed by the MC Master via the CLI setup dialog. L1 will become MC1.
13. Now repeat steps 11-12 for L2 and L3 to convert them to ArubaOS 8 MC2 and MC3.
14. Change aruba-master to MC1's IP.
15. Once MC1 is visible on the MC Master, the APs that were terminating on L1 will find MC1, upgrade their images, download the LMS-IP for MC1, terminate their tunnels on MC1, and broadcast the configured SSID.
16. Similarly, the APs on L2 and L3 will show up on MC2 and MC3, respectively.
17. Connect a wireless client to the SSID and test connectivity.
18. Optionally, configure AP Fast Failover via the MC Master to enable sub-second AP failover between the MCs.

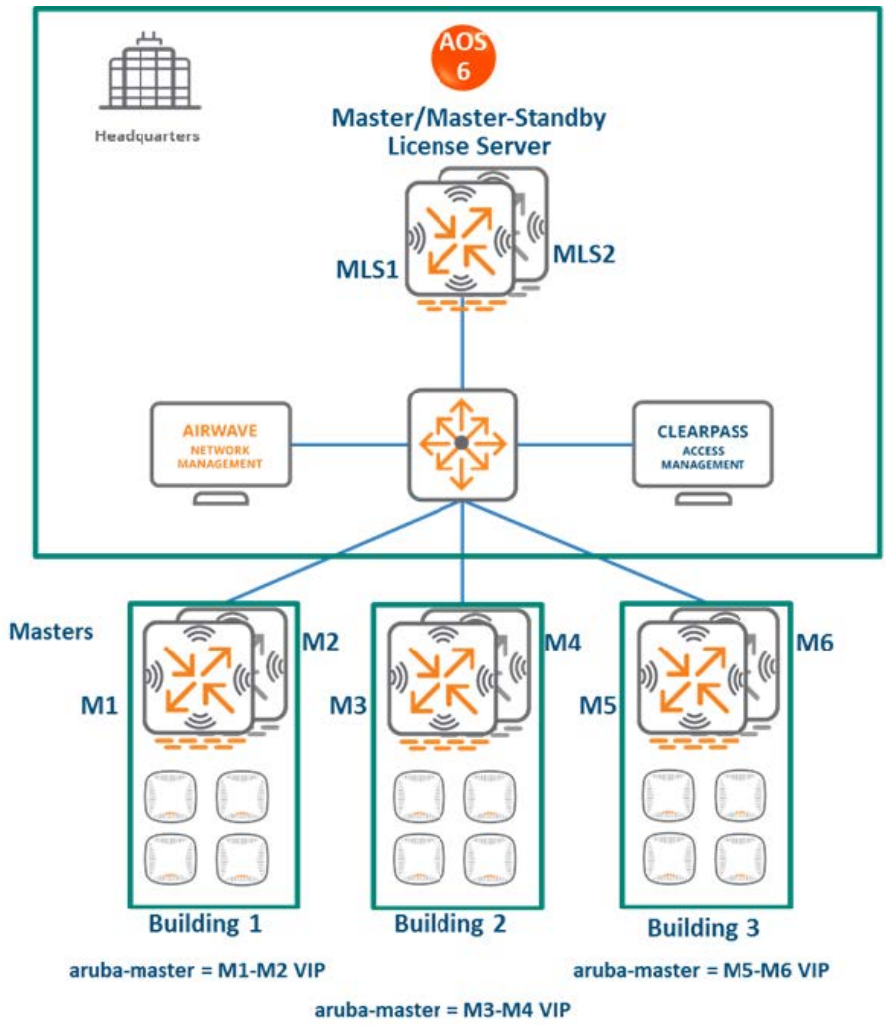
Campus2

1. Back up the existing configuration on the ArubaOS 6 masters and locals by navigating to **Maintenance > Backup Flash.**
2. Upgrade the image on master M3 to ArubaOS 8 and reboot the controller.
3. ProvisionM3 as a MC Master through the CLI setup dialog. M3 will now become MCM3.
4. Repeat steps 2 and 3 to convert M4 to MCM4.
5. Configure master redundancy between MCM1 and MCM2. The MC Master VIP will be used for configuration management.
6. Configure licensing on the MC Master.
7. Create a configuration hierarchy on the MC Master and whitelist the MAC addresses of controllers L4 and L5.
   - L4 and L5 will be whitelisted under **Managed Network > Campus2**
8. Create two AP groups with LMS IP of MC4 and MC5 respectively by navigating to **Managed Network > Campus2 > AP Groups.**
9. Create an SSID for each AP group by navigating to **Managed Network > (select node) > Tasks > Create a new WLAN.**
10. Whitelist the APs on the MC Master. This includes mapping them to their respective AP groups by navigating to **Managed Network > (select node) > Configuration > Access Points > Whitelist.**

11. Upgrade the image on local L4 to ArubaOS 8 and reboot it by navigating to **Maintenance > Image Management.**
12. Provision local L4 to be managed by the MC Master via the CLI setup dialog. L4 will become MC4.
13. Repeat steps 11-12 to convert L5 into MC5.
14. Change **aruba-master** to MC4's IP.
15. The APs that were terminating on L4 will find MC4, upgrade their images, download their LMS IP (i.e. MC4), terminate their tunnels on MC4, and broadcast the configured SSID
16. Similarly, the APs on L5 will show up on MC5 respectively.
17. Connect a wireless client to the SSID and test connectivity.
18. Optionally, configure AP Fast Failover via the MC Master to enable sub-second AP failover between the MCs.

All Masters

Figure 179 *All Masters Topology*



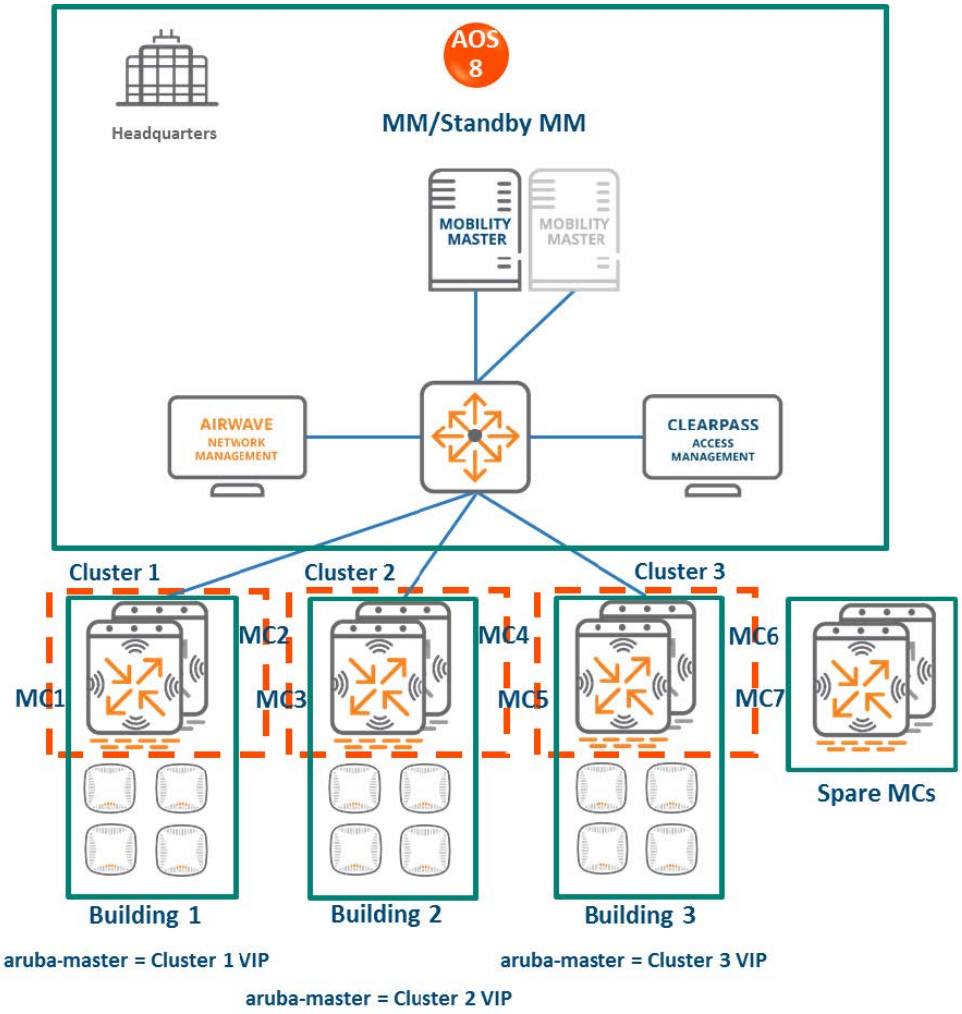
- In this ArubaOS 6 design, each site is managed by its own master controller, backed up by a standby master.
- There is a separate master/standby pair that functions as the license server for all sites.
- All the site masters are centrally managed by AirWave.

- The all-master design is typically deployed at sites that need to run different ArubaOS versions (for example, to test new ArubaOS features)

MM Terminating MCs

Topology

Figure 180 *MM Terminating MCs Topology*

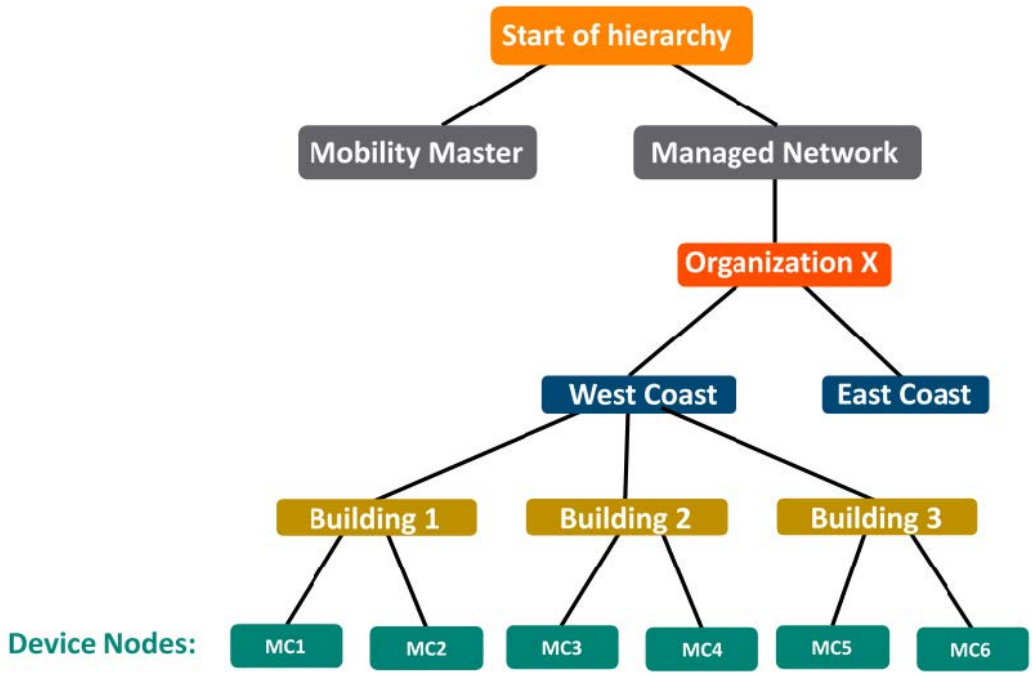


HQ/DC:

- The MM (either hardware or virtual) is deployed and configured along with a backup MM.
- All site controllers are centrally managed by the MM.
- **Building1:**
  - The ArubaOS 6 master and standby master become ArubaOS 8 MC1 and MC2.
  - A cluster can be formed between MC1 and MC2 for controller redundancy as well as client and AP load balancing.
- **Building2:** The ArubaOS 6 masters become ArubaOS 8 MC3 and MC4. Both MCs can become cluster members.
- **Building3:** The ArubaOS 6 masters become ArubaOS 8 MC5 and MC6. Both MCs can become cluster members.

- **License servers:**
  - The ArubaOS 6 master and standby master that were previously used as licensing servers become MCs managed by the MM.
  - These MCs can be repurposed. For example, they can be used as staging controllers to redirect APs in each site to their LMS controllers, or they can be added to the cluster at any site to provide additional controller redundancy as well as client and AP load balancing.

MM Terminating MCs Configuration Hierarchy



Design Benefits

- **Maximize benefits** - The MM terminating MCs design is ideal for fully leveraging the capabilities of ArubaOS 8.
- **Scalability** - New controllers can be easily added and managed by the MM.
- **Ease of migration** - If an existing deployment has multiple topologies, they can be migrated under the MM into their own nodes in the hierarchy.
- **Management** - Centralized configuration and management of controllers.
- **Hierarchical configuration model** - Configuration is performed on nodes (logical folders such as USA, West Coast, California, Santa Clara, etc.) and each controller is assigned to a particular node depending on location and context.
- **Clustering** - Having controllers in a cluster enables seamless client failover between controllers with no impact to user experience. The clustering feature also facilitates client roaming as well as AP and client load balancing. Clustering is required to support live upgrades.
- **Live Upgrade** - Upgrade a cluster of controllers in real time without end users experiencing any loss of connectivity or performance. There is no need for scheduling maintenance cycles for network upgrade.
- **AirMatch** - RF intelligence is centralized on the MM which significantly improves the RF management and interference mitigation capabilities of the WLAN.
- **REST API support**

- **Multi-version support** - Flexibility of upgrading individual controllers to test out new features or bug fixes. Controllers in a cluster need to run the same ArubaOS software version and may be upgraded together.
- **In-service software module upgrades** - Loadable Service Modules (LSMs) such as UCC, AirGroup, AppRF can be updated during runtime removing the need to schedule any maintenance cycles.

Design Caveats

- The MM does not terminate APs. APs can only be terminated on a MC.
- If the existing ArubaOS 6 deployment has more than 1000 controllers and/or 10,000 APs, then migration to an ArubaOS 8 MM deployment requires the deployment of multiple MMs.

Migration Requirements

- Requires purchase of virtual MM capacity licenses or the purchase of a hardware MM.
- A backup hardware MM may also be deployed in which case the licenses on each MM will be aggregated and synchronized across both MMs.
- Other licenses such as AP and PEF need to be migrated manually or via the My Networking Portal.

Migration Options

- Manual migration steps are detailed below.

Migration Strategy

Existing ArubaOS 6 Deployment

- **Building1:** Masters M1-M2
- **Building2:** Masters M3-M4
- **Building3:** Masters M5-M6
- **License servers:** Masters MLS1 and MLS2

New ArubaOS 8 Deployment

- MM managing MC1, MC2, MC3, MC4, MC5, MC6, MC7, and MC8.

Migration Procedure

Manual migration requires a complete rebuild of the existing ArubaOS 6 topology by performing the steps listed below:

MM Specific

1. Deploy the MM and perform initial setup.
2. Configure licensing on the MM.
3. Create a configuration hierarchy and whitelist the MAC addresses of M1-M6 on the MM. Whitelist each device under the following configuration hierarchies:
   - M1, M2 whitelisted under **Managed Network > Building1**
   - M3, M4 whitelisted under **Managed Network > Building2**
   - M5, M6 whitelisted under **Managed Network > Building3**
4. Repeat step 1 if you are installing a backup MM
5. Configure MM redundancy if a backup MM has been installed. The MM VIP will be used for configuration management.

Building 1

1. Configure clustering between MC1 and MC2 IPs and enable AP load balancing by navigating to **Managed Network > Building1 > Services > Cluster.**
2. Create a VIP between the cluster members MC1 and MC2 by navigating to **Managed Network > Building1 > Services > Redundancy > Virtual Router** Table. Optionally create VIPs for RADIUS COA.
3. Create an AP group by navigating to **Managed Network > Building1 > AP Groups.**
4. Create a new SSID by navigating to **Managed Network > (select node) > Tasks > Create a new WLAN.**
5. Whitelist the Building1 APs on the MM. This includes mapping them to the appropriate AP group by navigating to **Managed Network > Building1 > Configuration > Access Points > Whitelist.**
6. Back up the existing configuration on the ArubaOS 6 masters by navigating to **Maintenance > Backup Flash.**
7. Upgrade the image on local M1 to ArubaOS 8 and reboot it by navigating to **Maintenance > Image Management.**
8. Provision local M1 to be managed by the MM via the CLI setup dialog. M1 will now become MC1.
9. Repeat steps 6-7 to convert M2 to MC2.
10. In Building1, point **aruba-master** towards the cluster VIP for MC1 and MC2.
11. The APs that were terminating on M1 will find the cluster VIP, upgrade their images, terminate on either MC1 or MC2 (depending on how the cluster leader load balances the APs), and broadcast the configured SSID for Building1.
12. Connect a wireless client to the SSID and test connectivity.
13. Optionally, test seamless client failover by running a voice/video application and disconnecting the user's active controller.

Building 2

1. Configure clustering between MC1 and MC2 IPs and enable AP load balancing by navigating to **Managed Network > Building2 > Services > Cluster.**
2. Create a VIP between the cluster members MC1 and MC2 by navigating to **Managed Network > Building2 > Services > Redundancy > Virtual Router** Table. Optionally create VIPs for RADIUS COA.
3. Create an AP group by navigating to **Managed Network > Building1 > AP Groups.**
4. Create a new SSID by navigating to**Managed Network > Building2 > Tasks > Create a new WLAN.**
5. Whitelist the Building2 APs on the MM. This includes mapping them to the appropriate AP group by navigating to **Managed Network > Building2 > Configuration > Access Points > Whitelist.**
6. Back up the existing configuration on the ArubaOS 6 masters by navigating to **Maintenance > Backup Flash.**
7. Upgrade the image on mastee M3 to ArubaOS 8 and reboot it by navigating to **Maintenance > Image Management.**
8. Provision local M1 to be managed by the MM via the CLI setup dialog.M3 will now become MC3.
9. Repeat steps 6-7 to convert M4 to MC4.
10. In Building1, point aruba-master towards the cluster VIP for MC3 and MC4.
11. The APs that were terminating on M3 will find the cluster VIP, upgrade their images, terminate on either MC3 or MC4 (depending on how the cluster leader load balances the APs), and broadcast the configured SSID for Building 2.
12. Connect a wireless client to the SSID and test connectivity.
13. Optionally, test seamless client failover by running a voice/video application and disconnecting the user's active controller.

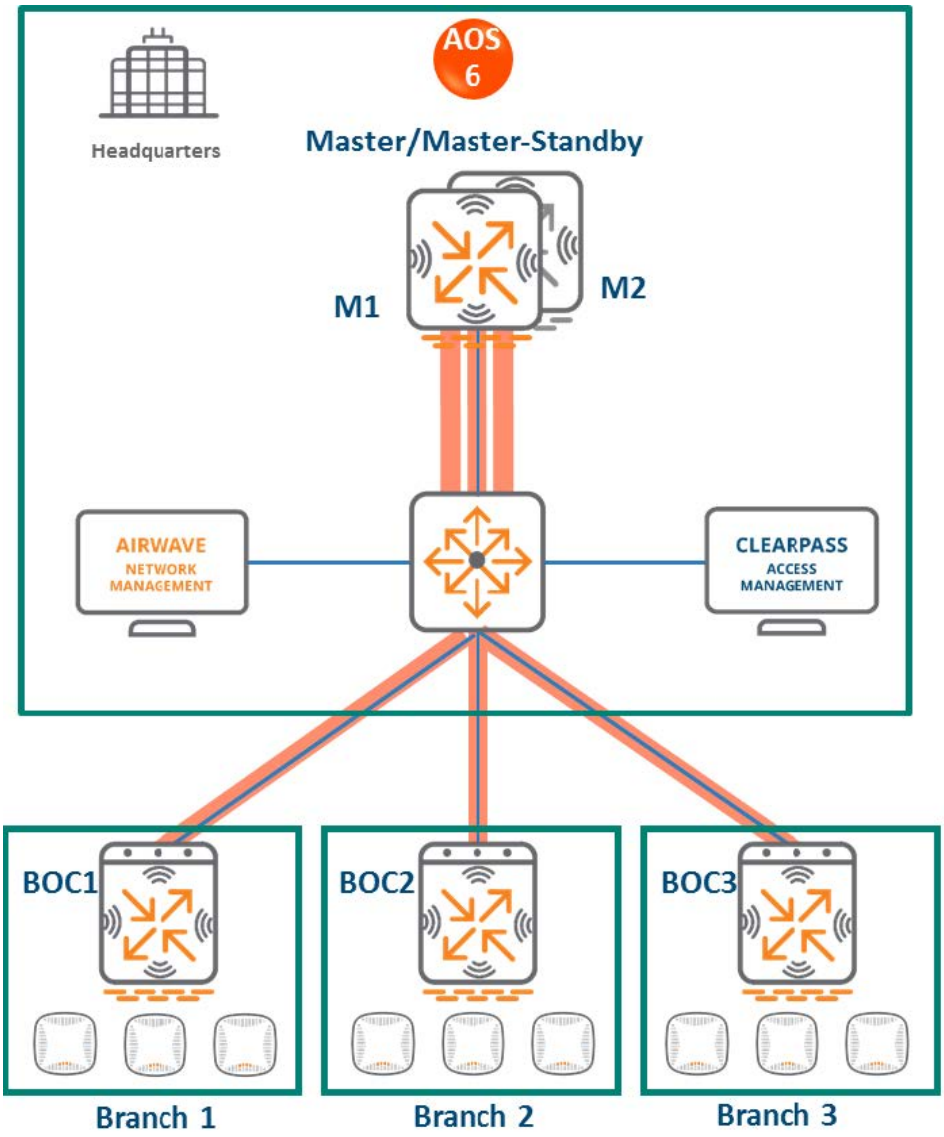
Follow the same procedure for Building 3.

Spares MC7 and MC8

- These can be relocated to any of the sites to be repurposed as cluster members for added controller redundancy as well as AP and client load balancing

Master and Branch Controllers

Figure 181 *Master and Branch Controllers Topology*



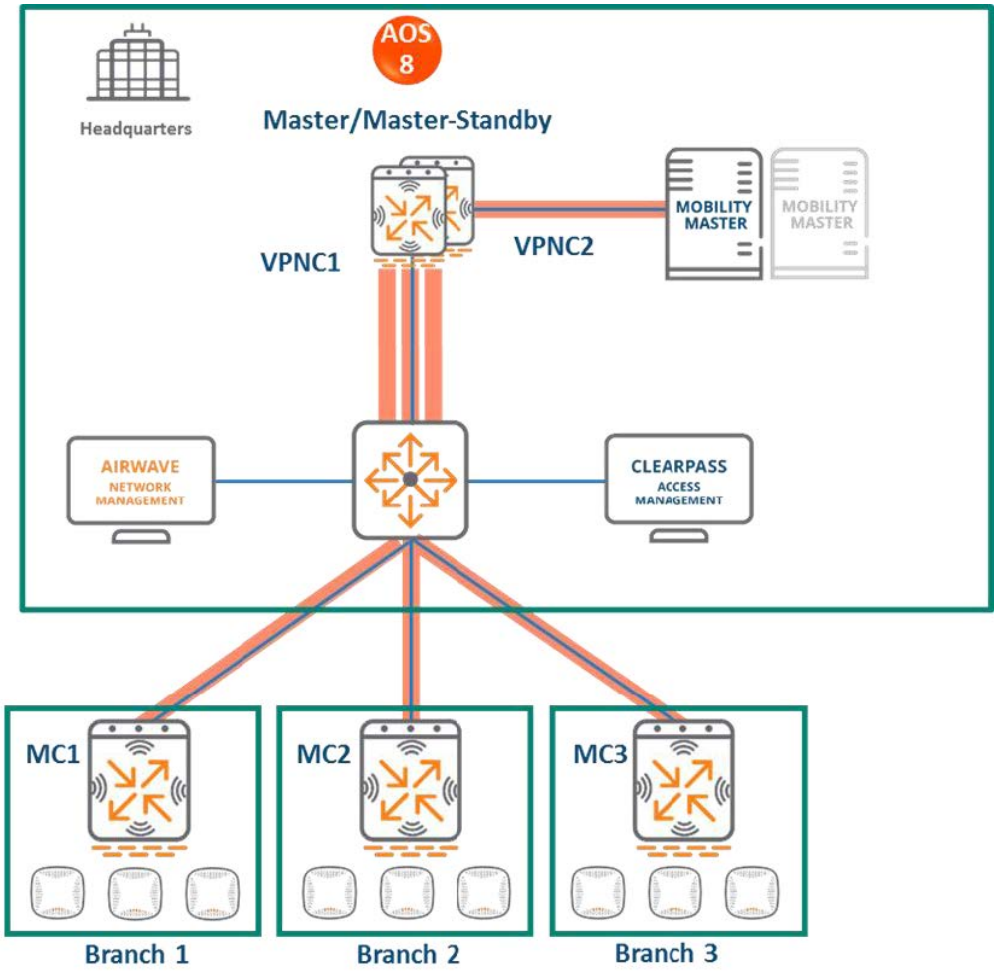
In this ArubaOS 6 design:

- A master controller manages geographically distributed branches.
- The master controller is backed up by a second master controller for redundancy.
- Each branch consists of one or more 7000 series controllers i.e. branch controllers/Branch Office Controllers (BOCs).
- Each branch controller uses ZTP to discover and build an IPsec connection with the master controller.
- Configuration for the branch controllers is managed on the master.

MM Terminating MCs

Topology

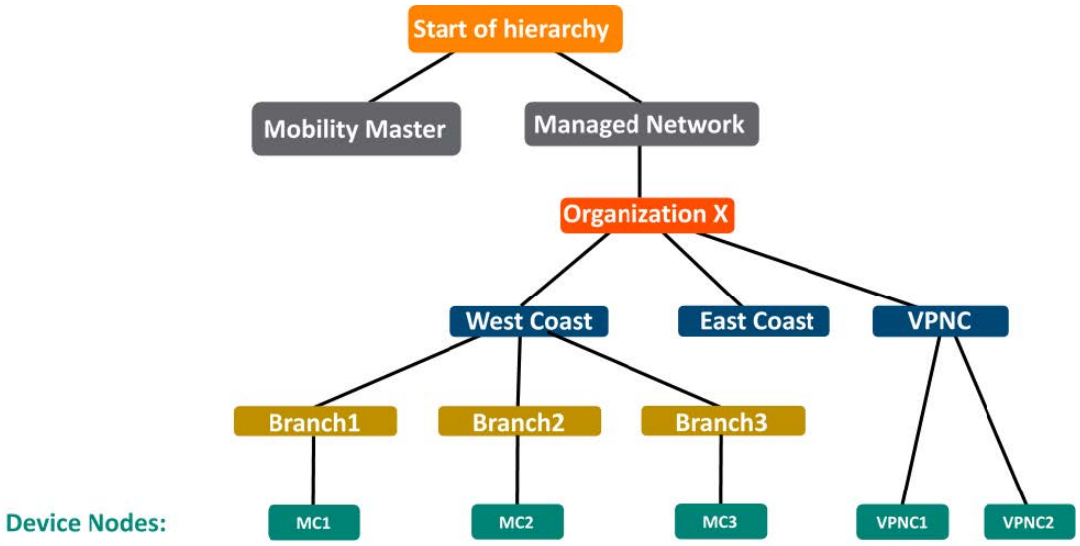
Figure 182 *MM Terminating MCs Topology*



In this design:

- An MM (either hardware or virtual) is deployed and configured, along with a backup MM
- Each ArubaOS 6 BOC (BOC1, BOC2, BOC3) becomes an ArubaOS 8 MC (MC1, MC2, MC3).
- The ArubaOS 6 master (M1) and standby master (M2) become two ArubaOS 8 VPNC MCs (MC4 and MC5).
- Branch MCs are capable of termination on the MM. However, using VPNCs is highly recommended if a deployment consists of distributed branches and user traffic originating from branches needs to reach corporate resources within HQ. User traffic requiring HQ access will be relatively high bandwidth and encryption / decryption is CPU intensive. Using VPNCs helps insulate the MM from the increased load
- APs terminating on L1, L2, and L3 will now terminate on MC1, MC2, and MC3 respectively.

Figure 183 *MM Terminating MCs Configuration Hierarchy*



Design Benefits

- **Maximize benefits** - The MM terminating MCs design is ideal for fully leveraging the capabilities of ArubaOS 8.
- **Scalability** - New controllers can be easily added and managed by the MM.
- **Ease of migration** - If an existing deployment has multiple topologies, they can be migrated under the MM into their own nodes in the hierarchy.
- **Management** - Centralized configuration and management of controllers.
- **Hierarchical configuration model** - Configuration is performed on nodes (logical folders such as USA, West Coast, California, Santa Clara, etc.) and each controller is assigned to a particular node depending on location and context.
- **Clustering** - Having controllers in a cluster enables seamless client failover between controllers with no impact to user experience. The clustering feature also facilitates client roaming as well as AP and client load balancing. Clustering is required to support live upgrades.
- **Live Upgrade** - Upgrade a cluster of controllers in real time without end users experiencing any loss of connectivity or performance. There is no need for scheduling maintenance cycles for network upgrade.
- **AirMatch** - RF intelligence is centralized on the MM which significantly improves the RF management and interference mitigation capabilities of the WLAN.
- **REST API support**
- **Multi-version support** - Flexibility of upgrading individual controllers to test out new features or bug fixes. Controllers in a cluster need to run the same ArubaOS software version and may be upgraded together.
- **In-service software module upgrades** - Loadable Service Modules (LSMs) such as UCC, AirGroup, AppRF can be updated during runtime removing the need to schedule any maintenance cycles.

Design Caveats

- The MM does not terminate APs. APs can only be terminated on a MC.
- If the existing ArubaOS 6 deployment has more than 1000 controllers and/or 10,000 APs, then migration to an ArubaOS 8 MM deployment requires deployment of multiple MMs.

Migration Requirements

- Requires purchase of virtual MM capacity licenses or a hardware MM.
- A backup hardware MM may also be deployed in which case the licenses on each MM will be aggregated and synchronized across both MMs.
- Other licenses such as AP and PEF need to be migrated manually or via the My Networking Portal.

Migration Options

- Manual migration steps are detailed below.

Migration Strategy

Existing ArubaOS 6 Deployment

- Branch1: BOC1
- Branch2: BOC2
- Branch3: BOC3
- HQ: M1, M2

New ArubaOS 8 Deployment

- MM managing MC1, MC2, MC3 and VPNC1, VPNC2.

Migration Procedure

Manual migration requires a complete rebuild of the existing ArubaOS 6 topology. Use the following steps to perform manual migration of a branch network. The ArubaOS 8 Branch Network ASE recipe may also be used to understand MM/VPNC/branch controller configuration in ArubaOS 8.

MM

1. Deploy the MM and perform initial setup.
2. Configure licensing on the MM.
3. Repeat step 1 if a backup MM is being installed.
4. Configure MM redundancy if a backup MM has been installed. The MM VIP will be used for configuration management.
5. Configure Activate, a configuration hierarchy, VPN peers, and whitelist the MAC addresses of M1, M2, BOC1, BOC2 and BOC3 on the MM. Whitelist each device under the following configuration hierarchies:
   - M1, M2 whitelisted under **Managed Network > VPNC**
   - BOC2 whitelisted under **Managed Network > Branch2**
   - BOC3 whitelisted under **Managed Network > Branch3**
6. Configure interfaces and VLANs and VPNC VIP.
7. Branch MC basic configuration - Configure interfaces, VLANs, DHCP pools for APs and users, IP VLAN pool of controller IPs for Branch MCs.
8. Uplink Configuration of Branch MCs - Add uplinks, load balancing, and policy based routing in Branch MCs.
9. Advertise routes of Branch MC to VPNCs.
10. Routing Configuration of VPNCs - Static routes and OSPF configuration in the VPNCs.
11. Create an AP group for Branch1 by navigating to **Managed Network > Branch1 > AP Groups**.

12. Create a new SSID by navigating to **Managed Network > Branch1 > Tasks > Create a new WLAN.**
13. Whitelist the Branch1 APs on the MM. This includes mapping them to the appropriate AP group by navigating to **Managed Network > Branch1 > Configuration > Access Points > Whitelist.**
14. Create an AP group and SSID for Branch2 by navigating to **Managed Network > Branch2 > AP Groups** or **Managed Network > Branch2 > Tasks > Create a new WLAN.**
15. Whitelist the Branch2 APs on the MM. This includes mapping them to the appropriate AP group by navigating to **Managed Network > Branch2 > Configuration > Access Points > Whitelist.**

Activate

1. Set up provisioning rules in Activate to whitelist the branch controllers and redirect them to the MM.
2. Optionally, if VPNCs are being used set up provisioning rules to whitelist them and redirect them to the MM.

VPNC

1. Back up the existing configuration on the ArubaOS 6 masters by navigating to **Maintenance > Backup Flash.**
2. Upgrade the image on master M1 to ArubaOS 8 and reboot it by navigating to **Maintenance > Image Management.**
3. Provision M1 to be a VPNC managed by the MM via the CLI setup dialog. M1 will now become VPNC1.
4. Repeat steps 2-3 to convert M2 into VPNC2.

Branch 1

1. Back up the existing configuration on the ArubaOS 6 BOC1 by navigating to **Maintenance > Backup Flash.**
2. Upgrade the image on BOC1 to ArubaOS 8 and reboot it by navigating to **Maintenance > Image Management.**
3. If provisioning rules have been created on Activate, the controller will perform ZTP, establish communication with the MM, and download its configuration.
4. Optionally, the controller may be manually configured. Provision BOC1 to be a MC managed by the MM via the CLI setup dialog. BOC1 will now become MC1.

Branch 2

1. Back up the existing configuration on the ArubaOS 6 BOC2 by navigating to **Maintenance > Backup Flash.**
2. Upgrade the image on BOC2 to ArubaOS 8 and reboot it by navigating to **Maintenance > Image Management.**
3. If provisioning rules have been created on Activate, the controller will perform ZTP, establish communication with the MM, and download its configuration.
4. Optionally, the controller may be manually configured. Provision BOC2 to be a MC managed by the MM via the CLI setup dialog. BOC2 will now become MC2.

Follow similar steps for Branch 3.