aruba
a Hewlett Packard
Enterprise company

Migration to ArubaOS 8

Authors:
Syed Ahmed
Andrew Tanguay

Contributors:
Jerrod Howard
Shiv Mehra

Tech Note

Copyright Information

Open Source Code

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

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

www.arubanetworks.com

3333 Scott Blvd

Santa Clara, CA 95054

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

Fax 408.227.4550

Contents

Revision History

The following table lists the revisions of this document:

Revision	Change Description
Revision 1.0.0	Initial Publication

Table 1 *Revision History*

About This Document

Overview

Aruba Tech Notes are brief best practice recommendation documents specifically designed to outline how a particular aspect of Aruba technology works as well as to advise customers how to deploy it with their Aruba solution to achieve optimal results. This document describes the concept of migration from ArubaOS 6 to ArubaOS 8.

Intended Audience and Scope

This guide is intended for administrators who are responsible for deploying and configuring ArubaOS 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

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

Conventions

Typographical Conventions

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

Style Type	Description
Italics	Italics are used to emphasize important terms and to mark the titles of books.
<Bolded>	Bolded words indicate an option that should be selected in the Graphical User Interface (GUI). The angled brackets indicate that the choices are part of a path in the GUI.
`Command Text`	Command text in this font will appear inside of a box and indicates commands that can be entered into the Command Line Interface (CLI).

`<Arguments>`	In the command examples, italicized text within single angle brackets represents items that should be replaced with information appropriate to your specific situation. For example: `# send <text message>` In this example, you would type “send” at the system prompt exactly as shown, followed by the text of the message you wish to send. Do not type the angle brackets.
`[Optional]`	Command examples enclosed in brackets are optional. Do not type the brackets.
`{Item A | Item B}`	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

Table 2 *Typographical Conventions*

Informational Icons

The following informational icons are used throughout this guide:

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

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

Indicates a risk of personal injury or death.

Graphical Icons

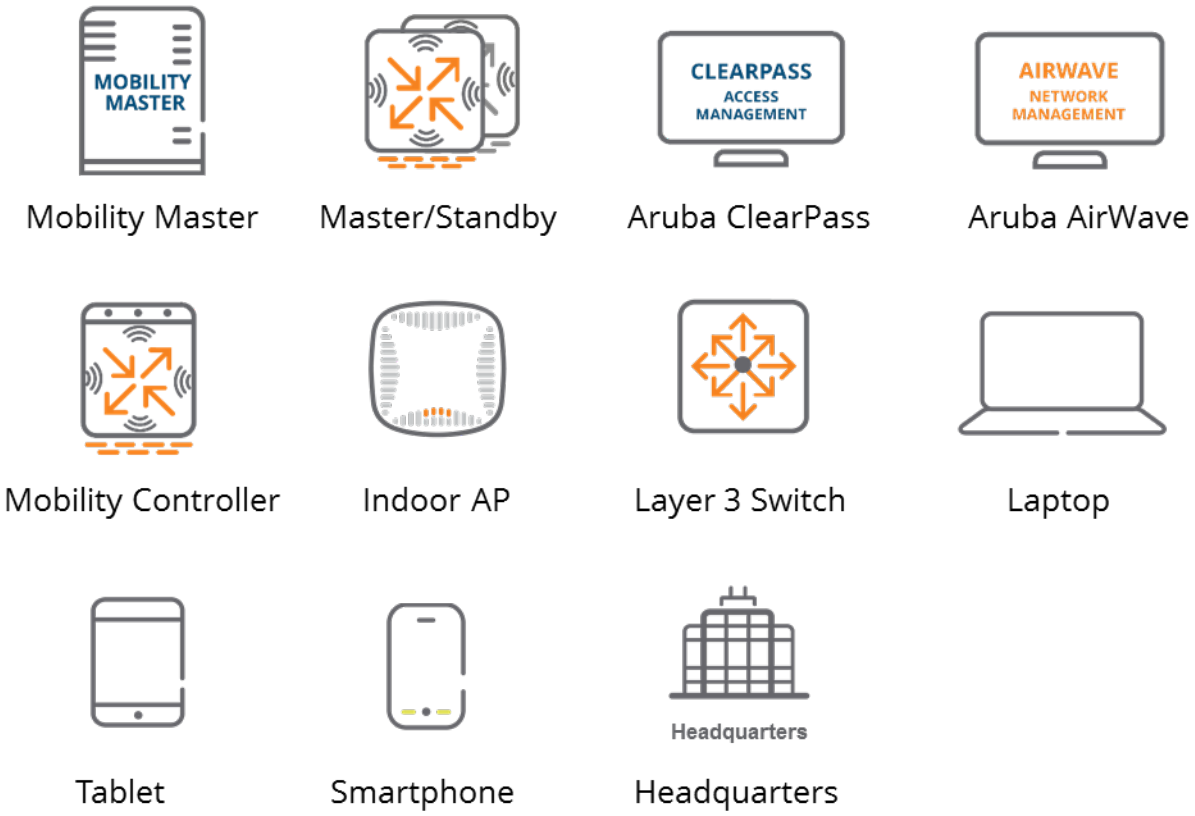

Figure 1 *Icon Set*

Migration Strategies

Migration of Aruba deployments from ArubaOS 6 to ArubaOS 8 involves a few more steps and precautions than performing a simple controller image upgrade. This chapter covers topics including migration methods, best practice recommendations on when to choose a particular method over another, and outlines how typical ArubaOS 6 network topologies can be migrated to ArubaOS 8. Depending on the ArubaOS 6 topology, migration can either be performed manually or by using the Migration Tool.

There is no automatic migration from 8.x standalone or Mobility Controller Master to ArubaOS 8 Mobility Master

Migration Tool

The Migration Tool is a VM-based server that can be used to migrate an ArubaOS 6 deployment to ArubaOS 8. The Migration Tool UI is used to supply IP addresses, credentials, and required roles for all of the controllers requiring migration. The tool then communicates with the Mobility Master, controllers, and VMware/KVM (if orchestrating), takes the required controller backups, upgrades the images to ArubaOS 8, and configures the controllers for communication with the Mobility Master.

Benefits

- Preserves existing WLAN configuration elements from ArubaOS 6 during migration which saves the time and effort required to possibly reconstruct them
- Multiple ArubaOS 6 deployment topologies (e.g. multiple master-locals) can be collapsed under a single Mobility Master
- Automates configuration backups, image downloads/upgrades, and license migration
- Supports both one-shot and staged migration approaches. E.g., the existing master can be used as a source for the Mobility Master configuration while other controllers are being migrated under the Mobility Master and the master itself may be migrated at a later stage
- Supports orchestration with both VMware and KVM

Supported Topologies for Migration

- Migrating Master-Local setup to Mobility Master or Master Controller Mode
- Migrating All-Master setup to Mobility Master
- Migrating to a stand-alone controller

It's important to note that the Migration Tool retains all aspects of the previous configuration including old and unused configuration elements. For additional details on the Migration Tool, please refer to the ArubaOS Migration Guide.

Manual Migration

Manual migration involves taking backups from all controllers, rebuilding them by individually upgrading each one to ArubaOS8, and performing the initial setup to convert them to Mobility Master-managed controllers or standalone controllers. Conversion to a Mobility Master-managed controller requires having the Mobility Master installed, configured, and ready to accept controller connections. A manual migration may also be performed by standing up a Mobility Master in parallel, building the configuration, and then moving one controller at a time.

Benefits

- While the Migration Tool allows for a safe and easy migration path for ArubaOS 6 deployments with standard network configuration, the topology and feature benefits introduced by ArubaOS 8 may require new configuration elements post migration. In such cases, it may be more effective to bring up a Mobility Master 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 (e.g. 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. For recommended topologies, please refer to the section on Migrating Different ArubaOS 6 Topologies later on in this chapter. Examples of topologies that can be migrated manually include the following:

- Master-Local to Mobility Master or Mobility Controller Master (MCM)
- All-Masters to Mobility Master
- Master-Branch (BOC) to Mobility Master
- Master/standby-master to standalone/standby-standalone
- Standalone to Mobility Master, Mobility Controller Master, or standalone
- Migrating to a standalone controller

Migration Tool vs. Manual Migration

There are no strict rules for determining whether to use the Migration Tool over manual migration or vice versa. The choice really comes down to context and the existing deployment's complexity. Existing deployments with a high degree of complexity may require a manual rebuild. The Migration tool may or may not be able to handle uncommon or very complex configuration elements (which may eventually get addressed over time with newer Migration Tool releases), so existing complexity will always need to be weighed against the capabilities of the tool. The points below provide a rough set of guidelines which can aid in determining which option is most appropriate for a given deployment:

- If migration is being performed primarily to support new topologies (or features that require moving to newer topologies) then it may be better to perform a manual migration
- The Migration Tool is suitable for collapsing multiple individual topologies under a single Mobility Master
- The Migration Tool is also suitable for deployments with basic Wi-Fi and guest features. However, deployments that use custom Captive Portal web pages and images may have to be rebuilt post migration

Migration Best Practice Recommendations

- Always backup everything in your existing topology prior to migration
- Always test the desired migration approach in a lab environment prior to migrating production deployments. The Migration Tool allows migration of local controllers without having to migrate the existing master controller which facilitates lab testing
- When lab testing, exercise caution when testing license migration via the "My Networking Portal" (MNP). There is a limitation of three license migrations
- If using Activate, make sure to update the ZTP settings if required, prior to migration

Migration Caveats

- Migration to ArubaOS 8 is not supported for 6000/M3, 3000, or 600 controller platforms. The prerequisite for migration is having 7000 and/or 7200 series controllers
- The 7000/7200 controller 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 before using the Migration Tool or the devices will require manual migration

- All controllers that are being migrated need to have their licenses in the same *My Networking Portal* account, otherwise license migration will not work. This applies to both manual Migration as well as the Migration Tool.
- 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 Mobility Controller Master in Mobility Controller Master mode
- The 7024 and lower models can only be converted to Mobility Master managed, standalone, or Mobility Controller Master managed controllers
- In scenarios where existing master-local deployments need to be migrated to a Mobility Controller Master managed deployment the Mobility Controller 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 Mobility Controller Master or on a new controller
- ArubaOS 8 does not currently have a migration path to take a standalone or Mobility Controller Master managed controller and bring it under a Mobility Master
- If a controller is repeatedly upgraded or downgraded between ArubaOS 6 and ArubaOS 8, subsequent migrations may fail due to temp files created on the controller that will 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

Migration to ArubaOS 8 requires 7000 or 7200 series controllers.

Controllers

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

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

Table *ArubaOS 8 Recommended Controllers*

Virtual Private Network Concentrators (VPNCs)

Mobility controllers can be configured as VPNCs to function as an IPSec termination point in the data center for controllers 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 mobility controller that is managed by the Mobility Master. VPNCs are placed under their own hierarchical node on the Mobility Master containing VPNC-specific configuration
- A VPNC may be backed up by a standby VPNC for redundancy purposes
- Though mobility controllers could terminate their IPSec connections directly on the Mobility Master (provided that the Mobility Master 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. As always, please refer to the latest ArubaOS release notes to confirm supported hardware:

- 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)

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 the 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 meaning APs terminate their active tunnels on the active master in addition to establishing standby tunnels to the standby master.

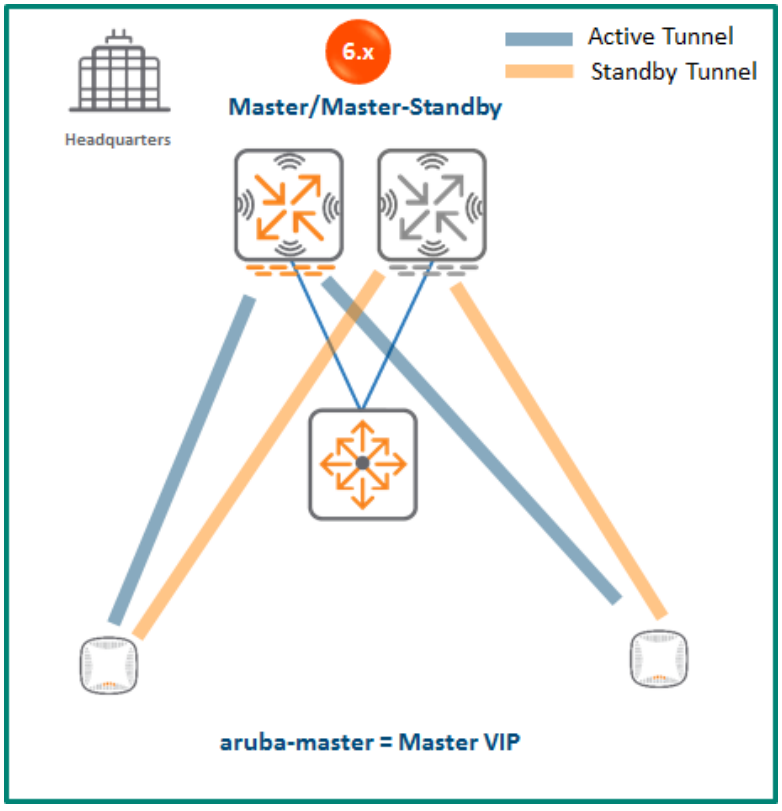

Figure 2 *ArubaOS 6 Master/Standby Architecture*

Since VRRP is being 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. I.e. APs will wait for eight missed heartbeats to the master before triggering failover to the standby master. However, the failover process will be instant and simultaneous for all APs unlike traditional VRRP failover which requires APs to re-bootstrap upon failover.

Mobility Master Terminating Mobility Controllers

Topology

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

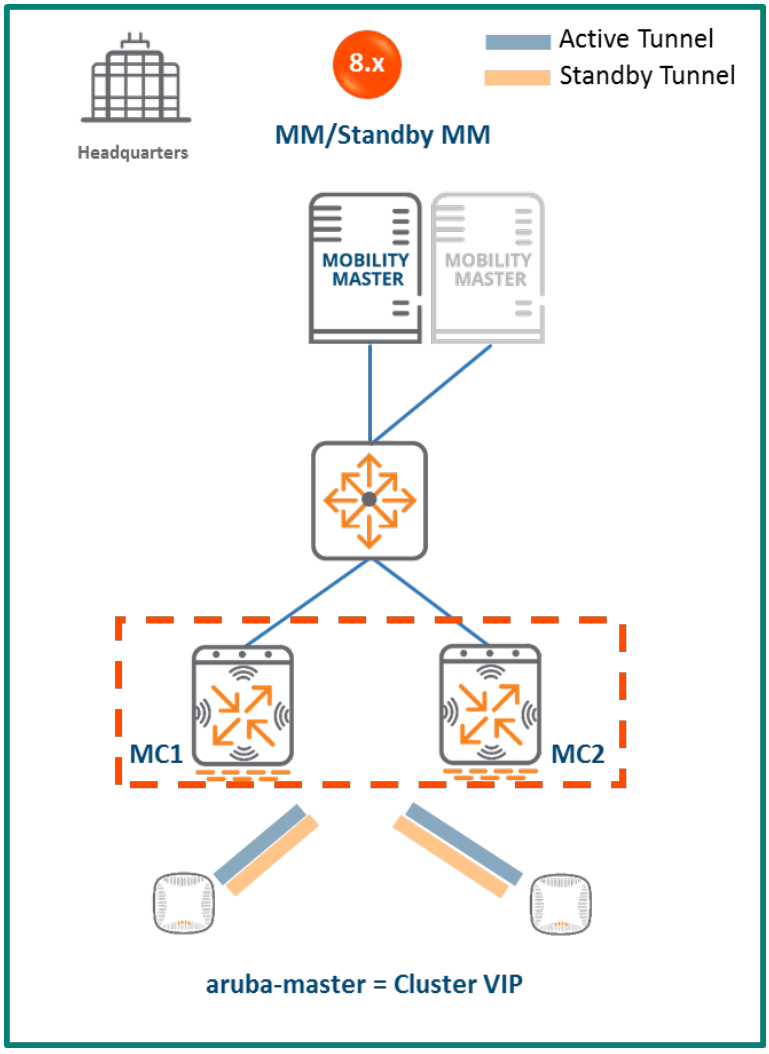

Figure 3 *Mobility Master Terminating Mobility Controllers*

Configuration Hierarchy

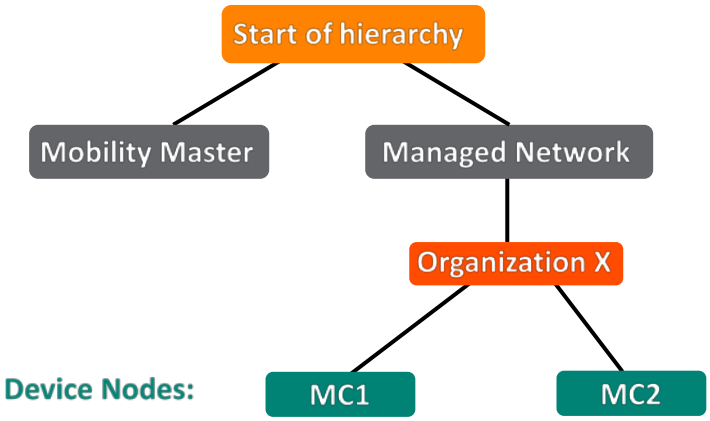

Figure 4 *Mobility Master Terminating Mobility Controllers Configuration Hierarchy*

Design Benefits

- **Maximize benefits** - The Mobility Master Terminating Mobility Controllers design is ideal for fully leveraging the capabilities of ArubaOS 8
- **Scalability** - New controllers can be easily added and managed by the Mobility Master
- **Ease of migration** - If an existing deployment has multiple topologies they can all be migrated under the Mobility Master 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 upgrades
- **AirMatch** - RF intelligence is centralized on the Mobility Master 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 etc. can be updated during runtime removing the need to schedule any maintenance cycles

Design Caveats

- The Mobility Master does not terminate APs. APs can only be terminated on a Mobility Controller

Migration Requirements

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

Migration Options

- Migration can occur manually or via the Migration Tool
- Manual migration steps are detailed below. To perform migration using the Migration Tool, please refer to the ArubaOS ArubaOS 8 Migration Guide

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

- Mobility Master Mobility Master 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 Mobility Master and perform initial setup
2. Configure licensing on the Mobility Master
3. Create a configuration hierarchy on Mobility Master and whitelist the active and standby master MAC addresses
4. Repeat step 1 if a backup Mobility Master is being installed as well
5. Configure Mobility Master redundancy if a backup Mobility Master has been installed. Going forward, the Mobility Master 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 and SSID. UI: **Managed Network>(select node)>AP Groups.** UI: **Managed Network>(select node)>Tasks>Create a new WLAN**
9. Whitelist the APs on the Mobility Master by populating the CPSec whitelist table (including mapping the APs to the appropriate AP group). UI: **Managed Network>(select node)>Configuration>Access Points>Whitelist**
10. Back up the existing configuration on the ArubaOS 6 master controllers. UI: **Maintenance>Backup Flash**
11. Upgrade the image on the active master to ArubaOS 8 and reboot it. UI: **Maintenance>Image Management**
12. Provision the master to be managed by Mobility Master via the CLI setup dialog. The master will now become MC1
13. Repeat steps 11-12 to convert the standby master to ArubaOS 8 as MC2
14. Change **aruba-master** to point to the cluster VIP
15. 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
16. Connect a wireless client to the SSID to test connectivity
17. Optionally, test seamless client failover by running a voice/video application and disconnecting the user's active controller

Standalone Mobility Controller and Standby Standalone

Topology

This ArubaOS 8 design consists of a standalone mobility controller backed up by another standalone mobility controller. As in the Master and Standby Master ArubaOS 6 design, VRRP is used between the two standalone 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 standalone controller in addition to setting up a standby tunnel to the standby standalone controller.

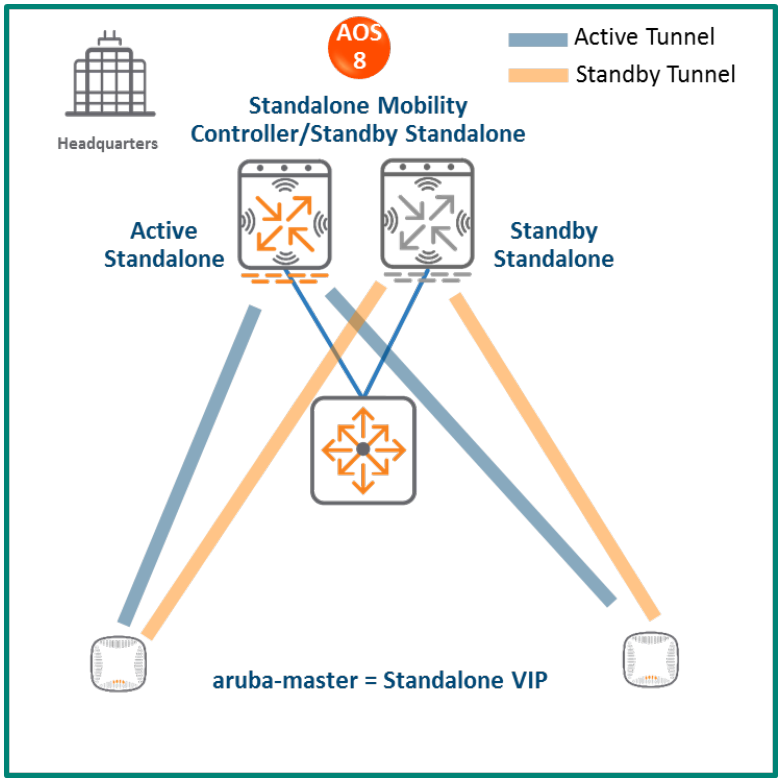

Figure 5 *Standalone Mobility Controller and Standby Standalone Topology*

Just as with the ArubaOS 6 Master and Standby Master design, the AP Fast Failover detection is not sub-second (i.e. APs will wait for eight missed heartbeats to the master), however the failover itself occurs quickly due to the APs already having standby tunnels to the standby standalone controller. The standalone becomes the new active controller in the event of a failure.

Design Benefits

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

Design Caveats

- APs can only terminate on the active standalone controller
- VRRP and AP Fast Failover are configured, however inter-controller heartbeats for AP Fast Failover is not supported in this design. AP Fast Failover detection will not be sub-second since the failover depends on VRRP latency. Upon detection the actual failover itself will be quick and simultaneous for all APs due to their existing standby tunnels

Migration Requirements

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

Migration Options

No migration tool support. 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 standalone and standby standalone 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 standalone controller via the CLI setup dialog. The master will now become an ArubaOS 8 standalone controller
4. Repeat steps 2-3 to convert the standby master into an ArubaOS 8 standalone controller
5. Configure licensing on the active standalone controller. The standby standalone controller will inherit licenses from the active standalone once database synchronization is configured as part of step 6

6. Configure master redundancy between the two standalone controllers. A VIP will be created between MC1 and MC2 as a result of the VRRP configuration. Going forward, configuration management will occur through the VIP
7. Create an AP group and SSID under the Mobility Master node (/mm in CLI). This will push the common configuration to both standalone controllers
8. Configure AP Fast Failover for both standalone controllers
9. Whitelist APs under **Mobility Master>Configuration>Access Points>Whitelist**
10. Change **aruba-master** to point to the standalone VIP
11. The APs will then find the VIP (i.e. active standalone controller), upgrade their images, terminate their tunnels on the VIP, 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 standalone controller

Master and Single Local

In this ArubaOS 6 design, a master controller is managing a local controller. The same controller models are recommended for the master and local. There can be two variations of this design:

Redundancy Model (also known as 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 in the event the APs lose connectivity to the local controller, they can instantly fail over to the master.

Capacity Model (also known as 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.

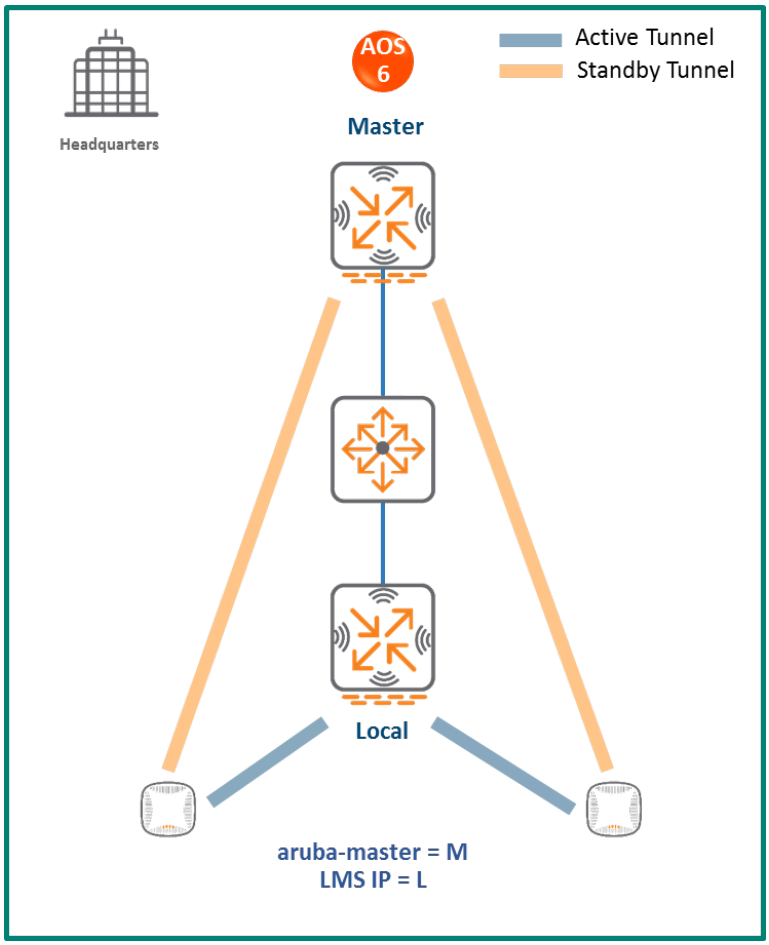

Figure 6 *Master and Single Local*

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 (i.e. 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 standalone controller. The standby standalone controller becomes the new active controller upon failover

Mobility Master Terminating Mobility Controllers

Topology

In this ArubaOS 8 design, a Mobility Master is initially deployed and configured. The ArubaOS 6 master and local controllers become Mobility Controllers managed by the Mobility Master. 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.

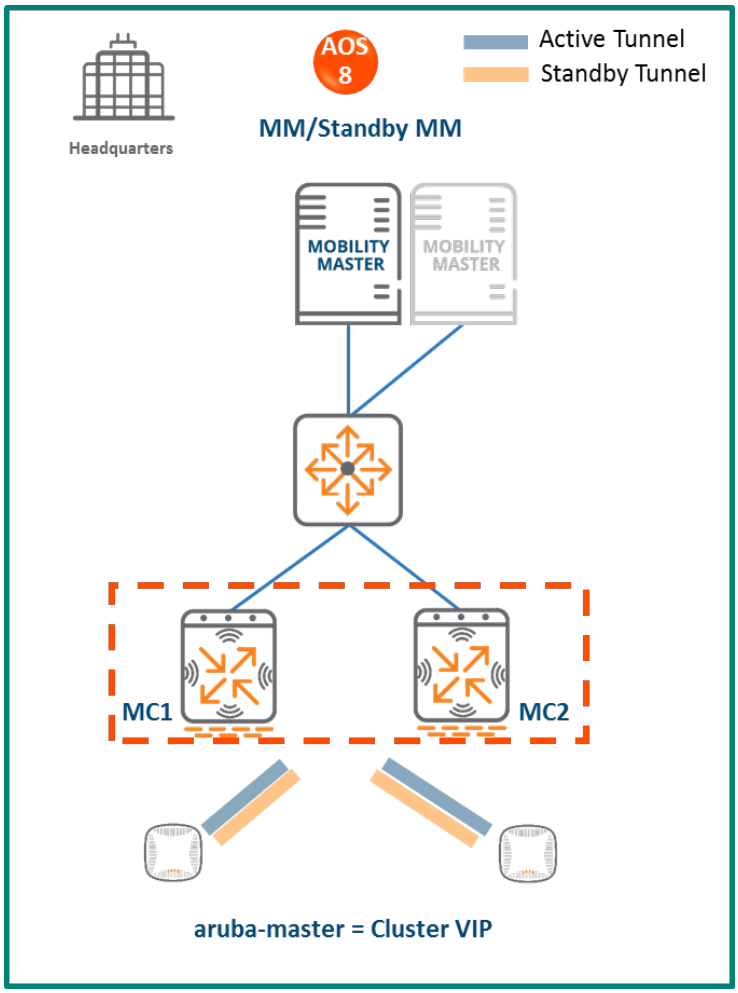

Figure 7 *Mobility Master Terminating Mobility Controllers Topology*

Configuration Hierarchy

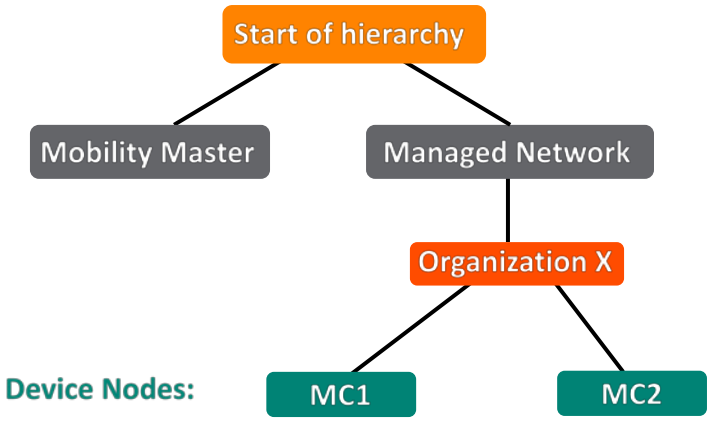

Figure 8 *Mobility Master Terminating Mobility Controllers Configuration Hierarchy*

Design Benefits

- **Maximize benefits** - The Mobility Master Terminating Mobility Controllers design is ideal for fully leveraging the capabilities of ArubaOS 8
- **Scalability** - New controllers can be easily added and managed by the Mobility Master
- **Ease of migration** - If an existing deployment has multiple topologies they can all be migrated under the Mobility Master 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 upgrades
- **AirMatch** - RF intelligence is centralized on the Mobility Master 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 etc. can be updated during runtime removing the need to schedule any maintenance cycles

Design Caveats

- The Mobility Master does not terminate any APs. APs can only be terminated on mobility controllers.

Migration Requirements

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

Migration Options

- Migration can occur manually or via the Migration Tool
- Manual migration steps are detailed below. To perform migration using the Migration Tool, please refer to the ArubaOS ArubaOS 8 Migration Guide

Migration Strategy

Existing ArubaOS 6 Deployment

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

New ArubaOS 8 Deployment

- Mobility Master backed up by a standby Mobility Master
- Mobility Master 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 by performing the following steps:

1. Deploy the Mobility Master and perform initial setup
2. Configure licensing on the Mobility Master
3. Create a configuration hierarchy on the Mobility Master and whitelist the master and local controller MAC addresses
4. Repeat step 1 if a Mobility Master is also being installed
5. Configure Mobility Master redundancy if a Mobility Master has been deployed. The Mobility Master VIP will be used moving forward for configuration management
6. Configure clustering between the Mobility 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 and SSID. UI**: Managed Network>(select node)>AP Groups**. UI: **Managed Network>(select node)>Tasks>Create a new WLAN**
9. Whitelist your APs on the Mobility Master and map them to the appropriate AP group. UI: **Managed Network>(select node)>Configuration>Access Points>Whitelist**
10. Back up the existing configuration on the ArubaOS 6 master and local. UI: **Maintenance>Backup Flash**
11. Upgrade the image on the local to ArubaOS 8 and reboot it. UI: **Maintenance>Image Management**
12. Provision the local to be managed by the Mobility Master via the CLI setup dialog. The local will now become MC1
13. Now repeat steps 11-12 to convert the master to MC2
14. Change **aruba-master** to point to the cluster VIP
15. The APs that were previously terminating on the local 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
16. Connect a wireless client to the SSID and test connectivity
17. Optionally, test seamless client failover by running a voice/video application and disconnecting the user's active controller

Standalone Mobility Controller with Master Redundancy

Topology

This ArubaOS 8 design consists of a standalone mobility controller backed up by another standalone mobility controller. VRRP is enabled between the two standalone controllers in an active-standby configuration. High Availability (AP Fast Failover) is also configured between the controllers so that APs set up a standby tunnel to the standby standalone controller in addition to terminating their tunnels on the active standalone.

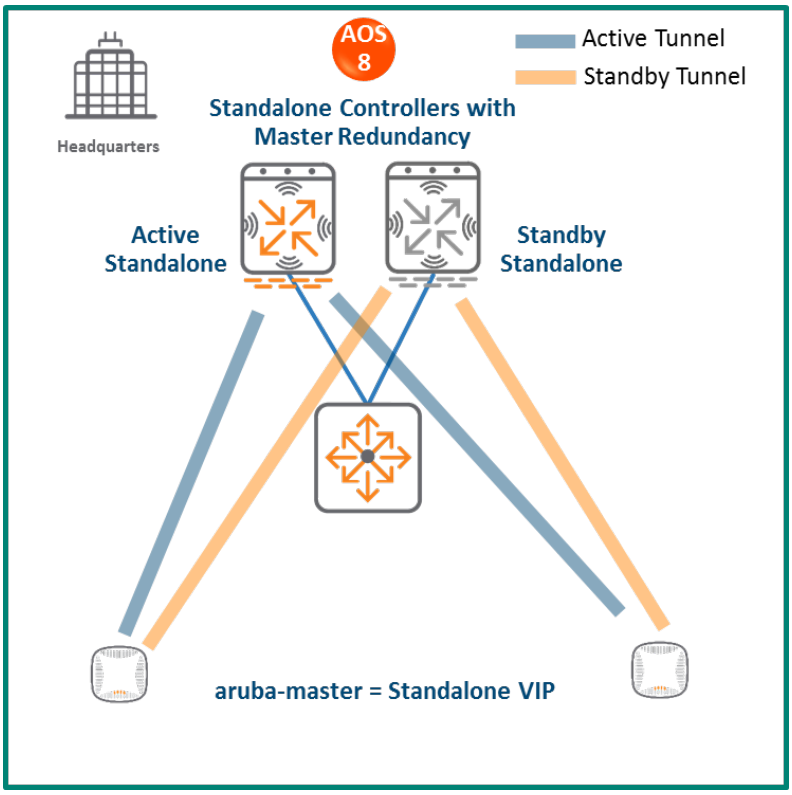

Figure 9 *Standalone Mobility Controller with Master Redundancy*

The AP Fast Failover detection is not sub-second (i.e. APs will wait for eight missed heartbeats to the master), however the failover itself occurs quickly due to the APs already having standby tunnels to the standby standalone controller. The standalone becomes the new active controller in the event of a failure.

Design Benefits

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

Design Caveats

- APs can only terminate on the active standalone controller
- No AP Fast Failover. The master redundancy configuration between the two standalone controllers uses VRRP to detect failover meaning that AP failover will not be sub-second since the failover mechanism is dependent on VRRP latency

Migration Requirements

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

Migration Options

No migration tool support. Migration can only be performed manually.

Migration Strategy

Existing ArubaOS 6 Deployment

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

New ArubaOS 8 Deployment

- Active standalone and standby standalone 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. Back up the existing configuration on the ArubaOS 6 master and local controller
2. Upgrade the image on the local to ArubaOS 8 and reboot the controller
3. Provision the local as an ArubaOS 8 standalone controller via the CLI setup dialog. The local will become a standalone controller
4. Upgrade the image on the master to ArubaOS 8 and reboot the controller
5. Provision the master as an ArubaOS 8 standalone controller via the CLI setup dialog. The master will become another standalone controller

6. Configure licensing on the active standalone controller. The standby standalone controller will inherit licenses from the active standalone once the database synchronization is configured as part of step 7
7. Configure master redundancy between the two standalone controllers. A VIP will be created as a result of the VRRP configuration. Going forward, configuration management will occur through the VIP
8. Navigate to **/mm** and create an AP group and SSID
9. Configure AP Fast Failover for both standalone controllers
10. Whitelist your APs under **Mobility Master>Configuration>Access Points>Whitelist**
11. Change **aruba-master** to point to the standalone VIP
12. The APs will then find the VIP (i.e. active standalone controller), upgrade their images, terminate their tunnels on the VIP, and broadcast the configured SSID
13. Connect a wireless client to the SSID and test connectivity
14. Optionally, test client failover by disconnecting the active standalone controller

Master and Multiple Locals (Single Campus)

In this ArubaOS 6 design, a master (backed up by a standby master) controller is managing 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.

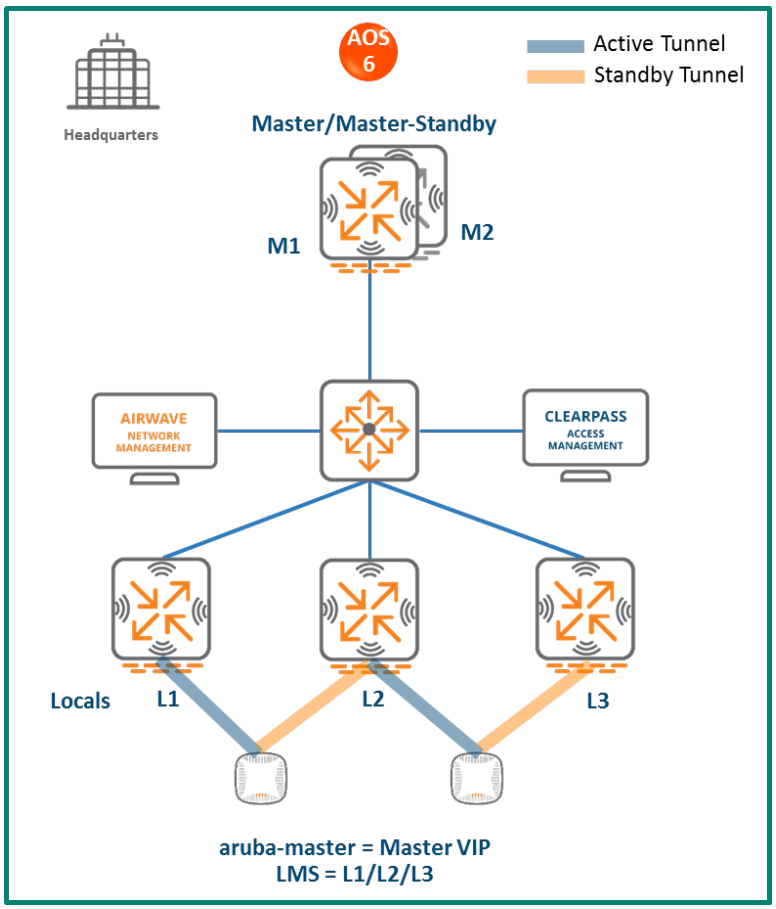

Figure 10 *Master Controller and Multiple Locals*

Mobility Master Terminating Mobility Controllers

Topology

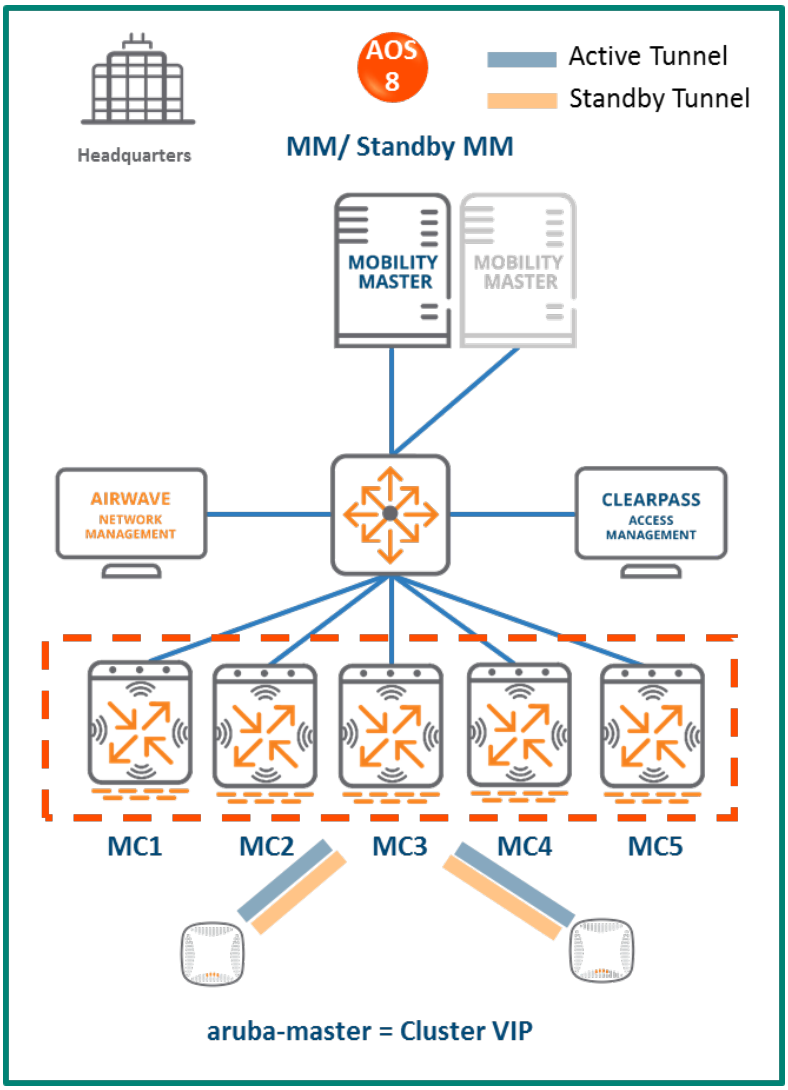

Figure 11 *Mobility Master Terminating Mobility Controllers Topology*

In this ArubaOS 8 design:

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

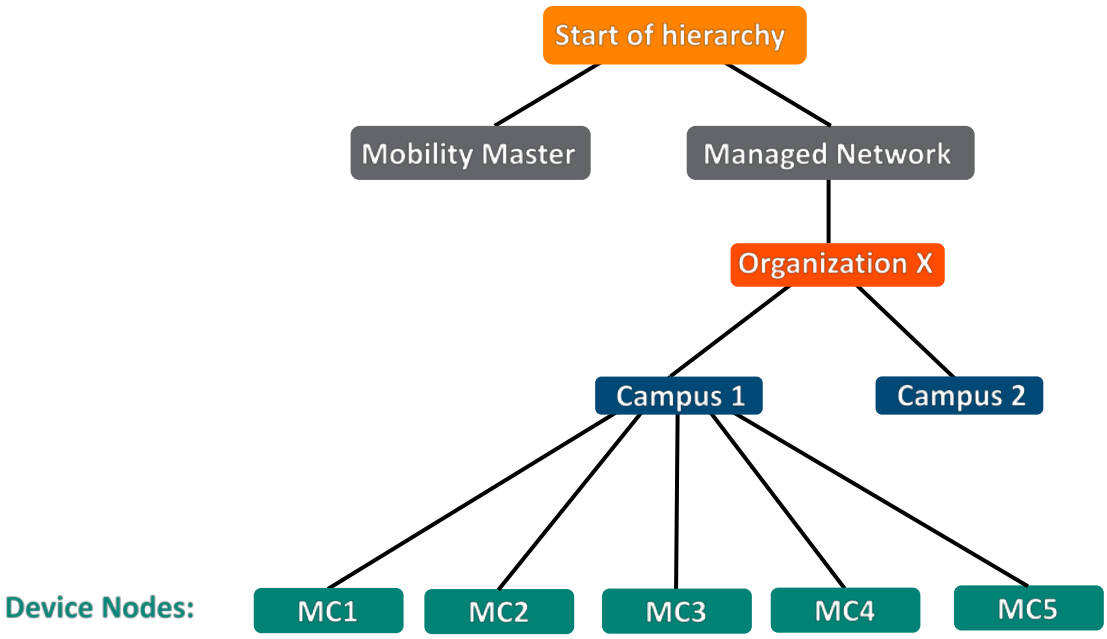

Figure 12 *Mobility Master Terminating Mobility Controllers Configuration Hierarchy*

Design Benefits and Caveats

- **Maximize benefits** - The Mobility Master Terminating Mobility Controllers design is ideal for fully leveraging the capabilities of ArubaOS 8
- **Scalability** - New controllers can be easily added and managed by the Mobility Master
- **Ease of migration** - If an existing deployment has multiple topologies they can all be migrated under the Mobility Master 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 upgrades
- **AirMatch** - RF intelligence is centralized on the Mobility Master 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 etc. can be updated during runtime removing the need to schedule any maintenance cycles.

Migration Requirements

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

Migration Options

- Migration can occur manually or via the Migration Tool
- Manual migration steps are detailed below. To perform migration using the Migration Tool, please refer to the ArubaOS ArubaOS 8 Migration Guide

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

- Mobility Master backed up by a standby Mobility Master
- Mobility Master managing MC1, MC2, MC3, MC4, and MC5
- APs terminating on:

- MC1, MC2, MC3 in the case of 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 the 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 Mobility Master and perform initial setup
2. Configure licensing on the Mobility Master
3. Create a configuration hierarchy and whitelist the MAC addresses of M1, M2, and L1-L3 on the Mobility Master
4. Repeat step 1 if installing a backup Mobility Master
5. Configure Mobility Master redundancy if a backup Mobility Master is being installed. Going forward, use the Mobility Master VIP for configuration management
6. Configure clustering between the Mobility 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 and SSID. UI: **Managed Network>(select node)>AP Groups**. UI: **Managed Network>(select node)>Tasks> Create a new WLAN**
9. Whitelist the APs on the Mobility Master and map them to the appropriate AP group. UI: **Managed Network>(select your node)>Configuration>Access Points>Whitelist**.
10. Back up the existing configuration on the ArubaOS 6 masters and locals. UI: **Maintenance>Backup Flash**
11. Upgrade the image on local L1 to ArubaOS 8 and reboot it. UI: **Maintenance>Image Management**
12. Provision local L1 to be managed by the Mobility Master via the CLI setup dialog. L1 will become ArubaOS 8 MC1
13. Repeat steps 11-12 for both L2 and L3 to convert them into ArubaOS 8 MC2 and MC3
14. 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
15. Change **aruba-master** to point to the cluster VIP
16. The APs that were terminating on the locals 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
17. Connect a wireless client to the SSID and test connectivity

18. Optionally, test seamless client failover by running a voice/video application and disconnecting the user's active controller

Mobility Controller Master Terminating Mobility Controllers

Topology

This ArubaOS 8 design consists of a hardware controller deployed as a Mobility Controller Master (optionally backed up by another Mobility Controller Master) that manages a group of mobility controllers.

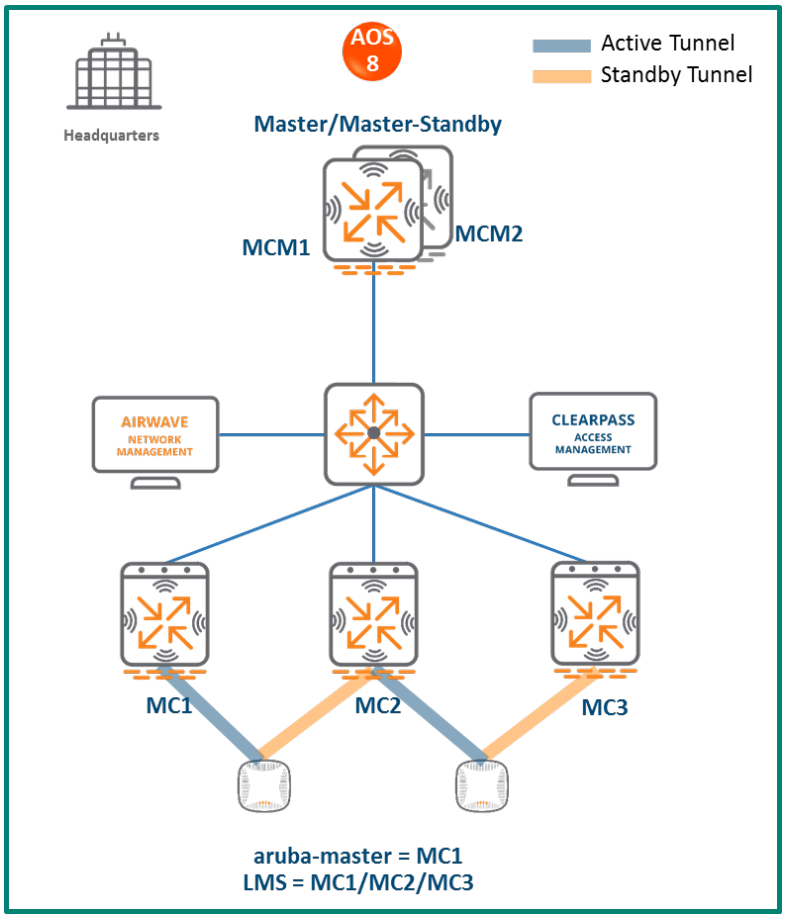

Figure 13 *Mobility Controller Master Terminating Mobility Controllers Topology*

This design helps transition deployments to ArubaOS 8 that are unable to deploy a Mobility Master. This Mobility Controller Master topology should eventually be migrated to a Mobility Master 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 Mobility Controller Masters (MCM1 and MCM2).

- The ArubaOS 6 local controllers (L1, L2 and L3) become ArubaOS 8 Mobility Controllers (MC1, MC2 and MC3).
- APs terminating on L1, L2, and L3 will now terminate on MC1, MC2, and MC3 respectively.

Configuration Hierarchy

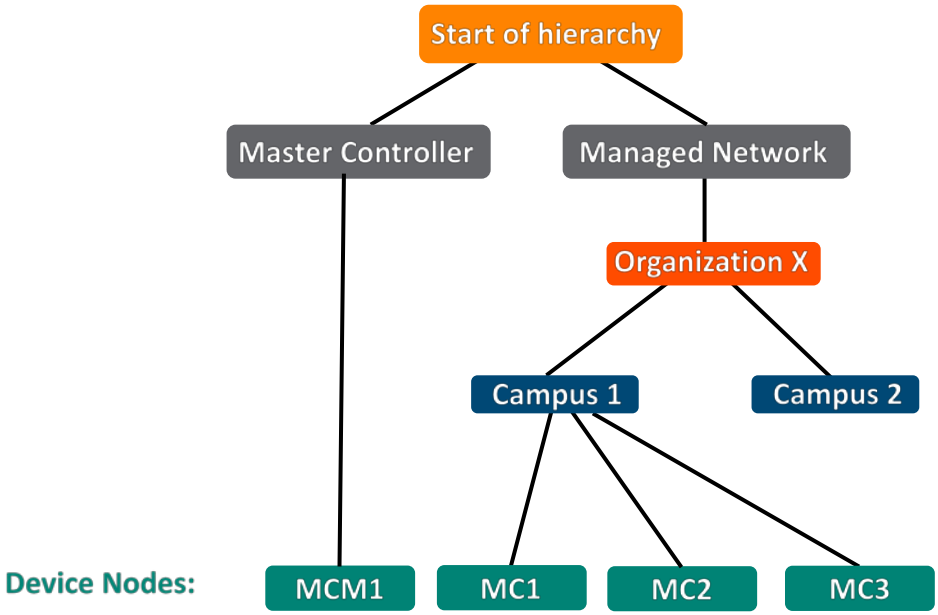

Figure 14 *Mobility Controller Master Terminating Mobility Configuration Hierarchy*

Design Benefits

- A similar topology is maintained in which the Mobility Controller Master manages the Mobility Controllers and no additional hardware is required as long as the Mobility Controller 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 Mobility Controller Master

Design Caveats

- Requires purchase of an Aruba 7030 or larger controller to serve as the Mobility Controller Master as well as the backup MCM if one is not already present
- AP termination on the Mobility Controller 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 Mobility Controllers but cannot failover to the Mobility Controller Master

- The clustering feature is not supported in a Mobility Controller Master deployment. AP Fast Failover between Mobility Controllers 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 Mobility Controller 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 Mobility Controller 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

- Migration can occur manually or via the Migration Tool
- Manual migration steps are detailed below. To perform migration using the Migration Tool, please refer to the ArubaOS ArubaOS 8 Migration Guide

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. UI: **Maintenance>Backup Flash**
2. Upgrade the image on master M1 to ArubaOS 8 and reboot the controller
3. Provision M1 as a Mobility Controller 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 Mobility Controller Master VIP will be used for configuration management moving forward
6. Configure licensing on the Mobility Controller Master
7. Create a configuration hierarchy on the Mobility Controller 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. UI: **Managed Network>(select node)>AP Groups**
9. Create an SSID for each AP group. UI: **Managed Network>(select node)>Tasks> Create a new WLAN**
10. Whitelist the APs on the Mobility Controller Master. This includes mapping them to their respective AP groups. UI: **Managed Network>(select node)>Configuration>Access Points > Whitelist**
11. Upgrade the image on local L1 to ArubaOS 8 and reboot it. UI: **Maintenance>Image Management**
12. Provision local L1 to be managed by the Mobility Controller 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 Mobility Controller 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 Mobility Controller Master to enable sub-second AP failover between the Mobility Controllers

Master and Multiple Locals (Multiple Campuses)

In this ArubaOS 6 design, a master controller backed up by a standby master is managing 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.

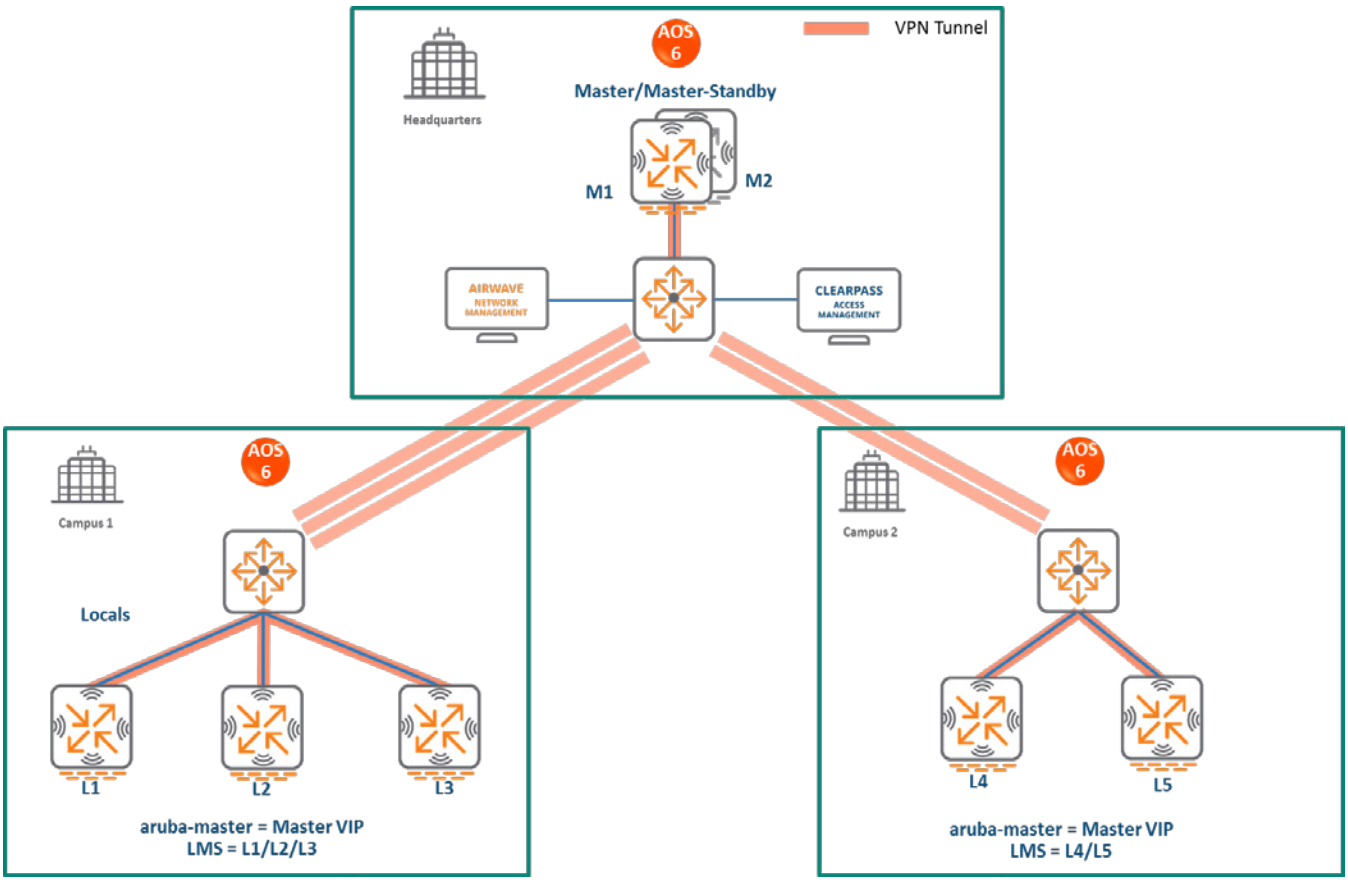

Figure 15 *Master and Multiple Locals (Multiple Campuses)*

Mobility Master Terminating Mobility Controllers

Topology

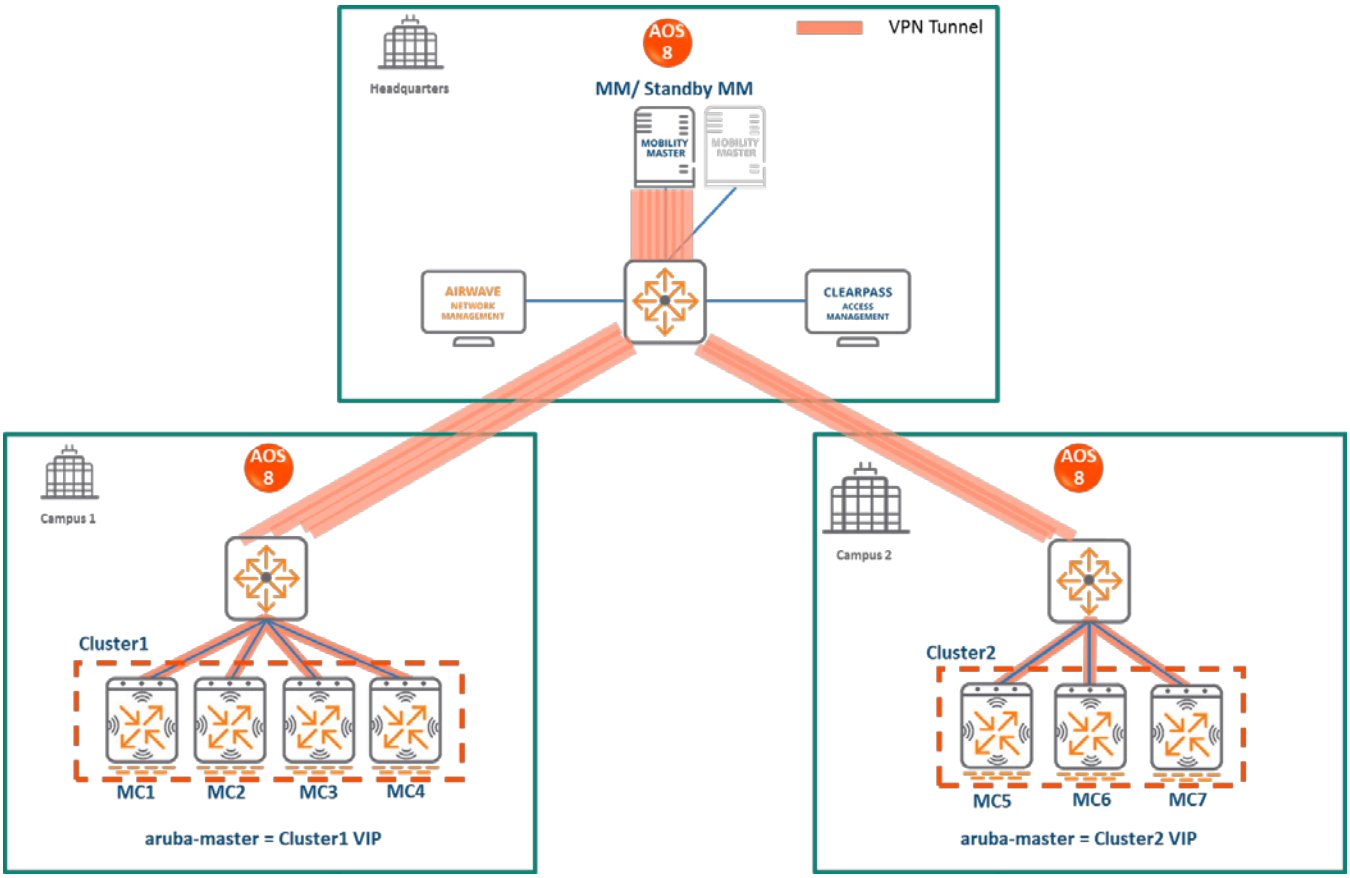

Figure 16 *Mobility Master Terminating Mobility Controllers Topology*

In this ArubaOS 8 design:

- A Mobility Master (either virtual or hardware) is deployed and configured along with a backup Mobility Master
- In Campus 1, each ArubaOS 6 local controller (L1, L2, and L3) becomes an ArubaOS 8 Mobility Controller (MC1, MC2, MC3)
- In Campus 2, each ArubaOS 6 local controller (L4 and L5) becomes an ArubaOS 8 Mobility Controller (MC5 and MC6)
- The Mobility Controllers in each campus are configured as a cluster and will share the AP and client load
- All Mobility Controllers terminate their IPSec tunnels on the Mobility Master
- 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 colocated, 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 Mobility Controllers (MC4 and MC7) which can be repurposed to become cluster members in each campus
- In the case of remote sites that are separated from the Mobility Master 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

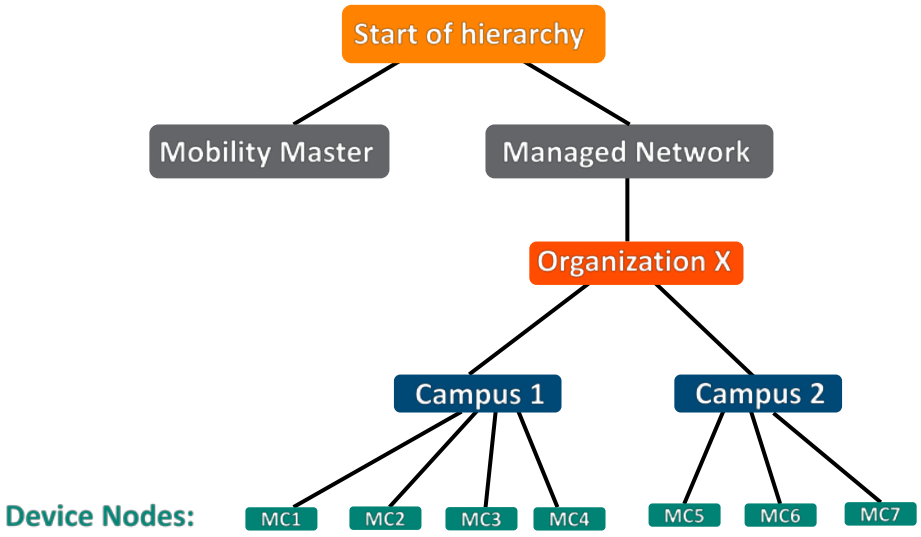

Figure 17 *Mobility Master Terminating Mobility Controllers Configuration Hierarchy*

Design Benefits

- **Maximize benefits** - The Mobility Master Terminating Mobility Controllers design is ideal for fully leveraging the capabilities of ArubaOS 8
- **Scalability** - New controllers can be easily added and managed by the Mobility Master
- **Ease of migration** - If an existing deployment has multiple topologies they can all be migrated under the Mobility Master 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 upgrades
- **AirMatch** - RF intelligence is centralized on the Mobility Master 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 etc. can be updated during runtime removing the need to schedule any maintenance cycles

Design Caveats

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

Migration Requirements

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

Migration Options

- Migration can occur manually or via the Migration Tool
- Manual migration steps are detailed below. To perform migration using the Migration Tool, please refer to the ArubaOS ArubaOS 8 Migration Guide

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

- Mobility Master backed up by a standby Mobility Master
- The Mobility Master 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. In the case of a multi-site campus, the APs could terminate on any of the three LMS IPs (MC1, MC2, or MC3)

MM specific:

1. Deploy the Mobility Master and perform initial setup
2. Configure licensing on the Mobility Master
3. Create a configuration hierarchy and whitelist the MAC addresses of M1, M2, L1-L5 on the Mobility Master. 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 Mobility Master is being installed
5. Configure Mobility Master redundancy if a backup Mobility Master is being installed. The Mobility Master VIP will be used for configuration management moving forward

Campus1:

1. Configure clustering between MC1-MC4. Also enable AP load balancing. UI: **Managed Network>Campus1>Services>Cluster**

2. Create a VIP (now referred to as "Cluster1 VIP") between the cluster members MC1-MC4. UI: **Managed Network>Campus1>Services>Redundancy>Virtual Router Table**. Optionally create VIPs for RADIUS COA
3. Create an AP group and SSID. UI: **Managed Network>Campus1>AP Groups.** UI: **Managed Network>Campus1>Tasks>Create a new WLAN**
4. Whitelist the Campus1 APs on the Mobility Master. This includes mapping them to the appropriate AP group. UI: **Managed Network>Campus1>Configuration>Access Points>Whitelist**
5. Back up the existing configuration on ArubaOS 6 controllers L1-L3 and M1. UI: **Maintenance>Backup Flash**
6. Upgrade the image on local L1 to ArubaOS 8 and reboot it. UI: **Maintenance>Image Management**
7. Provision local L1 to be managed by the Mobility Master via the CLI setup dialog. L1 will now become MC1
8. Repeat steps 6-7 to convert L2, L3, and M1 to MC2, MC3, and MC4 respectively
9. In the Campus1 network, point **aruba-master** towards the Cluster1 VIP
10. 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
11. Connect a wireless client to the SSID and test connectivity
12. Optionally, test seamless client failover by running a voice/video application and disconnecting the user's active controller

Campus2:

1. Configure clustering between the MC5, MC6 and MC7 and enable AP load balancing. UI: **Managed Network>Campus2>Services>Cluster**
2. Create a VIP (now referred to as "Cluster2 VIP") between the cluster members MC5, MC6, and MC7. UI: **Managed Network>Campus2>Services>Redundancy>Virtual Router Table**. Optionally create VIPs for RADIUS COA
3. Create an AP group and SSID. UI: **Managed Network>Campus2 > AP Groups.** UI: **Managed Network>Campus2>Tasks>Create a new WLAN**
4. Whitelist the Campus2 APs on the Mobility Master. This includes mapping them to the appropriate AP group. UI: **Managed Network>Campus1>Configuration>Access Points>Whitelist**
5. Back up the existing configuration on the ArubaOS 6 controllers L4, L5, and M2. UI: **Maintenance>Backup Flash**

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

Mobility Controller Master Terminating Mobility Controllers

Topology

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

This design helps transition deployments to ArubaOS 8 that are unable to deploy a Mobility Master. This Mobility Controller Master topology should eventually be migrated to a Mobility Master topology in order to take full advantage of the capabilities offered by ArubaOS 8.

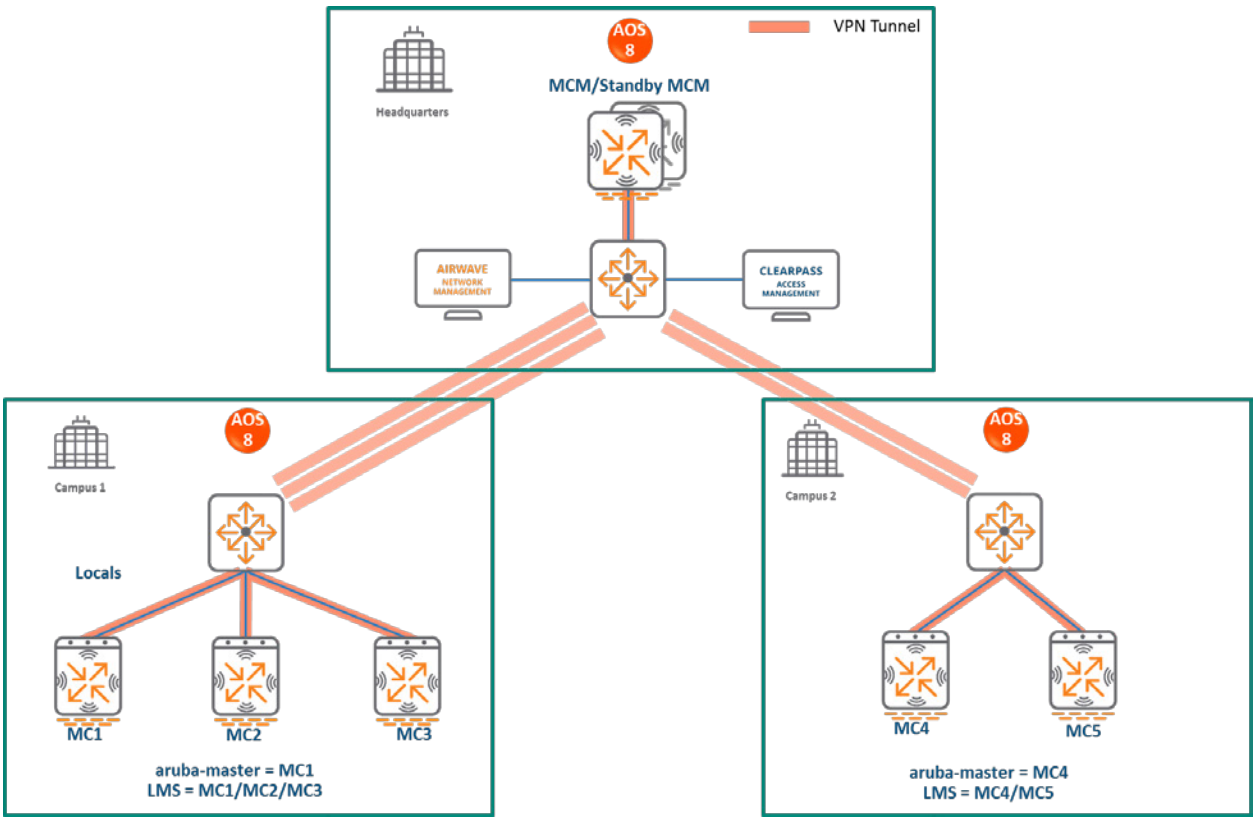

Figure 19 *Mobility Controller Master Terminating Mobility Controllers Topology*

In this design:

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

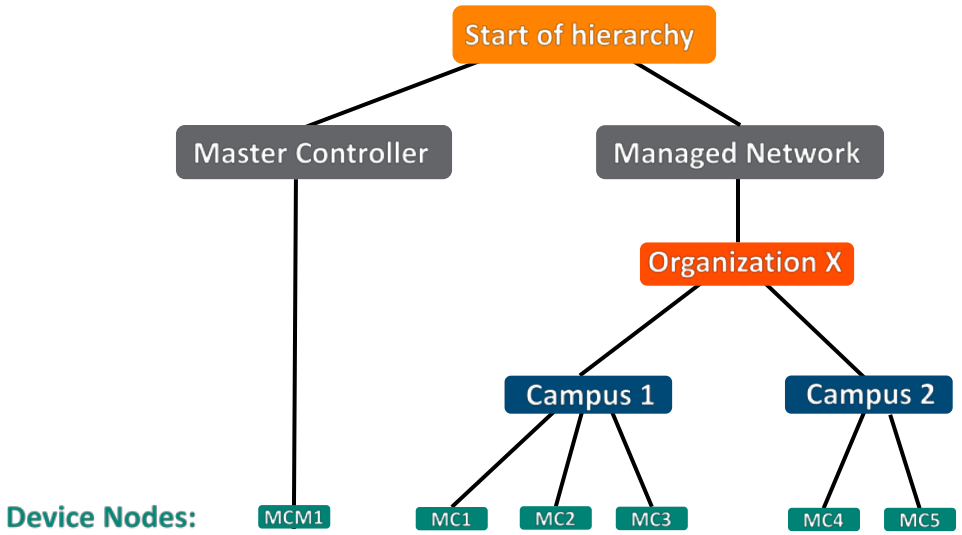

Figure 20 *Mobility Controller Master Terminating Mobility Controllers Configuration Hierarchy*

Design Benefits

- A similar topology is maintained in which the Mobility Controller Master manages the Mobility Controllers and no additional hardware is required as long as the Mobility Controller 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 Mobility Controller Master

Design Caveats

- Requires purchase of an Aruba 7030 or larger controller to serve as the Mobility Controller Master as well as the backup MCM if one is not already present
- AP termination on the Mobility Controller 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 Mobility Controllers but cannot failover to the Mobility Controller Master

- The clustering feature is not supported in a Mobility Controller Master deployment. AP Fast Failover between Mobility Controllers 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 Mobility Controller 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 Mobility Controller 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

- Migration can occur manually or via the Migration Tool
- Manual migration steps are detailed below. To perform migration using the Migration Tool, please refer to the ArubaOS ArubaOS 8 Migration Guide

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:

Mobility Controller Master specific:

1. Backup the existing configuration on the ArubaOS 6 masters and locals. UI: **Maintenance>Backup Flash**
2. Upgrade master M1 to ArubaOS 8 and reboot the controller. UI: **Maintenance>Image Management**
3. Provision M1 as a Mobility Controller 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 Mobility Controller Master VIP will be used for configuration management moving forward
6. Configure licensing on the Mobility Controller Master
7. Create a configuration hierarchy on the Mobility Controller 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. UI: **Managed Network>Campus1>AP Groups**
2. Create a common SSID or one for each AP group. UI: **Managed Network>Campus1>Tasks>Create a new WLAN**
3. Whitelist the APs on the Mobility Controller Master. This includes mapping them to the appropriate AP group. UI: **Managed Network>Campus1>Configuration>Access Points>Whitelist**
4. Upgrade the image on local L1 to ArubaOS 8 and reboot it. UI: **Maintenance>Image Management**
5. Provision local L1 to be managed by the Mobility Controller 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 Mobility Controller 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 Mobility Controller Master to enable AP failover between the MCs

Campus2:

1. Create two AP groups, each with LMS IP of MC1 and MC2 respectively. UI: **Managed Network>Campus2>AP Groups**
2. Create a common SSID or one for each AP group. UI: **Managed Network>Campus2>Tasks>Create a new WLAN**
3. Whitelist the APs on the Mobility Controller Master. This includes mapping them to the appropriate AP group. UI: **Managed Network>Campus2>Configuration>Access Points>Whitelist**
4. Upgrade the image on local L4 to ArubaOS 8 and reboot it. UI: **Maintenance>Image Management**
5. Provision local L4 to be managed by the Mobility Controller 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 Mobility Controller 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.

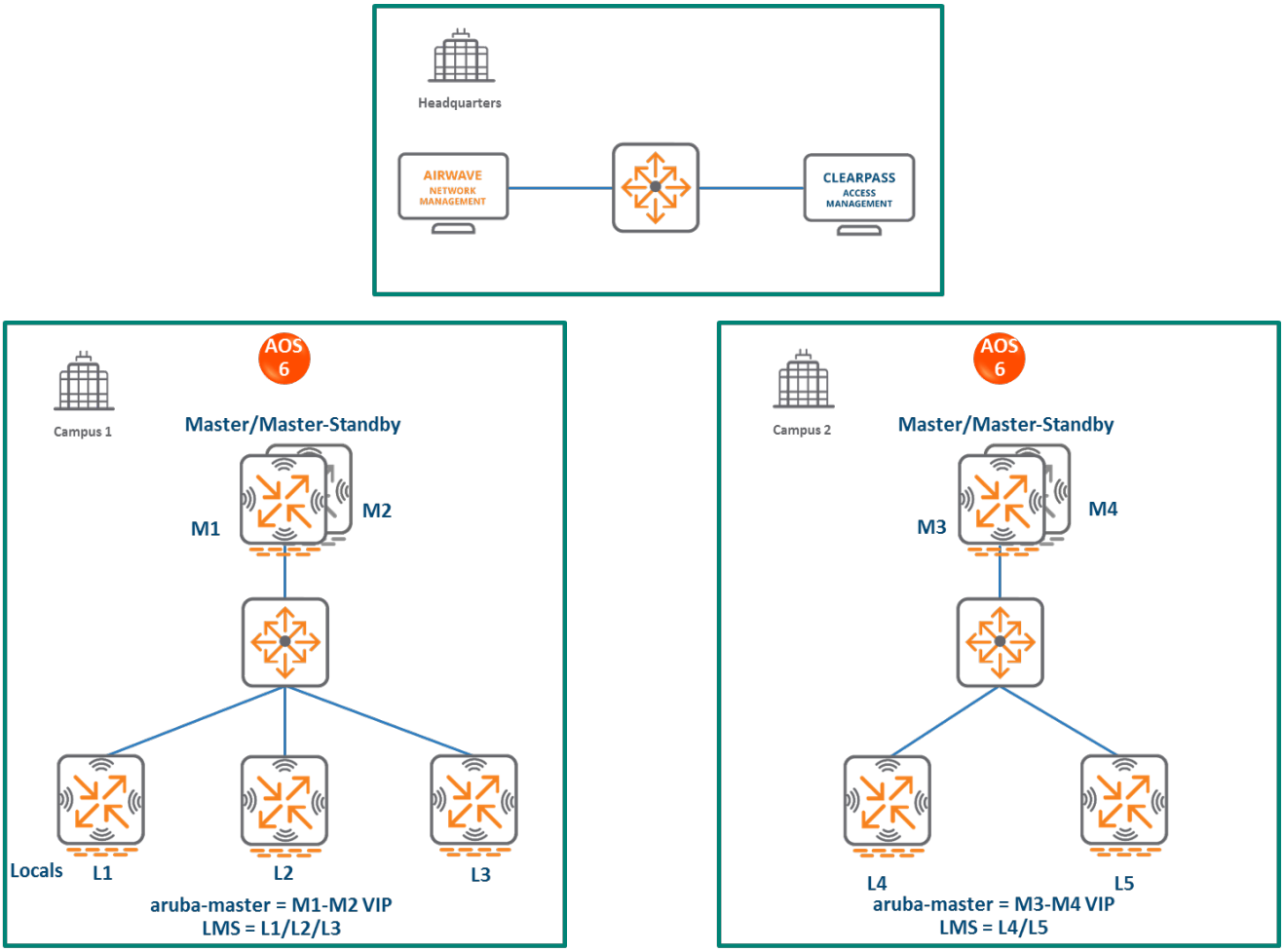

Figure 21 *Multiple Master-Locals*

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

Mobility Master Terminating Mobility Controllers

Topology

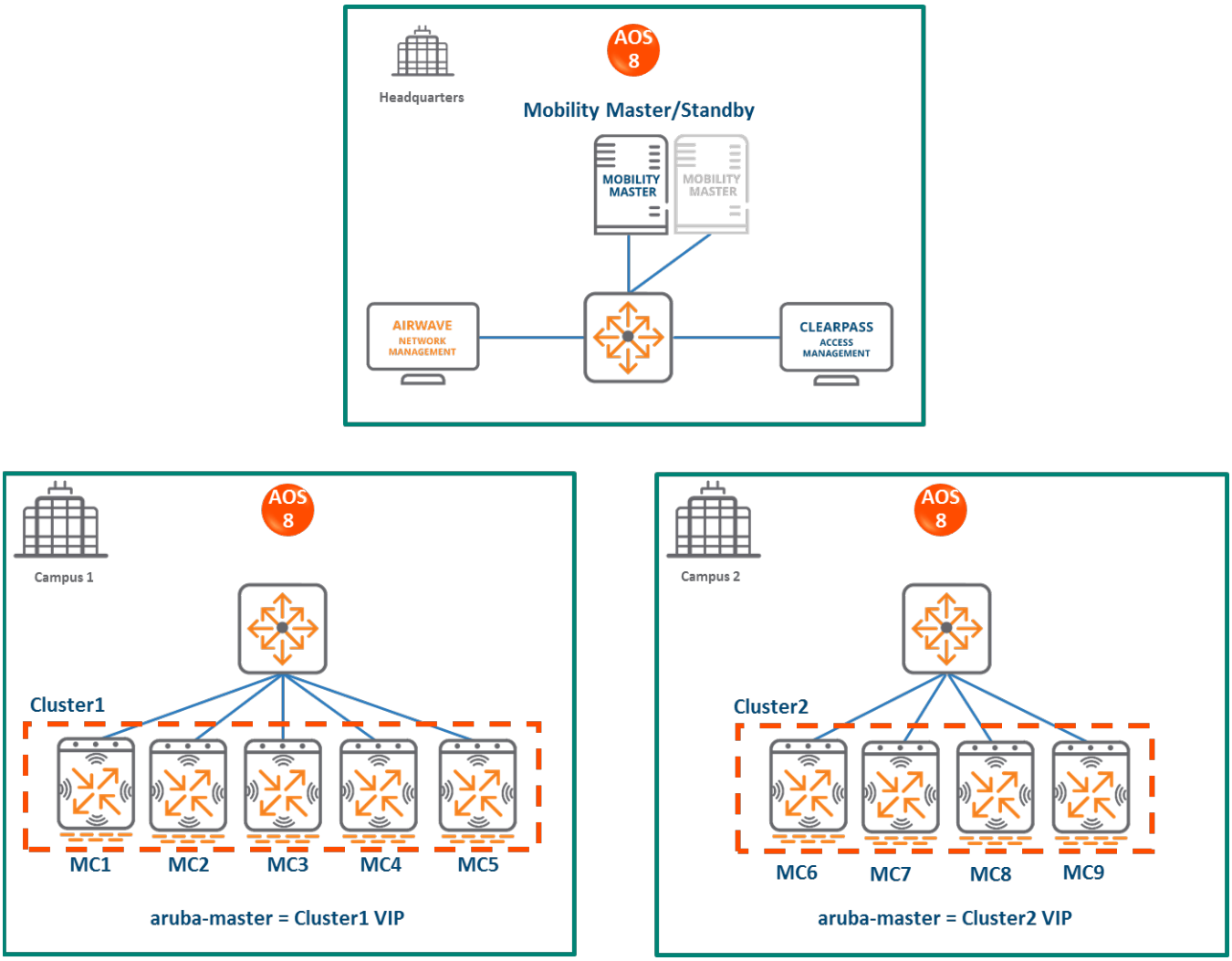

Figure 22 *Mobility Master Terminating Mobility Controllers Topology*

HQ/DC:

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

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

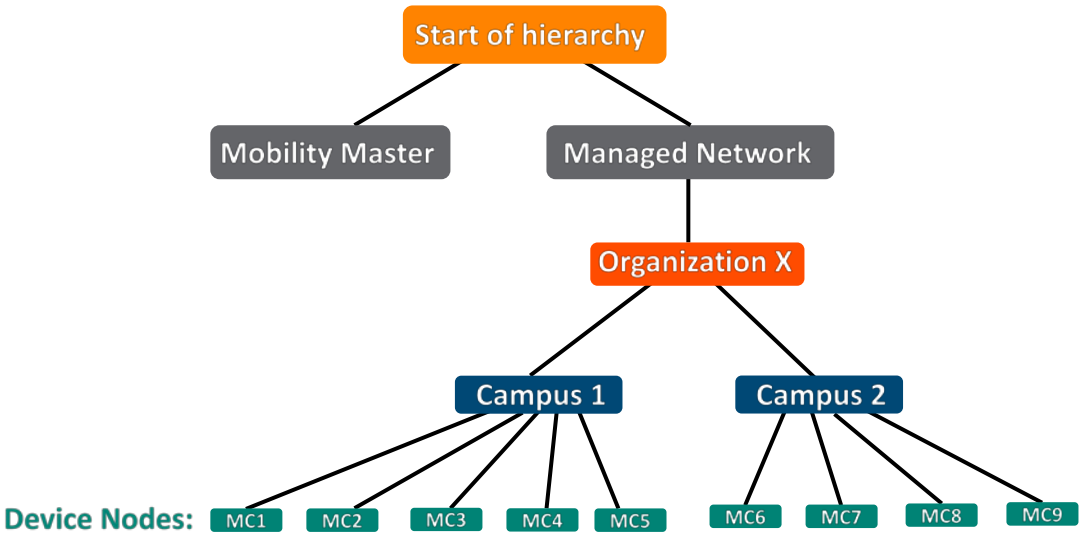

Figure 23 *Mobility Master Terminating Mobility Controllers Configuration Hierarchy*

Design Benefits

- **Maximize benefits** - The Mobility Master Terminating Mobility Controllers design is ideal for fully leveraging the capabilities of ArubaOS 8
- **Scalability** - New controllers can be easily added and managed by the Mobility Master

- **Ease of migration** - If an existing deployment has multiple topologies they can all be migrated under the Mobility Master 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 upgrades
- **AirMatch** - RF intelligence is centralized on the Mobility Master 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 etc. can be updated during runtime removing the need to schedule any maintenance cycles

Design Caveats

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

Migration Requirements

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

Migration Options

- Migration can occur manually or via the Migration Tool
- The Migration Tool is capable of migrating each master-local site to ArubaOS 8 individually. It does not support migration for multiple master-locals at the same time
- Manual migration steps are detailed below. To perform migration using the Migration Tool, please refer to the ArubaOS ArubaOS 8 Migration Guide

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

- Mobility Master backed up by a standby Mobility Master
- Mobility Master 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:

Mobility Master Specific

1. Deploy the Mobility Master and perform the initial setup
2. Configure licensing on the Mobility Master

3. Create a configuration hierarchy and whitelist the MAC addresses of M1-M4 and L1-L5 on the Mobility Master. 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 Mobility Master is being installed
5. Configure Mobility Master redundancy if a backup Mobility Master has been installed. The Mobility Master VIP will be used for configuration management moving forward

Campus1

1. Configure clustering between MC1-MC5 IPs. Also enable AP load balancing. UI: **Managed Network>Campus1>Services>Cluster**
2. Create a VIP between the cluster members MC1-MC5. UI: **Managed Network>Campus1>Services>Redundancy>Virtual Router Table**. Optionally create VIPs for RADIUS COA
3. Create an AP group and SSID. UI: **Managed Network>Campus1>AP Groups**. UI: **Managed Network>Campus1>Tasks>Create a new WLAN**
4. Whitelist the Campus1 APs on the Mobility Master. This includes mapping them to the appropriate AP group. UI: **Managed Network>Campus1>Configuration>Access Points>Whitelist**
5. Back up the existing configuration on the ArubaOS 6 masters M1, M2 and locals L1-L3. UI: **Maintenance>Backup Flash**
6. Upgrade the image on local L1 to ArubaOS 8 and reboot it. UI: **Maintenance>Image Management**
7. Provision local L1 to be managed by the Mobility Master, via the CLI setup dialog. L1 will now become MC1
8. Repeat steps 6-7 to convert L2, L3, M1, and M2 to MC2, MC3, MC4, and MC5 respectively
9. In the Campus1 network point **aruba-master** towards the cluster VIP for MC1-MC5
10. 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
11. Connect a wireless client to the SSID and test connectivity
12. Optionally, test seamless client failover by running a voice/video application and disconnecting the user's active controller

Campus2

1. Configure clustering between MC6-MC9 IPs and enable AP load balancing. UI: **Managed Network>Campus2>Services>Cluster**
2. Create a VIP between cluster members MC6-MC9. UI: **Managed Network>Campus2>Services>Redundancy>Virtual Router Table**. Optionally create VIPs for RADIUS COA
3. Create an AP group and SSID. UI: **Managed Network>Campus2>AP Groups**. UI: **Managed Network>Campus2>Tasks>Create a new WLAN**
4. Whitelist the Campus2 APs on the Mobility Master. This includes mapping them to the appropriate AP group. UI: **Managed Network>Campus2>Configuration>Access Points>Whitelist**
5. Back up the existing configuration on the ArubaOS 6 masters M3 and M4 as well as locals L4 and L5. UI: **Maintenance>Backup Flash**
6. Upgrade the image on local L4 to ArubaOS 8 and reboot the device. UI: **Maintenance>Image Management**
7. Provision local L4 to be managed by the Mobility Master via the CLI setup dialog. L4 will now become MC6
8. Repeat steps 6-7 to convert L5, M3, and M4 to MC7, MC8, and MC9 respectively
9. In the Campus2 network, point **aruba-master** towards the cluster VIP for MC6-MC9
10. 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
11. Connect a wireless client to the SSID and test connectivity
12. Optionally, test seamless client failover by running a voice/video application and disconnecting the user's active controller

Mobility Controller Master Terminating Mobility Controllers

Topology

In this ArubaOS 8 design, each site consists of a hardware controller deployed as a Mobility Controller Master (optionally backed up by another Mobility Controller Master) that manages a group of mobility controllers.

This design helps transition deployments to ArubaOS 8 that are unable to deploy a Mobility Master. This Mobility Controller Master topology should eventually be migrated to a Mobility Master topology in order to take full advantage of the capabilities offered by ArubaOS 8.

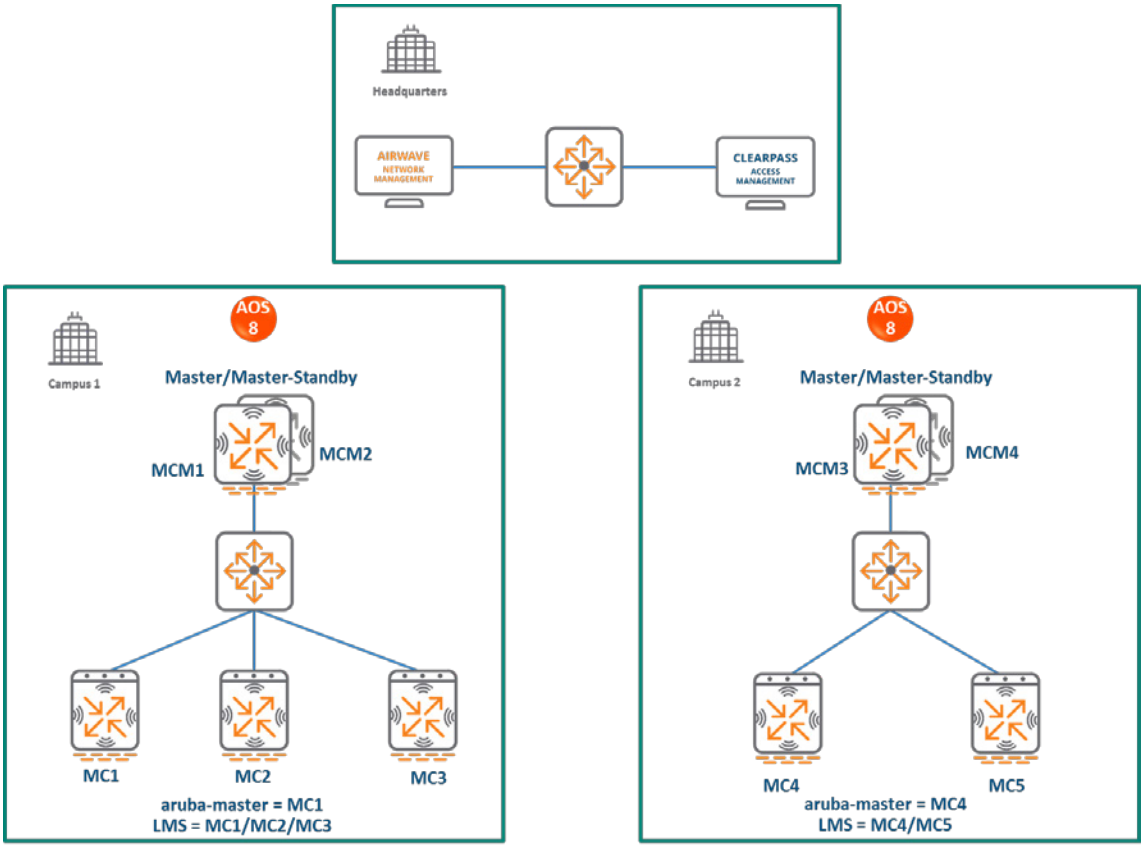

Figure 24 *Mobility Controller Master Terminating Mobility Controllers Topology*

In this design, each campus is still managed by its own Mobility Controller 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

Configuration Hierarchy

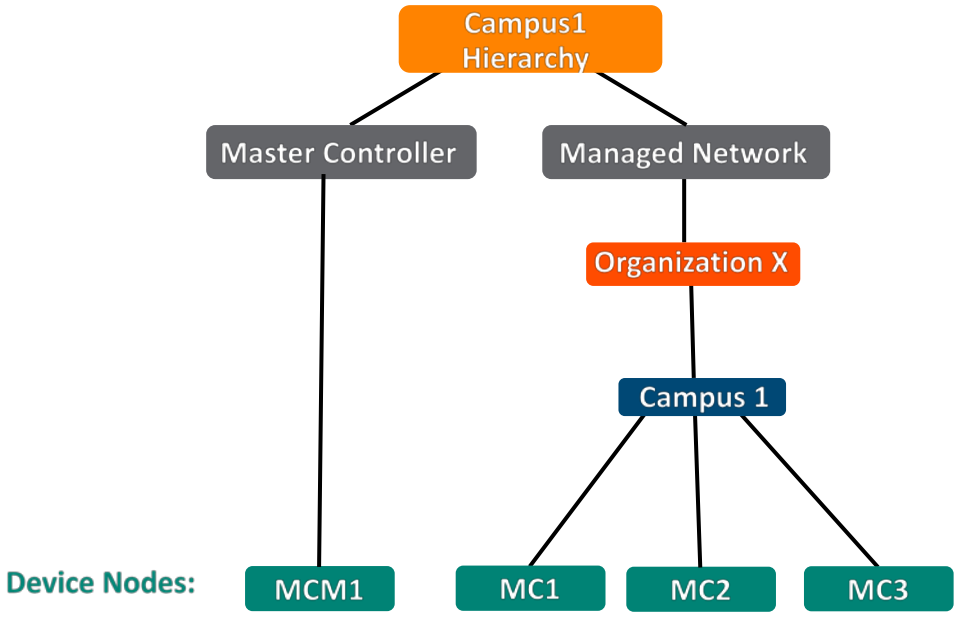

Figure 25 Mobility Controller Master Terminating Mobility Configuration Hierarchy Campus 1

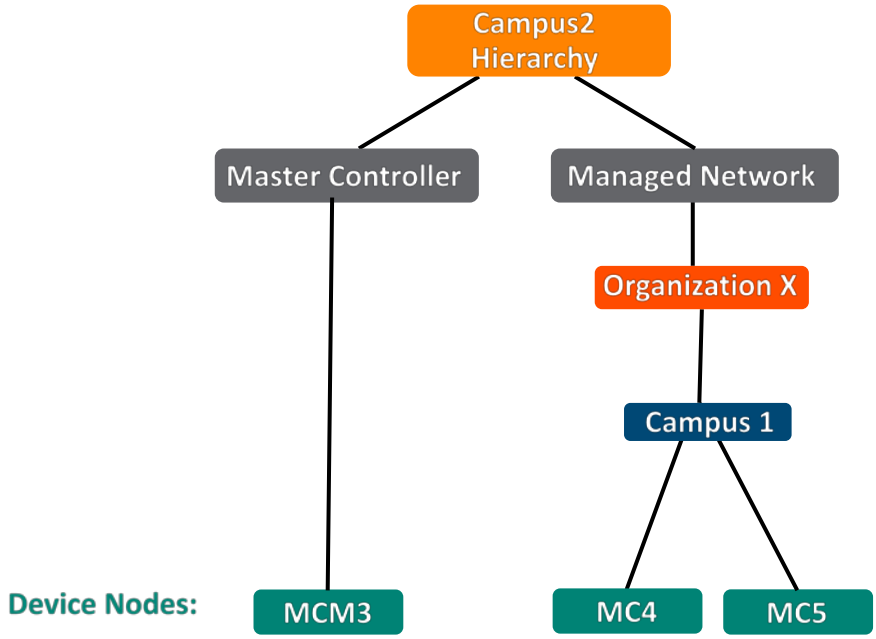

Figure 26 Mobility Controller Master Terminating Mobility Configuration Hierarchy Campus 2

Design Benefits

- A similar topology is maintained in which the Mobility Controller Master manages the Mobility Controllers and no additional hardware is required as long as the Mobility Controller 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 Mobility Controller Master

Design Caveats

- Requires purchase of an Aruba 7030 or larger controller to serve as the Mobility Controller Master as well as the backup MCM if one is not already present
- AP termination on the Mobility Controller 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 Mobility Controllers but cannot failover to the Mobility Controller Master
- The clustering feature is not supported in a Mobility Controller Master deployment. AP Fast Failover between Mobility Controllers 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 Mobility Controller 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 Mobility Controller 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

- Migration can occur manually or via the Migration Tool
- Manual migration steps are detailed below. To perform migration using the Migration Tool, please refer to the ArubaOS ArubaOS 8 Migration Guide

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:

Campus1

1. Backup the existing configuration on the ArubaOS 6 masters and locals. UI: **Maintenance> Backup Flash**
2. Upgrade master M1 to ArubaOS 8 and reboot the controller
3. Provision M1 as a Mobility Controller 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 Mobility Controller Master VIP will be used for configuration management going forward
6. Configure licensing on the Mobility Controller Master
7. Create a configuration hierarchy on the Mobility Controller Master and whitelist the MAC addresses of controllers L1-L3
   - L1-L3 will be whitelisted under **Managed Network>Campus1**
8. Create three AP groups, each with LMS IP of MC1, MC2, and MC3 respectively. UI: **Managed Network>Campus1>AP Groups**

9. Create a common SSID or one for each AP group. UI: **Managed Network>Campus1>Tasks>Create a new WLAN**
10. Whitelist the APs on the Mobility Controller Master. This includes mapping them to the appropriate AP group. UI: **Managed Network>Campus1>Configuration>Access Points>Whitelist**
11. Upgrade the image on local L1 to ArubaOS 8 and reboot it. UI: **Maintenance>Image Management**
12. Provision local L1 to be managed by the Mobility Controller Master via the CLI setup dialog. L1 now becomes MC1
13. 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 visibile on the Mobility Controller 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 be displayed on MC2 and MC3 respectively
17. Connect a wireless client to the SSID and test connectivity
18. Optionally, configure AP Fast Failover via the Mobility Controller Master to enable sub-second AP failover between the Mobility Controllers

Campus2

1. Backup the existing configuration on the ArubaOS 6 masters and locals. UI: **Maintenance>Backup Flash**
2. Upgrade master M3 to ArubaOS 8 and reboot the controller
3. Provision M3 as a Mobility Controller 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 MCM3 and MCM4. Going forward, use the Mobility Controller Master VIP for configuration management
6. Configure licensing on the Mobility Controller Master
7. Create a configuration hierarchy on the Mobility Controller Master and whitelist the MAC addresses of controllers L4 and L5
   - L4, L5 will be whitelisted under **Managed Network>Campus2**
8. Create two AP groups, each with LMS IP of MC4 and MC5 respectively. UI: **Managed Network>Campus2>AP Groups**
9. Create a common SSID or one for each AP group. UI: **Managed Network>Campus2>Tasks>Create a new WLAN**

10. Whitelist your APs on the Mobility Controller Master. This includes mapping them to the appropriate AP group. UI: **Managed Network>Campus2>Configuration>Access Points>Whitelist**
11. Upgrade the image on local L4 to ArubaOS 8 and reboot it. UI: **Maintenance>Image Management**
12. Provision local L4 to be managed by the Mobility Controller Master via the CLI setup dialog. L4 now becomes 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 Mobility Controller Master to enable sub-second AP failover between the Mobility Controllers

All Masters

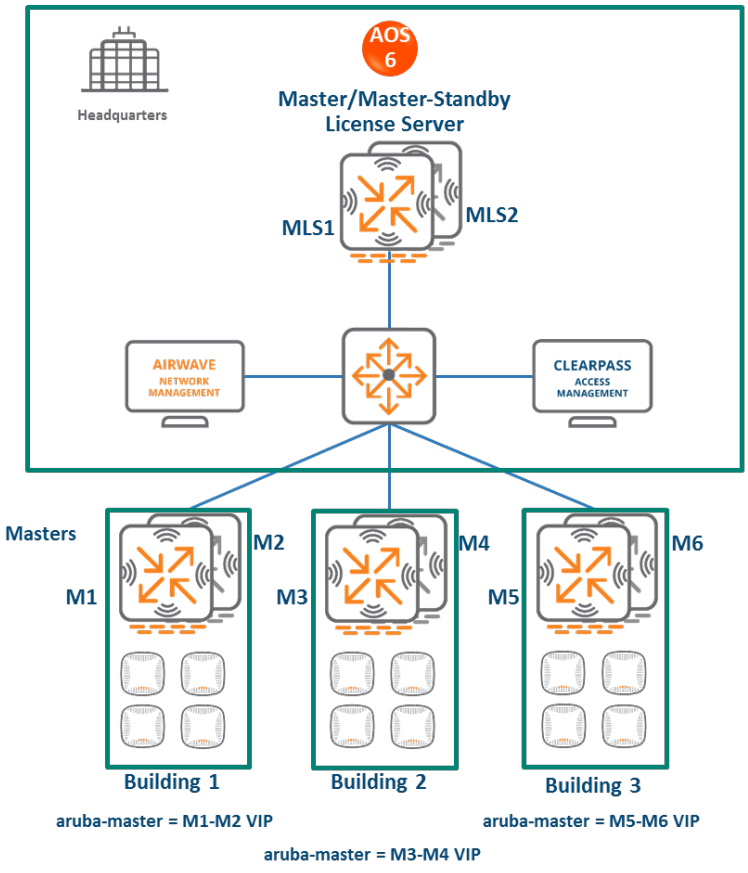

Figure 27 *All Masters Topology*

- 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

Mobility Master Terminating Mobility Controllers

Topology

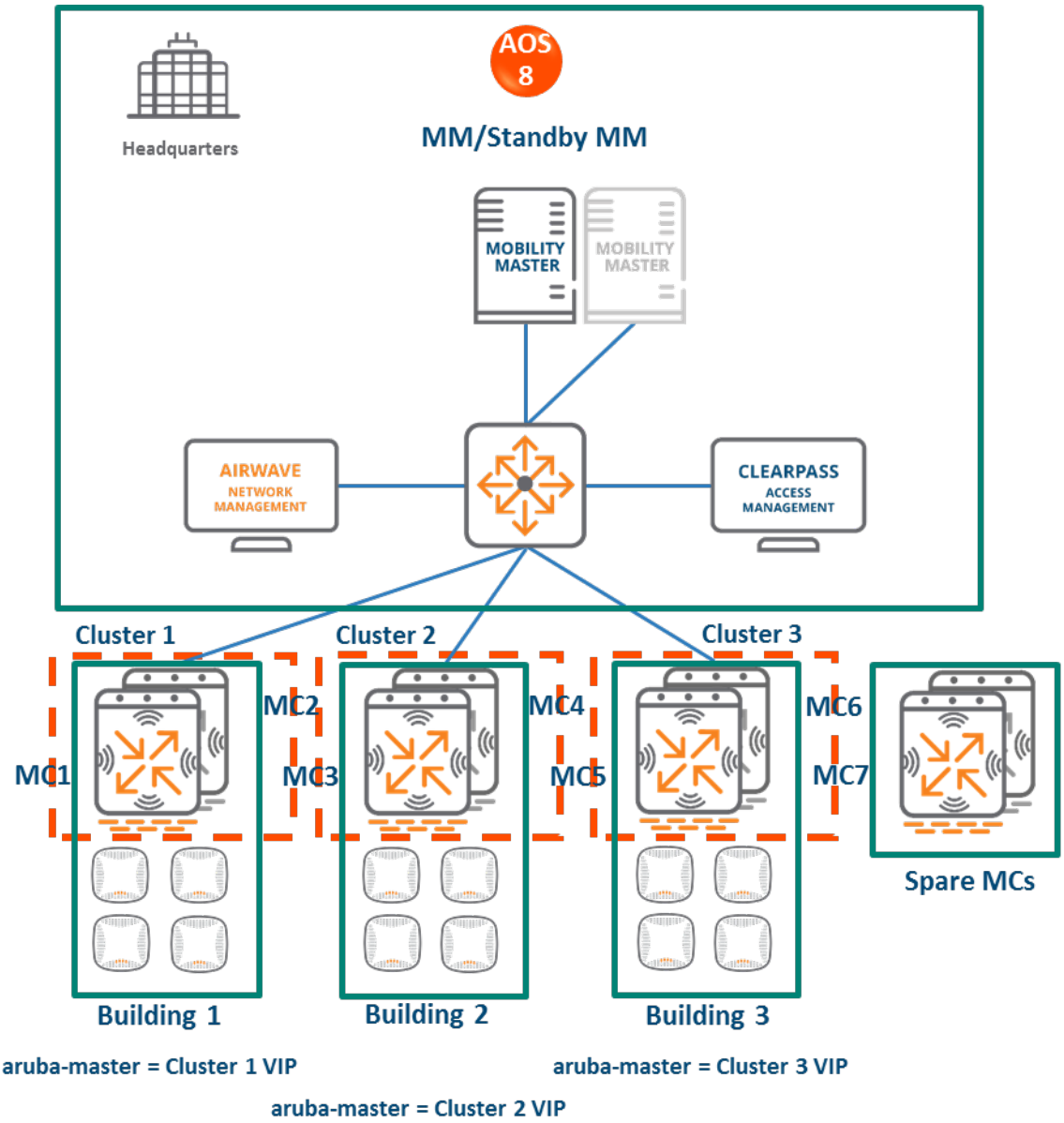

Figure 28 *Mobility Master Terminating Mobility Controllers Topology*

- **HQ/DC:**
  - A Mobility Master (either hardware or virtual) is deployed and configured along with a backup Mobility Master.
  - All site controllers are centrally managed by the Mobility Master
- **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 Mobility Controllers can become cluster members
- **Building3:** The ArubaOS 6 masters become ArubaOS 8 MC5 and MC6. Both Mobility Controllers can become cluster members
- **License servers:**
  - The ArubaOS 6 master and standby master that were previously being used as licensing servers become Mobility Controllers managed by the Mobility Master
  - These Mobility Controllers can be repurposed. E.g., 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

Configuration Hierarchy

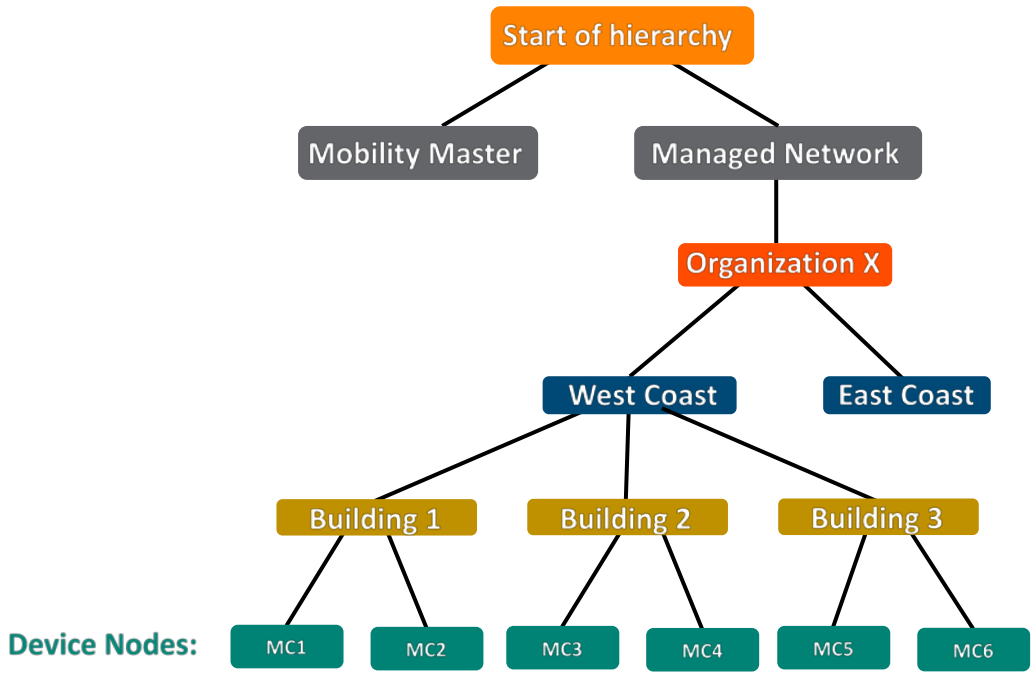

Figure 29 *Mobility Master Terminating Mobility Controllers Configuration Hierarchy*

Design Benefits

- **Maximize benefits** - The Mobility Master Terminating Mobility Controllers design is ideal for fully leveraging the capabilities of ArubaOS 8
- **Scalability** - New controllers can be easily added and managed by the Mobility Master
- **Ease of migration** - If an existing deployment has multiple topologies they can all be migrated under the Mobility Master 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 upgrades
- **AirMatch** - RF intelligence is centralized on the Mobility Master 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 etc. can be updated during runtime removing the need to schedule any maintenance cycles

Design Caveats

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

Migration Requirements

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

Migration Options

- Migration can be done manually or via the Migration Tool
- Manual migration steps are detailed below. To perform migration using the Migration Tool, refer to the ArubaOS ArubaOS 8 Migration Guide

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

- Mobility Master 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:

Mobility Master Specific:

1. Deploy the Mobility Master and perform initial setup
2. Configure licensing on the Mobility Master
3. Create a configuration hierarchy and whitelist the MAC addresses of M1-M6 on the Mobility Master. 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 Mobility Master
5. Configure Mobility Master redundancy if a backup Mobility Master has been installed. The Mobility Master VIP will be used for configuration management moving forward

Building 1:

1. Configure clustering between MC1 and MC2 IPs and enable AP load balancing. UI: **Managed Network>Building1>Services>Cluster**
2. Create a VIP between the cluster members MC1 and MC2. UI: **Managed Network>Building1>Services>Redundancy>Virtual Router Table**. Optionally create VIPs for RADIUS COA
3. Create an AP group and SSID. UI: **Managed Network>Building1>AP Groups**. UI: **Managed Network>Building1>Tasks>Create a new WLAN**
4. Whitelist the Building1 APs on the Mobility Master. This includes mapping them to the appropriate AP group. UI: **Managed Network>Building1>Configuration>Access Points>Whitelist**
5. Back up the existing configuration on the ArubaOS 6 masters. UI: **Maintenance>Backup Flash**
6. Upgrade the image on local M1 to ArubaOS 8 and reboot it. UI: **Maintenance>Image Management**
7. Provision local M1 to be managed by the Mobility Master via the CLI setup dialog. M1 will now become MC1
8. Repeat steps 6-7 to convert M2 to MC2
9. In Building1, point **aruba-master** towards the cluster VIP for MC1 and MC2
10. 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
11. Connect a wireless client to the SSID and test connectivity
12. Optionally, test seamless client failover by running a voice/video application and disconnecting the user's active controller

Building 2:

1. Configure clustering between MC3 and MC4 IPs and enable AP load balancing. UI: **Managed Network>Building2>Services>Cluster**

2. Create a VIP between the cluster members MC3 and MC4. UI: **Managed Network>Building2>Services>Redundancy>Virtual Router Table**. Optionally create VIPs for RADIUS COA
3. Create an AP group and SSID. UI: **Managed Network>Building2>AP Groups**. UI: **Managed Network>Building2>Tasks>Create a new WLAN**
4. Whitelist the Building2 APs on the Mobility Master. This includes mapping them to the appropriate AP group. UI: **Managed Network>Building2>Configuration>Access Points>Whitelist**
5. Back up the existing configuration on the ArubaOS 6 masters. UI: **Maintenance>Backup Flash**
6. Upgrade the image on master M3 to ArubaOS 8 and reboot it. UI: **Maintenance>Image Management**
7. Provision local M3 to be managed by the Mobility Master via the CLI setup dialog. M3 will now become MC3
8. Repeat steps 6-7 to convert M4 to MC4
9. In Building2 network, point **aruba-master** towards the cluster VIP for MC3 and MC4
10. 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
11. Connect a wireless client to the SSID and test connectivity
12. Optionally, test seamless client failover by running a voice/video application and disconnecting the user's active controller

Follow similar steps for Building3.

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

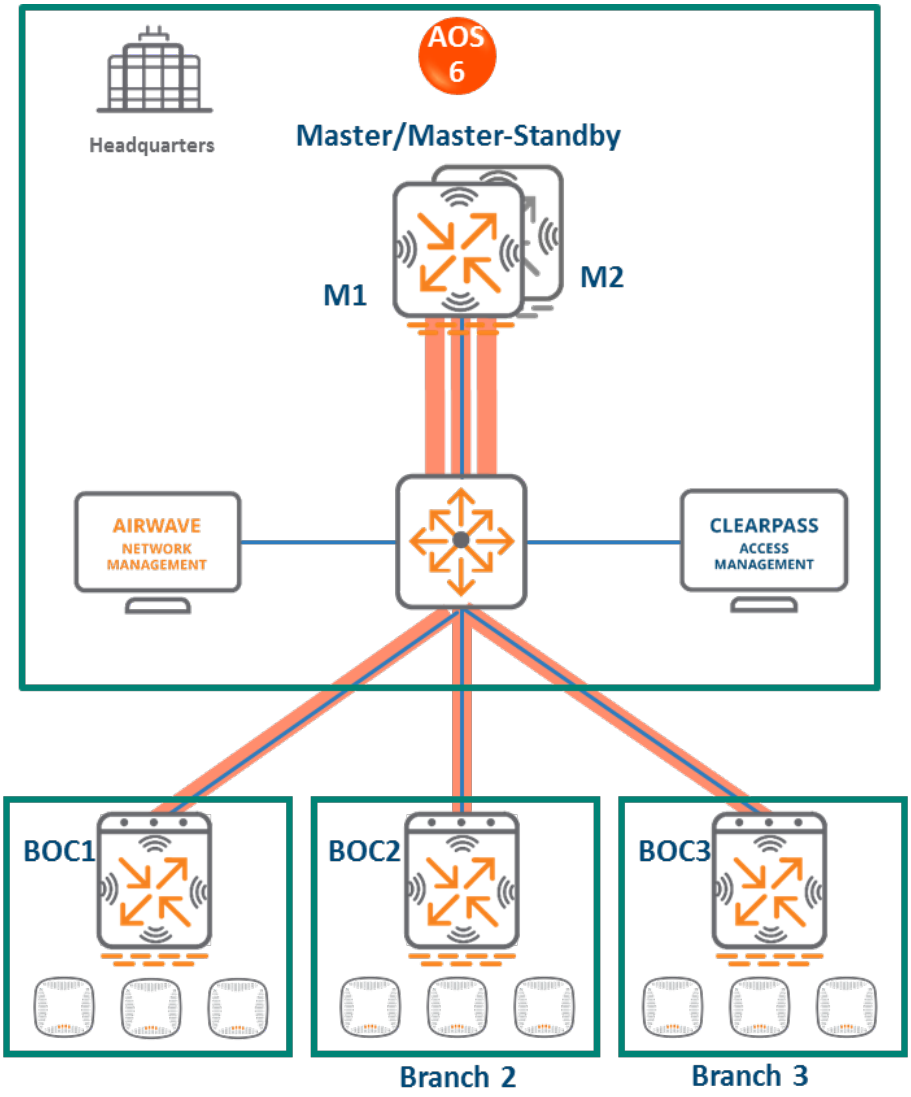

Figure 30 *Master and Branch Controllers Topology*

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

Mobility Master Terminating Mobility Controllers

Topology

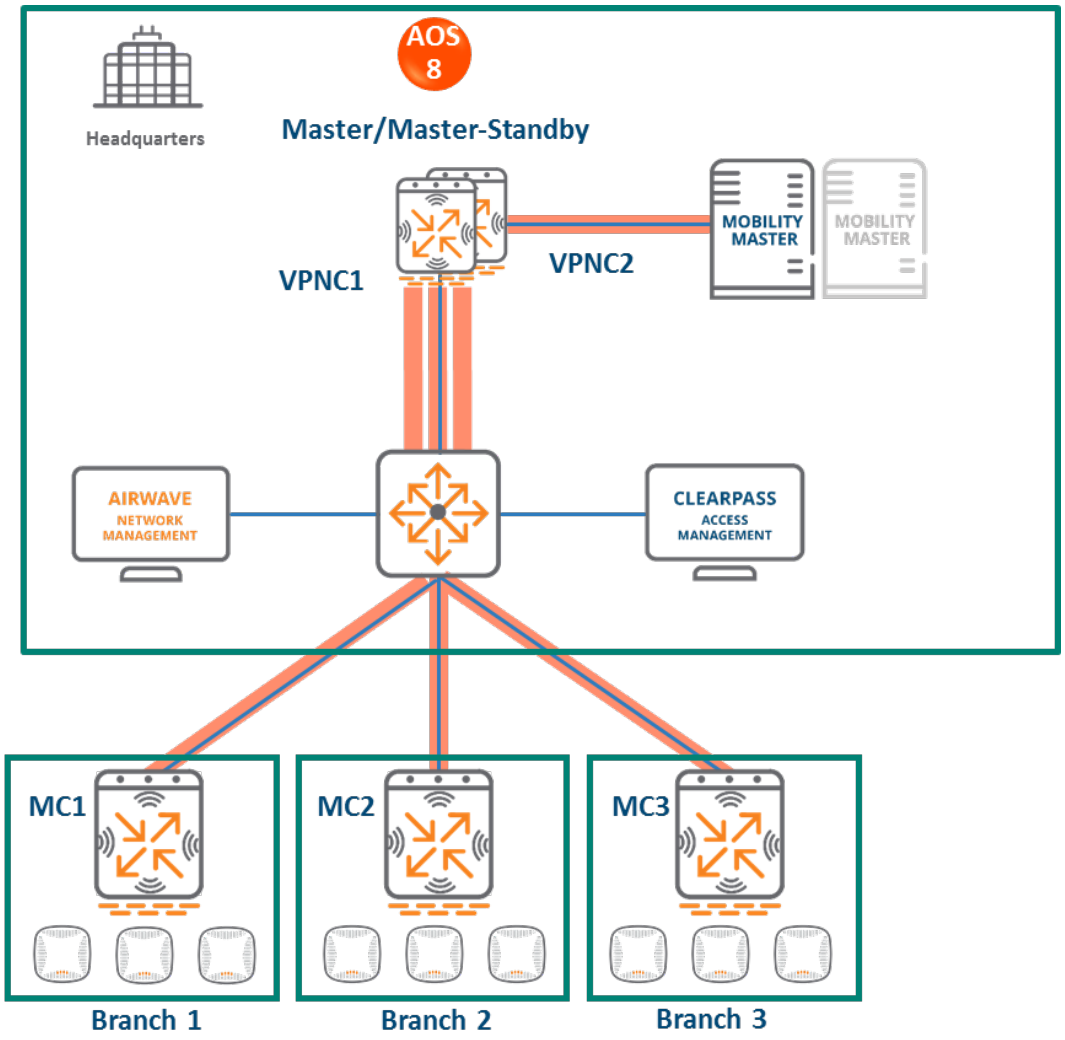

Figure 31 *Mobility Master Terminating Mobility Controllers Topology*

In this design:

- A Mobility Master (either hardware or virtual) is deployed and configured, along with a backup Mobility Master
- Each ArubaOS 6 BOC (BOC1, BOC2, BOC3) becomes an ArubaOS 8 Mobility Controller (MC1, MC2, MC3)
- The ArubaOS 6 master (M1) and standby master (M2) become two ArubaOS 8 VPNC Mobility Controllers (MC4 and MC5)
- Branch Mobility Controllers are capable of termination on the Mobility Master. 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 Mobility Master from the increased load

- APs terminating on L1, L2, and L3 will now terminate on MC1, MC2, and MC3 respectively

Configuration Hierarchy

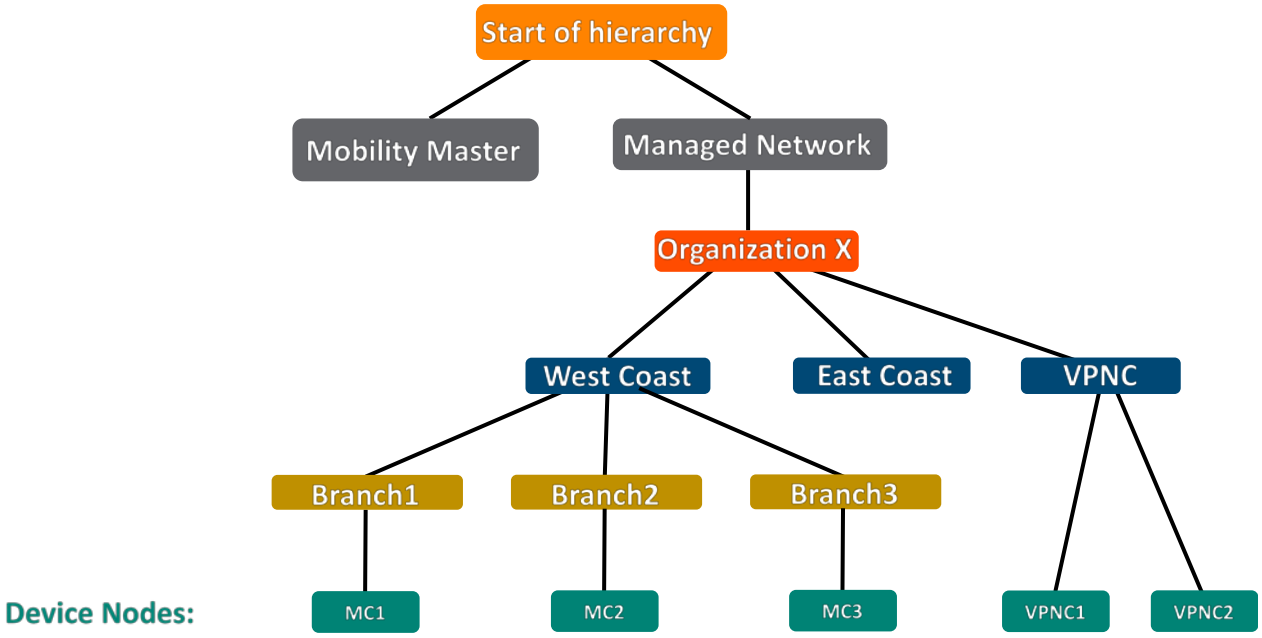

Figure 32 *Mobility Master Terminating Mobility Controllers Configuration Hierarchy*

Design Benefits

- **Maximize benefits** - The Mobility Master Terminating Mobility Controllers design is ideal for fully leveraging the capabilities of ArubaOS 8
- **Scalability** - New controllers can be easily added and managed by the Mobility Master
- **Ease of migration** - If an existing deployment has multiple topologies they can all be migrated under the Mobility Master 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 upgrades

- **AirMatch** - RF intelligence is centralized on the Mobility Master 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 etc. can be updated during runtime removing the need to schedule any maintenance cycles.

Design Caveats

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

Migration Requirements

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

Migration Options

- Migration can occur manually or via the Migration Tool
- The Migration Tool is capable of migrating each master-local site to ArubaOS 8 individually. It does not support migration for multiple master-locals at the same time
- Manual migration steps are detailed below. To perform migration using the Migration Tool, please refer to the ArubaOS ArubaOS 8 Migration Guide

Migration Strategy

Existing ArubaOS 6 Deployment

- **Branch1:** BOC1

- **Branch2:** BOC2
- **Branch3:** BOC3
- **HQ:** M1, M2

New ArubaOS 8 Deployment

- Mobility Master 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 ArubaOS8 Branch Network ASE recipe may also be used to understand Mobility Master/VPNC/branch controller configuration in ArubaOS 8

Mobility Master:

1. Deploy the Mobility Master and perform initial setup
2. Configure licensing on the Mobility Master
3. Repeat step 1 if a backup Mobility Master is being installed
4. Configure Mobility Master redundancy if a backup Mobility Master has been installed. The Mobility Master VIP will be used for configuration management moving forward
5. Configure Activate, a configuration hierarchy, VPN peers, and whitelist the MAC addresses of M1, M2, BOC1, BOC2 and BOC3 on the Mobility Master. 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 Mobility Controller basic configuration - Configure interfaces, VLANs, DHCP pools for APs & users, IP VLAN pool of controller IPs for Branch Mobility Controllers
8. Uplink Configuration of Branch Mobility Controllers - Add uplinks, load balancing, and policy based routing in Branch Mobility Controllers
9. Advertise routes of Branch Mobility Controller to VPNCs
10. Routing Configuration of VPNCs - Static routes and OSPF configuration in the VPNCs
11. Create an AP group and SSID for Branch1. UI: **Managed Network>Branch1>AP Groups**. UI: **Managed Network>Branch1>Tasks>Create a new WLAN**

12. Whitelist the Branch1 APs on the Mobility Master. This includes mapping them to the appropriate AP group. UI: **Managed Network>Branch1>Configuration>Access Points>Whitelist**
13. Create an AP group and SSID for Branch2. UI: **Managed Network>Branch2>AP Groups.** UI: **Managed Network>Branch2>Tasks>Create a new WLAN**
14. Whitelist the Branch2 APs on the Mobility Master. This includes mapping them to the appropriate AP group. UI: **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 Mobility Master
2. Optionally, if VPNCs are being used set up provisioning rules to whitelist them and redirect them to the Mobility Master as well

VPNC:

1. Back up the existing configuration on the ArubaOS 6 masters. UI: **Maintenance>Backup Flash**
2. Upgrade the image on master M1 to ArubaOS 8 and reboot it. UI: **Maintenance>Image Management**
3. Provision M1 to be a VPNC managed by the Mobility Master 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. UI: **Maintenance>Backup Flash**
2. Upgrade the image on BOC1 to ArubaOS 8 and reboot it. UI: **Maintenance>Image Management**
3. If provisioning rules have been created on Activate, the controller will perform ZTP, establish communication with the Mobility Master, and download its configuration
4. Optionally, the controller may be manually configured. Provision BOC1 to be a Mobility Controller managed by the Mobility Master via the CLI setup dialog. BOC1 will now become MC1

Branch 2:

1. Back up the existing configuration on the ArubaOS 6 BOC2. UI: **Maintenance>Backup Flash**
2. Upgrade the image on BOC2 to ArubaOS 8 and reboot it. UI: **Maintenance>Image Management**
3. If provisioning rules have been created on Activate, the controller will perform ZTP, establish communication with the Mobility Master, and download its configuration
4. Optionally, the controller may be manually configured. Provision BOC2 to be a Mobility Controller managed by the Mobility Master via the CLI setup dialog. BOC2 will now become MC2

Follow similar steps for Branch3.