Table of Contents

Introduction ...................................................................................................................................................... 1
  Purpose of This Guide ........................................................................................................................................ 1
  Customer Use Cases ...................................................................................................................................... 2

Mobile First Campus Design ........................................................................................................................ 3
  Campus Wireless LAN Design Using Mobility Controllers ........................................................................ 4
  Wireless Design Components .................................................................................................................... 20
  Campus Wired LAN Design .......................................................................................................................... 22
  Wired Design Components .......................................................................................................................... 34

Deploying the Mobile First Campus ........................................................................................................... 37
  Campus Wired LAN ....................................................................................................................................... 39
  Configuring the Access Switch .................................................................................................................... 39
  Configuring the Aggregation Switch ........................................................................................................... 54
  Configuring the Standalone Core Switches .................................................................................................. 68
  Configuring the Core Switches with a Combined Services Aggregation ...................................................... 73
  Campus Wireless LAN ................................................................................................................................... 84
  Configuring the Mobility Master .................................................................................................................... 84
  Configuring the Mobility Controller Cluster ................................................................................................ 95
  Configuring the Wireless LANs .................................................................................................................... 113
  Configuring the Access Points .................................................................................................................... 124

Summary ...................................................................................................................................................... 135

Validated Hardware and Software ............................................................................................................. 136

What’s New in This Version .......................................................................................................................... 137
Introduction

Wireless has become the primary network access method for today’s fast-changing mobile environments. In the past, wireless networks were a “nice to have,” but they have evolved into a mission-critical lane for connectivity and play a major role in business continuity and employee satisfaction. In recent years, the number of connected devices per user has increased to more than three, and some estimate it will rise to as many as five per user in the next few years. Employees have their company-supplied PCs, their personal tablets, company-supplied or personal smart phones, and even their smart watches connected to the corporate Wi-Fi network. Users move between locations with their devices and require always-on access. When visiting your employees on-site, guests expect to have access to the Internet from their wireless devices. The Aruba Mobile First Campus network is designed to allow people to move while connected, securely separate employee traffic from guest traffic and to allow enterprises to innovate without being tied to a wired infrastructure. It combines the best wireless products with a resilient wired infrastructure that is ready to support mobility and Internet of Things (IoT) devices, as well as end-to-end network management with multi-vendor access control.

Because most people work from both company-supplied and personal devices, wireless network access must be ubiquitous to accommodate the new mobile workplace. Guests want Internet access from their personal computers, tablets and smart phones, a desire that becomes a major challenge for IT departments due to the lack of control over the devices. In addition, many IoT devices connect wirelessly to today's networks. Building control systems, card readers, thermostats, and surveillance cameras do not have users associated with them. Their traffic is considered machine-to-machine and the devices require machine authentication, which differs from user authentication. Even devices that have traditionally used wired connections, such as shared printers, copy machines, multimedia devices, and high-end workstations, are moving to the wireless world. A network with a few hundred users can easily have over a thousand connected devices.

PURPOSE OF THIS GUIDE

This guide covers the Aruba Mobile First Campus design, including reference designs along with their associated hardware and software components. It contains an explanation of the requirements that shaped the design and the benefits it will provide your organization. The guide describes a single system that integrates access points (APs), access switches, aggregation switches, core switches, and network management with access-control and traffic-control policies.

Design Goals

The overall goal is to create a simple scalable design that is easy to replicate at different sites in your network. The components are limited to a specific set of products to help with operations and maintenance. The design has a target of sub-second failover when a network device or link between two network devices becomes unavailable.
The protocols are tuned for a highly-available network in all functional areas. The design deploys link aggregation and multi-chassis link aggregation between aggregation and access devices. Routed links are utilized at the core with layer-3 path redundancy.

The guide can be used to design new networks or to optimize and upgrade existing networks. It is not intended as an exhaustive discussion of all options, but rather to present the most commonly recommended designs, features, and hardware.

Audience

This guide is written for IT professionals who need to design an Aruba wired-and-wireless network for a large organization with 500 to 2500 users. These IT professionals can fill a variety of roles:

- Systems engineers who need a standard set of procedures for implementing solutions
- Project managers who create statements of work for Aruba implementations
- Aruba partners who sell technology or create implementation documentation

CUSTOMER USE CASES

With so many wireless devices on a network, performance and availability are key. Wireless clients with different capabilities support different performance levels. If the wireless network doesn't self-optimize, slower clients can degrade performance for faster clients. Clients need to intelligently connect to radios on APs to increase network efficiency and performance.

802.11ac Wave 2 Wi-Fi supports speeds greater than 1 Gbps. To accommodate the increased data rates, the APs support 2.5 and 5 Gbps over standards-based, unshielded twisted-pair copper, which works on existing building cabling using Aruba access switches. The access layer acts as a collection point for high-performance wired and wireless devices and must have enough capacity to support the bandwidth needs of today as well as scale for the future as the number of devices grow.

Endpoints that support the 802.3bz standard of 2.5 Gbps and 5 Gbps are starting to emerge with many more coming in the near future. At the other end of the bandwidth spectrum, there is a need to support the rapidly expanding IoT devices, and almost half of them are using wired ports, which means additional power over Ethernet (PoE) copper ports in the access wiring closet.

Security is also a critical part of the campus network. Users must be authenticated and given access to the services they need to do their jobs. IoT devices must be identified using machine authentication to prevent rouge devices from using the network. In addition to corporate-managed assets, users connect personal devices, guests need access to the Internet, and contractors need access to the Internet and the organization’s internal network.
This type of broad access must be accomplished while maintaining the security and integrity of the network. Connecting so many devices and user types increases the administrative burden, and the network should allow you to automate device onboarding in a secure manner.

Before wireless became the primary network access method, typical network designs provided two or more wired ports per user. It was common to run two network drops to each user’s desk and then have additional ports for conference rooms, network printers, and other shared areas, adding up to just over two ports per user. With the trend of users moving to wireless as the primary method of network access, the average wired ports per person is dropping. This trend will continue as more devices move to wireless for connectivity to the network. However, as more wired IoT devices use access switches for PoE, we do not see the number of wired ports dropping below an average of one per user within an organization.

This guide discusses the following use cases:

- Wireless as the primary access method for employees
- Wireless guest access for customers, partners, and vendors
- Switch stacking for simplified management, high availability, and scalability
- Link aggregation for high bandwidth, redundancy, and resiliency between switches
- High-performance core for non-stop forwarding of critical traffic
- IP multicast to efficiently propagate streaming traffic across the network

**Mobile First Campus Design**

This design is targeted for large organizations supporting up to 2500 users with multiple devices per user. The network could be a single building, a few floors in a larger building, or a group of small buildings located near each other. The wireless network requires a common wired local area network (LAN) design which consists of two or three tiers. The access layer is where wired devices and wireless APs connect to the network. The aggregation layer acts as a connection point for multiple access-layer switches. The core layer is used to interconnect aggregation-layer switches from multiple buildings or multiple floors in a building.

The three-tier design is used when there are several buildings in a campus that need to be connected and number of aggregation switches or the layout of the physical wiring plant makes more sense to connect everything to a central core.
For a network of 500 to 2500 users, the three-tier campus design is the most common, as shown in the following figure.

*Figure 1  Three-tier campus network*

The Mobile First Campus design uses access switches or switch stacks connected to a dual-switch aggregation layer. Both modular and stackable access switches are available, depending on the number of ports needed in the wiring closets. In smaller closets, stackable switches are more cost effective, but at a certain port density, modular access switches are less expensive than a stack of fixed access switches. The aggregation layer is dual-connected into a pair of high-speed core switches, which provide a maximum level of redundancy and resiliency for non-stop forwarding.

The aggregation layer also provides critical network services like WAN aggregation, Internet DMZ and data center servers for an organization. The aggregation switches need numerous 10 Gbps ports into the access layer and 40 Gbps ports into the core. The high-speed core switches must support a large number of 40 Gbps ports with enough capacity to grow and several 100 Gbps ports to connect between themselves.

In networks where 80% or more of the users are connecting via wireless but wired IoT devices continue to rise, the number of wired ports in the network is getting close to one per user. Aruba Campus Access APs are used for wireless access because they connect to centralized mobility controllers for ease of configuration and maximum operational flexibility. This design minimizes the number of different components in order to make operations, maintenance, and troubleshooting simpler.

**CAMPUS WIRELESS LAN DESIGN USING MOBILITY CONTROLLERS**

The Aruba Mobile First Campus wireless LAN (WLAN) provides network access for employees, wireless Internet access for guests, and connectivity for IoT devices. Regardless of their location on the network, wireless devices have the same experience when connecting to their services.
The benefits of the mobile-first wireless campus include:

- Location-independent network access improves employee productivity
- Hard-to-wire locations receive network connectivity without costly construction
- Wireless is plug-and-play, with wired LAN switches preconfigured to recognize APs
- Reliable wireless connectivity, including complete radio frequency (RF) spectrum management, is available with Aruba AirMatch
- Non-stop networking with a centralized master controller and controller clustering for seamless failover
- Live upgrades to perform operating system updates without an outage or service impact
- In-service module upgrades to dynamically update individual service modules without requiring an entire system reboot

Wireless networks today are engineered based on user capacity needs rather than basic wireless coverage. High-speed, high-quality wireless everywhere in the organization is required for today’s mobile-first environments. Each client should be able to connect to multiple APs from anywhere in the network. This enables low-latency roaming for real-time applications and allows the network to adapt during routine AP maintenance or an unscheduled outage. A higher density of APs allows the network to support more wireless devices while delivering better connection reliability.

**Aruba Mobility Master and Mobility Controllers**

For today’s wireless networks, they are two main deployment models: one where APs connect to dedicated controllers and one that is controllerless, which is also known as autonomous mode. The Aruba Mobility Master and mobility controllers offer centralized network engineering, IP services, security and policy controls, and app-aware platforms. The mobility controller is responsible for many of the operations that traditionally would be handled by an autonomous AP, and it delivers additional functionality for control, security, operation, and troubleshooting.

The Aruba WLAN design provides a centralized Mobility Master which is a next generation controller with significantly more functionality and flexibility than previous versions. The Mobility Master provides several new advanced features, like controller clustering, AirMatch RF management and the ability to put APs into zones. To achieve the highest levels of scalability, a pair of Mobility Masters centralize system management and configuration, but they do not terminate APs. Mobility controllers become managed devices under the Mobility Master and handle the AP terminations. Clustering the mobility controllers provides high availability, scalability and seamless roaming throughout an entire building or across many buildings in a campus.
Mobility Master Configuration Hierarchy

The Mobility Master is a centralized management platform in a multi-tier architecture that provides separation of management, control, and forwarding plane. It maintains all configurations, including its own, eliminating multiple points of contact to apply global and local configurations to each managed device. You organize your common configurations at a higher level of the hierarchy, and they are propagated to the lower levels. You configure group-specific or device-specific changes at the lower levels if they do not pertain to the higher-level devices. This type of hierarchy simplifies the configuration of design elements that are shared across common deployment types. The table below shows the group structures for the hierarchy.

<table>
<thead>
<tr>
<th>Category</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility Master</td>
<td>/</td>
<td>Configurations common to Mobility Master and its managed devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTE: Configuration changes are not allowed at the root.</td>
</tr>
<tr>
<td></td>
<td>/md</td>
<td>Configurations common to all managed devices. The user can create additional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>groups under this group.</td>
</tr>
<tr>
<td></td>
<td>/md/&lt;group name&gt;</td>
<td>The group name is used to differentiate the devices physically or by the type</td>
</tr>
<tr>
<td></td>
<td></td>
<td>of deployment, such as DMZ, Branch, Campus, RAPs, and so on.</td>
</tr>
<tr>
<td></td>
<td>/mm</td>
<td>Configurations common to the primary and standby Mobility Master (VRRP pair).</td>
</tr>
<tr>
<td></td>
<td>/mm/mynode</td>
<td>Configurations specific to a Mobility Master. This can only be edited on the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>respective Mobility Master.</td>
</tr>
</tbody>
</table>

The Mobility Master hierarchy streamlines the configuration process by supporting multiple configurations for multiple deployments at difference locations. Configuration elements can be mapped to one or more end devices, such as a managed device or VPN concentrator. Common configurations across devices are extracted to a shared template, which merges with device-specific configurations to generate the configuration for an individual device. The network can be organized in a hierarchy of up to five levels, including groups, sub-groups, and the managed devices that are added to these groups.
The following is an example of a configuration hierarchy with three levels.

Figure 2  Mobility Master configuration hierarchy

Mobility Controller Clustering

A cluster combines multiple mobility controllers to provide high availability and service continuity during failover events and live system upgrades by eliminating single points of failure. When you configure mobility controllers as members of the same cluster, they use a handshaking mechanism to determine cluster reachability and eligibility. This ensures the cluster members can see each other and the cluster is fully meshed.

Clustering provides the following benefits:

- **Seamless roaming**—WLAN client remain anchored to a single member of the cluster regardless of where they roam or to which AP they connect.

- **Client stateful failover**—In the event of a cluster member failure, connected clients fail over to a redundant cluster member.

- **Client load balancing**—Clients are automatically load-balanced within the cluster. If needed, clients are moved among cluster members in a stateful manner to prevent disruption of service.

- **AP load balancing**—APs are automatically load balanced across cluster members.

- **Live upgrades**—Mobility controllers and APs in a cluster are automatically upgraded without impacting the wireless users.

After the cluster is formed, a leader is elected to perform several responsibilities, like managing AP and user anchor controller roles. An anchor controller is a single mobility controller that manages the session activity between individual APs and users. When redundancy is enabled, the cluster leader assigns an active AP anchor controller...
(A-AAC) and standby AAC (S-AAC) for each AP. The cluster leader also dynamically load-balances the APs among the active cluster members. Once the AAC roles are chosen, tunnels are formed between the AP and the active and standby AACs as depicted in the diagram below.

*Figure 3*  Cluster redundancy—active and standby AP anchor controllers

An inter-controller heartbeat keeps the two cluster controllers synchronized. If the AP’s A-AAC fails or is taken out of service, the AP will failover to the S-AAC and the cluster leader will choose a new S-AAC.
The cluster leader also assigns an active user anchor controller (A-UAC) and standby UAC (S-UAC) for each WLAN user. If redundancy is disabled, the client stateful failover feature is not available. When a user joins the wireless network, tunnels are formed to the active and standby UACs as depicted in the diagram below.

**Figure 4** Cluster redundancy—active and standby user anchor controllers

An inter-controller heartbeat keeps the two cluster controllers synchronized. If the users A-UAC fails or is taken out of service, the users session is moved to the S-UAC and the cluster leader chooses a new S-UAC.
If the user roams to another AP, the tunnel is maintained to the original A-UAC and S-UAC even if the new AP has a different set of AACs. This means a user can seamlessly roam throughout an entire building or campus as depicted in the diagram below.

**Figure 5  Seamless roaming—active and standby user anchor controllers**

The functionality provided by the mobility controller in this design includes:

- Acting as a user-based application firewall
- Terminating user-encrypted sessions from wireless devices
- Providing certificate-based IPsec security to protect control channel information
- Performing user authentication such as 802.1X and captive portal authentication
- Providing guest access and captive portal services
- Providing self-contained management by way of a Mobility Master hierarchy with the master pushing configuration to other mobility controllers to reduce administrative overhead
- Delivering AP software updates automatically when the mobility controller is upgraded

This level of seamless, integrated functionality eliminates many of the challenges experienced with traditional systems integration of these services. Network administrators need to learn only one interface, which reduces deployment complexity and speeds problem resolution across a broad range of designs and solutions.

**Access Point Placement**

Aruba recommends doing a site survey for all wireless network installations. The main goal of a site survey is to determine the feasibility of building a wireless network on your site. It is also used to determine the best place for access points and other equipment, such as antennas and cables. With that in mind, the following guidelines can be used as a good starting point for most office environments.
For typical capacity in an office environment, we recommend placing APs approximately every 35-50 feet (10-15 meters). Each AP provides coverage for 1500-2500 square feet (150-250 square meters) with enough overlap for seamless client roaming. In traditional offices, the average space per user is approximately 175-200 square feet (15-20 square meters), and in open-office environments, the space per user can be as low as 75-100 square feet (7-10 square meters). With three devices per user, a traditional office layout with 50-foot AP spacing, and approximately ten users per 2000 square feet, an average of 30 devices are connected to each AP.

The numbers work out roughly the same in higher-density, open-office layouts with 35-foot AP spacing. Because users move around and are not evenly distributed, the higher density allows the network to handle spikes in device count and growth in the number of wireless devices over time. In an average 2500-user network with three devices per person, this works out to 7500 total devices, and with 30 devices per AP, this translates to approximately 250 APs for this example.

Whenever possible, APs should be placed near users and devices in offices, meeting rooms, and common areas, instead of in hallways. The following figure shows a sample office-floor layout with APs. The staggered spacing between APs is equal in all directions and ensures suitable coverage and seamless roaming.

*Figure 6  Sample office AP layout (not to scale)*
After studying your environment with the 35-50-foot (10-15 meter) rule in mind, make sure you also have enough capacity for the number of users. In an average office environment with APs every 35-50 feet (10-15 meters), the 30 devices per AP average will easily be satisfied. However, if you have high-density areas such as large conference rooms, cafeterias, or auditoriums, additional APs may be needed.

Channel Planning

The centralized Aruba AirMatch software is very good at automating channel assignment, and for most wireless installations, channel selection and transmit power can be left to its advanced algorithms. If you want to plan your channels on your own following the details in this section, please contact an Aruba or partner systems engineer or consulting systems engineer (SE/CSE) for verification of your design.

A typical 2.4-GHz channel layout uses the three available non-overlapping channels of 1, 6, and 11 in this band. Reused channels are separated as much as possible, but with only three available channels there will be some co-channel interference which is caused by two radios on the same channel. We recommend only using these three channels for your 2.4-GHz installations to avoid the more serious problem of adjacent channel interference which is caused by radios on overlapping channels or adjacent channels with radios too close together.

The 5-GHz band offers higher performance and suffers from less external interference than the 2.4-GHz band. It also has many more channels available so it is easier to avoid co-channel interference and adjacent channel interference. Because of the channel advantages, we recommend all capable clients connect on 5 GHz and we recommend converting older clients from 2.4 GHz to 5 GHz when possible. As with the 2.4-GHz spectrum, the radio management software handles the automatic channel selection for the 5-GHz spectrum.

Channel Width

An important decision for 5-GHz deployments is what channel width to use. Wider channel widths mean higher throughput for individual clients but fewer non-overlapping channels, while narrower channel widths results in less available bandwidth per client but more available channels.

In most office environments, 40-MHz-wide channels are recommended because they provide a good balance of performance and available channels. If you are in a high-density open-office environment or you know you will lose channels due to DFS interference, you should consider starting with 20-MHz channels.

Due to the high number of APs and increasing number of connected devices, there are almost no office environments that would benefit from 80-MHz-wide channels, let alone the much wider 160-MHz channels. We recommend you disable the 80-MHz-wide and 160-MHz-wide channels.
The following figure highlights the 40-MHz channel allocation for the 5-GHz band.

![Figure 7 802.11ac channel allocation for the 5-Ghz band](image)

Depending on country-specific or region-specific restrictions, some of the UNII-2/UNII-2 Extended Dynamic Frequency Selection (DFS) channels may not be available. In the past, it was common to disable unavailable channels, but today most organizations attempt to use all channels available in their country. In some areas DFS channels overlap with radar systems. If an AP detects radar transmissions on a channel, the AP stops transmitting on that channel for a time and moves to another channel. If specific DFS channels regularly detect radar in your environment, we recommend removing those channels from your valid-channel plan to prevent coverage problems.

Channel 144 is a recent addition to the 802.11ac standard and only newer 802.11ac wireless clients have support for it. If you have older 5-GHz devices, we recommend you disable channel 144. Using the recommended 40-MHz-wide channels, there are up to 12 channels available. Depending on local regulations and interference from radar or other outside sources, the total number of usable channels vary from location to location. A list of the 5-GHz channels available in different countries can be found at the following link:

https://en.wikipedia.org/wiki/List_of_WLAN_channels#5_GHz_(802.11a/h/j/n/ac/ax)

Power Settings

The optimum power settings vary based on your physical environment, and you should always follow the recommendations from your professional site survey to finalize your initial settings. With that in mind, use the following guidelines for a typical wireless design.

- In the 2.4-GHz band, set the minimum power threshold to 6 dBm and the maximum power to 9 dBm for open-office and walled-office environments
- In the 5-GHz band, set the minimum power threshold to 12 dBm and the maximum to 15 dBm for an open-office environment
- In the 5-GHz band, set the minimum power threshold to 15 dBm and the maximum to 18 dBm for a walled-office environment
- In all environments, do not exceed a power level difference of 6 dBm between the minimum and maximum settings on all radio bands
- In all environments, the minimum power level differences between equal coverage level 2.4-GHz radios and 5-GHz radios should be 6 dBm
After the initial settings are configured, the AirMatch software automatically adjusts power settings as needed and on an ongoing basis.

Spatial Streams

Spatial streaming is a transmission technique in multiple-input and multiple-output (MIMO) wireless communication that allows clients to transmit multiple streams on multiple antennas. The theoretical bandwidth depends on the number of spatial streams and channel width. The following table shows the maximum theoretical bandwidth for the different channel widths and number of available spatial streams.

Table 2  Theoretical bandwidth for 802.11ac at various channels widths and spatial stream counts

<table>
<thead>
<tr>
<th>Channels widths</th>
<th>Max available channels</th>
<th>1 spatial streams (1SS)</th>
<th>2 spatial streams (2SS)</th>
<th>3 spatial streams (3SS)</th>
<th>4 spatial streams (4SS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>20MHz</td>
<td>25</td>
<td>87 Mbps</td>
<td>173 Mbps</td>
<td>289 Mbps</td>
<td>347 Mbps</td>
</tr>
<tr>
<td>40MHz</td>
<td>12</td>
<td>200 Mbps</td>
<td>400 Mbps</td>
<td>600 Mbps</td>
<td>800 Mbps</td>
</tr>
<tr>
<td>80MHz</td>
<td>6</td>
<td>433 Mbps</td>
<td>867 Mbps</td>
<td>1.3 Gbps</td>
<td>1.73 Gbps</td>
</tr>
<tr>
<td>160MHz</td>
<td>2</td>
<td>867 Mbps</td>
<td>1.73 Gbps</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Both the client and the AP need to support the same number of spatial streams to maximize the advantages of this technology. In general, low-power clients like smart phones and low-cost tablets support a lower number of spatial streams and high-power tablets and laptops support a larger number of spatial streams. Aruba ClientMatch balances clients by capability across APs in the network, in order to maximize the service levels available to each type of client.

Site Survey

A site survey is an important tool that gives you a solid understanding of the radio frequency behavior at your site and, more importantly, where and how much interference you might encounter with your intended coverage zones. A site survey also helps you to determine what type of network equipment you need, where it goes, and how it needs to be installed. A good survey allows identification of AP mounting locations, existing cable plants, and yields a plan to get the wireless coverage your network requires. RF interacts with the physical world around it, and because all office environments are unique, each wireless network has slightly different characteristics. The recommendations listed in the section above are a good starting point, but a solid site survey allows you to customize the RF plan for your specific location.

If you want to provide ubiquitous multimedia coverage in a multi-floor/multi-building campus with uninterrupted service, you need a professional site survey to balance the elements required for success. Planning tools have evolved with the radio technologies and applications in use today, but a familiarity with the RF design elements and mobile applications is required to produce a good plan. Completing a site survey now yields good information that can be used again and again as the wireless network grows and continues to evolve.
RF Performance

After a successful site survey helps you properly place your APs, there are additional ways to provide long-term performance management for your wireless network. The Aruba AirMatch feature models the network and improves the user experience by optimizing the RF performance on an ongoing basis. The APs collect information about their RF neighborhood and forward the data to the AirMatch process running on the Mobility Master. AirMatch consumes the RF information from the entire network and generates a new RF plan each day. If the new plan has enough variance from the existing plan to warrant a change, an update is sent out to all APs at a predetermined time. However, AirMatch can only optimize the RF environment to a certain degree if the APs are not initially located correctly in your environment.

Aruba also provides an emerging tool called NetInsight, which uses machine learning-based network analytics to deliver recommendations for optimization around mobile workers, wireless and IoT devices. Data from multiple sources including your wireless infrastructure, DHCP and authentication servers are gathered in an onsite data collector. The data is compressed and sent via a secure tunnel to the NetInsight cloud instance where network connectivity and performance issues are analyzed by leveraging machine learning-based models using Aruba’s Wi-Fi expertise and the latest cloud technologies. A web-based dashboard allows you to view insights along with root causes, and more importantly, it provides recommendations to fix immediate and foreseeable network performance issues.

Channel Summary

The number of APs and their exact placement comes down to performance versus client density. In a high-density deployment, better performance is possible using a larger number of lower-bandwidth channels rather than fewer higher-bandwidth channels. One hundred wireless devices get better performance split between two radios on 20-MHz channels than they do on one radio using a 40-MHz channel. This is because the more channels you have to use, the better overall throughput is for a higher number of devices. As mentioned previously, a typical Aruba wireless installation uses the AirMatch software running on the Mobility Master and NetInsight running in the cloud for RF channel planning.

Mobility Master Features

The Mobility Master provides a flexible deployment, simplified operations and enhanced performance by centrally managing a cluster of mobility controllers. A Mobility Master design enables controller clustering, live upgrades, in-service upgrades, and multiple ArubaOS support, which drastically increases the availability and reliability of the wireless network.

With a Mobility Master design, your entire network can be upgraded to the latest operating system in real-time, with minimum downtime and no user impact. You can also dynamically update individual service modules, such as AppRF, AirGroup, AirMatch, north-bound APIs, Unified Communications Manager, and web content classification that reside on the Mobility Master, without requiring an entire system reboot. To further minimize network
downtime when upgrading to a new OS release, a new feature allows IT administrators to test a new version of software in one area without affecting the entire network. This feature can act as a gradual migration tool to adopt new innovations while minimizing risk.

AirMatch

AirMatch is an enhancement to the Adaptive Radio Management technology and is tuned for noisy, high-density environments. With automated channel, channel-widths and transmit power optimization, AirMatch ensures even channel use, assists in interference mitigation and maximizes system capacity. The capacity optimization is not just co-channel interference mitigation, because AirMatch also dynamically adjusts channel width. This ensures the best network capacity whether you are in a high-density environment like a lecture hall with 20 MHz channels or low-density environments with 80 MHz channels. AirMatch also minimizes effective isotropic radiated power (EIRP) variances across the network in order to give clients the best chances to make the right decisions. ClientMatch steps in to steer the clients that still behave poorly.

Simplified Operations and Deployment Flexibility

The Mobility Master consolidates all-master, single-master multiple local deployments and multiple-master local deployments into a single deployment model. ArubaOS uses a centralized, multi-tier architecture under a new user-interface that provides a clear separation between management, control, and forwarding functions. Network configuration can be directed from the Mobility Master to all the mobility controllers making the configuration process more efficient.

You have the flexibility of deploying a virtual machine (VM) or an x86-based hardware appliance depending on your environment and needs. If you already have a VM environment, you can benefit from ease of operation and right-size your VM by adjusting the CPU or memory. Moving to a VM-based deployment that has more memory and compute resources allows you to manage more services on the network. The virtual Mobility Master can run on open source KVM, VMWare ESXi hypervisor, or Microsoft HyperV.

Mobility Controller Features

Mobility controllers are managed devices under the Mobility Master and handle the AP terminations. Clustering the mobility controllers provides high availability, scalability, and seamless roaming throughout an entire building or across many buildings in a campus. With clustering, users are not affected by a controller failure, and their traffic continues to flow without noticeable impact. The user session information is shared across controllers in the cluster to ensure there is no single point of failure for any user.

To enhance scalability and resiliency, users are distributed evenly across controllers to prevent congestion on a single controller. This ensures the maximum amount of available throughput for each user even when large numbers of them gather in a single location requesting wireless services. Access points are automatically load balanced across the cluster for better resource utilization and high availability when a controller goes out of service. The AP load balancing is done in a seamless fashion so that users are not affected by the movement between
controllers. Users do not experience delays while roaming through a large campus on mission-critical applications such as Skype for Business. The controllers in a cluster work together to manage the devices and a user can roam across APs without getting a new IP address, re-authenticating, or losing firewall state information.

QoS

Quality of service (QoS) allows the network to prioritize traffic so high-priority traffic has preference over low priority traffic while ensuring all applications are treated fairly. With proper QoS, no individual type of traffic can monopolize the network bandwidth. Instead, pre-defined classes ensure that all traffic types are given some amount of bandwidth. Because the wireless access layer is where traffic enters the network from end-user devices, it is important for it to be one of the first policy enforcement points. Traffic entering the network should be classified and tagged based on your organization's requirements.

ClientMatch

Aruba ClientMatch technology is specifically built for enterprise wireless networks. AppRF Technology and Intelligent Application Identification combine to give you unparalleled visibility into the applications running on your wireless network. ClientMatch continually monitors a client's RF neighborhood to provide ongoing client band steering and load balancing along with enhanced AP reassignment for roaming mobile clients. This feature is recommended over the legacy band-steering and spectrum load-balancing features, which do not trigger AP changes for clients already associated to an AP.

ClientMatch dynamically optimizes Wi-Fi client performance as users roam and RF conditions change. If a device moves out of range of an AP or if RF interference unexpectedly impedes performance, ClientMatch steers it to a better AP. ClientMatch automatically groups multi-user MIMO (MU-MIMO) clients together on Wave 2 APs, so that the AP can transmit simultaneously to multiple clients, thereby realizing the expected Wave 2 throughput and capacity gains for the overall network.

AppRF

Aruba AppRF provides application awareness for thousands of apps, including GoToMeeting, Box, Skype for Business, SharePoint, and Salesforce.com. It also provides web content filtering, enabling IT to control where users can browse on the Internet. The feature uses a cloud database that contains always-up-to-date content and reputation information from millions of web pages.

The AppRF cloud database is updated in real-time with new information about malicious web addresses, enabling AppRF to catch new types of web attacks before they cause damage. To keep clients safe, you can configure them to use the web content filter even when they're not connected to an Aruba Instant network.

Aruba's deep packet inspection (DPI) of layer-4 through layer-7 traffic allows the AppRF feature to monitor mobile app usage and performance and to optimize bandwidth, priority, and network paths in real time, even for apps that are encrypted or appear as web traffic. DPI is vital to understanding usage patterns which may require changes to your network design and capacity while identifying many new types of applications.
Guest Wireless

Organizations often have a wide range of guests that request network access while they are on-site. Guests can include customers, partners, or vendors, and depending on their purpose, can vary in the type of devices they use and locations they visit in your organization. To accommodate the productivity of this diverse range of guest users and their specific roles, you should deploy guest access throughout the organization and not only in lobby or conference room areas.

The flexibility of the Aruba Mobile First Campus architecture allows the wireless network to provide guest and employee access over the same infrastructure. This integrated ability simplifies network operations and reduces capital and operational costs. The critical part of the architecture is to ensure that guest access does not compromise the security of the corporate network.

Using the organization’s existing WLAN provides a convenient, cost-effective way to offer Internet access for visitors and contractors. The wireless guest network:

- Provides Internet access to guests through an open wireless Service Set Identifier (SSID), with web access control in the firewall.
- Supports the creation of temporary guest authentication credentials that are managed by an authorized internal user.
- Keeps traffic on the guest network separate from the internal network in order to prevent a guest from accessing internal resources.

Every AP can be provisioned with controlled, open access to wireless connectivity and the Internet. From the wireless AP, guest traffic is securely tunneled back to the controller and placed into a separate VLAN with strict access to the Internet only.
For maximum security and for a simplified overall design, traffic is passed from the wireless guest network VLAN to the firewall protecting the organization's private assets, as depicted in the following figure.

**Figure 8**  Guest wireless network

To control connectivity, guest users are redirected to a captive portal and must present a username and password to connect to the guest network. The captive portal can be on the mobility controller or an external device. Because the guest traffic must pass through the firewall, strict rules are applied to prevent guest access to the internal corporate network. Lobby ambassadors or other administrative staff can assign temporary guest accounts that require a new password on a timed basis. This design provides the flexibility to tailor control and administration to the organization’s requirements while maintaining a secure network infrastructure.

**Campus Wireless LAN Design Summary**

The Aruba Mobile First Campus WLAN provides network access for employees, guests, and IoT devices. Regardless of their location, wireless devices have the same experience when connecting to their services.
The benefits of the mobile-first wireless campus include:

- Seamless network access for employees, guests and IoT devices.
- Plug and play deployment for APs.
- AirMatch and ClientMatch technology to maximize WLAN performance by dynamically choosing the best Wi-Fi channel and transmit power.
- AppRF and Intelligent Application Identification to provide visibility into the applications running on the wireless network.
- Non-stop networking with a centralized Mobility Master and controller clustering for seamless failover.
- Live upgrades to perform operating system updates without an outage or service impact.
- In-service module upgrades to dynamically update individual service modules without requiring an entire system reboot.

**WIRELESS DESIGN COMPONENTS**

You can deploy Aruba wireless in two main modes, controller-based or controllerless. With Aruba's Mobility Master and mobility controllers, certain features run on the master while others run on the cluster of controllers. This type of design is typically used in larger networks with more than 500 users, but there is no reason it cannot be used in smaller networks.

**Access Points**

The latest generation of Aruba APs, the 3xx models, are dual radio 802.11ac Wave 2 APs and support different throughput and client loads to meet different price points. The last digit in the model number denotes the antenna type. If the number is 4, then the AP has connectors for external antennas. If the number is 5, then the AP has internal antennas. For example, IAP-334 has external antennas and IAP-335 has internal antennas. In most office deployments, internal antenna models are preferred.

The following features are common across the 3xx APs:

- Unified AP for either controller-based (ArubaOS) or controllerless (InstantOS) deployment modes
- Dual Radio 802.11ac AP with MU-MIMO
- Built-in Bluetooth Low-Energy radio
- Advanced Cellular Coexistence to minimize interference from cellular networks
- QoS for app visibility and control
Access Point Options

**Aruba 340 Series Access Points**—The Aruba 340 Series is the highest performance AP and supports HPE Smart Rate uplink so it can use the full performance of 3.5 Gbps on two 5-GHz bands or 1.7 Gbps in the 5-GHz band and 800Mbps in the 2.4-GHz band, for a combined bandwidth of 2.5 Gbps. This model is ideal for organizations that require very high density and next generation performance for auditoriums, high-density office environments, or public venues. The Aruba 340 series requires ArubaOS and Aruba InstantOS 8.3 software.

- Dual Radio 4x4 802.11ac AP with MU-MIMO
- Optional dual 5-GHz mode supported, where the 2.4-GHz radio is converted to a second 5-GHz radio
- Antenna polarization diversity for optimized RF performance
- HPE Smart Rate and Gigabit Ethernet uplink ports with Link Aggregation Control Protocol (LACP) support for increased capacity
- Hitless PoE failover between both Ethernet ports

**Aruba 330 Series Access Points**—The Aruba 330 Series is a high-performance AP and supports HPE Smart Rate uplink so it can use the full performance of 1.7 Gbps in 5-GHz band and 600Mbps in 2.4-GHz band for a combined bandwidth of 2.3 Gbps. This model is ideal for organizations that require high density and next generation performance for auditoriums, high-density office environments, or public venues.

- Antenna polarization diversity for optimized RF performance
- HPE Smart Rate and Gigabit Ethernet uplink ports with LACP support for increased capacity
- Hitless PoE failover between both Ethernet ports

**Aruba 310 Series Access Points**—The Aruba 310 Series is a medium-performance AP that supports 1.7 Gbps in the 5GHz band and 300 Mbps in the 2.4-GHz band with a single Gigabit Ethernet uplink. This model is ideal for organization who need to support medium density environments, such as schools, retail branches, hotels, and enterprise offices that don't require multi-gigabit performance.

**Aruba 300 Series Access Points**—The Aruba 300 Series is an entry-level AP that supports 1.3 Gbps in the 5-GHz band and 300 Mbps in the 2.4-GHz band with a single Gigabit Ethernet uplink. This model is ideal for organizations with medium density environments who want the latest technology but don't need the higher level of performance.

Mobility Master and Mobility Controllers

You can deploy the Aruba Mobility Master either as a virtual appliance or on an x86-based hardware appliance. The Aruba 7200 series mobility controller is optimized for mobile application delivery in order to ensure the best mobility experience over Wi-Fi. The Aruba 7000 Series mobility controllers optimize cloud services and secure
enterprise applications for hybrid WAN at branch offices, while reducing the cost and complexity of deploying and managing the network. The virtual mobility controllers run on x86 platforms, and you can integrate them into your existing virtual machine environments.

Mobility Master and Mobility Controller Options

The Mobility Master provides centralized configuration and visibility, multi-tenant with multizone, controller clustering with hitless failover, automatic user and AP load balancing and seamless roaming. They support live upgrades, multiple OS and high performance WiFi with AirMatch.

The mobility controllers support Aruba’s Next-Generation Mobility Firewall with AppRF technology as well as other enterprise-critical capabilities like authentication, encryption, IPv4 and IPv6 services, Adaptive Radio Management, ClientMatch, and RFProtect spectrum analysis and wireless intrusion protection.

Table 3   Maximum scaling capabilities

<table>
<thead>
<tr>
<th>Device</th>
<th>Mobility controllers</th>
<th>Access points</th>
<th>Clients</th>
<th>Cluster members</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility Master</td>
<td>1000</td>
<td>10,000</td>
<td>100,000</td>
<td>2</td>
</tr>
<tr>
<td>7200 Mobility Controllers</td>
<td>N/A</td>
<td>2048</td>
<td>32,768</td>
<td>12</td>
</tr>
<tr>
<td>7000 Mobility Controllers</td>
<td>N/A</td>
<td>64</td>
<td>4096</td>
<td>4</td>
</tr>
<tr>
<td>Mobility Controllers Virtual Appliance (MC-VA)</td>
<td>N/A</td>
<td>1000</td>
<td>16,000</td>
<td>4</td>
</tr>
</tbody>
</table>

CAMPUS WIRED LAN DESIGN

The campus LAN not only provides wired and wireless connectivity for local users but becomes the core for interconnecting the WAN, data center, and Internet access, making it a critical part of the network. Campus networks require a high availability design to support the mission-critical applications and real-time multimedia communications that drive the organizational operations.

To accommodate growth in the number of devices, network engineers build wired LANs in layers. A typical wired LAN with 500 to 2500 users has an access layer, an aggregation layer and a core layer. With the Aruba Mobile First Campus design, trunks between the layers use multiple links that are actively forwarding traffic for a higher-performance network while reducing the complexity involved in traditional two-layer redundant designs. Breaking the LAN design into layers accomplishes several things that are beneficial to your organization.

• Limiting functions of the individual layers make the network easier to operate and maintain
• Modular building blocks quickly scale as the network grows
• A repeatable design is faster to deploy across multiple locations
Access Layer

The access layer provides layer-2 connectivity to the network for wired and wireless devices. Because the access layer connects client devices to network services, it plays an important role in protecting users, application resources, and the network itself from human error and malicious attacks. This protection includes verifying the devices are allowed on the network, making sure the devices cannot provide unauthorized services to end users and cannot take over the role of other devices on the network. The access layer also provides automated services like PoE, QoS, and VLAN assignments in order to reduce operational requirements.

Many types of end-user devices connect to the access layer, such as PCs, laptops, smart phones, tablets, and other devices such as printers, video surveillance, and wireless APs. In this design, we use separate VLANs for employee wired, employee wireless, and guest wireless traffic. Employee wired traffic is used by the trusted devices cabled to the LAN switches. Employee wireless is used by trusted devices on Wi-Fi. Employee wired and wireless traffic both have access to all internal resources and the Internet. The guest wireless network is used by untrusted wireless devices, which only have access to the Internet. Employee and guest traffic is segmented on the network, as depicted in the following diagram.

Figure 9  Employee and guest VLANs
Access Layer Switching Features

The following features highlight several of the key aspects of the Aruba access layer design.

Stacking

Stacking allows multiple access switches connected to each other through Ethernet connections or dedicated stacking ports to behave like a single switch. Stacking increases the port density by combining multiple physical devices into one virtual fabric, allowing management and configuration from one IP address. This reduces the total number of managed devices while better utilizing the port capacity in an access wiring closet. The members of a stack share the uplink ports, which provides additional bandwidth and redundancy.

There are three stacking-device roles:

- **Commander** — Conducts overall management of the stack and manages the forwarding databases, synchronizing them with the standby.

- **Standby** — Provides redundancy for the stack and takes over stack-management operations if the commander becomes unavailable or if an administrator forces a commander failover.

- **Members** — Are not part of the overall stack management; however, they must manage their local subsystems and ports to operate correctly as part of the stack. The commander and standby are also responsible for their own local subsystems and ports.

When connecting three or more switches into a logical switch stack, a ring topology is recommended. In a three-switch stack, connect switch one to switch two, connect switch two to switch three and connect switch three back to switch one to form a ring as shown in the diagram below. If a switch stack has three or more members, we recommend assigning the commander role to a switch that does not have uplinks to minimize forwarding delays when the commander becomes unavailable.

![Figure 10: Three-switch ring topology and roles](image-url)
QoS

QoS for the wired LAN provides the same benefits for wired clients as was discussed previously for wireless clients on the WLAN. Because the access layer is where traffic enters the network, it is important for it to be one of the QoS first policy enforcement points.

Security Services

Security at the access layer protects end users and the network from configuration errors and malicious attacks. The following security services are recommended at the access layer:

• **Port Security**—Enables you to limit the number of MAC address allowed on a port, stopping MAC flooding attacks. MAC addresses can be learned by the switch or statically configured, and if there is a violation, you have the option of sending an alarm, disabling the port, or both.

• **DHCP Snooping**—Stops IPv4 DHCP starvation attacks, in which an attacker repeatedly requests an address from a DHCP server until no more addresses are available, causing a denial of service to other users. It also prevents rogue DHCP servers by only allowing replies from a trusted server on a trusted switch port, typically the uplink ports to the aggregation layer.

• **ARP Protect**—Stops man-in-the-middle attacks caused by ARP cache poisoning, by verifying the source IP-MAC binding information in the DHCP snooping table. This prevents hosts from sending spoofed ARP messages to fool devices into sending traffic to the wrong address.

• **Dynamic IP Lockdown**—Stops devices from forging their source IP address by inspecting the IP-MAC binding information in the DHCP snooping table. This prevents hosts from injecting traffic into the network to bypass security based on IP source address or to hide their location by forging their source IP address.

• **BPDU Protection**—Prevents loops in the network by putting a non-trunk port into a disabled state for a specified amount of time when it receives a BPDU from another device. This is normally caused by a rouge device being connected to an access port on a switch.

• **DHCPv6 Snooping**—Stops IPv6 DHCP starvation attacks, in which an attacker repeatedly requests address from an IPv6 DHCP server until no more addresses are available, causing a denial of service to other users. It also prevents rogue IPv6 DHCP servers by only allowing replies from a trusted server on a trusted switch port, typically the uplink ports to the aggregation layer.

• **IPv6 RA Guard**—Stops rogue IPv6 clients from advertising themselves as routers. The IPv6 RA Guard feature on the switch analyzes router advertisements (RAs) and filters out the ones sent by unauthorized devices.
IP Multicast

The access layer switches use a key IP multicast feature called IGMP snooping. IGMP snooping is designed to prevent hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. The feature provides layer-2 switches with a mechanism to prune multicast traffic from ports that do not contain an active multicast listener.

Aggregation Layer

The aggregation layer acts as the boundary between layer-2 switching and layer-3 routing. The aggregation layer provides layer-3 services, routing LAN traffic between networks in the campus and out of the campus to other networks across the WAN. Because layer-2 networks are terminated at the aggregation layer, it segments the network into smaller broadcast domains. As more access layer switches are added, it becomes difficult to interconnect them with a full mesh because meshing uses the uplink ports quickly and daisy-chaining limits the overall performance of the network. The aggregation layer increases network scalability by providing a single place to interconnect the access layer switches, giving you high performance and single hop connectivity between all switches in the aggregation block. The services aggregation block also becomes the ideal location for connecting other network services, such as the WAN aggregation, Internet DMZ, and server rooms or data center for a large organization.

Figure 11  Aggregation layer—routing and switching boundary
Aggregation Layer Switching Features

The following features highlight key aspects of the Aruba aggregation layer design.

Multi-Chassis Link Aggregation

Multi-Chassis Link Aggregation Group (MC-LAG) allows the aggregation layer switch pair to appear as a single device to other devices in the network, such as the access layer switches. MC-LAG allows all uplinks between switch stacks to be active and passing traffic for higher capacity and availability, as shown in the right side of the following figure. Older, redundant designs relied on Spanning Tree Protocol (STP), which blocks redundant links, as shown in the left side of the following figure. It can take up to 50 seconds for a traditional spanning-tree port to transition from blocking to a forwarding state and traffic is not forwarded during the re-convergence time. MC-LAG ports are always forwarding, so the re-convergence time for active traffic on a failed link is less than 100 ms.

![Figure 12: Traditional spanning tree vs MC-LAG](image)

From an STP standpoint, the access to aggregation layer MC-LAG connection looks like a single link, removing all loops in the topology and preventing link or switch failures from causing STP re-convergence.

Depending on the switch model, the Aruba switches support MC-LAG using either backplane stacking or virtual switching framework (VSF), in order to appear as a single switch to other devices in the network.

The benefits of multi-chassis link aggregation are as follows:

- **Performance and Capacity**—A stack creates a pool of network ports with optimized forwarding, so any member of the stack can utilize the shared uplinks in order to meet network demands. MC-LAG combines links from individual switches in the stack, allowing them to act as one connection, which increases the performance of the uplinks.

- **Resiliency and Redundancy**—If a MC-LAG member switch fails, the other member continues to operate, which reduces recovery time. Links to the switches in a MC-LAG group are split across the stack members which provides additional bandwidth, link redundancy, and physical device redundancy.

- **Simplifies Management and Configuration**—Even though a stack consists of multiple physical devices, a stack is managed as a single device with a single configuration, which simplifies network design and management.
IP Routing

In a large organization, all departments need to be connected and sharing information. To accomplish this in an easy, scalable manner, a dynamic routing protocol is needed. Open Shortest Path First (OSPF) is a dynamic, link-state, standards-based routing protocol that is commonly deployed in campus networks. OSPF provides fast convergence and excellent scalability, making it a good choice for large networks because it can grow with the network without the need for redesign.

OSPF uses areas which provides segmentation of the network to limit routing advertisements and allow for route summarization. Area segmentation is normally done on logical network boundaries, such as buildings or locations, and it helps minimize the impact of routing changes across the network. In large networks with WANs, multiple OSPF areas are very useful, but in a typical campus networks of less than 2500 users a single area is recommended.

The access switches have a default gateway in the management VLAN for operational access, and the VLANs are terminated at the aggregation layer switches. The Internet is accessed using a static default route originating from the DMZ firewall.
IP Multicast

IP multicast allows a single IP data stream to be replicated by the network and sent from a single source to multiple receivers. IP multicast is much more efficient than sending multiple unicast streams or flooding a broadcast stream that would propagate everywhere. Common examples of multicast traffic in a campus network are IP telephony music on hold and IP video broadcast streaming.

This design uses protocol independent multicast (PIM) sparse mode to route multicast traffic on the network. Rather than build a separate routing table, PIM uses the unicast routing table. In our case, the routing table created by OSPF is used for reverse path forwarding. The three mechanisms to route multicast in this design are the rendezvous point (RP), bootstrap router (BSR), and Internet Group Management Protocol (IGMP).

The BSR is elected from a list of candidate-BSRs configured on the network. There can only be a single active BSR on the network. The BSR advertises RP information to all PIM-enabled routers in the network, freeing you from having to statically configure the RP address on each router in the network. The BSR also allows for backup RPs to be configured for multicast groups. If a primary RP fails, the network can switch to the backup automatically. Typically, routers in the core of the network are configured as the BSR candidate routers.

The RP is the root of the multicast tree for multicast traffic using sparse mode. Because it is the root for shared multicast traffic, the RP is normally placed at the core of the network or at the point where the most multicast senders are located. Multiple RPs can be configured for redundancy, although only one RP can be active for a multicast group. Multicast sources are registered to the RP when the local multicast router sends a unicast register message to the RP.

When a client wants to join a multicast group, it sends an IGMP message to its local multicast router. The local multicast router, called the designated router (DR), forwards the join message towards the RP and all routers in the path do the same until the join reaches the RP. Multicast traffic is forwarded back down the shared tree to the client. Periodic join messages are sent to the RP for each multicast group with active clients. If a DR wants to stop traffic from a multicast group because it no longer has active clients it can send a prune message to the RP. To prevent the DR from flooding traffic to all clients on a local subnet, layer-2 switches snoop the IGMP messages and only forward traffic to clients that have sent a join message.

The 802.11 standard states that multicast traffic over WLAN must be transmitted at the lowest basic rate so all clients are able to decode it. We recommend enabling Dynamic Multicast Optimization (DMO) to allow the AP to convert the multicast traffic to unicast for each client device. Unicast packets are transmitted at the higher unicast rate which decreases the airtime utilization and increases overall throughput. IGMP snooping must be enabled on the layer-2 switches for DMO to work.

The following figure shows a multicast source registered with the RP and sending traffic to clients that have joined the multicast group. Note that clients not receiving the multicast stream have not joined the group.
Core Layer

In a large LAN environment, there are often multiple aggregation layer switches. When access layer switches are located in multiple geographically dispersed buildings, you can save costly fiber-optic runs between buildings by placing an aggregation layer switch in each of those buildings. As networks grow beyond three aggregation switch pairs in a single location, organizations should add a core layer to optimize the design.

Additional aggregation layer switches are also needed when the number of access layer switches connecting to a single aggregation point exceeds the performance of the pair of aggregation switches. In a modular and scalable design, you can co-locate aggregation layer switches for data center, WAN connectivity, and Internet edge services. If your network is not large enough to warrant a standalone core, you can combine the core switch functions with the services aggregation functions using a larger modular switch for increased port capacity.

In environments where multiple aggregation layer switches exist in close proximity and where fiber optics provide high-bandwidth interconnects, a standalone core layer reduces the network complexity. The standalone core layer uses separate core switches acting independently of each other with dual equal-cost multi-path (ECMP) connections into all aggregation layer switch blocks, as shown in the following figure.
You can also combine the core and services functionality into a single pair of switches. When combining the core and services, we recommend stacking the two core-services switches together to allow the infrastructure devices in the services aggregation to use MC-LAG when connecting to them. This is the same design as the access-aggregation switches and the services-aggregation switches discussed previously. If you decide you want to add a standalone core later, you can re-use the combined core-services switches as your services aggregation.
The diagram below shows the core switch with a combined services aggregation in the Mobile First Campus design.

![Core and services](image)

**Figure 16  Core and services**

Core Layer Switching Features

The core layer of the LAN is a critical part of the scalable network, yet it is one of the simplest by design. The aggregation layer provides the fault and control domains and the core represents the 24x7x365 nonstop connectivity between the aggregation switch pairs.

For the fastest core layer convergence, build triangles not squares in order to take advantage of ECMP routing, which provides the best deterministic convergence. ECMP is an advanced routing strategy where next-hop packet forwarding occurs over multiple paths with identical routing metric calculations.

When considering core topologies, it is also important to use point-to-point links because link up/down changes are propagated almost immediately to the underlying protocols. Topologies with redundant ECMP links are the most deterministic and convergence is measured in milliseconds, rather than topologies that rely on indirect notification and timer-based detection, where convergence is non-deterministic and often measured in seconds.

High Performance

- The fully distributed architecture of the core switch provides up to 19.2 Tbps switching capacity with up to 7.142 billion packets per second of throughput because all switching and routing is performed in the line modules.
- A scalable system design provides investment protection in order to support future technologies and higher-speed connectivity.
Resiliency and High Availability

- The redundant and load-sharing fabrics, fan assemblies, and power supplies increases total performance and power availability while providing hitless, stateful failover.
- Hot-swappable modules allow replacement of hardware without impacting other modules.
- Separate data and control paths keeps service processing isolated, which increases security and performance of the core devices.
- ECMP enables multiple equal-cost point-to-point links in a high-speed routed environment to increase link redundancy and scale the bandwidth between devices.

Campus Wired LAN Design Summary

The Aruba Mobile First Campus wired LAN provides network access for employees, APs, and IoT devices. The campus LAN also becomes the core for interconnecting the WAN, data center, and Internet access, making it a critical part of the network.

The simplified access, aggregation, and core design provides the following benefits:

- An intelligent access layer provides protection from attacks while maintaining user transparency within their layer-2 VLAN boundaries.
- Redundant uplinks forward traffic, providing higher bandwidth and resiliency without creating layer-2 STP loops in the network.
- The MC-LAG aggregation layer reduces complexity while improving recovery times during network failures.
- The aggregation and core layers provide IP routing using OSPF and IP multicast using PIM sparse mode with redundant BSRs and RPs.
- The services aggregation is the logical place to connect critical networking devices such as corporate servers, WAN routers, and Internet-edge firewalls.
- The core is a high-speed dual-switch interconnect that provides path redundancy and sub-second failover for non-stop forwarding of packets.
- Combining the core and services aggregation into a single layer allows the network to scale when a stand-alone core is not required.
WIRED DESIGN COMPONENTS

The wired LAN in the Mobile First Campus uses a hierarchical, modular design. Each layer performs specific functions helping to simplify the design, making the network easier to deploy, manage, and maintain. Although there are many hardware choices that will work at the different layers in the network, this design focuses on products that are the most common and easily supported options in each layer of the network, with general guidance on which option to choose.

Access Switches

The access layer connects wired devices to the network, such as APs, workstations, multi-function printers, and other devices that don’t support Wi-Fi or need higher performance than a wireless connection can provide. The access layer also provides PoE to devices such as APs, IP phones, and IP cameras.

The following features are common across the Aruba access switches:

- Support for security and network management with Aruba ClearPass, Aruba AirWave, and cloud-based Aruba Central
- REST APIs for the software-defined network
- PoE for APs, IP phones, and IoT devices

The number of ports needed in an access closet and the performance required will decide what access switch model is the best fit for your network.

Access Layer Switching Options

**Aruba 5400R**—The Aruba 5400R chassis supports a variety of interface modules that provide copper and fiber interfaces in different speeds and densities. At the access layer, the switch supports up to 96 HP Smart Rate Multi-Gigabit or 288 1-GbE ports with PoE+. This switch is ideal for organizations that need large numbers of access ports in high density areas of their network (majority of access closets with 96+ ports).

- Layer-3 modular switch with VSF stacking, tunnel node, ACLs, robust QoS, low latency, and resiliency
- HPE Smart Rate for high-speed multi-gigabit bandwidth (IEEE 802.3bz) and PoE+
- Scalable line-rate 40 GbE for wireless traffic aggregation

**Aruba 3810M**—The Aruba 3810M is available with either 24 or 48 1-GbE access ports with PoE+ (30W) on each port and either 4 SPF+ ports or 2 40-GbE ports on an optional expansion module. The 3810M is also available in a model with 40 1-GbE ports and 8 HPE Smart Rate ports capable of 1, 2.5, 5, or 10 GbE. The 3810M supports backplane stacking with up to 10 switches in a single stack and advanced layer-3 services. This switch is ideal for organizations that have larger access closets requiring larger switch stacks, are deploying or planning on deploying
802.11ac Wave 2 APs, and want a switch with high performance and room for future growth.

- Layer-3 switch with backplane stacking, tunnel node, ACLs, robust QoS, low latency, and resiliency
- HPE Smart Rate for high-speed multi-gigabit bandwidth (IEEE 802.3bz) and PoE+
- Modular line-rate 10-GbE and 40-GbE ports for wireless aggregation

**Aruba 2930M**—The Aruba 2930M is available with either 24 or 48 1-GbE access ports with PoE+ (30W) on each port and either 4 SPF+ ports or 2 40-GbE ports on an optional expansion module. The 2930M is also available in a model with 40 1-GbE ports and 8 HPE Smart Rate ports capable of 1, 2.5, 5, or 10 GbE. The 2930M supports backplane stacking with up to 10 switches in a single stack and dynamic layer-3 services. This switch is designed for organizations wanting to create a digital workplace optimized for mobile users with an integrated wired and wireless access network.

- Layer-3 switch with backplane stacking, tunnel node, ACLs, and robust QoS
- HPE Smart Rate for high-speed multi-gigabit bandwidth (IEEE 802.3bz) and up to 1440 W PoE+
- Modular 10-GbE or 40-GbE uplinks
- Models with 24 ports of HPE Smart Rate with IEEE 802.3bz

**Aruba 2930F**—The Aruba 2930F is available with either 24 or 48 1-GbE access ports and 370W PoE+. The switch supports VSF, allowing you to stack up to 4 switches using available front ports. While the 2930F supports basic layer-3 features, it is typically deployed as a layer-2 switch. This switch is ideal for organizations that have smaller access closets requiring only one or two switches, are looking for good performance, and who can accept a limited feature set in return for lower cost.

- Layer-3 switch with VSF stacking, tunnel node, ACLs, and robust QoS
- Convenient built-in 1GbE or 10GbE uplinks and up to 740 W PoE+

**Aggregation Switches**

The aggregation layer provides connectivity for all the access layer switches and connects to any external networks in the campus LAN. The aggregation layer is responsible for layer-3 routing in this design and it handles all traffic between networks on the campus LAN and traffic leaving the LAN for the data center, the WAN or the Internet. For high availability, the aggregation layer consists of a pair of switches acting as a single switch. If a switch fails or needs to be taken out of service for maintenance, the other switch continues forwarding traffic without interruption to the LAN services.
The following features are common across the aggregation switches:

- HPE Smart Rate for high-speed multi-gigabit bandwidth (IEEE 802.3bz) and PoE+
- Support for security and network management with Aruba ClearPass, Aruba AirWave Network, and cloud-based Aruba Central
- REST APIs for the software-defined network

Aggregation Layer Switching Options

**Aruba 5400R**—The Aruba 5400R chassis supports a variety of interface modules that provide copper and fiber interfaces in different speeds and densities. The switch supports up to 96 10-GbE ports (SFP+ and 10GBASE-T), 96 HP Smart Rate Multi-Gigabit, or 288 1-GbE ports with PoE+. This switch is ideal for organizations that need to aggregate many access switches and may need to connect servers, firewalls or other network appliances directly to the aggregation layer.

- Layer-3 modular switch with VSF stacking, static routing, RIP routing, OSPF routing, ACLs, robust QoS, policy-based routing, low latency, and resiliency
- Scalable line-rate 40GbE for wireless traffic aggregation

**Aruba 3810**—The Aruba 3810M is available in a 16 port SFP+ and a two-module slot model. The module slots allow for an additional 8 SFP+ or 2 40-GbE ports. This switch is ideal for organizations with a small LAN who to aggregate 1 or 10-GbE connected access switches.

- Layer-3 switch with backplane stacking, static routing, RIP routing, OSPF routing, ACLs, robust QoS, policy-based routing, low latency, and resiliency
- Modular line-rate 10-GbE and 40-GbE ports for wireless aggregation

Core Switches

The core layer provides high-speed routing to the aggregation blocks using a pair of redundant switches. The two switches are dual connected to all aggregation layer devices using an ECMP routing strategy where next-hop packet forwarding can occur over multiple paths that have the same routing metric. You can use ECMP with most routing protocols, including OSPF, because it is a per-hop decision.

Core Layer Switching Options

The 8400/8320 switches support the following features:

- Advanced layer-2/3 feature set includes QoS, BGP, OSPF, VRF, VRRP and IPv6
- Intelligent monitoring and visibility with Aruba Network Analytics Engine
Aruba 8400—The Aruba 8400 chassis supports line rate 10GbE/40GbE/100GbE port density, very low latency, and scalability for support of full Internet routes. The switch supports up to 256 10GbE (SFP/SFP+), or 64 40GbE (QSFP+), or 48 ports 40/100GbE (QSFP28) with eight slots for line modules and provides up to 19.2 Tbps switching capacity with up to 7.142 billion packets per second of throughput.

- Carrier-class high availability with redundant management, power and fabric

Aruba 8320—The Aruba 8320 compact switch supports line rate 10GbE/40GbE port density and very low latency. The switch supports up to 48 10GbE (SFP/SFP+), or 32 40GbE (QSFP+) and provides up to 2.5 Tbps switching capacity with up to 1905 million packets per second of throughput.

- High availability with redundant power supplies and fans

Aruba 5400R—The Aruba 5400R chassis supports a variety of interface modules that provide copper and fiber interfaces in different speeds and densities. The switch supports up to 96 10-GbE ports (SFP+ and 10GBASE-T), 96 HP Smart Rate Multi-Gigabit, or 288 1-GbE ports with PoE+. This switch is ideal for organizations that may need to connect servers, firewalls or other network appliances directly to the core layer.

- Layer-3 modular switch with VSF stacking, static routing, RIP routing, OSPF routing, ACLs, robust QoS, policy-based routing, low latency, and resiliency
- Scalable line-rate 40GbE for wireless traffic aggregation

The next section of this guide helps you deploy the Mobile First Campus design in your organization.

### Deploying the Mobile First Campus

The Aruba Mobile First Campus design provides wired and wireless connectivity for local users. The wired LAN interconnects the wireless APs, WAN, data center, and Internet DMZ, making it a critical part of the network. Campus networks require a high-availability design to support mission-critical applications and real-time multimedia communications that drive organizational operations.
The Mobile First Campus Design provides the following benefits:

- Specific functions of individual layers make the network easier to operate and maintain
- Modular building blocks quickly scale as the network grows
- Location-independent network access improves employee and guest productivity
- Hard-to-wire locations receive network connectivity without costly construction
- Plug-and-play wireless deployment with wired LAN switches preconfigured to recognize APs
- Centralized control of wireless environment is easy to manage and operate
- Reliable wireless connectivity, including complete RF spectrum management is available with key Aruba management features

Simple, repeatable designs are easier to deploy, manage, and maintain. This design shows the most common and best supported options with general guidance for which option to choose. An overview of the Mobile First Campus design for 500 to 2500 users is shown in the following diagram.

*Figure 17  Mobile First Campus design overview*
CAMPUS WIRED LAN

The wired LAN uses a hierarchical design model. Each layer performs specific functions helping to simplify the solution. In a typical network of 500 to 2500 users, the wired LAN has a core layer, an aggregation layer, and an access layer. With the Aruba design, the trunks between the layers use multiple active links forwarding traffic for a higher-performance network while reducing the complexity involved in traditional redundant campus designs.

Wired Access

The access layer in this design provides layer-2 connectivity to the network for wired and wireless devices. The layer-2 switches range from a single 2930F, 2930M, and 3810M to stacks of 2930Fs, 2930Ms and 3810Ms, along with a pair of stacked 5406. They are dual-connected to the dual-switch aggregation layer. Each uplink is connected to one of the two switches at the aggregation layer. If the access switches are stacked, the distributed ports are connected from different physical switches in the access layer.

The access switches are layer-2 and they contain two VLANs, one for management and one for employee wired. The VLANs for the employee wireless and guest wireless move from the access layer in the Instant AP design into the services aggregation because the wireless traffic is tunneled at layer-2 to the centralized controllers. For management purposes, each switch has an IP address in the management VLAN with a default gateway configured as the first-hop aggregation switch.

Procedures

**Configuring the Access Switch**

1.1 Configure access switch stacking
1.2 Configure access-switch base features
1.3 Configure uplink ports from access to aggregation
1.4 Configure access-switch VLANs
1.5 Configure device profile for wireless access points
1.6 Configure the access-switch default gateway
1.7 Configure multicast IGMP snooping
1.8 Configure access-switch port-security features

Use this section for the access layer and repeat it for each wired access switch. This section can be used for stand-alone switches, switch stacks, or modular access switches.
The diagram below shows the wired access switch location in the Mobile First Campus design.

**Figure 18**  Mobile First Campus design—wired access

1.1 **Configure access switch stacking**

Optional

This optional procedure is for switch platforms with backplane stacking modules using stack cables or front plane stacking using VSF. If you are not using a switch stack in this area of your network, skip this procedure.

Stacking allows multiple access switches connected to each other through dedicated stacking ports or Ethernet connections to behave like a single switch. Stacking increases the port density by combining multiple physical devices into one virtual fabric, allowing management and configuration from one IP address. This reduces the total number of managed devices while better utilizing the port capacity in an access wiring closet. The members of a stack share the uplink ports, providing additional bandwidth and redundancy.
There are three stacking-device roles:

- **Commander**—Conducts overall management of the stack, and manages the forwarding databases, synchronizing them with the standby.

- **Standby**—Provides redundancy for the stack and takes over stack management operations if the commander becomes unavailable or if an administrator forces a commander failover.

- **Members**—Are not part of the overall stack management; however, they must manage their local subsystems and ports to operate correctly as part of the stack. The commander and standby are also responsible for their own local subsystems and ports.

The device role is determined by member priority. When all switches in the stack are booted simultaneously, the switch with the highest priority becomes commander and the next highest priority becomes standby. The stacking priority can be set to any value between 1 and 255, and the default value is 128.

When connecting three or more switches into a logical switch stack, a ring topology is recommended. In a three-switch stack, connect switch one to switch two, connect switch two to switch three and connect switch three back to switch one to form a ring as shown in the diagram below. If a switch stack has three or more members, we recommend assigning the commander role to a switch that does not have uplinks to minimize forwarding delays when the commander becomes unavailable.

**Figure 19**  Three-switch ring topology and roles

If you are planning to use dedicated stacking modules with 2930M or 3810M switches, choose option 1. If you are planning to use Ethernet ports and VSF with 5400R or 2930F switches, choose option 2.

**Option 1: Backplane stacking**

The backplane stacking feature allows you to connect as many as ten switches into a single logical switch for data plane and management functions. One switch is designated as the commander, a second switch is configured as the standby, and other switches are designated as role member.
The following tables show the configuration details for backplane stacking.

**Table 4  Backplane stacking for two-member switch stacks**

<table>
<thead>
<tr>
<th>Stacking member ID</th>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stacking priority</th>
<th>230 (Standby)</th>
<th>250 (Commander)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uplink</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Table 5  Backplane stacking for three-member or more switch stacks**

<table>
<thead>
<tr>
<th>Stacking member ID</th>
<th>Switch 1</th>
<th>Switch 2</th>
<th>Switch 3+</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Stacking priority</td>
<td>230 (Standby)</td>
<td>250 (Commander)</td>
<td>128 (Member) default</td>
</tr>
<tr>
<td>Uplink</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

On a stack of three or more switches, assign the Commander role to a switch without uplinks. If your stack only has two switches, pick either switch for the Commander role because they both have uplink ports.

Follow the steps below to connect the switches and statically assign their roles.

**Step 1:** Install the backplane stacking modules in all switches and connect the cables in a ring or mesh topology.

**Step 2:** Power-on each switch.

**Step 3:** Display the member ID for each switch, using the `show stacking` command.

```
show stacking
...
ID  Mac Address       Model                                 Pri Status
--- ----------------- ------------------------------------- --- ---------------
1   ecebb8-17f300     Aruba JL073A 3810M-24G-PoE+-1-slot... 128 Commander
*2  ecebb8-177480     Aruba JL073A 3810M-24G-PoE+-1-slot... 128 Member
3   ecebb8-175480     Aruba JL073A 3810M-24G-PoE+-1-slot... 128 Standby
```

**Note** When the switches see each other through the stacking modules, stacking is enabled by default and member ID numbers are automatically assigned.
Note: The * indicates the physical switch you are using to view the stack.

Step 4: Following the guidelines in Table 4 and Table 5, determine the switch that will receive the Commander role and the switch that will receive the Standby role. If you have more than 2 switches in a stack, the additional switches will receive the Member role.

Step 5: On the stacking member that will receive the Commander role, configure the highest priority.

```
stacking member 2 priority 250
```

Step 6: On the stacking member that will receive the Standby role, configure the second highest priority.

```
stacking member 1 priority 230
```

Step 7: Save the configuration for all stack members.

```
write memory
```

Step 8: Reboot the switch stack for the changes to take effect.

```
boot system
This will reboot the system from the primary image.
Continue (y/n)? y
```

Step 9: After the switch stack reboots, verify stack status changes with the `show stacking` command.

```
show stacking
...
ID    Mac Address       Model                                 Pri Status
---    ----------------- ------------------------------------- --- ---------------
1      ecebb8-17f300     Aruba JL073A 3810M-24G-PoE+-1-slot... 230 Standby
*2     ecebb8-177480     Aruba JL073A 3810M-24G-PoE+-1-slot... 250 Commander
3      ecebb8-175480     Aruba JL073A 3810M-24G-PoE+-1-slot... 128 Member
```
Option 2: VSF stacking

VSF stacking allows switches to connect to each other through Ethernet ports in order to behave like a single logical switch. Like backplane stacking, the VSF fabric uses unique member IDs to identify and manage its members.

The VSF stack can have as many as four switches. The stack is formed using VSF links, which are logical interfaces comprised of same-speed physical interfaces. With the recommended ring topology, two logical VSF links are required per switch, one for each adjacent switch. For two-switch VSF stacks, only one logical VSF link is required.

The following tables show the configuration details for VSF stacking.

### Table 6  VSF stacking for two-member switch stacks

<table>
<thead>
<tr>
<th>Switch 1</th>
<th>Switch 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSF member</td>
<td>1</td>
</tr>
<tr>
<td>VSF links</td>
<td>1</td>
</tr>
<tr>
<td>Priority</td>
<td>230 (Standby)</td>
</tr>
<tr>
<td>VSF domain</td>
<td>200</td>
</tr>
<tr>
<td>Uplink</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Table 7  VSF stacking for three-member or four-member switch stacks

<table>
<thead>
<tr>
<th>Switch 1</th>
<th>Switch 2</th>
<th>Switch 3+</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSF member</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>VSF links</td>
<td>1 and 2</td>
<td>1 and 2</td>
</tr>
<tr>
<td>Priority</td>
<td>230 (Standby)</td>
<td>250 (Commander)</td>
</tr>
<tr>
<td>VSF domain</td>
<td>300</td>
<td>300</td>
</tr>
<tr>
<td>Uplink</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

On a stack of three or more switches, assign the Commander role to a switch without uplinks. If your stack has only two switches, pick either switch for the Commander role because they both have uplink ports.

Follow the steps below to connect the switches and statically assign their roles in the stack.

Caution  To prevent the half-configured links from causing problems, configure VSF prior to cabling the switches together.
Step 1: Following the guidelines in Table 6 and Table 7, determine the switch that will receive the Commander role and the switch that will receive the Standby role. If you have more than 2 switches in a stack, the additional switches will receive the Member role.

Step 2: On the switch that will receive the Standby role, configure the first member number ID with VSF link 1 and assign physical ports to it.

```
vsf member 1 link 1 A1-A2
```

**Note** To enable a VSF link, you must bind a minimum of one physical interface to it. The physical interfaces assigned to a VSF link automatically form an aggregate VSF link. A VSF link goes down only if all its VSF physical interfaces are down.

Step 3: For switches in a stack of three or more, configure the same member number ID with VSF link 2 and assign physical ports to it. Skip this step for two-member VSF switch stacks, because a second link is not needed.

```
vsf member 1 link 2 A3-A4
```

Step 4: Assign the Standby role to the switch, by configuring it with the second highest priority.

```
vsf member 1 priority 230
```

Step 5: Enable and save the configuration for the VSF domain.

```
vsf enable domain 300
```

This will save the current configuration and reboot the switch.

Continue (y/n)? y

Step 6: Connect to the switch that will receive the Commander role.

Step 7: Configure the member number ID with VSF link 1 and assign physical ports to it.

```
vsf member 2 link 1 A1-A2
```

Step 8: For switches in a stack of three or more, configure the same member number ID with VSF link 2 and assign physical ports to it. Skip this step for two-switch VSF stacks, because a second link is not needed.

```
vsf member 2 link 2 A3-A4
```

Step 9: Assign the Commander role to the switch, by configuring it with the highest priority.

```
vsf member 2 priority 250
```
Step 10: Enable and save the configuration for the VSF domain.

```
vsf enable domain 300
```

This will save the current configuration and reboot the switch.

Continue (y/n)?  y

Step 11: If there are no additional switches, skip to Step 16.

Step 12: Connect to a switch that will receive the Member role.

Step 13: Configure the member with VSF links 1 and 2, and assign physical ports to the links.

```
vsf member 3 link 1 A1-A2
vsf member 3 link 2 A3-A4
```

Step 14: Enable and save the configuration for the VSF domain.

```
vsf enable domain 300
```

This will save the current configuration and reboot the switch.

Continue (y/n)?  y

Step 15: For each additional switch in VSF stack, repeat Step 12 through Step 14, changing the variables according to the switch member ID and the physical ports assigned to the link.

Step 16: After all the switches in the stack are configured and rebooted, connect the VSF Ethernet ports.

Step 17: Use the following command to verify the VSF stack is operational.

```
show vsf topology
```

Example: Two-member VSF stack

```
VSF member’s interconnection with links:
Stby        Cmdr
+----+   +----+
| 1  |1==1|  2 |
+----+   +----+
```
Example: Three-member VSF stack

VSF member’s interconnection with links:

```
Stby     Cmdr
+----+    +----+    +----+
| 1  |1==2| 2 |1==2| 3 |
+----+    +----+    +----+
       2          1
+==================+
```

1.2 Configure access-switch base features

In this procedure, you configure the base features for each access switch.

The switch has two levels of access: manager and operator. The manager has access to all areas of the configuration and has the ability to make configuration changes. The operator has access to the status, counters, and the event log, but the operator has read-only access to the command line interface and thus cannot make changes. You can only have one username and password for each level of access. The usernames are optional but we recommend changing them for additional security.

On each access switch, perform the following steps:

**Step 1:** Configure the switch host name.

```
hostname Access-Switch
```

**Step 2:** Configure the restricted operator username and password.

```
password operator user-name adminOper plaintext [passwordOper]
```

**Step 3:** Configure the unrestricted manager username and password

```
password manager user-name adminMgr plaintext [passwordMgr]
```

**Step 4:** Enable the SSH for inbound connections.

```
ip ssh
```

**Step 5:** Enable the secure copy protocol (SCP).

```
ip ssh filetransfer
```

**Step 6:** For increased security, turn off telnet server in order to only allow inbound SSH connections.

```
no telnet-server
```
Step 7: Configure a login banner.

```bash
banner motd #
Property of example.com !! Unauthorized use prohibited !!
#
```

Step 8: Configure the network time protocol (NTP) with time zone and daylight savings time.

The time zone offset is entered as the difference in minutes from Coordinated Universal Time (UTC). The negative value means the amount of time behind UTC. The NTP iburst feature provides faster time synchronization.

```bash
time daylight-time-rule continental-us-and-canada
time timezone -480
timesync ntp
ntp unicast
ntp server 10.2.120.70 iburst
ntp enable
```

Step 9: If the date on your device is not current, use the time command to set the date to today's date. The current date is required so that, in the next step, you can create a valid certificate.

```bash
time MM/DD/YYYY
```

Step 10: Configure HTTP Secure (HTTPS) for web access to the switch.

```bash
crypto pki identity-profile https_Profile subject
Enter Common Name(CN) : ExampleSwitch
Enter Org Unit(OU) : ExampleOrgUnit
Enter Org Name(O) : ExampleOrg
Enter Locality(L) : Roseville
Enter State(ST) : California
Enter Country(C) : US
crypto pki enroll-self-signed certificate-name https_Certificate
web-management ssl
```

Step 11: For additional security, turn off plaintext HTTP management.

```bash
no web-management plaintext
```
Step 12: Enable the simple network management protocol version 3 (SNMPv3).

snmpv3 enable
SNMPv3 Initialization process.
Creating user ‘initial’
Authentication Protocol: MD5
Enter authentication password: [password]
Privacy protocol is DES
Enter privacy password: [password]

User ‘initial’ has been created
Would you like to create a user that uses SHA? [y/n] y

User creation is done. SNMPv3 is now functional.
Would you like to restrict SNMPv1 and SNMPv2c messages to have read only access (you can set this later by the command ‘snmpv3 restricted-access’)? [y/n] n

Step 13: Create full read-write, limited read-write and read-only users for SNMPv3.

snmpv3 user NetAdminRW auth sha [passwordRW] priv aes [passwordRW]
snmpv3 user NetAdminLimited auth sha [passwordLimited] priv aes [passwordLimited]
snmpv3 user NetAdminR auth sha [passwordRO] priv aes [passwordRO]

Step 14: For additional security, remove the SNMP server community public from the configuration.

no snmp-server community public

1.3 Configure uplink ports from access to aggregation

The uplink ports use the link aggregation control protocol (LACP) to combine two or more physical ports into a single trunk interface. By default, the uplink trunks use source and destination IP addresses to load-balance traffic between the physical interfaces. If a VLAN is not specified in the link-keepalive command, the unidirectional link detection (UDLD) packets are sent untagged.

Step 1: Configure the dual-port trunks with LACP.

trunk 2/Al, 3/Al trk11 lACP
Step 2: Configure UDLD on the uplink ports, set the interval to 70 (70 at 100-ms increments = 7 seconds) and the retries to 6.

```plaintext
interface 2/A1,3/A1 link-keepalive
  link-keepalive interval 70
  link-keepalive retries 6
```

Step 3: Enable Spanning Tree Protocol (STP) globally on the switch.

```plaintext
spanning-tree enable
```

Step 4: Increase the logging level to informational, for visibility to additional link and trunk status events.

```plaintext
logging severity info
```

### 1.4 Configure access-switch VLANs

The layer-2 access switches need an IP address on the management VLAN, for operational purposes. The non-trunk ports are configured as untagged in the wired VLAN. The trunk ports are configured as tagged for the user VLANs and untagged for VLAN 777.

VLAN hopping is a computer security exploit that uses double tagging to attack network resources on a VLAN. The basic concept behind all VLAN hopping attacks is for an attacking host on a VLAN to gain access to traffic on other VLANs that would normally not be accessible.

Double tagging can be mitigated by creating an unused VLAN that will only be configured as the native VLAN on uplink trunk interfaces. The unused VLAN 777 does not have an IP address and it is not connected to anything else on the switch.

The following table provides the VLAN assignments for the Mobile First Campus design.

#### Table 8 Access switch—VLAN assignments, IP subnets, and port tagging

<table>
<thead>
<tr>
<th>VLAN name</th>
<th>VLAN ID</th>
<th>IP address</th>
<th>Tagged/untagged ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>10</td>
<td>10.2.0.10/22</td>
<td>Tagged Trk11</td>
</tr>
<tr>
<td>Wired</td>
<td>20</td>
<td>N/A</td>
<td>Untagged 1/1-1/48 (all non-trunk ports) Tagged Trk11</td>
</tr>
<tr>
<td>Anti-VLAN hopping</td>
<td>777</td>
<td>N/A</td>
<td>Untagged Trk11</td>
</tr>
</tbody>
</table>
On each access switch, perform the following steps:

**Step 1:** For each VLAN in Table 8, configure the VLAN.

Example: Management VLAN

```yaml
vlan 10
  name Management
  tagged Trk11
  ip address 10.0.2.10 255.255.252.0
exit
```

Example: Anti-VLAN hopping VLAN with no IP address

```yaml
vlan 777
  name Anti-VLAN hopping
  untagged Trk11
exit
```

**Step 2:** Enable Rapid Per-VLAN Spanning Tree protocol (Rapid-PVST).

```bash
spanning-tree mode rapid-pvst
```

**Step 3:** Use the management VLAN IP address to configure the source address for SNMP responses from the switch.

```bash
snmp-server response-source 10.2.0.10
```

### 1.5 Configure device profile for wireless access points

In this procedure, the access VLAN you previously configured for management is added to the device profile that the switches apply to traffic received from a connected AP.

The device profile in this design is used to apply the untagged VLAN command to the port where the AP is connected. The untagged VLAN is used by the AP to communicate with other APs and the mobility controllers.

On each access switch, perform the following steps:

**Step 1:** Configure the device profile name.

```bash
device-profile name "Aruba-AP-Profile"
  untagged-vlan 10
```
Step 2: Configure the device profile type.

```bash
device-profile type "aruba-ap"
associate "Aruba-AP-Profile"
enable
```

1.6 Configure the access-switch default gateway

The IP default gateway is necessary to forward traffic sourced from the switch to the management VLAN and the rest of the network, using the IP address of the aggregation switch as its next hop router.

On each access switch, perform the following step:

**Step 1:** Configure the IP default gateway for the management VLAN.

```bash
ip default-gateway 10.2.0.1
```

1.7 Configure multicast IGMP snooping

This procedure enables multicast IGMP snooping for the layer-2 access switches.

On each access switch, perform the following step:

**Step 1:** Configure multicast IGMP snooping.

Example: Wired VLAN

```bash
vlan 20 ip igmp
```
Repeat this step for each of your VLANs where you want to send or receive multicast traffic.

1.8 Configure access-switch port-security features

This procedure configures port security for the access switches. DHCP snooping for IPv4 and IPv6 stops DHCP starvation attacks and it also prevents rogue DHCP servers from servicing requests on your network. ARP protect stops man-in-the-middle attacks caused by ARP cache poisoning. Dynamic IP lockdown stops devices from forging their source IP address by inspecting the IP-MAC binding information in the DHCP snooping table. IPv6 RA guard stops rogue IPv6 clients from advertising themselves as routers. BPDU protection prevents loops in the network by putting a non-trunk port into a disabled state for a specified amount of time when it receives a BPDU from another switch.
**Caution** Although these features are recommended for a secure access layer, they should be applied after the network is fully operational, in order to avoid problems during the initial stages of building the network. Apply the features one at a time and check the logs if connectivity problems begin.

Step 1: Enable DHCP snooping and configure it on all VLANs and trust the trunk interface.

```bash
dhcp-snooping
dhcp-snooping vlan 10 20 777
dhcp-snooping trust trk11
```

Step 2: Enable DHCPv6 snooping and configure it on all VLANs and trust the trunk interface.

```bash
dhcpv6-snooping
dhcpv6-snooping vlan 10 20 777
dhcpv6-snooping trust trk11
```

Step 3: Enable ARP protection and configure it on all VLANs, except the management VLAN 10 and trust the trunk interface.

```bash
arp-protect
arp-protect vlan 20 777
arp-protect trust trk11
```

Step 4: Enable IP source guard globally.

```bash
ip source-lockdown
```

Step 5: Configure IPv6 RA guard on the range of non-trunk ports.

```bash
ipv6 ra-guard ports ethernet 1/1-1/48
```
Step 6: (Optional) Configure spanning tree BPDU protection on the range of non-trunk ports and configure the port to be disabled for 60 seconds.

Caution  This command shuts down a port for 60 seconds if a device that sends BPDU is connected. Certain IP phones with built-in switches send BPDU, so you have to trust ports with these types of devices.

spanning-tree 1/1-1/48 bpdu-protection
spanning-tree bpdu-protection-timeout 60

Wired Aggregation

The access-aggregation layer provides connectivity for the access switches and connects to the core layer using ECMP uplinks. The service-aggregation layer provides connectivity to the external networks in the campus and connects to the core layer using ECMP uplinks. The aggregation switches are layer-3 and utilize OSPF for the routing protocol.

Procedures

Configuring the Aggregation Switch

2.1 Configure aggregation-switch stacking
2.2 Configure the aggregation-switch base features
2.3 Configure uplink ports
2.4 Configure aggregation-switch VLANs
2.5 Configure multicast IGMP snooping
2.6 Configure OSPF routing
2.7 Configure IP multicast routing

Use this section for the aggregation layer and repeat it for each aggregation switch. This section can be used for standalone switches, switch stacks or modular aggregation switches.
The diagram below shows the access and services aggregation switch locations in the Mobile First Campus design.

**Figure 20**  Mobile First Campus design—access and services aggregation

### 2.1 Configure aggregation-switch stacking

**Optional**

This optional procedure is for switch platforms with backplane stacking modules using stack cables or front plane stacking using VSF. Skip this procedure if you are not using a switch stack in this area of your network.

Stacking allows multiple access switches connected to each other through dedicated stacking ports or Ethernet connections to behave like a single switch. Stacking increases the port density by combining multiple physical devices into one virtual fabric, allowing management and configuration from one IP address. The members of a stack share the uplink ports providing additional bandwidth and redundancy.
There are three stacking device roles:

- **Commander**—Conducts overall management of the stack, and manages the forwarding databases, synchronizing them with the standby.

- **Standby**—Provides redundancy for the stack and takes over stack management operations if the commander becomes unavailable, or if an administrator forces a commander failover.

- **Members**—Are not part of the overall stack management; however, they must manage their local subsystems and ports to operate correctly as part of the stack. The commander and standby are also responsible for their own local subsystems and ports.

The device role is determined by member priority. When all switches in the stack are booted simultaneously, the switch with the highest priority becomes commander and the next highest priority becomes standby. The stacking priority can be set to any value between 1 and 255, and the default value is 128.

In this design, we recommend a maximum of two switches in the stack for the aggregation layer. Smaller networks can use two 3810M switches and larger networks can use two 5400R switches.

If you are planning to use dedicated stacking modules with 3810M switches, choose option 1. If you are planning to use Ethernet ports and VSF with 5400R switches, choose option 2.

**Option 1: Backplane Stacking**

The backplane stacking feature allows you to connect as many as ten switches into a single logical switch for data plane and management functions. In the aggregation layer, we recommend only using two switches. One switch is designated as the commander and the second switch is configured in the standby role.

The table below shows the configuration details for backplane stacking.

<table>
<thead>
<tr>
<th>Table 9</th>
<th>Backplane stacking for two-member switch stacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch 1</td>
<td>Switch 2</td>
</tr>
<tr>
<td>Stacking member ID</td>
<td>1</td>
</tr>
<tr>
<td>Stacking priority</td>
<td>230 (Standby)</td>
</tr>
<tr>
<td>Uplink</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Follow the steps below to connect the switches and statically assign their roles.

**Step 1:** Install the backplane stacking modules in all switches and connect the cables.

**Step 2:** Power-on each switch.
Step 3: Display the member ID for each switch using the **show stacking** command.

```
show stacking
...
ID   Mac Address       Model                                 Pri Status
    ----------------- ------------------------------------- --- ---------------
    ---                      ------------------------------ ---
 1  9457a5-8c3080     Aruba JL075A 3810M-16SFP+-2-slot S... 128 Commander
*2  9457a5-8c9000     Aruba JL075A 3810M-16SFP+-2-slot S... 128 Standby
```

Step 4: Assign the Commander role to a switch, by configuring the switch to have the highest priority.

```
stacking member 2 priority 250
```

Step 5: Assign the Standby role to the other switch, by configuring the switch to have the second highest priority.

```
stacking member 1 priority 230
```

Step 6: Save the configuration for all stack members.

```
write memory
```

Step 7: Reboot the switch stack for the changes to take effect.

```
boot system
  This will reboot the system from the primary image.
  Continue (y/n)? y
```

Step 8: After the switch stack reboots, verify stack status changes with the **show stacking** command.

```
show stacking
...
ID   Mac Address       Model                                 Pri Status
    ----------------- ------------------------------------- --- ---------------
    ---                      ------------------------------ ---
 1  9457a5-8c3080     Aruba JL075A 3810M-16SFP+-2-slot S... 230 Standby
*2  9457a5-8c9000     Aruba JL075A 3810M-16SFP+-2-slot S... 250 Commander
```

**Option 2: VSF Stacking**

VSF stacking allows switches to connect to each other through Ethernet ports in order to behave like a single logical switch. Like backplane stacking, the VSF fabric uses unique member IDs to identify and manage its members.

The VSF stack is formed using VSF links, which are logical interfaces comprised of same-speed physical interfaces. For two-member VSF switch stacks, only one logical VSF link is required.
In the aggregation layer, we recommend only using two switches. One switch is designated as the Commander and the second switch is configured in the Standby role.

The table below shows the configuration details for VSF stacking.

<table>
<thead>
<tr>
<th>Table 10</th>
<th>VSF stacking for two-member switch stacks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Switch 1</td>
</tr>
<tr>
<td>VSF member</td>
<td>1</td>
</tr>
<tr>
<td>VSF links</td>
<td>1</td>
</tr>
<tr>
<td>Priority</td>
<td>230 (Standby)</td>
</tr>
<tr>
<td>VSF domain</td>
<td>200</td>
</tr>
<tr>
<td>Uplink</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Follow the steps below to connect the switches and statically assign their roles in the stack.

**Step 1:** Configure the first member number ID with VSF link 1 and assign physical ports to it.

`vsf member 1 link 1 A1-A2`

**Step 2:** Assign the Standby role to the switch, by configuring it with the second highest priority.

`vsf member 1 priority 230`

**Step 3:** Enable and configure VSF domain.

`vsf enable domain 200`

This will save the current configuration and reboot the switch.

Continue (y/n)? y

**Step 4:** Connect to the second switch.

**Step 5:** Configure the second member number ID with VSF link 1 and assign physical ports to it.

`vsf member 2 link 1 A1-A2`

**Step 6:** Assign the Commander role to the switch, by configuring it with the highest priority.

`vsf member 2 priority 250`

**Step 7:** Enable and configure VSF domain.

`vsf enable domain 200`

This will save the current configuration and reboot the switch.

Continue (y/n)? y
Step 8: After both switches in the stack are configured and rebooted, connect the VSF Ethernet ports.

Step 9: Use the following command to verify the VSF stack is operational.

    show vsf topology

Example: Two-member VSF stack

| VSF member’s interconnection with links: |
| Stby     | Cmdr |
| +---+    | +---+ |
| | 1 |1==1| 2 |
| +---+    | +---+ |

2.2 Configure the aggregation-switch base features

In this procedure, you configure the base features for each aggregation switch.

The switch has two levels of access: manager and operator. The manager has access to all areas of the configuration and has the ability to make changes. The operator has access to the status, counters, and the event log, but the operator has read-only access to the command line interface and thus cannot make changes. You can only have one username and password for each level of access. The usernames are optional, but we recommend changing them for additional security.

On each aggregation switch, perform the following steps:

Step 1: Configure the switch host name.

    hostname Aggregation-Switch

Step 2: Configure the restricted operator username and password.

    password operator user-name adminOper plaintext [passwordOper]

Step 3: Configure the unrestricted manager username and password

    password manager user-name adminMgr plaintext [passwordMgr]

Step 4: Enable SSH for inbound connections.

    ip ssh

Step 5: Enable SCP.

    ip ssh filetransfer
Step 6: For increased security, turn off telnet server in order to only allow inbound SSH connections.

    no telnet-server

Step 7: Configure a login banner.

    banner motd #
    Property of example.com !! Unauthorized use prohibited !!
    #

Step 8: Configure the NTP with time zone and daylight savings time. The iburst feature provides faster time synchronization. The time zone offset is entered as the difference in minutes from UTC. The negative value means the amount of time behind UTC.

    time daylight-time-rule continental-us-and-canada
    time timezone -480
    timesync ntp
    ntp unicast
    ntp server 10.2.120.70 iburst
    ntp enable

Step 9: If the date on your device is not current, use the time command to set the date to today's date. The current date is required so that, in the next step, you can create a valid certificate.

    time MM/DD/YYYY

Step 10: Configure HTTPS for web access to the switch.

    crypto pki identity-profile https_Profile subject
    Enter Common Name (CN) : ExampleSwitch
    Enter Org Unit (OU) : ExampleOrgUnit
    Enter Org Name (O) : ExampleOrg
    Enter Locality (L) : Roseville
    Enter State (ST) : California
    Enter Country (C) : US
    crypto pki enroll-self-signed certificate-name https_Certificate
    web-management ssl

Step 11: For additional security, turn off plaintext HTTP management.

    no web-management plaintext
Step 12: Enable the simple network management protocol version 3 (SNMPv3).

```bash
snmpv3 enable
SNMPv3 Initialization process.
Creating user ‘initial’
Authentication Protocol: MD5
Enter authentication password: [password]
Privacy protocol is DES
Enter privacy password: [password]

User ‘initial’ has been created
Would you like to create a user that uses SHA? [y/n] y

User creation is done. SNMPv3 is now functional.
Would you like to restrict SNMPv1 and SNMPv2c messages to have read only access (you can set this later by the command ‘snmpv3 restricted-access’)? [y/n] n

Step 13: Create full read-write, limited read-write and read-only users for SNMPv3.

```bash
snmpv3 user NetAdminRW auth sha [passwordRW] priv aes [passwordRW]
snmpv3 user NetAdminLimited auth sha [passwordLimited] priv aes [passwordLimited]
snmpv3 user NetAdminR auth sha [passwordRO] priv aes [passwordRO]
```

Step 14: For additional security, remove the SNMP server community public from the configuration.

```bash
no snmp-server community public
```

2.3 Configure uplink ports

The uplink ports use LACP to combine two or more physical ports into a single trunk interface. By default, the uplink trunks use source and destination IP addresses to load-balance traffic between the physical interfaces. If a VLAN is not specified in the link-keepalive command, the UDLD packets are sent untagged

On each aggregation switch, perform the following steps:

Step 1: Configure the dual-port trunks with LACP.

```bash
trunk 1/A1,2/A1 trk11 lacp
```
Step 2: Configure UDLD on the uplink ports.

```
int 1/A1,2/A1 link-keepalive
```

Repeat this step for each set of uplink ports.

Step 3: Configure the keepalive interval to 70 (70 at 100-ms increments = 7 seconds) and the retries to 6.

```
link-keepalive interval 70
link-keepalive retries 6
```

Step 4: Enable STP globally on the switch. Configure the spanning tree priority to 0, which is the highest priority and makes the aggregation switch the spanning tree root bridge.

```
spanning-tree enable
spanning-tree priority 0
```

Step 5: Increase the logging level to informational for visibility to additional link and trunk status events.

```
logging severity info
```

### 2.4 Configure aggregation-switch VLANs

This procedure configures the VLANs for the aggregation switch. The aggregation switch is the default gateway for the user or services VLANs. The non-trunk ports are configured as untagged in the wired or data center VLANs. The uplink trunk ports from the access layer are configured as tagged for the user VLANs and untagged for VLAN 777.

The uplink ports into the core layer are configured as point-to-point for ECMP routing. They use a 30-bit mask because each subnet only needs two IP addresses. The aggregation switch has four separate connections into the core to allow two redundant paths into each of the standalone core switches. The uplink ports can be individual physical interfaces or lag interfaces that use the link aggregation control protocol (LACP) to combine two or more physical ports into a single trunk interface. In the examples shown below, single ports are used between the aggregation and core layers.

VLAN hopping is a computer security exploit that uses double tagging to attack network resources on a VLAN. The basic concept behind all VLAN hopping attacks is for an attacking host on a VLAN to gain access to traffic on other VLANs that would normally not be accessible.
Double tagging can be mitigated by creating an unused VLAN that will only be configured as the native VLAN on uplink trunk interfaces. The unused VLAN 777 does not have an IP address and it is not connected to anything else on the switch.

When you are using a centralized DHCP server, the `ip helper-address` command allows remote DHCP servers to provide end-station IP addresses for the VLAN. The helper command points to the IP address of the central DHCP server. If you have more than one DHCP server servicing the same VLAN, you can list multiple helper commands on an interface. The DHCP client accepts the first offer it receives.

The following tables provide the VLAN assignments for the Mobile First Campus design. If you are configuring an access aggregation switch, use the information from the first table. If you are configuring a services aggregation switch, use the information from the second table.

**Table 11  Access-aggregation switch—VLAN assignments, IP addresses, and tagging**

<table>
<thead>
<tr>
<th>VLAN name</th>
<th>VLAN ID</th>
<th>IP address</th>
<th>IP helper address</th>
<th>Tagged/untagged ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>10</td>
<td>10.2.0.1/22</td>
<td>10.2.120.40</td>
<td>Tagged Trk11-Trk15</td>
</tr>
<tr>
<td>Wired</td>
<td>20</td>
<td>10.2.4.1/22</td>
<td>10.2.120.40</td>
<td>Untagged 1/1-1/48 (all non-trunk ports) Tagged Trk11-Trk15</td>
</tr>
<tr>
<td>Core 1-1</td>
<td>200</td>
<td>10.2.200.2/30</td>
<td>N/A</td>
<td>Tagged 1/B22 (core switch 1, port 1)</td>
</tr>
<tr>
<td>Core 1-2</td>
<td>208</td>
<td>10.2.200.10/30</td>
<td>N/A</td>
<td>Tagged 2/B22 (core switch 1, port 2)</td>
</tr>
<tr>
<td>Core 2-1</td>
<td>216</td>
<td>10.2.200.18/30</td>
<td>N/A</td>
<td>Tagged 1/B24 (core switch 2, port 1)</td>
</tr>
<tr>
<td>Core 2-2</td>
<td>224</td>
<td>10.2.200.26/30</td>
<td>N/A</td>
<td>Tagged 2/B24 (core switch 2, port 2)</td>
</tr>
<tr>
<td>Anti-VLAN hopping</td>
<td>777</td>
<td>N/A</td>
<td>N/A</td>
<td>Untagged Trk11-Trk15</td>
</tr>
</tbody>
</table>

**Table 12  Services-aggregation switch—VLAN assignments, IP addresses, and tagging**

<table>
<thead>
<tr>
<th>VLAN name</th>
<th>VLAN ID</th>
<th>IP address</th>
<th>IP helper address</th>
<th>Tagged/Untagged ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless</td>
<td>30</td>
<td>10.2.8.1/22</td>
<td>10.2.120.40</td>
<td>Tagged 1/A1-1/A2,2/3-2/8 (mobility controllers)</td>
</tr>
<tr>
<td>Guest</td>
<td>40</td>
<td>10.2.12.1/22</td>
<td>10.2.120.40</td>
<td>Tagged 1/A1-1/A2,2/3-2/8 (mobility controllers)</td>
</tr>
<tr>
<td>Data Center</td>
<td>120</td>
<td>10.2.120.1/24</td>
<td>N/A</td>
<td>Untagged 1/1-1/48 (all non-trunk ports)</td>
</tr>
<tr>
<td>Internet DMZ</td>
<td>140</td>
<td>10.2.140.1/24</td>
<td>N/A</td>
<td>Tagged 1/47-1/48 (firewall)</td>
</tr>
<tr>
<td>Mobility Controllers</td>
<td>160</td>
<td>10.2.160.1/24</td>
<td>N/A</td>
<td>Tagged 1/A1-1/A2,2/3-2/8 (mobility controllers)</td>
</tr>
<tr>
<td>Core 1-1</td>
<td>800</td>
<td>10.2.208.1/30</td>
<td>N/A</td>
<td>Tagged 1/1 (core switch 1, port 1)</td>
</tr>
<tr>
<td>Core 1-2</td>
<td>804</td>
<td>10.2.208.5/30</td>
<td>N/A</td>
<td>Tagged 1/2 (core switch 1, port 2)</td>
</tr>
<tr>
<td>Core 2-1</td>
<td>808</td>
<td>10.2.208.9/30</td>
<td>N/A</td>
<td>Tagged 2/1 (core switch 2, port 1)</td>
</tr>
<tr>
<td>Core 2-2</td>
<td>812</td>
<td>10.2.208.13/30</td>
<td>N/A</td>
<td>Tagged 2/2 (core switch 2, port 2)</td>
</tr>
</tbody>
</table>
On each aggregation switch, perform the following steps:

**Step 1:** Configure the aggregation VLANs.

**Example: Management VLAN with helper address**

```plaintext
vlan 10
  name "Management"
  tagged Trk11-Trk15
  ip address 10.2.0.1 255.255.252.0
  ip helper-address 10.2.120.40
  exit
```

**Example: Core VLAN without helper address**

```plaintext
vlan 200
  name "Core 1-1"
  tagged 1/B22
  ip address 10.2.200.2 255.255.255.252
  exit
```

**Example: Anti-VLAN hopping VLAN without IP address and helper address**

```plaintext
vlan 777
  name Anti-VLAN hopping
  untagged Trk11-Trk15
  exit
```

Repeat this step for each VLAN that matches the type of switch you are configuring.

**Step 2:** Enable Rapid-PVST. Configure the spanning tree priority on the access VLANs to 0, which is the highest priority and makes the aggregation switch the spanning tree root bridge.

**Example: Management, wired, and anti-VLAN hopping VLANs**

```plaintext
spanning-tree mode rapid-pvst
spanning-tree vlan 10,20,777 priority 0
```
Step 3: Use the lowest IP address to configure the source address for SNMP responses from the switch.

Example: Management VLAN

```bash
snmp-server response-source 10.2.0.1
```

### 2.5 Configure multicast IGMP snooping

This procedure enables multicast IGMP snooping for the service-aggregation switch because IGMP snooping must be enabled for DMO to work on the APs. You do not need to configure IGMP snooping on the access-aggregation switches.

On the service aggregation switch, perform the following step:

**Step 1:** Configure multicast IGMP snooping.

Example: Wireless VLAN

```bash
vlan 30 ip igmp
```

Repeat this step for each of your VLANs where you want to send or receive multicast traffic.

### 2.6 Configure OSPF routing

This procedure configures OSPF as the layer-3 routing protocol. This design uses area backbone (0.0.0.0) for the entire campus network. Redistribute the connected and static routes, restrict the routes to the 10.2.0.0/16 network and enable nonstop forwarding. Configure the user and services VLANs as passive, because there are no devices that need routing protocol updates attached to them.

On each aggregation switch, perform the following steps:

**Step 1:** Configure the loopback interface.

```bash
interface loopback 1
ip address 10.2.255.10
```

**Step 2:** Enable IP routing. Configure the router ID as the IP address of the loopback interface from the previous step.

```bash
ip routing
ip router-id 10.2.255.10
```
Step 3: Configure OSPF.

    router ospf
      area backbone
      redistribute connected
      redistribute static
      restrict 10.2.0.0 255.255.0.0
      nonstop
      enable
      exit

Step 4: Configure the loopback interface.

    interface loopback 1
      ip ospf 10.2.255.10 area backbone

Step 5: Configure the user or services VLANs with passive mode.

Example: Management VLAN with passive mode

    vlan 10
      ip ospf 10.2.0.1 passive
      ip ospf 10.2.0.1 area backbone
      exit

Repeat this step for each user or services VLAN with an IP address.

Step 6: Configure the core VLANs without passive mode.

Example: Core VLAN without passive mode

    vlan 200
      ip ospf 10.2.200.2 area backbone
      exit

Repeat this step for each core VLAN.
2.7 Configure IP multicast routing

This procedure enables multicast routing for the layer-3 aggregation switches. The design is based on sparse mode multicast operation.

Step 1: Enable IP multicast routing in global configuration mode.

    ip multicast-routing

Step 2: Enable PIM.

    router pim
    enable

Step 3: Configure PIM sparse mode on the VLANs and allow any IP address to source multicast streams.

Example: Wired VLAN on access-aggregation

    vlan 20
    ip pim-sparse
    ip-addr any
    exit
    exit

Example: Wireless VLAN on service-aggregation

    vlan 30
    ip pim-sparse
    ip-addr any
    exit
    exit

Repeat this step for each of your VLANs where you want to send or receive multicast traffic.

Wired Core

The core layer provides high-speed layer-3 connectivity for the aggregation layer switches. It can also provide services aggregation functions when needed. The decision to use a standalone core layer depends on the number of aggregation layer switches and if your services are combined in a single location or spread across several aggregation blocks. With this Mobile First Campus architecture, you can start with a combined core and services design, and then migrate to a standalone core when needed. The ECMP uplinks between the access aggregation switches, and the core layer remains the same with either model.
Use this section for the core layer and repeat it for each core switch. This section describes configuring both standalone core switches and core switches with a combined services aggregation. Choose the group of procedures that match the type of core network you are deploying.

### Procedures

#### Configuring the Standalone Core Switches

- 3.1 Configure the core-switch base features
- 3.2 Configure uplink ports from core to aggregation
- 3.3 Configure OSPF routing
- 3.4 Configure IP Multicast

The standalone core switches do not use stacking technologies to combine them into a single logical switch. Each standalone core switch operates on its own and uses ECMP routing techniques to load-balance traffic to and from the aggregation layer switches.

The diagram below shows the standalone core switches in the Mobile First Campus design.

**Figure 21** Mobile First Campus design—standalone core
3.1 Configure the core-switch base features

In this procedure, you configure the base features for the core switch.

The switch has two levels of access: administrator and operator. The administrator has access to all areas of the configuration and has the ability to make changes. The operator has access to the status, counters, and the event log, but the operator has read-only access to the command line interface and thus cannot make changes.

Complete this procedure on each core switch.

Step 1: Configure the switch host name.

```
hostname Core-Switch
```

Step 2: Configure the unrestricted administrator password.

```
user admin password
Changing password for user admin
Enter password: [passwordAdmin]
Confirm new password: [passwordAdmin]
```

Step 3: Enable SSH server for inbound connections in the default vrf.

```
ssh server vrf default
```

Step 4: Configure a login banner.

```
banner motd #
    Property of example.com !! Unauthorized use prohibited !!
#
```

Step 5: Configure the network time protocol (NTP) with time zone and daylight savings time.

```
clock timezone pst8pdt
ntp server 10.80.2.219
```

Step 6: If the date on your device is not current, use the `clock date` command to set the date to today's date.

```
clock date YYYY-MM-DD
```

Step 7: Configure HTTP Secure (HTTPS) server for web access.

```
https-server vrf default
```
Step 8: Configure SNMP server in the default vrf.

   snmp-server vrf default

Step 9: Configure SNMP server community to override the default name public.

   snmp-server community NetAdminPriv

Step 10: Create full read-write, limited read-write, and read-only users for SNMPv3.

   snmpv3 user NetAdminRW auth sha auth-pass plaintext [passwordRW] priv aes priv-pass plaintext [passwordRW]
   snmpv3 user NetAdminLimited auth sha auth-pass plaintext [passwordLimited] priv aes priv-pass plaintext [passwordLimited]
   snmpv3 user NetAdminRO auth sha auth-pass plaintext [passwordRO] priv aes priv-pass plaintext [passwordRO]

### 3.2 Configure uplink ports from core to aggregation

The procedure configures the uplink ports from the core switch to the aggregation switch. The uplink ports are point-to-point for ECMP routing. They use a 30-bit mask because each subnet only needs two IP addresses. The uplink ports can be individual physical interfaces or lag interfaces that use LACP to combine two or more physical ports into a single trunk interface. By default, the LACP trunks use source and destination IP addresses to load-balance traffic between the physical interfaces.

This procedure describes how to configure both individual physical and lag interfaces. Repeat the appropriate options below for each uplink interface.

**Option 1: Using Individual Physical interfaces**

Step 1: Configure the physical interface.

   interface 1/1/1
     no shutdown
     ip address 10.2.200.17/30

Step 2: Repeat this procedure for each uplink interface.
Option 2: Using Lag Interfaces

Step 1: Configure the lag interface.

```bash
interface lag 1
    no shutdown
    ip address 10.2.204.9/30
    lacp mode active
```

Step 2: Configure the physical interfaces for the dynamic lag group.

```bash
interface 1/2/5
    no shutdown
    lag 1

interface 1/2/6
    no shutdown
    lag 1
```

Step 3: Repeat this procedure for each uplink interface.

Configure OSPF routing

This procedure configures OSPF as the layer-3 routing protocol. This design uses area backbone (0.0.0.0) for the entire campus network. Use the router loopback IP address as the OSPF router ID. Redistribute the connected and static routes.

Perform this procedure on each core switch.

Step 1: Configure the loopback interface.

```bash
interface loopback 1
    ip address 10.2.255.50/32
```

Step 2: Configure OSPF.

```bash
router ospf 1
    router-id 10.2.255.50
    redistribute connected
    redistribute static
    area 0.0.0.0
    enable
```
Step 3: Configure the interface for OSPF.

Example: Loopback interface

```
interface loopback 1
  ip ospf 1 area 0.0.0.0
```

Example: Physical interface

```
interface 1/1/1
  ip ospf 1 area 0.0.0.0
```

Example: Lag interface

```
interface lag 1
  ip ospf 1 area 0.0.0.0
```

Repeat this step for each interface.

3.4 Configure IP Multicast

This procedure enables multicast routing for the core switch. The design is based on sparse-mode multicast operation. You use BSRs and RPs to provide a simple yet scalable way to provide a highly resilient RP environment. Make the core switches the primary and secondary BSR and RP candidates, because they are in the middle of the network and all multicast traffic must pass through them anyway.

The BSR priority range is from 0-255 and the default is 0. The candidate with the highest value becomes the BSR for the domain.

The RP priority range is from 0-255 and the default is 192. The candidate with the lowest value becomes the RP for the defined group of multicast prefixes.

Do not use the interfaces between the switches as the source IP interfaces because if one of the switches goes down, the adjacent port on the other switch also goes down. We recommend you use the interfaces that point to the services aggregation layer as the source for both the BSR and RP.

Perform the following steps on each core switch.

Step 1: Configure PIM sparse mode on the interfaces with IP addresses.

Example: Physical interface

```
interface 1/1/1
  ip pim-sparse enable
```
Example: Lag interface

```plaintext
interface lag 1
  ip pim-sparse enable
```

Repeat this step for each active interface.

**Step 2:** Enable PIM and configure the switch as a BSR candidate by using a source IP interface pointing at the services aggregation switch, and then select a priority that makes one of them higher than the other.

```plaintext
router pim
  enable
  bsr-candidate source-ip-interface 1/1/1
  bsr-candidate priority 60
```

**Step 3:** Configure the switch as a candidate RP by using a source IP interface pointing at the services aggregation switch, a group prefix of 224.0.0.0/4, and then select a priority that makes one of them lower than the other.

```plaintext
rp-candidate source-ip-interface 1/1/1
rp-candidate group-prefix 224.0.0.0/4
rp-candidate priority 40
```

Skip to the next section of the guide.

---

**Procedures**

**Configuring the Core Switches with a Combined Services Aggregation**

4.1 Configure core-services switch stacking
4.2 Configure the core-services switch base features
4.3 Configure uplink ports from core-services to aggregation
4.4 Configure core-services switch VLANs
4.5 Configure OSPF routing
4.6 Configure IP multicast routing

If you are planning to combine the core and services functionality into a single pair of switches, we recommend stacking them together to allow the infrastructure devices in the services aggregation to use MC-LAG when connecting to the switches. This is the same design as the access-aggregation switches and the services-aggregation switches discussed previously. If you decide you want to add a standalone core later, you can re-use the combined core-services switches as your services aggregation.
If the number of ARP entries in your environment exceeds 4000 wireless clients, we recommend using a standalone core and a separate services aggregation block as outlined in the previous procedure.

The diagram below shows the core switch with a combined services aggregation in the Mobile First Campus design.

**Figure 22  Mobile First Campus design—core and services aggregation**

### 4.1 Configure core-services switch stacking

This procedure enables switch stacking on the pair of core-services switches. Stacking allows multiple switches connected to each other through dedicated stacking ports or Ethernet connections to behave like a single switch. Stacking increases the port density by combining multiple physical devices into one virtual fabric, allowing management and configuration from one IP address. The members of a stack share the uplink ports providing additional bandwidth and redundancy.
There are three stacking device roles:

- **Commander**—Conducts overall management of the stack and manages the forwarding databases, synchronizing them with the standby.

- **Standby**—Provides redundancy for the stack and takes over stack management operations if the commander becomes unavailable, or if an administrator forces a commander failover.

- **Members**—Are not part of the overall stack management; however, they must manage their local subsystems and ports to operate correctly as part of the stack. The commander and standby are also responsible for their own local subsystems and ports.

The device role is determined by member priority. When all switches in the stack are booted simultaneously, the switch with the highest priority becomes commander and the next highest priority becomes standby. The stacking priority can be set to any value between 1 and 255, and the default value is 128.

VSF stacking allows switches to connect to each other through Ethernet ports in order to behave like a single logical switch. The VSF fabric uses unique member IDs to identify and manage its members.

The VSF stack is formed using VSF links, which are logical interfaces comprised of same-speed physical interfaces. For two-member VSF switch stacks, only one logical VSF link is required.

In the core layer, we recommend only using two switches. One switch is designated as the Commander and the second switch is configured in the Standby role.

The table below shows the configuration details for VSF stacking.

<table>
<thead>
<tr>
<th>Table 13</th>
<th>VSF stacking for two-member switch stacks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>VSF member</td>
<td></td>
</tr>
<tr>
<td>VSF links</td>
<td></td>
</tr>
<tr>
<td>Priority</td>
<td></td>
</tr>
<tr>
<td>VSF domain</td>
<td></td>
</tr>
<tr>
<td>Uplink</td>
<td></td>
</tr>
</tbody>
</table>

Follow the steps below to connect the switches and statically assign their roles in the stack.

**Step 1:** Configure the first member number ID with VSF link 1 and assign physical ports to it.

```
vsf member 1 link 1 A1-A2
```

**Step 2:** Assign the Standby role to the switch by configuring it with the second highest priority.

```
vsf member 1 priority 230
```
Step 3: Enable and configure VSF domain.
   vsf enable domain 200
   This will save the current configuration and reboot the switch.
   Continue (y/n)?  y

Step 4: Connect to the second switch.

Step 5: Configure the second member number ID with VSF link 1 and assign physical ports to it.
   vsf member 2 link 1 A1-A2

Step 6: Assign the Commander role to the switch by configuring it with the highest priority.
   vsf member 2 priority 250

Step 7: Enable and configure VSF domain.
   vsf enable domain 200
   This will save the current configuration and reboot the switch.
   Continue (y/n)?  y

Step 8: After both switches in the stack are configured and rebooted, connect the VSF Ethernet ports.

Step 9: Use the following command to verify the VSF stack is operational.
   show vsf topology

Example: Two-member VSF stack
   VSF member’s interconnection with links:
   Stby    Cmdr
   +----+    +----+
   | 1  |l==1|  2  |
   +----+    +----+

4.2 Configure the core-services switch base features

In this procedure, you configure the base features for the core-services switch. The switch has two levels of
access: manager and operator. The manager has access to all areas of the configuration and has the ability to
make changes. The operator has access to the status, counters, and the event log, but the operator has read-
only access to the command line interface and thus cannot make changes. You can only have one username and
password for each level of access. The usernames are optional, but we recommend changing them for additional
security.
Step 1: Configure the switch host name.

    hostname Core-Services-Switch

Step 2: Configure the restricted operator username and password.

    password operator user-name adminOper plaintext [passwordOper]

Step 3: Configure the unrestricted manager username and password

    password manager user-name adminMgr plaintext [passwordMgr]

Step 4: Enable SSH for inbound connections.

    ip ssh

Step 5: Enable SCP.

    ip ssh filetransfer

Step 6: For increased security, turn off telnet server in order to only allow inbound SSH connections.

    no telnet-server

Step 7: Configure a login banner.

    banner motd #
    Property of example.com !! Unauthorized use prohibited !!
    #

Step 8: Configure the NTP with time zone and daylight savings time. The iburst feature provides faster time synchronization. The time zone offset is entered as the difference in minutes from UTC. The negative value means the amount of time behind UTC.

    time daylight-time-rule continental-us-and-canada
    time timezone -480
    timesync ntp
    ntp unicast
    ntp server 10.2.120.70 iburst
    ntp enable

Step 9: If the date on your device is not current, use the time command to set the date to today’s date. The current date is required so that, in the next step, you can create a valid certificate.

    time MM/DD/YYYY
Step 10: Configure HTTPS for web access to the switch.

```plaintext
crypto pki identity-profile https_Profile subject
Enter Common Name(CN) : ExampleSwitch
Enter Org Unit(OU) : ExampleOrgUnit
Enter Org Name(O) : ExampleOrg
Enter Locality(L) : Roseville
Enter State(ST) : California
Enter Country(C) : US
crypto pki enroll-self-signed certificate-name https_Certificate
web-management ssl
```

Step 11: For additional security, turn off plaintext HTTP management.

```plaintext
no web-management plaintext
```

Step 12: Enable the simple network management protocol version 3 (SNMPv3).

```plaintext
snmpv3 enable
SNMPv3 Initialization process.
Creating user ‘initial’
Authentication Protocol: MD5
Enter authentication password: [password]
Privacy protocol is DES
Enter privacy password: [password]

User ‘initial’ has been created
Would you like to create a user that uses SHA? [y/n] y

User creation is done. SNMPv3 is now functional.
Would you like to restrict SNMPv1 and SNMPv2c messages to have read only access (you can set this later by the command ‘snmpv3 restricted-access’)? [y/n] n
```

Step 13: Create full read-write, limited read-write and read-only users for SNMPv3.

```plaintext
snmpv3 user NetAdminRW auth sha [passwordRW] priv aes [passwordRW]
snmpv3 user NetAdminLimited auth sha [passwordLimited] priv aes [passwordLimited]
snmpv3 user NetAdminR auth sha [passwordRO] priv aes [passwordRO]
```
Step 14: For additional security, remove the SNMP server community public from the configuration.

    no snmp-server community public

### 4.3 Configure uplink ports from core-services to aggregation

The procedure configures the uplink ports from the core-services switch to the aggregation switch. The uplink ports use LACP to combine two or more physical ports into a single trunk interface. By default, the uplink trunks use source and destination IP addresses to load balance traffic between the physical interfaces. If a VLAN is not specified in the link-keepalive command, the UDLD packets are sent untagged.

**Step 1:** Configure the dual-port trunks with LACP.

    trunk A7-A8 trk1 lacp

Repeat this step for each trunk.

**Step 2:** Configure UDLD on the uplink ports.

    int A7-A8 link-keepalive

Repeat this step for each set of uplink ports.

**Step 3:** Configure the keepalive interval to 70 (70 at 100-ms increments = 7 seconds) and the retries to 6.

    link-keepalive interval 70
    link-keepalive retries 6

**Step 4:** Enable STP globally on the switch. Configure the spanning tree priority to 0, which is the highest priority and makes the core switch the spanning tree root bridge.

    spanning-tree enable
    spanning-tree priority 0

**Note** A root bridge should always be statically defined to prevent a rogue or misconfigured switch from altering the STP topology.

**Step 5:** Increase the logging level to informational for visibility to additional link and trunk status events.

    logging severity info
4.4 Configure core-services switch VLANs

This procedure configures the VLANs for the core-services switch. The core-services switch is the default gateway for the wireless user and services VLANs. The non-trunk ports are configured as untagged in the data center VLAN.

The uplink ports are configured as point-to-point for ECMP routing. They use a 30-bit mask because each subnet only needs two IP addresses. The uplink ports can be individual physical interfaces or lag interfaces that use LACP to combine two or more physical ports into a single trunk interface.

When you are using a centralized DHCP server, the `ip helper-address` command allows remote DHCP servers to provide end-station IP addresses for the VLAN. The helper command points to the IP address of the central DHCP server. If you have more than one DHCP server servicing the same VLAN, you can list multiple helper commands on an interface. The DHCP client accepts the first offer it receives.

The following tables provides the VLAN assignments for the Mobile First Campus design.

**Table 14  Core-Services switch—VLAN assignments, IP addresses, and tagging**

<table>
<thead>
<tr>
<th>VLAN name</th>
<th>VLAN ID</th>
<th>IP address</th>
<th>IP helper address</th>
<th>Tagged/untagged ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless</td>
<td>30</td>
<td>10.2.8.1/22</td>
<td>10.2.120.40</td>
<td>Tagged 1/A1-1/A2,2/3-2/8 (mobility controllers)</td>
</tr>
<tr>
<td>Guest</td>
<td>40</td>
<td>10.2.12.1/22</td>
<td>10.2.120.40</td>
<td>Tagged 1/A1-1/A2/2/3-2/8 (mobility controllers)</td>
</tr>
<tr>
<td>Data Center</td>
<td>120</td>
<td>10.2.120.1/24</td>
<td>N/A</td>
<td>Untagged 1/1-1/48 (all non-trunk ports)</td>
</tr>
<tr>
<td>Internet DMZ</td>
<td>140</td>
<td>10.2.140.1/24</td>
<td>N/A</td>
<td>Tagged 1/47-1/48 (firewall)</td>
</tr>
<tr>
<td>Mobility Controllers</td>
<td>160</td>
<td>10.2.160.1/24</td>
<td>N/A</td>
<td>Tagged 1/A1-1/A2,2/3-2/8 (mobility controllers)</td>
</tr>
<tr>
<td>Core 1-1</td>
<td>800</td>
<td>10.2.208.1/30</td>
<td>N/A</td>
<td>Tagged 1/1 (core switch 1, port 1)</td>
</tr>
<tr>
<td>Core 1-2</td>
<td>804</td>
<td>10.2.208.5/30</td>
<td>N/A</td>
<td>Tagged 1/2 (core switch 1, port 2)</td>
</tr>
<tr>
<td>Core 2-1</td>
<td>808</td>
<td>10.2.208.9/30</td>
<td>N/A</td>
<td>Tagged 2/1 (core switch 2, port 1)</td>
</tr>
<tr>
<td>Core 2-2</td>
<td>812</td>
<td>10.2.208.13/30</td>
<td>N/A</td>
<td>Tagged 2/2 (core switch 2, port 2)</td>
</tr>
</tbody>
</table>

**Step 1:** Configure the VLANs.

**Example: Wireless VLAN with helper address**

```bash
vlan 30
    name "Wireless"
    tagged 1/A1-1/A2,2/3-2/8
    ip address 10.2.8.1 255.255.252.0
    ip helper-address 10.2.120.40
exit
```
Example: Data center VLAN without helper address

```
vlan 120
    name "Data Center"
    untagged 1/1-1/48
    ip address 10.2.120.1 255.255.255.0
exit
```

Example: Core VLAN without helper address

```
vlan 800
    name "Core 1-1"
    tagged 1/1
    ip address 10.2.208.1 255.255.255.252
exit
```

Repeat this step for each VLAN in the previous table.

**Step 2:** Enable Rapid-PVST. Configure the spanning tree priority on the access VLANs to 0, which is the highest priority and makes the core-services switch the spanning tree root bridge.

Example: Wireless and guest VLANs

```
spanning-tree mode rapid-pvst
spanning-tree vlan 30,40 priority 0
```

**Step 3:** Use the lowest IP address to configure the source address for SNMP responses from the switch.

Example: Wireless VLAN

```
snmp-server response-source 10.2.8.1
```

### 4.5 Configure OSPF routing

This procedure configures OSPF as the layer-3 routing protocol. This design uses area backbone (0.0.0.0) for the entire campus network. Redistribute the connected and static routes, restrict the routes to the 10.2.0.0/16 network and enable nonstop forwarding. Configure the service VLANs as passive, because there are no devices that need routing protocol updates attached to the service VLANs.

**Step 1:** Configure the loopback interface.

```
interface loopback 1
    ip address 10.2.255.30
```
Step 2: Enable IP routing. Configure the router ID as the IP address of the loopback interface from the previous step.

```
ip routing
ip router-id 10.2.255.30
```

Step 3: Configure OSPF.

```
router ospf
  area backbone
  redistribute connected
  redistribute static
  restrict 10.2.0.0 255.255.0.0
  nonstop
  enable
  exit
```

Step 4: Configure the loopback interface for OSPF.

```
interface loopback 1
  ip ospf 10.2.255.30 area backbone
```

Step 5: Configure the service VLANs for OSPF.

Example: Data center VLAN with passive mode

```
vlan 120
  ip ospf 10.2.120.1 passive
  ip ospf 10.2.120.1 area backbone
  exit
```

Example: Core VLAN without passive mode

```
vlan 800
  ip ospf 10.2.208.1 area backbone
  exit
```

Repeat this step for each service VLAN.
4.6 Configure IP multicast routing

This procedure enables multicast routing for the core switches. The design is based on sparse mode multicast operation. BSRs and RPs are used to provide a simple yet scalable way to provide a highly resilient RP environment.

The BSR priority range is from 0-255 and the default is 0. The candidate with the highest value becomes the BSR for the domain.

The RP priority range is from 0-255 and the default is 192. The candidate with the lowest value becomes the RP for the defined group of multicast prefixes.

Step 1: Enable IP multicast routing in global configuration mode.

    ip multicast-routing

Step 2: Enable PIM and configure the switch as a BSR candidate with a source VLAN and priority.

    router pim
    enable
    bsr-candidate
    bsr-candidate source-ip-vlan 120
    bsr-candidate priority 50

Step 3: Configure the switch as a candidate RP with a source VLAN and a group prefix of 224.0.0.0 to 240.0.0.0. Set the RP candidate hold time and the priority.

    rp-candidate source-ip-vlan 120
    rp-candidate group-prefix 224.0.0.0 240.0.0.0
    rp-candidate hold-time 150 priority 50

Step 4: Configure PIM sparse mode on the service VLANs and allow any IP address to source multicast streams.

Example: Data center VLAN

    vlan 120
    ip pim-sparse
    ip-addr any
    exit
    exit

Repeat this step for each of your VLANs where you want to send or receive multicast traffic.
CAMPUS WIRELESS LAN

The WLAN provides network access for employees, wireless Internet access for guests, and connectivity for IoT devices. Regardless of their location on the network, wireless devices have the same experience when connecting to their services.

The wireless configuration consists of a Mobility Master pair, mobility controller cluster, and campus APs with employee and guest WLANs and VLANs. The APs use a management VLAN to communicate between each other and the mobility controllers. The employee traffic is tunneled from the employee SSID to the employee VLAN and the guest traffic from the guest SSID to the guest VLAN on the uplink ports of the mobility controllers. A policy created in the mobility controller allows the employees to access the entire network, while the guests can access the guest VLAN, DHCP server, DNS service, and HTTP/HTTPS, in order to access web sites on the Internet.

**Procedures**

**Configuring the Mobility Master**

5.1 Configure the Mobility Master system setup
5.2 Configure Mobility Master redundancy
5.3 Configure Mobility Master database synchronization
5.4 Install and enable licenses

Use this section to configure the Mobility Master. The diagram on the next page shows the Mobility Master pair in the services aggregation of the Mobile First Campus design. They also are commonly deployed in the virtual server environment of the data center.
The Aruba Mobility Master acts as a single point of configuration for global policies such as firewall rules, authentication, and RF to simplify the administration and maintenance of a wireless network. The design uses a centralized, multi-tier architecture that provides a clear separation between management, control, and forwarding functions. The Mobility Master provides the management and control, while the mobility controllers provide the forwarding.

The Mobility Master runs ArubaOS 8 and centrally manages the cluster of mobility controllers. The Mobility Master consolidates all-master, single master-multiple local, and multiple master-local deployments from previous versions of ArubaOS into a single centralized deployment model.

The Mobility Master can be deployed as a virtual machine or on a hardened appliance. To learn more about the virtual appliance installation, please refer to ArubaOS 8.3.0.0 Virtual Appliance Installation Guide.
The information from the following table includes the Mobility Master virtual router ID, IP addresses, priority and VLANs used in the procedures below.

Table 15  Example Mobility Master virtual router ID, VLAN ID, IP addresses and priority

<table>
<thead>
<tr>
<th>Name</th>
<th>Virtual router ID</th>
<th>Virtual IP address</th>
<th>Priority</th>
<th>VLAN ID</th>
<th>VLAN name</th>
<th>Local IP address</th>
<th>Peer IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example-MM1</td>
<td>120</td>
<td>10.2.120.100</td>
<td>200</td>
<td>120</td>
<td>AMS-Office-SC-MM</td>
<td>10.2.120.80</td>
<td>10.2.120.90</td>
</tr>
<tr>
<td>Example-MM2</td>
<td>120</td>
<td>10.2.120.100</td>
<td>100</td>
<td>120</td>
<td>AMS-Office-SC-MM</td>
<td>10.2.120.90</td>
<td>10.2.120.80</td>
</tr>
</tbody>
</table>

For physical wired redundancy, it is recommended you configure the Mobility Master virtual machines on two different host machines. Each virtual machine has a single connection into the virtual switch and the virtual switch is dual-connected to two physical interfaces on the host machine. The host machines are dual-connected to two different physical switches in your services aggregation, as depicted in the diagram below.

Figure 24  Mobility Master physical wired redundancy

5.1  Configure the Mobility Master system setup

This procedure configures the system setup for the Mobility Master.

Step 1: After the wired network is fully operational, connect a pair of Mobility Masters to two different physical switches in the services aggregation switch stack and power them on.

The initial power-on sequence takes several minutes to complete.
Step 2: Open a console session into the **primary Mobility Master** and enter the following values in the setup dialog.

Enter System name [ArubaMM]: **Example-MM1**
Enter Controller VLAN ID [1]: **120**
Enter Controller VLAN port [GE 0/0/0]:
Enter Controller VLAN port mode (access|trunk) [access]:
Enter VLAN interface IP address [172.16.0.254]: **10.2.120.80**
Enter VLAN interface subnet mask [255.255.255.0]:
Enter IP default gateway [none]: **10.2.120.1**
Enter DNS IP address [none]: **10.2.120.50**
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: **no**
Enter Country code (ISO-3166), <ctrl-I> for supported list: **us**
You have chosen Country code US for United States (yes|no)?: **yes**
Enter the controller’s IANA Time zone [America/Los_Angeles]:
Enter Time in UTC [14:59:52]: **22:04:00**
Enter Date (MM/DD/YYYY) [5/10/2018]:
Enter Password for admin login (up to 32 chars): [password]
Re-type Password for admin login: [password]

Current choices are:

System name: Example-MM1
Controller VLAN id: 120
Controller VLAN port: GE 0/0/0
Controller VLAN port mode: access
VLAN interface IP address: 10.2.120.80
VLAN interface subnet mask: 255.255.255.0
IP Default gateway: 10.2.120.1
Option to configure VLAN interface IPV6 address: no
Country code: us
IANA Time Zone: America/Los_Angeles

If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no)yes
Step 3: For the standby Mobility Master, repeat the previous step changing the variables as required.

5.2 Configure Mobility Master redundancy

This procedure configures redundancy for the Mobility Master pair. To maintain a highly redundant network, the administrator configures a second Mobility Master to act as a hot standby for the primary Mobility Master using the Virtual Router Redundancy Protocol (VRRP).

When the master is unavailable, the standby becomes the master and takes ownership of the virtual IP address. All network elements (APs and other controllers) are configured to access the virtual IP address, thereby providing a transparent redundant solution.

The priority level of the VRRP instance is used in the election mechanism for the master. The highest priority value becomes the VRRP master. The default priority value is 100, so use a higher number on the primary Mobility Master.

Note For Mobility Master virtual appliances in a VMware vSphere environment, promiscuous mode needs to be turned on for VRRP to work. For security reasons, we recommend a separate virtual machine group in vSwitch for ports using VRRP and that you only allow promiscuous mode in that group.

Step 1: Browse to the primary Mobility Master, enter the following information, and then click Log in.

- Username—admin
- Password—[password]
Step 2: Click the icon on the top left of the page to expend the menu and navigate to Mobility Master > Example-MM1 > Configuration > Services > Redundancy > Virtual Router Table, and then click +.

![Virtual Router Table]

Step 3: In the New Virtual Router window at the bottom of the page, enter the following information, and then click Submit.

- ID—120
- IP version—IPv4
- Authentication password—[password]
- Retype authentication password—[password]
- IP address—10.2.120.100 (virtual IP address)
- Priority—200 (this is the primary Mobility Master)
- Enable router pre-emption—Enabled
- Admin state—UP
- VLAN—120 (VLAN from the Mobility Master system setup)
- Leave the rest of the fields blank

Step 4: At the top right of the page, click Pending Changes > Deploy changes > Close.
Step 5: Navigate to Mobility Master > Example-MM1 > Configuration > Services > Redundancy > Master Redundancy, enter the following information, and then click Submit.

- Database synchronization slider—Disabled (will be enabled in a subsequent step)
- Master VRRP—120 (virtual router ID from previous step)
- IP address of peer—10.2.120.90 (IP address of standby Mobility Master)
- Authentication—IPSec Key (this field and the following two will not show up until you enter an IP address of the peer)
- IPSec key of peer—[password]
- Retype IPSec key—[password]

Step 6: Click Pending Changes > Deploy changes > Close.

Step 7: Navigate to Mobility Master > Example-MM1 > Configuration > Interfaces > VLANs, and then click +.

Step 8: In the New VLAN window, enter the following information, and then click Submit.

- VLAN name—AMS-Office-SC-MM
- VLAN ID/Range—120

Step 9: Click Pending Changes > Deploy changes > Close.

Step 10: Browse to the standby Mobility Master, enter the following information, and then click Log in.

- Username—admin
- Password—[password]
Step 11: Navigate to Configuration > Services > Redundancy > Virtual Router Table, and then click +.

![Virtual Router Table]

Step 12: In the New Virtual Router window, enter the following information, and then click Submit.

- ID—120
- IP version-IPv4
- Authentication password—[password]
- Retype authentication password—[password]
- IP address—10.2.120.100 (virtual IP address)
- Priority—100 (this is the standby Mobility Master)
- Admin state—UP
- VLAN—120
- Leave the rest of the fields blank

Step 13: Click Pending Changes > Deploy changes > Close.
Step 14: Navigate to Configuration > Services > Redundancy > Master Redundancy, enter the following information, and then click Submit.

- Database synchronization slider—**Disabled** (will be enabled in a subsequent step)
- Master VRRP—**120** (virtual router ID from previous step)
- IP address of peer—**10.2.120.80** (IP address of primary Mobility Master)
- Authentication—**IPSec Key** (this field and the following two will not show up until you enter an IP address of the peer)
- IPSec key of peer—[password]
- Retype IPSec key—[password]

Step 15: Click Pending Changes > Deploy changes > Close.

Step 16: Navigate to Configuration > Interfaces > VLANs, and then click +.

Step 17: In the New VLAN window, enter the following information, and then click Submit.

- VLAN name—**AMS-Office-SC-MM**
- VLAN ID/Range—**120**

Step 18: Click Pending Changes > Deploy changes > Close.
5.3 Configure Mobility Master database synchronization

This procedure configures the synchronization between the redundant Mobility Master databases. The standby Mobility Master must synchronize its database from the primary Mobility Master after the APs are communicating with the mobility controllers over a secure channel. This ensures that all certificates, IPsec keys, and campus AP whitelist entries are available to the backup master.

You should also synchronize the database immediately when APs are added or removed from the campus AP whitelist to ensure that the backup master has the latest settings.

**Note** The database synchronization must be configured on the top-level Mobility Master folder and not at the individual device level.

Step 1: Login to the primary Mobility Master and navigate to Mobility Master > Configuration > Services > Redundancy > Master Redundancy, enter the following information, and then click Submit.

- Database synchronization slider—Enabled
- Sync period—60 (default)
- Master VRRP—Blank
- IP Address of peer—Blank

Step 2: Click Pending Changes > Deploy changes > Close.

5.4 Install and enable licenses

This procedure installs and enables ArubaOS licenses. To learn more about licenses and licensing features, see the ArubaOS 8.3.0.x Licensing Guide.
Step 1: Navigate to Mobility Master > Configuration > System > Licensing > Mobility Master Licenses, and then on the bottom left of the page, click +.

![Usage Mobility Master Licenses](image)

Step 2: Paste your previously obtained licenses into the Install Licenses window, and then click OK and Submit.

Step 3: Click Pending Changes > Deploy changes > Close.

Step 4: Navigate to Mobility Master > Configuration > System > Licensing > Usage, and then click Global License Pool.

Step 5: In the Usage for Global License Pool window, enable the following features, and then click Submit.

- PFE—Enable
- RF Protect—Enable

![Usage for Global License Pool](image)

Step 6: Click Pending Changes > Deploy changes > Close.
**Procedures**

**Configuring the Mobility Controller Cluster**

- 6.1 Initial mobility controller setup
- 6.2 Configure the hierarchy
- 6.3 Adopt mobility controllers in the Mobility Master
- 6.4 Add adopted mobility controllers to local group
- 6.5 Configure LACP interfaces
- 6.6 Configure mobility controller clustering
- 6.7 Configure mobility controller cluster VRRP for AP provisioning

Use this section to configure the mobility controller cluster. The diagram below shows the mobility controller cluster in the services aggregation of the Mobile First Campus design.

*Figure 25  Mobile First Campus design—mobility controller cluster*
The mobility controllers can be deployed as virtual machines or as dedicated hardware devices. To learn more about the virtual appliance installation, please refer to ArubaOS 8.3.0.0 Virtual Appliance Installation Guide.

### 6.1 Initial mobility controller setup

This procedure configures the initial system setup for the mobility controller. The information from the following table includes the IP addresses and VLANs used in the procedures below.

**Table 16 Example mobility controllers IP addresses and VLAN ID**

<table>
<thead>
<tr>
<th>Name</th>
<th>IP address</th>
<th>Default gateway</th>
<th>VLAN ID</th>
<th>VLAN name</th>
<th>Master switch IP address (VRRP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aruba-MC-1</td>
<td>10.2.160.10/24</td>
<td>10.2.160.1</td>
<td>160</td>
<td>AMS-Office-SC-MC</td>
<td>10.2.120.100</td>
</tr>
<tr>
<td>Aruba-MC-2</td>
<td>10.2.160.20/24</td>
<td>10.2.160.1</td>
<td>160</td>
<td>AMS-Office-SC-MC</td>
<td>10.2.120.100</td>
</tr>
<tr>
<td>Aruba-MC-3</td>
<td>10.2.160.30/24</td>
<td>10.2.160.1</td>
<td>160</td>
<td>AMS-Office-SC-MC</td>
<td>10.2.120.100</td>
</tr>
<tr>
<td>Aruba-MC-4</td>
<td>10.2.160.40/24</td>
<td>10.2.160.1</td>
<td>160</td>
<td>AMS-Office-SC-MC</td>
<td>10.2.120.100</td>
</tr>
</tbody>
</table>

**Step 1:** After the Mobility Masters are operational, power on your mobility controllers.

The initial power-on sequence takes several minutes to complete.

**Step 2:** From a console session, enter the following values in the setup dialog.

- Enter Option (partial string is acceptable): full-setup
- Are you sure that you want to stop auto-provisioning and start full setup dialog? (yes/no): yes
- Enter System name [Aruba7024]: **Aruba-MC-1**
- Enter Switch Role (standalone|md) [md]:
- Enter IP type to terminate IPSec tunnel (ipv4|ipv6) [ipv4]:
- Enter Master switch IP address or FQDN: **10.2.120.100**
- Is this a VPN concentrator for managed device to reach Master switch (yes|no) [no]:
- This device connects to Master switch via VPN concentrator (yes|no) [no]:
- Is Master switch Virtual Mobility Master? (yes|no) [yes]:
- Master switch Authentication method (PSKwithIP|PSKwithMAC) [PSKwithIP]:
- Enter IPSec Pre-shared Key: **[password]**
- Re-enter IPSec Pre-shared Key: **[password]**
Do you want to enable L3 Redundancy (yes|no) [no]:
Enter Uplink Vlan ID [1]: 160
Enter Uplink port [GE 0/0/0]:
Enter Uplink port mode (access|trunk) [access]: trunk
Enter Native VLAN ID [1]:
Enter Uplink Vlan IP assignment method (dhcp|static) [static]:
Enter Uplink Vlan Static IP address [172.16.0.254]: 10.2.160.10
Enter Uplink Vlan Static IP netmask [255.255.255.0]:
Enter IP default gateway [none]: 10.2.160.1
Enter DNS IP address [none]: 10.2.120.50
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
Do you want to configure dynamic port-channel (yes|no) [no]:
This controller is restricted, please enter country code (US|PR|GU|VI|MP|AS|FM|MH) [US]:
You have chosen Country code US for United States (yes|no)?: yes
Enter the controller’s IANA Time zone [America/Los_Angeles]:
Enter Time in UTC [14:59:52]: 22:04:00
Enter Date (MM/DD/YYYY) [5/10/2018]:
Do you want to create admin account (yes|no) [yes]:
Enter Password for admin login (up to 32 chars): [password]
Re-type Password for admin login: [password]

Current choices are:

System name: Aruba-MC-1
Switch Role: md
IP type to terminate IPSec tunnel: ipv4
Master switch IP address or FQDN: 10.2.120.100
Is this VPN concentrator: no
Connect via VPN concentrator: no
IPSec authentication method: PSKwithIP
Vlan id for uplink interface: 160
Uplink port: GE 0/0/0
Uplink port mode: trunk
Native VLAN id: 1
Uplink Vlan IP assignment method: static
Uplink Vlan static IP Address: 10.2.160.10
Uplink Vlan static IP net-mask: 255.255.255.0
Uplink Vlan IP default gateway: 10.2.160.1
Option to configure VLAN interface IPV6 address: no
Country code: US
IANA Time Zone: America/Los_Angeles
Admin account created: yes

Note: These settings require IP-Based-PSK configuration on Master switch

If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no) yes

Step 3: For each additional mobility controller, repeat Step 2, changing the variables as required.

6.2 Configure the hierarchy

This procedure configures the hierarchical groups. For more information about Mobility Master configuration hierarchy, see Chapter 1 of the ArubaOS 8.3.0.x User Guide.

The following is an example of the configuration hierarchy used in this guide with the corresponding menu hierarchy shown on the right-hand side.
Step 1: Login to the primary Mobility Master, navigate to Managed Network, and then on the right side, click +.

Step 2: In the Add window, enter the following information, and then click Submit.

- Select—Group
- Name—AMS

Step 3: For each additional level-1 group, repeat Step 1 and Step 2, changing the variable as required.
Step 4: After completing your level-1 groups, navigate to Managed Network > AMS, and then click +.

Step 5: In the Add window, enter the following information, and then click Submit.

- Select—Group
- Name—Office

Step 6: For each additional level-2 group, repeat Step 4 and Step 5, changing the variable as required.

Step 7: After completing your level-2 groups, navigate to Managed Network > AMS > Office, and then click +.

Step 8: In the Add window, enter the following information, and then click Submit.

- Select—Group
- Name—Santa-Clara

Step 9: For each additional level-3 group, repeat Step 7 and Step 8, changing the variable as required.
6.3  Adopt mobility controllers in the Mobility Master

This procedure configures the Mobility Master to adopt mobility controllers into the system.

Step 1: Navigate to Mobility Master > Configuration > Controllers > Local Controller IPSec Keys, and then on the lower left side click +.

![Local Controller IPSec Keys](image)

Step 2: In the Add New IPSec Controller window, enter the following information, and then click Submit.

- Authentication—IPSec Key (default)
- Local controller IPV4—10.2.160.10 (IP address of mobility controller)
- IPSec key—[password]
- Retype IPSec key—[password]

Step 3: For each additional mobility controller, repeat Step 1 and Step 2, changing the variables as required.

Step 4: Click Pending Changes > Deploy changes > Close.

6.4  Add adopted mobility controllers to local group

This procedure adds the adopted mobility controllers to the local group.

Step 1: To obtain the MAC address of the mobility controllers, SSH into the primary Mobility Master and issue the show switches command.

**Note** It will take several minutes for the mobility controllers to establish their secure connections to the Mobility Master and for them to appear in the show switches command.
The MAC address and associated IP address for each mobility controller can be found under the **Configuration State** column as shown in the partial output of the command below.

```
show switches
```

Step 2: Navigate to Managed Network > AMS > Office > Santa-Clara and then click +.

Step 3: In the Add window, enter the following information, and then click Submit.

- **Select**—Controller
- **Hostname**—Aruba-MC-1
- **MAC address**—00:0b:86:bb:bb:a7 (from the show switches command)
- **Type**—A7024 (must match the type of controller)

Step 4: For each additional mobility controller, repeat Step 2 and Step 3, changing the variables as required.

Step 5: Click Pending Changes > Deploy changes > Close.
6.5 Configure LACP interfaces

Optional

This optional procedure configures LACP interfaces on the mobility controllers. If you have virtual mobility controllers or you do not plan to use LACP interfaces in your environment, skip to the next procedure.

For physical wired redundancy, it is recommended you configure the mobility controllers with LACP interfaces and connect them to two different physical switches in your services aggregation, as depicted in the diagram below.

To make it easier to identify the ports where your mobility controllers are connected to your LAN switches, it is recommended you turn on LLDP in the mobility controllers before enabling LACP.

Step 1: Navigate to Managed Network > AMS > Office > Santa-Clara > Aruba-MC-1 > Configuration > Interfaces > Ports, and then click GE-0/0/24.
Step 2: At the bottom of the GE-0/0/24 window, click Show advanced options, scroll down to the bottom again, enter the following information, and then click Submit.

- LLDP Transmission—Enable (slider bar to the right)
- Transmit Interval—30 seconds (default)
- Transmit hold—4 seconds (default)
- Fast Transmit Interval—1 second (default)
- Fast Transmit hold—4 seconds (default)
- LLDP Reception—Enable

Step 3: For each additional LLDP interface on each mobility controller, repeat Step 1 and Step 2, choosing the correct interface as required.

Step 4: Click Pending Changes > Deploy changes > Close.

Step 5: Navigate to Managed Network > AMS > Office > Santa-Clara > Aruba-MC-1 > Configuration > Interfaces > Ports, and then in the Port Channel section, click +.
Step 6: From the New Port Channel window, enter the following information, and then click Submit.

- ID—**PC-0** (choose the first available channel)

![New Port Channel](image)

Step 7: From the PC-0 section next to Port members, click Edit.

Step 8: From the Available/Selected Ports window, select the ports for this port channel in the left window, move them to the right window, and then click OK.

![Available/Selected Ports](image)

Step 9: From PC-0 section, enter the following information, and then click Submit.

- Protocol—**LACP**
- LACP mode—**active**
- Admin state—**Enable**
- Trust—**Enable**
- Mode—**Trunk**
- Native VLAN—**160**
• Allow VLANs—Allow specified VLANs (user VLANs will be added in a subsequent step)

Step 10: For each additional LACP interface on each mobility controller, repeat Step 5 through Step 9, choosing the correct interfaces as required.

Caution: After you deploy the changes, the controllers will become unavailable on the network until you add matching LACP configurations on the corresponding ports on the services aggregation switch.

Step 11: Click Pending Changes > Deploy changes > Close.
Step 12: To obtain the corresponding LAN switch port numbers for your mobility controllers, SSH into the services aggregation switch and issue the `show lldp info remote-device` command.

The switch local ports for each mobility controller can be found under the LocalPort column as shown in the partial output of the command below.

![LLDP Remote Devices Information](image)

Step 13: Configure the dual-port trunks with LACP.

```
trunk 1/1,2/1 trk11 lacp
```

Repeat this step for each mobility controller trunk.

Step 14: Configure the service aggregation user VLANs with the LACP trunk interfaces.

The following table provides the VLAN assignments for the user VLANs.

### Table 17 Services-aggregation switch—VLAN assignments, IP addresses, and tagging

<table>
<thead>
<tr>
<th>VLAN name</th>
<th>VLAN ID</th>
<th>IP address</th>
<th>IP helper address</th>
<th>Tagged/Untagged ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless</td>
<td>30</td>
<td>10.2.8.1/22</td>
<td>10.2.120.40</td>
<td>Tagged Trk11-Trk14 (mobility controllers)</td>
</tr>
<tr>
<td>Guest</td>
<td>40</td>
<td>10.2.12.1/22</td>
<td>10.2.120.40</td>
<td>Tagged Trk11-Trk14 (mobility controllers)</td>
</tr>
<tr>
<td>Mobility Controllers</td>
<td>160</td>
<td>10.2.160.1/24</td>
<td>N/A</td>
<td>Untagged Trk11-Trk14 (mobility controllers)</td>
</tr>
</tbody>
</table>

Example: Wireless Employee VLAN tagged

```
vlan 30
  tagged Trk11-Trk14
exit
```
Example: Mobility controller VLAN untagged

```
vlan 160
    untagged Trk11-Trk14
    exit
```

Repeat this step for each user VLAN.

### 6.6 Configure mobility controller clustering

This procedure configures mobility controller layer-2 clustering. A cluster combines multiple controllers together to provide high availability and load balancing for all clients and ensures service continuity when a failover occurs.

For more information about controller clustering, see Chapter 18 of the [ArubaOS 8.3.0.x User Guide](https://www.arubanetworks.com/support/documentation).

The individual mobility controller VRRP IP addresses configured in this procedure allow authorization servers, like Aruba ClearPass or RADIUS, to make a change of authorization request for users on specific mobility controllers to the virtual IP address created below. When the mobility controller is taken out of service, the standby mobility controller servicing the user handles the requests from the authorization server. The table and diagram below show the VRRP IP addresses the authentication servers use to communicate with the individual mobility controllers in the cluster.

#### Table 18  Mobility controller VRRP IP addresses and VLANs

<table>
<thead>
<tr>
<th>Mobility controller</th>
<th>IP address</th>
<th>Multicast VLAN</th>
<th>VRRP IP address</th>
<th>VRRP VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aruba-MC-1</td>
<td>10.2.160.10</td>
<td>160</td>
<td>10.2.160.110</td>
<td>160</td>
</tr>
<tr>
<td>Aruba-MC-2</td>
<td>10.2.160.20</td>
<td>160</td>
<td>10.2.160.120</td>
<td>160</td>
</tr>
<tr>
<td>Aruba-MC-3</td>
<td>10.2.160.30</td>
<td>160</td>
<td>10.2.160.130</td>
<td>160</td>
</tr>
<tr>
<td>Aruba-MC-4</td>
<td>10.2.160.40</td>
<td>160</td>
<td>10.2.160.140</td>
<td>160</td>
</tr>
</tbody>
</table>
Step 1: Navigate to Managed Network > AMS > Office > Santa-Clara > Configuration > Services > Clusters, and then click +.

Step 2: In New Cluster Profile window, click +.

Step 3: In the Add Controller window, enter the following information, and then click OK.

- IP version—IPv4
- IP address—10.2.160.10 (IP address of mobility controller)
- Group—None (default)
- Priority—Blank (default)
- MCastVLAN—160 (VLAN ID for multicast traffic)
- VRRP-IP—10.2.160.110 (VRRP IP address of this mobility controller for authorization servers)
- VRRP-VLAN—160 (VLAN ID for this VRRP instance)
Note: For a mobility controller virtual appliance in VMware vSphere, promiscuous mode and forged retransmits need to be allowed for VRRP to work. For security reason, create a separate virtual machine group in vSwitch for ports using VRRP and only allow promiscuous mode in that group.

Step 4: For each additional mobility controller, repeat Step 2 and Step 3, changing the variables as required.

Step 5: After all the mobility controllers have been added, in the New Cluster Profile window, enter the following information, and then click Submit.

- Name—AMS-Office-SC-Cluster
- Active client rebalance threshold—50 (default)
- Standby client rebalance threshold—75 (default)
- Unbalance threshold—5 (default)
- Heartbeat threshold—0 (default)
- Redundancy—Enabled

Step 6: Click Pending Changes > Deploy changes > Close.
Step 7: Navigate to Managed Network > AMS > Office > Santa-Clara > Aruba-MC-1 > Configuration > Services > Clusters > Cluster Profile, enter the following information, and then click Submit.

- Cluster group-membership—AMS-Office-SC-Cluster
- Exclude VLANs—1

Step 8: For each additional mobility controller, repeat Step 7.

Step 9: Click Pending Changes > Deploy changes > Close.

### 6.7 Configure mobility controller cluster VRRP for AP provisioning

This procedure configures a cluster-wide VRRP for AP provisioning.

The cluster-wide VRRP IP address configured in this procedure is for AP controller discovery. The virtual IP address is configured at the cluster level and is used in DHCP and DNS servers for dynamic discovery or it is statically defined in the Mobility Master. The table and diagram below show the VRRP IP address the APs use to find the mobility controller cluster.

<table>
<thead>
<tr>
<th>Cluster</th>
<th>VRRP ID</th>
<th>VRRP IP address</th>
<th>VRRP VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Santa-Clara</td>
<td>160</td>
<td>10.2.160.100</td>
<td>160</td>
</tr>
</tbody>
</table>

![Figure 29](image-url)
Step 1: Navigate to Managed Network > AMS > Office > Santa-Clara > Configuration > Interfaces > VLANs, and then click +.

Step 2: In the New VLAN window, enter the following information, and then click Submit.

- VLAN name—**AMS-Office-SC-MC**
- VLAN ID/Range—**160**

![VLANs Table](image)

**Note** This step is naming the uplink VLAN already configured in the initial mobility controller setup procedure, which makes it available at the cluster level for the step below.

Step 3: Click Pending Changes > Deploy changes > Close.

Step 4: Navigate to Managed Network > AMS > Office > Santa-Clara > Configuration > Services > Redundancy > Virtual Router Table, and then click the +.

Step 5: In the New Virtual Router window, enter the following information, and then click Submit.

- ID—**160**
- IP version—IPv4
- Authentication password—*[password]*
- Retype authentication password—*[password]*
- IP address—**10.2.160.100** (cluster-wide VRRP IP address for controller discovery)
- Admin state—UP
- VLAN—**160** (VLAN ID for this VRRP instance)
Note: For a mobility controller virtual appliance in VMware vSphere, promiscuous mode and forged retransmits need to be allowed for VRRP to work. For security reason, create a separate virtual machine group in vSwitch for ports using VRRP and only allow promiscuous mode in that group.

**Step 6:** Click Pending Changes > Deploy changes > Close.

**Procedures**

**Configuring the Wireless LANs**

1. Configure external RADIUS server
2. Configure WLAN for employee SSID
3. Configure the employee SSID security
4. Configure the employee SSID access rules
5. Configure WLAN for guest SSID
6. Configure the guest SSID security
7. Configure local VLANs for employee and guest SSIDs
8. Configure mobility controller interface with VLANs
9. Configure mobility controller guest VLAN with an IP address

Use this section to configure the wireless LANs. The diagram on the next page shows wireless VLANs in the Mobile First Campus design.
**7.1 Configure external RADIUS server**

This procedure configures the Mobility Master with an external RADIUS server that authenticates users on the WLAN. The ArubaOS software allows you to use an external authentication server or the internal user database of the Mobility Master to authenticate clients to the wireless network.

**Step 1:** Navigate to Managed Network > Configuration > Authentication > Auth Server > All Servers, and then click +.

**Step 2:** In the New Server window, enter the following information, and then click Submit.

- Name—**Example-RADIUS**
- IP address—**10.2.120.41** (IP address of external RADIUS server)
- Type—**RADIUS**
Step 3: Navigate to Managed Network > Configuration > Authentication > Auth Server > All Servers, and then select Example-RADIUS.

![All Servers Table]

Step 4: In the Server Options window, enter the following information, and then click Submit:

- IP address—10.2.120.41 (External RADIUS server added previously)
- Auth port—1812 (default)
- Accounting port—1813 (default)
- Shared key—[password]
- Retype key—[password]

Step 5: Click Pending Changes > Deploy changes > Close.

### 7.2 Configure WLAN for employee SSID

This procedure configures the WLAN for employees. A WLAN can be configured to provide different network access or services to users on the same physical network. For example, you can configure a WLAN to provide access to guest users and another WLAN to provide access to employee users through the same APs.

Step 1: Navigate to Managed Network > Configuration > WLANs, and then click +.

Step 2: In the New WLAN window, on the General page, enter the following information, and then click Next.

- Name (ssid)—Example-Employee
- Primary usage—Employee
- Broadcast on—All APs
- Forwarding mode—Tunnel
Step 3: In the New WLAN window on the VLANs page, enter the following information, and then click Next.

- VLAN—1 (this will be changed in a subsequent procedure)

### 7.3 Configure the employee SSID security

This procedure configures employee SSID security. Employee security for the Wi-Fi network can be done with a WPA-2 personal passphrase or you can choose to have every employee authenticate with a username and password using WPA-2 enterprise.

**Note**  
WPA-2 Enterprise is used to enable 802.1X authentication for a wireless network. The wireless client authenticates against the RADIUS server using an EAP-TLS exchange, and the mobility controller acts as a relay. Both the client and the RADIUS server use certificates to verify their identities.

With certain operating systems, the certificate is not automatically imported from the RADIUS server and requires manual installation in order for WPA-2 Enterprise to work. If the certificate is self-signed and generated on the RADIUS server, the certificate must be exported from the RADIUS server. From a Windows client, the certificate must be imported into the Trusted Root Certification Authorities store.

If you are planning to use WPA-2 personal with passphrase access, choose option 1. If you are planning to use WPA-2 enterprise authentication, choose option 2.

**Option 1: WPA-2 personal with passphrase access**

**Step 1:** In the New WLAN window on the Security page, enter the following information, and then click Next.

- Security Level slider—Personal
- Key management—WPA-2 Personal
- Passphrase—[password]
- Retype—[password]
Step 2: Skip to the next procedure.

Option 2: WPA-2 enterprise with username and password

Step 1: In the New WLAN window on the Security page, enter the following information, and then from inside the Auth servers box, click +.

- Security Level slider—Enterprise
- Key management—WPA-2 Enterprise

Step 2: In the Add Existing Server window, select Example-RADIUS, and then click OK and Next.
7.4 Configure the employee SSID access rules
This procedure configures the employee SSID access rules.

Step 1: In the New WLAN window on the Access page, enter the following information, and then click Finish.
  • Default role—authenticated

Step 2: Click Pending Changes > Deploy changes > Close.

7.5 Configure WLAN for guest SSID
This procedure configures the WLAN for a guest SSID.

Step 1: Navigate to Managed Network > Configuration > WLANs, and then click +.

Step 2: In New WLAN window on the General page, enter the following information, and then click Next.
  • Name (ssid)—Example-Guest
  • Primary usage—Guest
  • Broadcast on—All APs
  • Forwarding mode—Tunnel
Step 3: In the New WLAN window on the VLANs page, enter the following information, and then click Next.
  
  • VLAN—1 (this will be changed in a subsequent procedure)

7.6 Configure the guest SSID security

This procedure configures the guest SSID for security. You can use WPA-2 personal encrypted passphrase for all your guests, or you can require them to authenticate with a unique username and password. If you choose to require a passphrase, the most common captive portal is a simple acknowledgement splash page detailing the terms and conditions for using the guest network.

Step 1: In the New WLAN window on the Security page, enter the following information, and then click Next.
  
  • Security Level slider—Internal captive portal with email registration

Step 2: In the New WLAN window on the Access page, click Finish.

Note  A new default role for this WLAN is created using the SSID name prepended to the guest-logon role name. The rules from the guest-logon role are copied to the new role. This allows you to customize the guest role for this WLAN without modifying the original guest logon.

The default role for this guest WLAN: Example-Guest-guest-logon

Step 3: Click Pending Changes > Deploy changes > Close.

7.7 Configure local VLANs for employee and guest SSIDs

This procedure configures the local VLANs for employee and guest SSIDs.
Step 1: For the employee VLAN, navigate to Managed Network > AMS > Office > Santa-Clara > Configuration > WLANs > Example-Employee > VLANs, click Show VLAN details, and then click +.

Step 2: In the New VLAN window, enter the following information, and then click Submit.

- VLAN name—AMS-Office-SC-Employee
- VLAN ID/Range—330

Step 3: In the Example-Employee window, in the VLAN menu, select the name you created in the previous step, and then click Submit.

- VLAN—AMS-Office-SC-Employee
Step 4: For the guest VLAN, navigate to Managed Network > AMS > Office > Santa-Clara > Configuration > WLANs > Example-Guest > VLANs, click Show VLAN details, and then click +.

Step 5: In the New VLAN window, enter the following information, and then click Submit.

- VLAN name—**AMS-Office-SC-Guest**
- VLAN ID/Range—**340**

Step 6: In the Example-Guest window, on the VLAN menu, select the name you created in the previous step, and then click Submit.

- VLAN—**AMS-Office-SC-Guest**

![Image of VLAN configuration](image)

Step 7: Click Pending Changes > Deploy changes > Close.

### 7.8 Configure mobility controller interface with VLANs

This procedure configures the uplink interface in the mobility controller to allow user and guest VLANs to access the port.
Step 1: Navigate to Managed Network > AMS > Office > Santa-Clara > Aruba-MC-1 > Configuration > Interfaces > Ports, and then click GE-0/0/24.

Step 2: In the GE-0/0/24 window, enter the following information, and then in the VLAN section, click +.

- PoE—Disable
- Mode—Trunk
- Allowed VLANs—Allow specified VLANs
Step 3: In the Add Allowed VLAN window, enter the following information, and then click OK and Submit.

- VLAN—**160,330,340**

Step 4: For each additional mobility controller, repeat Step 1 through Step 3, changing the variables as required.

Step 5: Click Pending Changes > Deploy changes > Close.

### 7.9 Configure mobility controller guest VLAN with an IP address

A guest captive portal is a method of authentication that presents a web page that requires action on the part of the user before network access is granted. The required action can be agreeing to an acceptable-use policy or entering a user ID and password, which are validated against a database of authorized users. The captive portal requires an IP address in order to reply to the client and send the web portal redirection to the client.

This procedure configures a DHCP IP address on the guest VLAN of the mobility controller.

Step 1: Navigate to Managed Network > AMS > Office > Santa-Clara > Aruba-MC-1 > Configuration > Interfaces > VLANs, click AMS-Offices-SC-Guest, click 340, click IPv4, enter the following information, and then click Submit.

- IP assignment—**DHCP**

![IP Address Assignment](image)

Repeat this step for the guest VLANs on each mobility controller.

Step 2: Click Pending Changes > Deploy changes > Close.
Use this section to configure the access points. The figure below shows the wireless access points in the access layer of the Mobile First Campus design.

**Figure 31 Mobile First Campus design—wireless access points**
8.1 Configure AP Group

This procedure configures an AP group. Use an AP group to apply a set of features to a group of APs. You can also configure a feature for a specific AP. Any values that you configure for a specific AP override the same values configured for the AP group to which the AP belongs.

Step 1: Navigate to Managed Network > Configuration > AP Groups, and then click +.

Step 2: In the New AP Group window, enter the following information, and then click Submit.
  - Name—Example-AP-Group

Step 3: Navigate to Managed Network > Configuration > AP Groups > Example-AP-Group > WLANs, and then click +.

Step 4: In the Select WLAN window, enter the following information, and then click Submit.
  - Virutal-ap—Example-Employee

Step 5: For the guest WLAN, repeat Step 3 and Step 4, changing the variable as required.

Step 6: Click Pending Changes > Deploy changes > Close.

8.2 Remove SSID from default AP group

This procedure removes the employee and guest SSIDs from the default AP group. An AP group is a set of APs to which the same configuration is applied. There is an AP group called “default” to which all APs are assigned.

Step 1: Navigate to Managed Network > Configuration > AP Groups > default > WLANs, select Example-Employee, and then click the trash can icon on the right.

Step 2: In the Are you sure you want to delete window, click Delete.

Step 3: For the guest WLAN, repeat Step 1 and Step 2.

Step 4: Click Pending Changes > Deploy changes > Close.
**8.3 Configure the power settings**

This procedure configures the power settings for the 5-GHz and 2.4-GHz radios. In the 2.4-GHz band, set the minimum power threshold to 6 and the maximum power to 9 for open-office and walled-office environments. In the 5-GHz band for an open-office environment, set the minimum power threshold to 12 and the maximum to 15. In the 5-GHz band for a walled-office environment, set the minimum power threshold to 15 and the maximum to 18.

Enable background spectrum monitoring. When background spectrum monitoring is enabled, APs continue to provide normal access service to clients. They also monitor RF interference from neighboring APs and non-Wi-Fi sources, such as cordless phones and microwaves, on the channel they are servicing clients.

If you are in an open-office environment, choose Option 1. If you are in a walled-office environment, choose Option 2.

**Option 1: Open-office environment**

**Step 1:** Navigate to Managed Network > Configuration > AP Groups > Example-AP-Group > Example-Employee > Radio.

**Step 2:** In the 2.4 GHz section, enter the following information.

- Radio mode—ap-mode (default)
- Background spectrum monitoring—Enabled
- Min Transmit EIRP (dBm) slider—6
- Max Transmit EIRP (dBm) slider—9
Step 3: In the 5 GHz section, enter the following information.

- Radio mode—**ap-mode** (default)
- Spectrum monitoring—**Enabled**
- Min Transmit EIRP (dBm) slider—12
- Max Transmit EIRP (dBm) slider—15

**Note**  In all environments, the minimum power level differences between equal coverage level 2.4-GHz radios and 5-GHz radios should be 6 dBm. The difference between the min and max Transmit EIRP settings should not exceed 6 dBm for all radios.

Step 4: Skip to the next procedure.

**Option 2: Walled-office environment**

Step 1: Navigate to Managed Network > Configuration > AP Groups > Example-AP-Group > Example-Employee > Radio.

Step 2: In the 2.4 GHz section, enter the following information.

- Radio mode—**ap-mode** (default)
- Background spectrum monitoring—**Enabled**
- Min Transmit EIRP (dBm) slider—6
- Max Transmit EIRP (dBm) slider—9
Step 3: In the 5 GHz section, enter the following information.

- Radio mode—*ap-mode* (default)
- Spectrum monitoring—**Enabled**
- Min Transmit EIRP (dBm) slider—15
- Max Transmit EIRP (dBm) slider—18

**Note** In all environments, the minimum power level differences between equal coverage level 2.4-GHz radios and 5-GHz radios should be 6 dBm. The difference between the min and max Transmit EIRP settings should not exceed 6 dBm for all radios.

---

8.4 **Disable 80 MHz-wide channels in the 5 GHz band**

This procedure disables 80 MHz wide channels in the 5 GHz band.

Step 1: At the bottom of the **Radio** tab in the 5 GHz section, click **Edit**.
Step 2: On the **Valid 5 GHz Channels** page in the **UNII-1** section, disable the 80 MHz channels by matching the colors as depicted below.

- 80 MHz—Gray (disabled)
- 40 MHz—Orange (enabled)
- 20 MHz—Orange (enabled)

Repeat this step for the remaining UNII sections on the page.

Step 3: After all sections are complete, click OK, and then click Submit.

Step 4: Click Pending Changes > Deploy changes > Close.

Step 5: For each additional WLAN, repeat Procedure 1.10 and Procedure 1.11.

**8.5 Enable control plane security and auto certificate provisioning**

This procedure enables Control Plane Security (CPSec) and auto certificate provisioning. ArubaOS supports secure IPsec communications between a controller and campus APs using public-key self-signed certificates created by each Mobility Master. The controller certifies its APs by issuing them certificates. If the Mobility Master has any associated mobility controllers, it sends a certificate to each mobility controller, which in turn sends certificates to their associated APs.
The mobility controller maintains a whitelist that contains records of all campus APs connected to the network. The campus AP whitelist is used to add valid campus APs to the secure network or revoke network access to any suspected rogue or unauthorized APs. If all APs on the network are valid, such as during the initial configuration, automatic certificate provisioning can be enabled to send certificates from the controller to each AP. This automatically provisions them and adds them to the AP whitelist.

When the controller sends a certificate to the AP, that AP must reboot before it can connect to the controller over a secure channel. If you are enabling CPSec for the first time on a large network, your users may experience several minutes of interrupted connectivity while each AP receives its certificate and establishes its secure connection.

**Step 1:** Navigate to Managed Network > Configuration > System > CPSec > Control Plane Security, slide the buttons to the right for the selections below, and then click Submit.

- Enable CPSEC slider—Enable
- Enable auto cert provisioning slider—Enable

**Step 2:** Click Pending Changes > Deploy changes > Close.

### 8.6 Convert Instant Access Points to a Campus Access Points

Optional

This optional procedure converts instant access points (IAPs) to campus access points (CAPs). If you have existing IAPs or APs running older software and you want the Aruba mobility controller to manage them, they need to be converted to CAP mode using the steps below.

If you have newer APs running the latest software, you can skip this procedure by allowing the AP to discover the controllers by using the information from Procedure 1.14.

**Step 1:** Connect the AP to a PoE port on an access switch.

**Step 2:** When the Radio Status light is blinking green, from your wireless PC, connect to the open SSID that has the name “SetMeUp-XX:XX:XX”.
Note  Connecting to the SSID automatically opens your default web browser, but you should get a security warning saying the site is not secure.

Step 3: In the web browser that opens, click the option to proceed to the webpage. The following screenshot shows an example of the message you see in your browser. Based on your browser type, you might see a slightly different message.

This site is not secure
This might mean that someone’s trying to fool you or steal any info you send to the server. You should close this site immediately.

- Close this tab
- More information

Your PC doesn’t trust this website’s security certificate.
Error Code: DLG_FLAGS_INVALID_CA
- Go on to the webpage (not recommended)

Note  If your browser does not allow you to proceed to the web page due to security settings, you may have to use a different browser.
The other option is to browse directly to the DHCP IP address on the uplink port of the AP.

Step 4: On the Virtual Controller welcome page, enter the following information, and then click Log In.
- Username—admin
- Password—admin (default)

Step 5: At the top of the page on the right hand side, navigate to Maintenance > Convert, enter the following information, and then click Convert Now.
- Convert one or more Access Points to—Campus APs managed by a Mobility Controller
- Hostname or IP Address of Mobility Controller—\textbf{10.2.160.100} (VRRP IP address)
Step 6: In the **Confirm Access Point Conversion** window, click **Convert Now**.

**Note**  The conversion process takes several minutes, and then the APs reboot to join the cluster.

### 8.7 Provision access points to the mobility controller AP group

This procedure provisions the APs to the mobility controller AP group.

An AP can discover the IP address of the controller from a DNS server, from a DHCP server, or using the Aruba Discovery Protocol.

At boot time, the AP builds a list of managed device IP addresses and then tries these addresses in order until it successfully reaches a managed device. This list of IP addresses provides an enhanced redundancy scheme for managed devices that are located in multiple data centers separated across layer-3 networks. The AP constructs its list of managed device addresses as follows:

- If the provisioning parameter is set to a DNS name, that name is resolved and all resulting addresses are put on the list. If is set to an IP address, that address is put on the list.
- If the provisioning parameter is not set and a managed device address was received in DHCP option 43, that address is put on the list.
- If the provisioning parameter is not set and no address was received via DHCP option 43, you use AP discovery protocol (ADP) to discover a managed device address and that address is put on the list.
- Managed device addresses derived from the server-name and server-ip provisioning parameters and the default managed device name aruba-master are added to the list. Note that if a DNS name resolves to multiple addresses, all addresses are added to the list.

Most DHCP servers can send a variety of optional information, including the Vendor-Specific Option Code, also called option 43. Here is how option 43 works for an Aruba AP:

1. The DHCP client on an Aruba AP adds an optional piece of information called the Vendor Class Identifier Code (Microsoft DHCP option 60) in its DHCP request. The value of this code is: ArubaAP
2. The DHCP server sees the Vendor Class Identifier Code in the request and checks to see if it has option 43 configured. If it does, it sends the Vendor-Specific Option Code (option 43) to the client. The value of this option is the VRRP IP address of the Aruba mobility controller cluster.
3. The AP receives a response from the DHCP server and checks if option 43 is returned. If it is, the AP contacts the mobility controller cluster using the supplied IP address.
Microsoft Windows-based DHCP server

The Microsoft Windows-based DHCP server requires option 60 and option 43 configured for an Aruba AP. Because option 60 is not a predefined option on a Windows DHCP server, you must add it to the option list for the server. The information below is required when creating option 60:

- **Name**—Aruba access point
- **Data**—Type String
- **Code**—60
- **Description**—Aruba AP vendor class identifier

When option 60 is added to the DHCP scope, the following string value is required:

- **String value**—ArubaAP

When option 43 is added to the DHCP scope, the following value is required:

- **ASCII**—10.2.160.100 (VRRP IP address of the mobility controller cluster)

After the APs have discovered the controllers in your network, they need to be provisioned in an AP group.

**Step 1:** Navigate to Managed Network > AMS > Office > Santa-Clara > Configuration > Access Points > Campus APs, select the AP and then click Provision.
Step 2: In the window with AP's MAC address below the Campus APs window, enter the following information, and then click **Submit**.

- **Name**—305-AG1-AC2-21
- **AP group**—**Example-AP-Group**
- **Controller discovery**—**Static**
- **Controller IP/DNS name**—10.2.160.100 (VRRP IP address of mobility controller cluster)
- **IP**—**DHCP**
- **Deployment**—**Campus**

![MAC address configuration screen](image)

Step 3: On the **Access Points will be Rebooted** screen, click **Continue & Reboot**.

Step 4: For each additional AP you want to provision, repeat Step 1 through Step 3.
Summary

The flow of information is a critical component to a well-run organization. The Aruba Mobile First Campus design provides a prescriptive solution, based on best practices and tested topologies. This allows you to build a robust network that accommodates your organization’s requirements. Whether users are located at a large LAN location or at a smaller remote site, this design provides a consistent set of features and functionality for network access, which helps improve user satisfaction and productivity while reducing operational expense.

Figure 32  Mobile First Campus design

The Mobile First Campus design provides a consistent and scalable methodology of building your network, improving overall usable network bandwidth and resilience and making the network easier to deploy, maintain, and troubleshoot.
**Validated Hardware and Software**

The following list of hardware and software was validated for this guide:

### Wired Core

<table>
<thead>
<tr>
<th>Product name</th>
<th>Software version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aruba 8400</td>
<td>10.00.0015</td>
</tr>
<tr>
<td>Aruba 8320</td>
<td>10.00.0015</td>
</tr>
<tr>
<td>Aruba 5400R</td>
<td>16.04.0010</td>
</tr>
</tbody>
</table>

### Wired Aggregation

<table>
<thead>
<tr>
<th>Product name</th>
<th>Software version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aruba 5400R</td>
<td>16.04.0010</td>
</tr>
<tr>
<td>Aruba 3810M</td>
<td>16.04.0010</td>
</tr>
</tbody>
</table>

### Wired Access

<table>
<thead>
<tr>
<th>Product name</th>
<th>Software version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aruba 5400R</td>
<td>16.04.0010</td>
</tr>
<tr>
<td>Aruba 3810M</td>
<td>16.04.0010</td>
</tr>
<tr>
<td>Aruba 2930M</td>
<td>16.04.0010</td>
</tr>
<tr>
<td>Aruba 32930F</td>
<td>16.04.0010</td>
</tr>
</tbody>
</table>

### Wireless Mobility Master

<table>
<thead>
<tr>
<th>Product name</th>
<th>Software version</th>
</tr>
</thead>
<tbody>
<tr>
<td>MM-VA-1K</td>
<td>8.3.0.0 (ArubaOS)</td>
</tr>
</tbody>
</table>

### Wireless Mobility Controller

<table>
<thead>
<tr>
<th>Product name</th>
<th>Software version</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCVA-250</td>
<td>8.3.0.0 (ArubaOS)</td>
</tr>
<tr>
<td>Aruba 7010</td>
<td>8.3.0.0 (ArubaOS)</td>
</tr>
<tr>
<td>Aruba 7024</td>
<td>8.3.0.0 (ArubaOS)</td>
</tr>
</tbody>
</table>
Wireless Access Points

<table>
<thead>
<tr>
<th>Product name</th>
<th>Software version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aruba 330 Series AP</td>
<td>8.3.0.0 (ArubaOS)</td>
</tr>
<tr>
<td>Aruba 310 Series AP</td>
<td>8.3.0.0 (ArubaOS)</td>
</tr>
<tr>
<td>Aruba 300 Series AP</td>
<td>8.3.0.0 (ArubaOS)</td>
</tr>
</tbody>
</table>

What’s New in This Version

The following changes have been made since Aruba last published this guide.

- This is a new guide
You can use the feedback form to send suggestions and comments about this solution brief.