TECHNICAL WHITE PAPER

ARUBA MOBILE-FIRST REFERENCE ARCHITECTURE GUIDE

ENABLING THE MOBILE WORKPLACE

a Hewlett Packard Enterprise company

CONTENTS

INTRODUCTION

Transforming the enterprise for the Idea Economy

We live and work in the Idea Economy. It has never been easier to turn ideas into new products, services, applications, and industries. It's easier for you, easier for your competitors, and easier for companies you may not even know about yet.

It's an age of relentless, disruptive change for businesses and governments. Every Fortune 1000 company today is at risk of missing a market opportunity, not securing their enterprise, and being disrupted by a new idea or business model. In the Idea Economy, anyone can change the world.

And yet the winners aren't always those with the best ideas. Rather, they are companies of every size that can execute on good ideas and deliver value faster and better than their competitors.

That means using the power of technology to quickly fuel the power of ideas. In the Idea Economy, IT strategy and business strategy are increasingly inseparable. And so IT's role must evolve from providing technical services to generating business value.

In our view, businesses must change along four axes in order to survive and thrive in the Idea Economy. They must transform to a hybrid infrastructure; protect the digital enterprise; empower the data driven organization; and enable workplace productivity.

Transform
to a hybrid infrastructure
Protect
your digital enterprise
Enable
workplace productivity
Empower
the data-driven organization

Figure 1. Transformation areas for the Idea Economy

Success in the Idea Economy requires a partner that can bring all these elements together, aligned to your industry and your enterprise.

- **Transform to a Hybrid Infrastructure**
  Enterprises need to create and deliver new value instantly and continuously from all of their applications. This requires a hybrid infrastructure that maximizes performance and cost. It must provide the on-demand foundation for 100 percent of the apps and workloads that power the enterprise.
- **Protect your digital enterprise**
  Today's massive data breaches demonstrate the security risks of a hyper-connected world. The threat landscape is wider and more diverse than ever before.
  HPE can help you manage risk in all its forms. We offer solutions for the full cyber-attack lifecycle, from threat research to intrusion monitoring and forecasting with big data. We also have backup and recovery options to ensure compliance and business continuity in the event of an incident.
- **Empower the Data-Driven Organization**
  In a hyper-connected world, companies need solutions that extract value from vast, unpredictable troves of data. For

instance, analytic insights could unlock the value of a connected car driving through a smart city – as human, machine and business data reveal real time opportunities for commerce.

HPE has bet on efficient, open-source solutions that help you generate real-time, actionable insights from your data. The result is better and faster decision making.

- **Enable Workplace Productivity**

  The nature of work is changing. Employees are virtual. Alliances are ad hoc. Work happens anywhere, anytime, on any device. In the Idea Economy, companies must deliver experiences that empower employees and customers to create better outcomes.

Understanding a mobile-first workplace

One key factor to enable workplace productivity is to understand the mobility requirement. In the past mobility was understood as WiFi roaming. But while roaming is required, it is not enough. Mobility, today, means that employees are able to connect to corporate resources, applications, conferences and collaboration tools anytime and anywhere, and using a variety of devices to maximize their productivity.

The HPE Mobile-first network combines Aruba mobility components and HPE Networking switching and routing infrastructure to build an end-to-end solution.

It includes a secure and easy to use access control infrastructure that provides the same user experience to employees in a campus, a branch, a home office or on the road independently of their connection, wired or wireless, local or remote. This infrastructure also provides a simple and trustable guest services management solution.

The HPE Mobile-first solution provides IT professionals a comprehensive view of the network, and the right tools to manage it and to implement changes in an agile manner.

Mobile-first network solution

The HPE Mobile-first network is an end-to-end mobile workplace solution. It enables enterprises to provide secure mobile connectivity to employees and guests.

In a mobile workplace the boundaries between campus, branch and remote clients tend to disappear. Enterprises need to provide seamless connection to information resources and applications independently from the user location. The HPE Mobile-first solution integrates all types of sites, including small remote offices and individual remote clients.

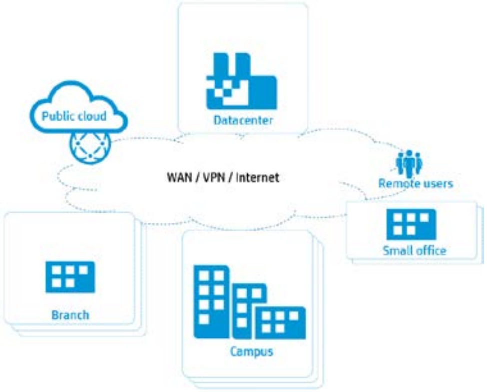


Figure 2. Mobile-first network scope

The solution integrates a mobility infrastructure, a switching infrastructure, and location-based services.

Mobility infrastructure

The mobility infrastructure is based on the Aruba hierarchical model. The top of this hierarchy is composed of a network management platform: Airwave, an access control platform: ClearPass Policy Manager (CPPM), and a pair of mobility controllers: master mobility controllers. These components are located in the enterprise's data center.

The campus portion of the infrastructure is composed of two or more local mobility controllers and APs. The local controllers work in synch with Airwave, CPPM and the master controllers to perform their mobility functions. In the recommended configuration, local controllers act as the policy enforcement and aggregation point for APs: all WLAN client traffic is tunneled between the AP and the controller, delivered to and received from the wired infrastructure at the controller.

The Aruba solution offers two options for branch offices. The traditional controller-based scheme is based on a branch mobility controller and several APs. These controllers have two branch specific features: zero-touch deployment and a controller-to-controller VPN to the data center. As in the campus, the branch controller acts as as the WLAN policy enforcement and traffic aggregation point. Client traffic can be forwarded on a VLAN by VLAN base, some VLANs can be placed in the branch's wired network, for example for collaboration and printing, while other VLANs can be encapsulated in the VPN to access applications in the data center.

The second option for the branch does not require a controller, it is based on the Aruba Instant AP technology. Instant APs connected to a single L2 segment form an Aruba Instant Cluster, in which one of the APs acts as a virtual controller. Instant clusters also support zero-touch deployment and a virtual controller-to-master controller VPN to the data center. In this model, WLAN traffic that needs to stay in the branch, is forwarded to the wired LAN locally at the AP (bridging mode) while traffic on certain VLANs is tunneled to the master controller by the virtual controller.

Remote clients can connect to the network in two ways. If the user is working from a static location like a telecommuter in a home office an Aruba Remote AP can be deployed. This AP will establish a VPN to the master controller and the client will be able to access the resources in the same as as in any corporate office. If the user is on the road, Aruba offers a software solution called Virtual Intranet Access (VIA) for Windows or MAC.

Another way of describing the Aruba solution is by placing its components in a logical four-layer operating model: management, control, aggregation, and access.

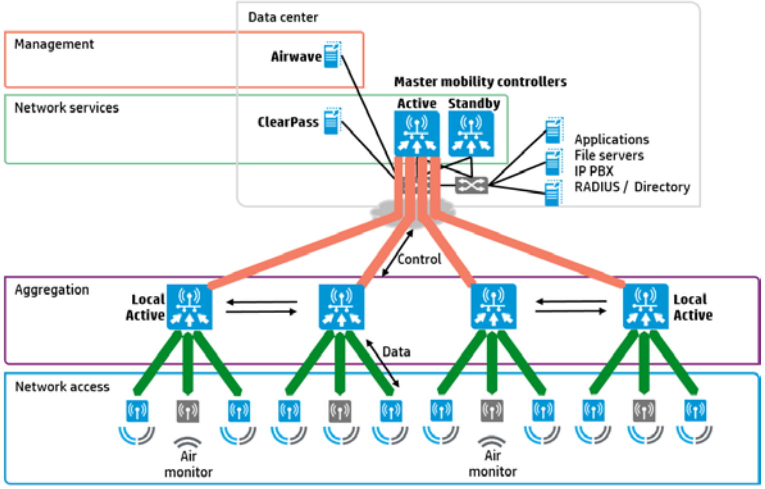


Figure 3. WLAN logical design

- **Management**: The management layer consists of AirWave®. AirWave provides a single point of management for the WLAN, including reporting, heat maps, centralized configuration, and troubleshooting.

- **Network services**: The network services layer consists of master mobility controllers and ClearPass (CPPM). The master controllers provide a control plane for the Aruba WLAN that spans the physical geography of the wired network. The control plane does not directly deal with user traffic or APs. Instead the control plane provides services such as whitelist coordination, valid AP lists, CPsec certificates, RFProtect™ coordination, and RADIUS or AAA proxy.
- **Aggregation**: The aggregation layer is the interconnect point where the AP, air monitor (AM), and SM traffic aggregates. This layer provides a logical point for enforcement of roles and policies on centralized traffic that enters or exits the enterprise LAN.
- **Network access**: The network access layer is comprised of APs, AMs, and SMs that work together with the aggregation layer controllers to overlay the Aruba WLAN.

Switching infrastructure

HPE offers a switching portfolio with options for the data center, campus, branch and home offices.

In the data center, the FlexFabric architecture includes different options that match different DC sizes and requirements including traditional models and next generation technologies like VXLAN. The same applies to campuses and branches, depending on the geographical distribution and feature requirements, different models can be applied.

WLAN analytics and location services

Besides the LAN infrastructure, customers may need to deploy WLAN analytics and/or location services. Aruba Analytics and Location Engine (ALE) and Aruba Meridian offer latest generation technologies to satisfy these needs.

- Aruba Analytics and Location Engine
  The Analytics and Location Engine (ALE) works with Aruba WLANs to collect presence data about Wi-Fi-enabled mobile devices while protecting personal privacy. This data is then integrated with third-party analytics solutions that translate it into actionable business intelligence.
- Aruba Meridian
  Unlike a hardware-only approach, the Aruba Networks Mobile Engagement Solution integrates best-in-class enterprise Wi-Fi and Aruba Location Services with self-service device onboarding and mobile app platforms into one integrated solution that's quick and easy to deploy.

The Aruba Mobile Engagement Solution leverages user, location, device and other contextual data to engage guests in a more meaningful way. This enables enterprise venues to deliver compelling, personalized information to their mobile devices while protecting their privacy. Visitors who connect to a venue's Wi-Fi can specify their preferences so enterprise businesses know how they want to be engaged. And when they download a venue's custom-branded Meridian mobile app, they can opt-in to get personalized, location-relevant push notifications.

The solution integrates the following components:

- **Aruba gigabit Wi-Fi** – controller-managed and controllerless wireless LANs and high-performance access points – connect many thousands of devices and apps to create a memorable user experience.
- **ClearPass Guest** securely connects visitors to Wi-Fi with a custom-branded device onboarding portal that offers targeted in-browser branding and advertising and encourages mobile app downloads.
- **Aruba's Meridian** - mobile app platform enables venues to quickly and easily create mobile apps or improve existing apps with features such as turn-by-turn directions within venues.
- **Aruba Location Services** - powered by Aruba Beacons integrate with the Meridian mobile app platform to enhance the visitor experience with location-aware features like a glowing blue dot on an indoor map and relevant push notifications based on a user's real-time location.

For details on these applications, see the Mobile-first Solutions section in this document.

MOBILE-FIRST DATA CENTER

An enterprise-wide mobile-first network requires a number of elements in the data center. These elements form the center of the mobility solution and provide end-to-end network management and control.

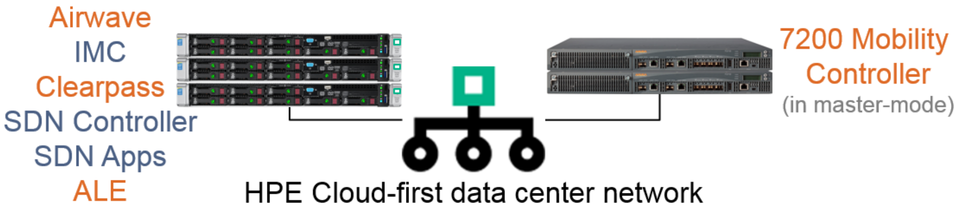


Figure 4. Data center components

Network management components

Aruba Airwave, as stated in the introduction, is the main component of the mobility infrastructure's management layer. This platform can manage the Aruba WLAN infrastructure and switches.

In those cases in which the solution includes HPE FlexNetwork WAN, data center, and/or campus LAN switches and routers, HPE Intelligent Management Center (IMC) can supplement Airwave for a complete management solution. IMC is an end to end management platform for the switching infrastructure. Its base software includes network discovery, configuration management, VLAN and ACL management and more. Additional IMC modules can be deployed to form a complete solution.

Airwave

The AirWave system is a multi-vendor Network Monitoring system which collects network and RF stats from various network components via SNMP, Syslog, Telnet/SSH. Administrators can gleam an end-to-end visibility into their wireless network to understand where potential issues are being seen and correlate that to the problems that end users are experiencing.

AirWave collects information from devices using several different methods, including:

- SNMP Polling – this method is used to collect information about Clients, APs and Controllers
- SNMP Traps can be configured for the controller to send data such as Client associations and roaming, ARM RF events etc.
- SSH - Airwave connects to the controllers using SSH for configuration management and auditing
- AMON (Advanced Monitoring) – A proprietary Aruba protocol that provides detailed and varied data to Airwave, including Channel Utilization, Interference, Firewall data, RF Health, and optionally Client monitoring data
- Syslog - Controllers can send syslog data to Airwave, which acts as a syslog server
- HTTPS - All communication between Instant and Airwave is done via HTTPS

Once AirWave collects the data, there are three ways to extract information from AirWave for consumption by Helpdesk or WLAN experts. These include –

- Reactive troubleshooting

In this situation admins investigate client/AP/Controller/Switch where the issue has been reported and study the WLAN patterns and behavior. You can refer to: Troubleshooting WLAN Issues with AirWave Wireless

- Pro-active Triggering

In this scenario admins specify thresholds of specific metrics that can allow admins to highlight specific events where the network was performing outside the acceptable design limits. AirWave can either pro-actively send these alerts to appropriate teams or just store them away in context with the offending device so that when admins are investigating a situation, they have these events highlight scenarios which were deemed a problem.

- Reporting

This mechanism is best to look at trending information.

IMC

HPE IMC's base system components and add-on modules aligns with all areas of the ISO Telecommunications Management Network's highly regarded FCAPS model (for Fault, Configuration, Accounting, Performance, and Security).

Table 1. IMC features and modules mapped to the FCAPS model

FCAPS category	IMC Base Platform	Add-on Modules
Fault	Alarms management Syslog and Trap manager	
Configuration	Intelligent configuration center Compliance center VLAN and ACL manager	IPsec VPN manager MPLS VPN manager Wireless services manager QoS manager BIMS Voice services manager Virtual application networks manager Remote site manager
Accounting	Network assets	User Behavior Analysis Service operations manager Intelligent analysis Reporter
Perfomance	Performance management Virtual network management	Network traffic analyzer Application performance manager vMON Service health manager
Security	Security control center	User access manager TACACS+ authentication manager Endpoint admission defense

Control layer components

ClearPass Policy Manager (CPPM) is recommended as the access control platform. It provides 802.1X, MAC-based and captive portal-based authentication, guest registration, device onboarding, and device health-check.

A pair of Aruba 7200 Mobility Controllers forms the top of the WLAN hierarchy and provides and central point of management and control for all campus and branch controllers. It also provides a termination point for controller- and Instant-based VPNs for branch connectivity to the data center.

Finally, the mobility-first architecture offers the option of deploying the Virtual Application Network / Software-based Network (VAN/SDN) solution. The VAN/SDN solution is based on the HPE VAN/SDN Controller and a set of HPE and 3rd party SDN apps. The SDN controller and apps can be deployed in the data center or, for performance reasons, in the campus core.

ClearPass Policy Manager

The Aruba ClearPass Access Management System provides a window into your network and covers all your access security requirements from a single platform. You get complete views of mobile devices and users and have total control over what they can access.

With ClearPass, IT can centrally manage network policies, automatically configure devices and distribute security certificates, admit guest users, assess device health, and even share information with third-party solutions—through a single pane of glass, on any network and without changing the current infrastructure.

- Role-Based and Device-Based Access:
  The Aruba ClearPass Policy Manager™ platform provides role-based and device-based network access control for employees, contractors, and guests across any wired, wireless, and VPN infrastructure.
  ClearPass works with any multivendor network and can be extended to business and IT systems that are already in place.
- Self-Service Capabilities:
  ClearPass delivers a wide range of unique self-service capabilities. Users can securely onboard their own devices for enterprise use or register AirPlay, AirPrint, Digital Living Network Alliance (DLNA), and Universal Plug and Play (UPnP) devices that are enabled for sharing, sponsor guest Wi-Fi access, and even set up sharing for Apple TV and Google Chromecast.
- Leveraging Contextual Data
  The power of ClearPass comes from integrating ultra-scalable AAA (authentication, authorization, and accounting) with policy management, guest network access, device onboarding, and device health checks with a complete understanding of context.
  From this single ClearPass policy and AAA platform, contextual data is leveraged across the network to ensure that users and devices are granted the appropriate access privileges.
  ClearPass leverages a user's role, device, location, application use, and time of day to execute custom security policies, accelerate device deployments, and streamline network operations across wired networks, wireless networks, and VPNs.
  Third-Party Security and IT Systems: ClearPass can be extended to third-party security and IT systems using REST-based APIs to automate work flows that previously required manual IT intervention. It integrates with mobile device management to leverage device inventory and posture information, which enables better-informed policy decisions.
- Key features:
  - Role-based network access enforcement for multivendor Wi-Fi, wired, and VPN networks
  - High performance, scalability, High Availability, and load balancing
  - A Web-based user interface that simplifies policy configuration and troubleshooting
  - Network Access Control (NAC), Network Access Protection (NAP) posture and health checks, and Mobile Device Management (MDM) integration for mobile device posture checks
  - Auto Sign-On and single sign-on (SSO) support via Security Assertion Markup Language (SAML) v2.0
  - Advanced reporting of all user authentications and failures
  - HTTP/RESTful APIs for integration with third-party systems, Internet security, and MDM
  - Device profiling and self-service onboarding
  - Guest access with extensive branding and customization and sponsor-based approvals
  - IPv6 administration support
- Advanced Policy Management:
  - Employee access
    ClearPass Policy Manager offers user and device authentication based on 802.1X, non-802.1X, and Web Portal access methods. To strengthen security in any environment, you can concurrently use multiple authentication protocols, such as PEAP, EAP-FAST, EAP-TLS, EAP-TTLS, and EAP-PEAP-Public.

For fine-grained control, you can use attributes from multiple identity stores, such as Microsoft Active Directory, LDAP-compliant directory, ODBC-compliant SQL database, token servers, and internal databases across domains within a single policy.

Additionally, you can add posture assessments and remediation to existing policies at any time.

  - Built-in device profiling

    ClearPass provides a built-in profiling service that discovers and classifies all endpoints, regardless of device type. You can obtain a variety of contextual data (such as MAC OUIs, DHCP fingerprinting, and other identity-centric device data) and use this data within policies.

    Stored profiling data identifies device profile changes and dynamically modifies authorization privileges. For example, if a printer appears as a Windows laptop, ClearPass Policy Manager can automatically deny access.

  - Access for unmanaged endpoints

    Unmanaged non-802.1X devices (such as printers, IP phones, and IP cameras) can be identified as known or unknown upon connecting to the network. The identity of these devices is based on the presence of their MAC address in an external or internal database.

  - Secure configuration of personal devices

    ClearPass Onboard fully automates the provisioning of any Windows, Mac OS X, iOS, Android, Chromebook, and Ubuntu devices via a built-in captive portal. Valid users are redirected to a template based interface to configure required SSIDs and 802.1X settings, and download unique device credentials.

    Additional capabilities include the ability for IT to revoke and delete credentials for lost or stolen devices, and the ability to configure mobile email settings for Exchange ActiveSync and VPN clients on some device types.

  - Customizable visitor management

    ClearPass Guest simplifies work flow processes so that receptionists, employees, and other non-IT staff can create temporary guest accounts for secure Wi-Fi and wired network access. Self-registration allows guests to create their credentials.

  - Device health checks

    ClearPass OnGuard, as well as separate OnGuard persistent or dissolvable agents, performs advanced endpoint posture assessments. Traditional NAC health-check capabilities ensure compliance and network safeguards before devices connect.

    You can use information about endpoint integrity (such as status of anti-virus, anti-spyware, firewall, and peer-to-peer applications) to enhance authorization policies. Automatic remediation services are also available for non-compliant devices.

- CPPM Hardware and Virtual Appliances: CPPM can be deployed either as a dedicated hardware appliance or a virtual machine running on top of VMware ESX/ESXi or Microsoft Hyper-V. ClearPass supports a 500, 5,000, or a 25,000 endpoints hardware or virtual appliance.
- CPPM Clusters: to increase scalability and redundancy, appliances, both virtual and hardware, within a cluster. The cluster feature allows for shared configuration and databases. However, it does not provide a virtual IP address for the cluster, so failover/redundancy for captive portal for Guest relies on Domain Name System (DNS) lookup or load balancing. RADIUS clients must define a primary and backup RADIUS server.
- Publisher/Subscriber Model: ClearPass uses a publisher/subscriber model to provide multiple-box clustering. Another term for this model is hub and spoke, where the hub corresponds to the publisher, and the spokes correspond to the subscribers.

  There is at most one active publisher in this model, and a potentially unlimited number of subscribers.

  The publisher node has full read/write access to the configuration database. All configuration changes must be made on the publisher. The publisher node sends configuration changes to each subscriber.

Subscriber nodes maintain a local copy of the configuration database, and each subscriber has read-only access to a local copy of the configuration database.

A background replication process handles the task of updating the configuration database based on the configuration changes received from the publisher.

Network Address Translation (NAT) is not supported between the publisher and subscriber nodes.

Aruba 7200 Mobility Controller Series

The Aruba Mobility Controller is the heart of the Aruba dependent access point (AP) WLAN architecture. 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 functionality that the mobility controller provides includes:

- Acting as a user-based stateful firewall
- Terminating user-encrypted sessions from wireless devices
- Performing Layer 2 switching and Layer 3 routing
- Providing clientless Layer 3 mobility
- Acting as an IPsec virtual private network (VPN) concentrator for site-to-site and client-based VPNs
- Providing certificate-based IPsec security to protect control channel information
- Terminating Internet-based remote APs (RAPs)
- Providing wired firewall services
- Performing user authentication with 802.1X and captive portal authentication, among others
- Providing guest access and captive portal services
- Provisioning services
- Providing advanced RF services with Adaptive Radio Management™ (ARM™) and spectrum analysis
- Providing location services and RF coverage “heat maps” of the deployment
- Performing rogue detection and containment
- Providing self-contained management by way of a master/local hierarchy with one controller 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 solutions.

This Aruba 7200 Mobility Controller series includes 4 models:

- Aruba 7240 mobility controller
- Aruba 7220 mobility controller
- Aruba 7210 mobility controller
- Aruba 7205 mobility controller

These controllers can be deployed at the Network services layer or at the Aggregation layer. At the first they act as master controller and at the latter they act as a local controller.

Note: Appendix A includes a detailed comparison of the Aruba 7200 mobility controller models.

The master controller role

Aruba 7200 Mobility Controllers are capable of assuming two operating roles in the system: master and local. Controllers operating in master mode are usually referred to as master controllers or master mobility controllers.

Master controllers are located in the data center while local controllers are located onsite in the campus forming a master/local cluster. A typical master/local cluster consists of one master mobility controller (or redundant pair) and one or more local mobility controllers.

The master/local hierarchy allows organizations to build scalable WLAN networks with no additional management platforms as long as the network is contained to a single master/local cluster.

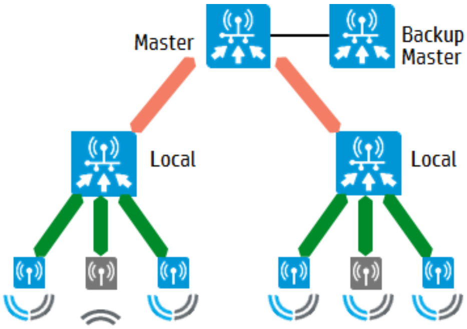


Figure 5. Master/local mobility controller cluster

The master is the central point of coordination and configuration of the network. The master processes all wireless security events and sends policy-based configuration to the locals.

The role of the master is to provide a single point of policy configuration and coordination for the WLAN in smaller deployments. The master can receive configuration and coordination information from the AirWave for larger or more distributed deployments. In smaller, single-controller deployments, the master also can perform all functions of the local. The communication channel between the master and locals uses IPsec. Aruba recommends that APs or clients not be terminated on the master in large deployments. The master should be allowed to perform the network coordination and control functions.

Masters are responsible for the following functions in the WLAN:

- Policy configuration: configuration in the Aruba solution is split between policy and local configurations. Local configuration relates to physical interfaces, IP networking, and VLANs, which are different for each mobility controller. Policy configuration is centered on the operation of APs and users, including AP settings such as the SSID name, encryption, regulatory domain, channel, power, and ARM settings. Policy configuration extends beyond APs and also covers user authentication, firewall policy, mobility domains (IP mobility), IPsec, and system management. The policy is pushed to all locals in the form of profiles, and profiles combine to create the configuration for the dependent APs.
- AP white lists: two types of white lists exist in the system, one for RAPs and one for CAPs that use CPsec. These lists determine which APs can connect to the mobility controllers. Unauthorized devices are prevented from connecting to the network.
- Wireless security coordination: wireless intrusion prevention activities involve looking for rogue (unauthorized) APs and monitoring for attacks on the WLAN infrastructure or clients. The master processes all data collected by Aruba APs and AMs. Instructions to disable a rogue AP or blacklist a client from the network are issued through the master.
- Valid AP list: all mobility controllers in the network must also know all legitimate APs that operate on the WLAN. These APs must be added to the valid AP list. This list prevents valid APs from being falsely flagged as rogue APs. This is important when APs that are attached to two different locals are close enough to hear each other’s transmissions. The valid AP list helps ARM to differentiate between APs that belong to the network and those that are neighbors. Unlike

traditional wireless intrusion detection system (WIDS) solutions, the master controller automatically generates the valid AP list without network administrator intervention. All Aruba APs are automatically learned and added to the list, but valid third-party APs must be added manually. If more than one master/local cluster exists, AirWave should be deployed to coordinate APs between clusters.

- RF visualization: the Aruba RF visualization tools provide a real-time view of the network coverage. This information is based on the AP channel and power settings and the data collected from AMs and APs listening to transmissions during their scanning periods. This information provides a real-time picture of the RF coverage as heard by the APs.
- Location: locating users in the WLAN is more difficult with mobile clients and IP mobility. The IP address of the client is no longer synonymous with location. The Aruba WLAN scans off of the configured channel, so it is possible to hear clients operating on other channels. This information can then be used to triangulate users and rogue devices to within a small area. This information is displayed on the master and allows for devices to be located quickly. This speed is critically important for physical security and advanced services such as E911 calling.
- Initial AP configuration: when an AP first boots up, it contacts its master to receive the configuration generated by the master. The master compares the AP information and determines its group assignment, and then redirects that AP to the proper local.
- Control plane security: when CPsec is enabled, the master generates the self-signed certificate and acts as the certificate authority (CA) for the network. The master issues certificates to all locals in the network, which in turn certify APs. If more than one master exists in the network, the network administrator assigns a single master as the trust anchor for that network. The trust anchor issues certificates to the other master controllers in the network.
- Authentication and roles: user authentication methods and role assignments are created on the master and then propagated to locals throughout the network. A database exists to authenticate users in small deployments or for guest access credentials that can be leveraged by all the mobility
- Centralized licensing

Master controller redundancy

To achieve high availability of the master controller, use the master redundancy model. In this scenario, two controllers are used at the network services layer: one controller is configured as the active master and the other controller acts as standby master. This setup is known as “hot standby” redundancy. The two controllers run a VRRP instance between them and the database and RF planning diagram is synchronized periodically. The virtual IP (VIP) address that is configured in the VRRP instance is used by local mobility controllers, wired APs, and wireless APs that attempt to discover a mobility controller. That VIP address is also used for network administration. The DNS query made by APs to find the master controller resolves to this VIP. The synchronization period is a configurable parameter with a recommended setting of 30 minutes between synchronizations.

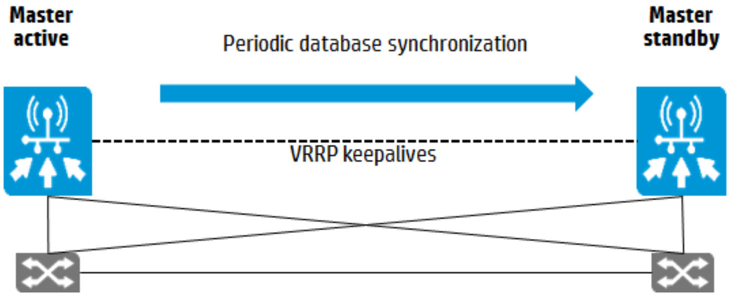


Figure 6. Hot-standby redundancy

In this configuration, one controller is always the active master controller and the other is always the standby master controller. When the active controller fails, the standby controller becomes the active master. Disable preemption in this setup. When preemption is disabled, the original master controller does not automatically become the active master after it has recovered and instead acts as the backup master controller. The recommended network attachment method is to have each master controller configured in a full mesh with redundant links to separate data center distribution switches. The example network uses a VRRP instance named 130 for redundancy.

WLAN analytics component: ALE server

While the Aruba Meridian location service is deployed as a cloud/mobile device-based application, Aruba ALE requires the deployment of a specific server in the data center. See a description of ALE in the Solutions section of this document.

Data center switching infrastructure

The components described above are connected to the data center LAN. HPE offers a variety of networking options for the data center. See some details on these options in Appendix C.

MOBILE-FIRST CAMPUS

Campus reference designs

HPE offers a rich portfolio for the campus network devices.

This section shows four models as a reference for the design of campus LANs:

- Small-medium size Mobile-first campus
- Large Mobile-first campus
- Small-medium traditional campus
- Large traditional campus

Mobile-first medium size campus

The first design is ideal for a medium size campus network in which the large majority of clients is wireless. It combines Aruba WLAN local controllers and APs with HPE switches. It has the advantage of enabling SDN applications acting on both wired and wireless clients. Additionally, it includes SmartRate ports to support the connections of APs overs 2.5 Gbps Ethernet links.

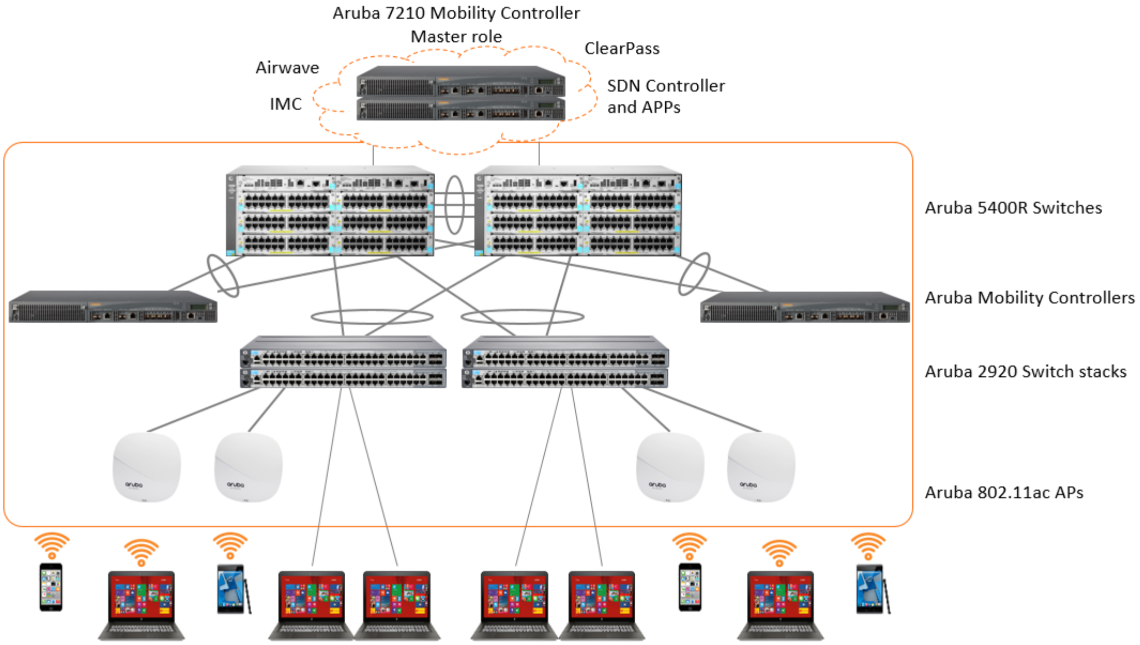


Figure 7. Mobile-first medium size campus

- Core
  A pair of Aruba 5400R switches form the core of the campus LAN.
  As all the wired and wireless client traffic converges at this point, having Aruba 5400R switches at the core allows for the deployment of the VAN/SDN solution.
  5400R switches support Distributed Trunking (DT), a technology that makes two devices look as a single device from the Layer 2/Ethernet point of view. With this feature other devices, switches, routers, controllers can be connected using Link Aggregation Groups (port trunks) eliminating the need for MSTP.
  In terms of Layer 3/IP, both devices still behave individually. In the design shown here, core switches provide, among others, the routing function inside the campus LAN, while access switches and APs forward in Layer 2 only. In this case,

DT needs to be complemented with VRRP to provide the redundant IP gateway function for the access and client devices and from the point of view of the campus edge router, these two devices act as individual OSPF neighbors/peers.

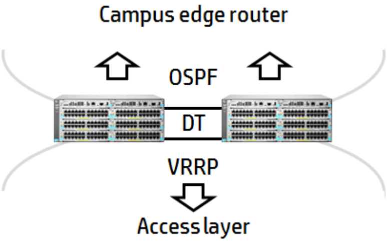


Figure 8. DT and Layer 3 protocols in the small campus core with layer 2 forwarding in the access layer

- Local mobility controllers
  Two (or more) Aruba 7200 Mobility Controllers are connected to the 5400Rs to provide the WLAN control set of functions and terminate the tunnels from the APs.
  These controllers operate in local mode and are bound to the master controllers located in the data center. For details see the Local mobility controllers section later in this chapter.
- Access switches
  Depending on the requirements, different types of access switches can be deployed. They can be summarized in 3 categories: layer 2 stackable, layer 3 stackable, and layer 3 modular. The product lines recommended in each case are:
  - layer 2 stackable: Aruba 2920 Switch Series
  - layer 3 stackable: Aruba 3800 Switch Series
  - layer 3 modular: Aruba 5400R Switch Series

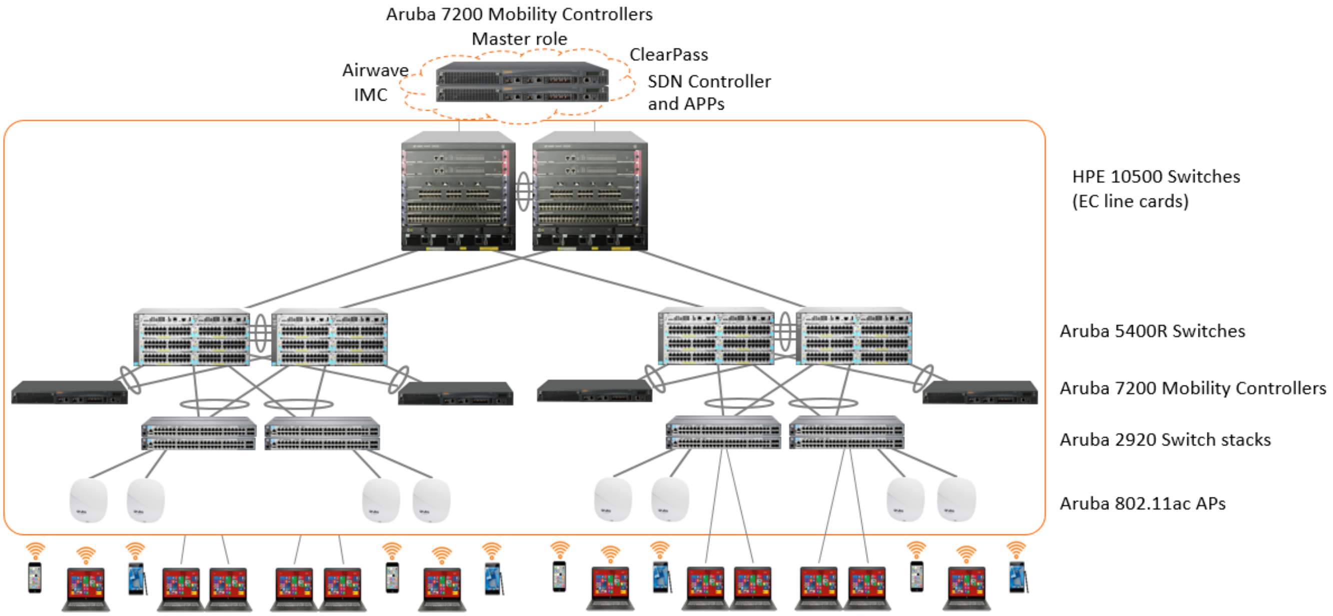
  The first option is optimal in terms of cost, while the third can be required in those cases in which MultiGig Ethernet/Aruba SmartRate ports are required. Finally, if routing is required in the access layer, the second and the third options are recommended.
- Access points
  Aruba 802.11ac access points are the main choice for the Mobile-first campus. They can be connected to either the access switches, as in the traditional designs, or, if distance permits, directly to the core switches.
  All WLAN control and data traffic is tunneled back to the local controllers. Wireless client traffic is then converted into Ethernet frames, and forwarded to the wired LAN.
- SDN control

The VAN/SDN controller can be located in the data center or in the campus. The decision will be based on the SDN Apps to be deployed, the amount of traffic expected between the Aruba switches and the controller and the data center – campus link bandwidth.

Mobile-first large campus

The second reference design presents a network model for a large campus.

The large campus Mobile-first design is based on the small campus design. Each building in a large campus looks exactly like a small campus, except for the uplinks that instead of connecting to the campus edge router connect to the core switch.



- Core
  A pair of HPE FlexNetwork 10500 switches are the core of the LAN.
  The 10500 switch is ideal for the core of large campuses as it offers high density of high speed Ethernet ports including 10GbE, 40GbE and even 100GbE. For example, 5400R switches can connect to the core using 40GbE connections or 10GbE link aggregation groups.
  The 10500 switch also supports advanced protocols like MPLS L3VPNs, L2VPNs and VPLS, and L2 VxLAN.
  When the 10500 switches are configured to create an IRF-fabric, they behave as a single device from every point of view – layer 2 through layer 7 – simplifying the LAN routing design. Any device that supports link aggregation can be connected to the IRF-fabric using a link aggregation group with member-ports on each 10500. Additionally device with an IP interface, a layer 3 switch, a router, a server, interacts with the IRF-fabric as if it were a single IP gateway and a single IP routing protocol neighbor/peer.
- Aggregation switches: A pair of Aruba 5400R switches form the aggregation layer.
  As all the wired and wireless client traffic converges at this point, having Aruba 5400R switches in this layer allows for the deployment of the VAN/SDN solution.
  5400R switches support Distributed Trunking (DT), a technology that makes two devices look as a single device from the Layer 2/Ethernet point of view. With this feature other devices, switches, routers, controllers can be connected using Link Aggregation Groups (port trunks) eliminating the need for MSTP.
  In terms of Layer 3/IP, both devices still behave individually. In the design shown here, core and aggregation switches provide, among others, the routing function inside the campus LAN, while access switches and APs forward in Layer 2 only. In this case, DT on the 5400R switches needs to be complemented with VRRP to provide the redundant IP gateway function for the access and client devices and from the point of view of the campus edge router, these two devices act as individual OSPF neighbors/peers.
- Local mobility controllers
  Two (or more) Aruba 7200 Mobility Controllers are connected to the 5400Rs to provide the WLAN control set of functions and terminate the tunnels from the APs.
  These controllers operate in local mode and are bound to the master controllers located in the data center. For details

see the Local mobility controllers section later in this chapter.

- Access switches
  Depending on the requirements, different types of access switches can be deployed. They can be summarized in 3 categories: layer 2 stackable, layer 3 stackable, and layer 3 modular. The product lines recommended in each case are:
  - layer 2 stackable: Aruba 2920 Switch Series
  - layer 3 stackable: Aruba 3800 Switch Series
  - layer 3 modular: Aruba 5400R Switch Series

  The first option is optimal in terms of cost, while the third can be required in those cases in which MultiGig Ethernet/Aruba SmartRate ports are required. Finally, if routing is required in the access layer, the second and the third options are recommended.
- Access points
  Aruba 802.11ac access points are the main choice for the Mobile-first campus. They can be connected to either the access switches, as in the traditional designs, or, if distance permits, directly to the aggregation switches.
  All WLAN control and data traffic is tunneled back to the local controllers. Wireless client traffic is then converted into Ethernet frames, and forwarded to the wired LAN.
- SDN control
  The VAN/SDN controller can be located in the data center or in the campus. The decision will be based on the SDN Apps to be deployed, the amount of traffic expected between the Aruba switches and the controller and the data center – campus link bandwidth. In a large campus, the best practice is to deploy the SDN controllers locally.

Traditional medium size campus

This reference design applies to traditional small campus LANs in which the majority of the clients are Ethernet with a smaller proportion or WiFi clients. It also applies to cases in which virtualization technologies as MPLS L2VPNs, VPLS or L2 VxLAN are required.

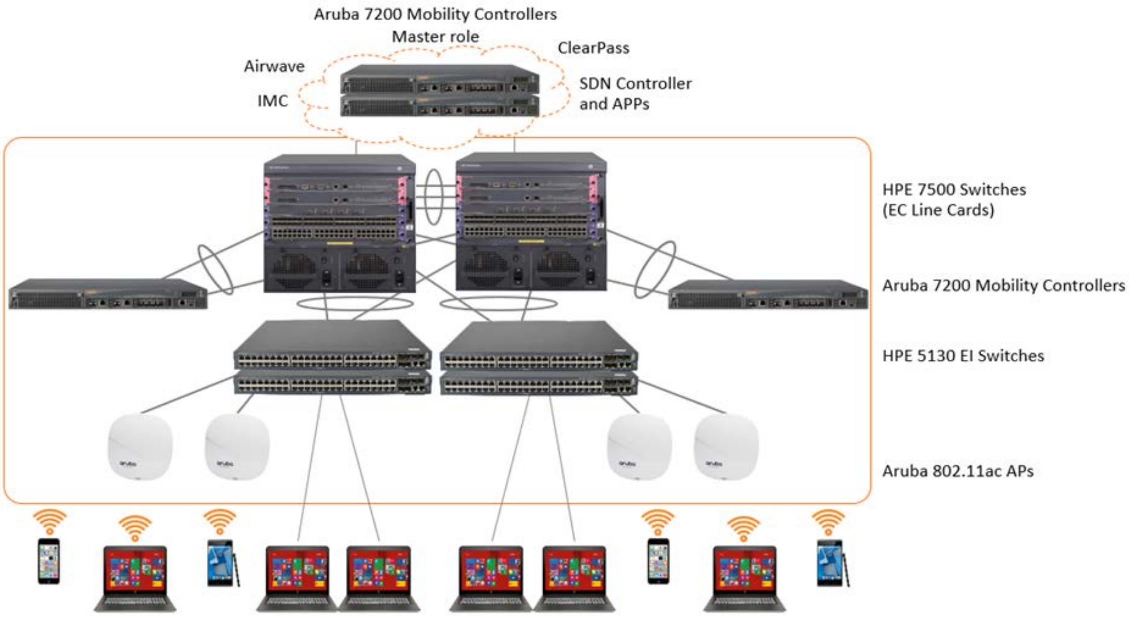


Figure 9. Traditional medium size campus

- Core

A pair of HPE FlexNetwork 7500 switches are the core of the LAN.
The 7500 switch is ideal for the core of traditional small and medium size campuses as it offers high speed Ethernet ports including 10GbE, 40GbE, along with advanced protocols like MPLS L3 VPNs, L2VPNs and VPLS, and L2 VxLAN.
When the 7500 switches are configured to create an IRF-fabric, they behave as a single device from every point of view – layer 2 through layer 7 – simplifying the LAN routing design. Any device that supports link aggregation can be connected to the IRF-fabric using a link aggregation group with member-ports on each 10500. Additionally device with an IP interface, a layer 3 switch, a router, a server, interacts with the IRF-fabric as if it were a single IP gateway, and a single IP routing or MPLS protocol neighbor/peer.

- Local mobility controllers
  Two (or more) Aruba 7200 Mobility Controllers are connected to the 7500 switches to provide the WLAN control set of functions and terminate the tunnels from the APs.
  These controllers operate in local mode and are bound to the master controllers located in the data center. For details see the Local mobility controllers section later in this chapter.
- Access switches
  Depending on the requirements, different types of access switches can be deployed. They can be summarized in 3 categories: layer 2 / stackable, layer 3 / stackable, and layer 3 / modular. The product lines recommended in each case are:
  - layer 2 stackable: HPE FlexNetwork 5130 EI Switch Series
  - layer 3 or MPLS VPN-VPLS stackable: HPE FlexNetwork 5500 HI Switch Series
  - layer 3 or MPLS VPN-VPLS modular: HPE FlexNetwork 7500 Switch Series

  The first option is optimal in terms of cost. If routing or MPLS VPNs are required in the access layer, the second and the third options are recommended.
- Access points
  Aruba 802.11ac access points are the main choice for the traditional campus. All WLAN control and data traffic is tunneled back to the local controllers. Wireless client traffic is then converted into Ethernet frames, and forwarded to the wired LAN.

Traditional large campus

This reference design applies to traditional large campus LANs in which the majority of the clients are Ethernet with a smaller proportion or WiFi clients. It also applies to cases in which virtualization technologies as MPLS L2VPNs, VPLS or L2 VxLAN are required.

- Core
  A pair of HPE FlexNetwork 10500 switches are the core of the LAN.
  The 10500 switch is ideal for the core of large campuses as it offers high density of high speed Ethernet ports including 10GbE, 40GbE and even 100 GbE. For example, 5400R switches can connect to the core using 40GbE connections or 10GbE link aggregation groups.
  The 10500 switch also supports advanced protocols like MPLS L3 VPNs, L2VPNs and VPLS, and L2 VxLAN.
- Aggregation
  A pair of HPE FlexNetwork 7500 switches are the aggregation layer of the LAN.
  The 7500 switch is ideal for the aggregation layer of large traditional campuses as it offers high speed Ethernet ports including 10GbE, 40GbE, along with advanced protocols like MPLS L3 VPNs, L2VPNs and VPLS, and L2 VxLAN.
  In those cases in which the campus is composed of extremely large buildings and the aggregation layer requires a higher port density, the 7500 switches can be replaced with 10500 switches.

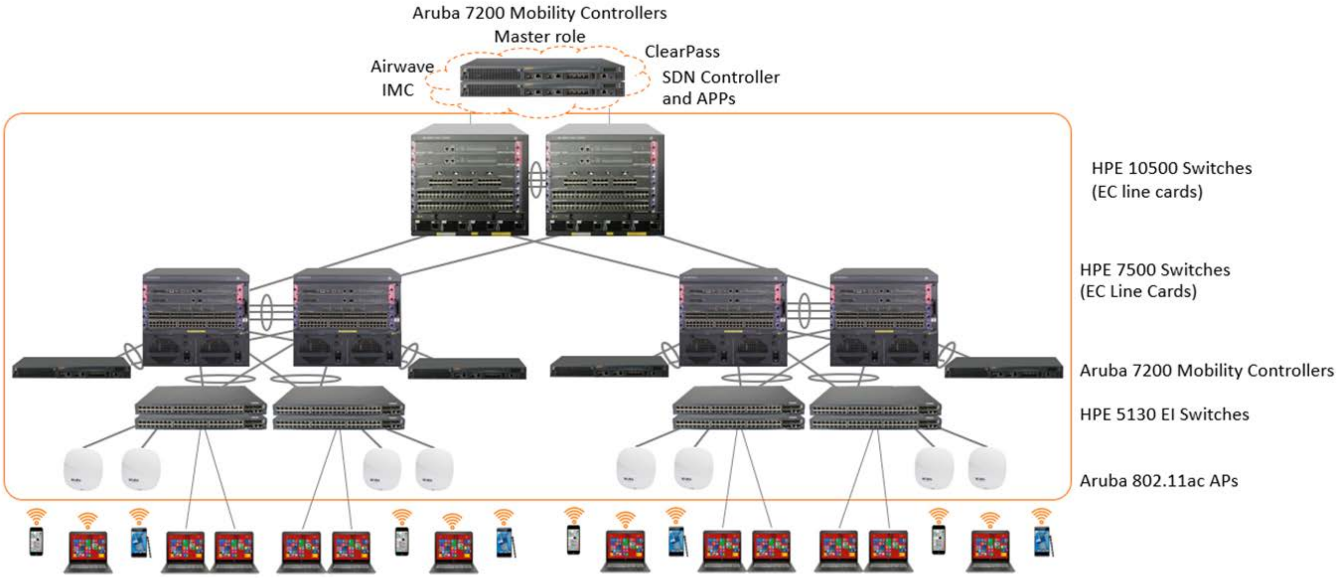


Figure 10. Traditional large campus

When the 10500 and 7500 switches are configured to create an IRF-fabric, they behave as a single device from every point of view – layer 2 through layer 7 – simplifying the LAN routing design. Any device that supports link aggregation can be connected to the IRF-fabric using a link aggregation group with member-ports on each 10500. Additionally device with an IP interface, a layer 3 switch, a router, a server, interacts with the IRF-fabric as if it were a single IP gateway, and a single IP routing or MPLS protocol neighbor/peer.

- Local mobility controllers

  Two (or more) Aruba 7200 Mobility Controllers are connected to the 7500 switches to provide the WLAN control set of functions and terminate the tunnels from the APs.

  These controllers operate in local mode and are bound to the master controllers located in the data center. For details see the Local mobility controllers section later in this chapter.

- Access switches

  Depending on the requirements, different types of access switches can be deployed. They can be summarized in 3 categories: layer 2 / stackable, layer 3 / stackable, and layer 3 / modular. The product lines recommended in each case are:

  - layer 2 stackable: HPE FlexNetwork 5130 EI Switch Series
  - layer 3 or MPLS VPN-VPLS stackable: HPE FlexNetwork 5500 HI Switch Series
  - layer 3 or MPLS VPN-VPLS modular: HPE FlexNetwork 7500 Switch Series

  The first option is optimal in terms of cost. If routing or MPLS VPNs are required in the access layer, the second and the third options are recommended.

- Access points

Aruba 802.11ac access points are the main choice for the traditional campus. All WLAN control and data traffic is tunneled back to the local controllers. Wireless client traffic is then converted into Ethernet frames, and forwarded to the wired LAN.

Additional campus components

In addition to the components recommended in the reference designs, network administrators may consider:

- HPE VSR, MSR or HSR routers for the campus WAN edge

- HPE TippingPoint Next Generation Firewall
- HPE TippingPoint IPS
- HPE VAN/SDN controller and SDN apps (located in the data center or in the campus)
- HPE IMC and IMC modules (located in the data center or in the campus)

Local Mobility Controllers

The local mobility controller manages logically attached APs and handles user sessions on the network. The locals process the majority of the traffic on the network. When the locals manage CAPs, the locals are typically deployed either in the distribution layer or network data center, depending on the distribution of traffic in the enterprise. In the case of RAPs, branch office controllers (BOCs), and Virtual Intranet Access™ (VIA™) agents, the locals are typically located in the network DMZ. In some networks, the DMZ mobility controllers may be stand-alone masters that also provide local functionality.

Local controllers are responsible for the following functions in the WLAN:

- AP, AM, and SM configuration, management, and software updates
  All Aruba APs are dependent APs, which means they do not, in most instances, store configuration settings in the way that a traditional autonomous AP would. Instead, at boot time each AP downloads its current configuration from the local. When changes are made in the system configuration, they are automatically pushed to all APs. Whenever an AP boots, it will always have the current configuration, and changes are reflected immediately throughout the network. When the software on the mobility controller is updated, the APs automatically download a new image and upgrade themselves. This software check, like the configuration download, is part of the AP boot process, and it insures that each AP has the current operating image and configuration without user intervention.
- Device session termination
  An Aruba network is focused on the client devices. In the system a single user may have multiple devices, each with it's own sessions and profile. Device sessions are any information transmitted from a client device across the WLAN. Device sessions can include human users on a wireless device, wireless IP cameras, medical equipment, and scanner guns. Every user in an Aruba system is identified when they authenticate to the system (by WLAN, IPsec, or wired with captive portal), and their login (and optionally device) information is used to place the device in the appropriate role based on that login. The role of the device defines what that device, and ultimately the user, is allowed to do on the network. This definition is enforced by a stateful firewall, and a role-based policy is applied to every device.
- ARM assignments and load balancing
  Aruba ARM controls aspects of AP and client performance. All WLANs operate in unlicensed space, so the chance that something will interfere with transmissions is very high. Aruba has developed a system to work around interference automatically and help clients have a better operating experience. These features include automatically tuning the WLAN by configuring AP power and channel settings, as well as scanning for better channels and avoiding interference. ARM also handles AP load balancing and co-channel interference from other APs and clients. Airtime fairness ensures that slower speed clients do not bring down the throughput of higher-speed clients. Using band steering, when the system detects a client that is capable of operating on the 5 GHz band (the majority of modern clients), the system automatically attempts to steer that client to the cleaner band. More information on ARM can be found in Aruba 802.11n Networks VRD available at http://www.arubanetworks.com/vrd.
- RFProtect™ security enforcement and blacklisting
  While the master handles the processing of security event information, the local directs the actions of the AMs for enforcement of wireless security policy. Enforcement can take different shapes, including containing rogue APs by performing denial-of-service (DoS) attacks wirelessly, ARP cache poisoning on the wire, shielding valid clients from connecting to rogue APs, and blacklisting clients so that they are unable to attach to the WLAN.

- RFProtect spectrum analysis
  When an AP is performing spectrum scanning, the visualizations of the RF data are generated on the local. This data is pushed to the client's web browser and can be saved for later analysis.
- CPsec AP certification
  When CPsec is enabled in the WLAN, the AP and local mobility controller establish an IPsec tunnel between the two devices using certificates. The local is responsible for issuing these certificates and adding APs to the white list. When the AP boots up and tries to contact the local, the certificates are used to build an IPsec tunnel between the devices.
- Mobility
  Supports Layer 2 (VLAN) mobility and Layer 3 (IP) mobility, which allows users to roam seamlessly between APs on different mobility controllers without session interruption. This mobility is a key component to support VoIP sessions, where sessions must be preserved.
- Quality of service (QoS)
  The locals support QoS on the wired and wireless side. This support includes translating DiffServ and ToS bits set on packets into Wi-Fi Multimedia™ (WMM®) markings and back. The Aruba Policy Enforcement Firewall™ (PEF™) also allows the administrator to mark packets with the appropriate level of QoS, and to change markings on packets entering the system.

Local controller redundancy

The local controllers at the aggregation layer also use VRRP instances to provide redundancy. However, a different redundancy model called active-active redundancy is used. In this model, the two local controllers terminate APs on two separate VRRP VIP addresses. Each Aruba controller is the active local controller for one VIP address and the standby local controller for the other VIP. The controllers share a set of APs and divide the load among them. The APs are configured in two different AP groups, each with a different VIP as the LMS IP address.

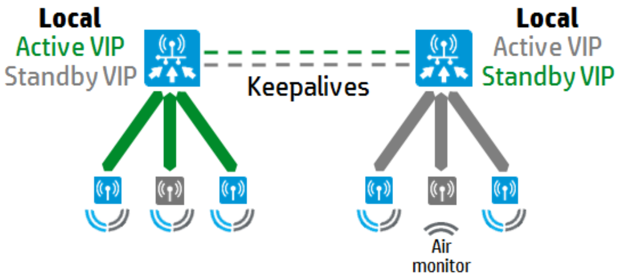


Figure 11. Active-active redundancy

When an active local controller becomes unreachable, the APs that are managed by that controller fail over to the standby controller for that VRRP instance. Under these conditions, one controller terminates the entire AP load in the network. Therefore each controller must have sufficient processing power and licenses to accommodate all of the APs that are served by the entire cluster. Though the controllers are designed to support 100% capacity, do not load the mobility controllers past the 80% capacity so that the network is more predictable and allows headroom. Aruba recommends that each mobility controller be run at only 40% capacity, so that when a failover occurs, the surviving mobility controller carries only an 80% load. This load gives the mobility controller the room to operate under the failover conditions for a longer period of time.

In this model, preemption should be disabled so that APs are not automatically forced to fail back to the original primary controller after it recovers. Whenever an AP fails over to a different controller, all the clients served by that AP get disconnected. So if a controller malfunctions and reboots constantly, then the APs served by that controller will "flap" between the original controller and standby controller if preemption is enabled. When preemption is disabled, the network administrator has sufficient time to troubleshoot the issue without this ping pong effect. The APs do not automatically fail back to the original controller, so this model requires that the mobility controller is sized appropriately to carry the entire planned failover AP capacity for an extended period of time.

Aruba 802.11ac APs

Another key component of the Mobile-first solution is the Aruba access point (AP). Aruba offers a variety of 802.11ac AP models:

- for indoors: 320 series, 220 series, 227 APs (ruggedized), 210 series, 200 Series, and 205H series
- for outdoors: 270 series

Aruba 802.11ac wireless access points can be deployed as controller-managed or controller-less Aruba Instant APs depending on the design, scope and scale of your wireless network. The 802.11ac Wave 2 APs come with multi-user MIMO aware ClientMatch to boost network efficiency.

Aruba APs support a variety of common features:

- Aruba AP operating modes
  - Controller-managed AP or Remote AP (RAP) running ArubaOS. When managed by Aruba Mobility Controllers, 228 APs offer centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding
  - Aruba Instant AP running InstantOS. In Aruba Instant mode, a single AP automatically distributes the network configuration to other Instant APs in the WLAN. Simply power-up one Instant AP, configure it over the air, and plug in the other APs – the entire process takes about five minutes
  - Spectrum analysis identifies sources of RF interference
  - Air monitor provides wireless intrusion protection
  - Hybrid AP serves Wi-Fi clients and provides wireless intrusion protection and spectrum analysis
  - Secure enterprise mesh
- ClientMatch Technology
  - Eliminates sticky clients by continuously gathering session performance metrics from mobile devices. This information is then used to steer each mobile device to the best AP and radio on the WLAN
  - Extends the client steering technology with MU-MIMO client awareness. This feature automatically identifies MU-MIMO capable mobile devices and steers those devices to the closest MU-MIMO capable Aruba access point. If a mobile device moves away from an AP or if RF interference impedes performance, ClientMatch automatically steers the device to a better AP
- Advanced Cellular Coexistence (ACC)
  - Aruba's Advanced Cellular Coexistence (ACC) feature enables WLANs to perform at peak efficiency by minimizing interference from 3G/4G LTE networks, distributed antenna systems and commercial small cell/femtocell equipment

The following two tables include a summary of the Aruba 802.11ac APs and their main features.

Table 2. 802.11ac APs summary

Indoor 802.11ac APs	320 Series	220 Series	210 Series	200 Series
Models	AP-325 / AP-324	AP-225 / AP-224	AP-215 / AP-214	AP-205 / AP-204
Max data rate 5 GHz band	1.733 Mbps	1.300 Mbps	1.300 Mbps	875 Mbps
Max data rate 2.4 GHz band	800 Mbps	600 Mbps	450 Mbps	300 Mbps
Integrated omnidirectional antennas	AP-325: 8	AP-225: 6	AP-215: 6	AP-205: 4
RP-SMA connectors for ext. antennas	AP-324: 4	AP-224: 3	AP-214: 3	AP-204: 2
Mu-MIMO streams	3x3:3	n/a	n/a	n/a
Su-MIMO streams	4x4:4	3x3:3	3x3:3	2x2:2
Operating modes	All	All	All	All
ClientMatch technology	Yes	Yes	Yes	Yes
Advanced Cellular Coexistence (ACC)	Yes	Yes	Yes	Yes
Integrated Bluetooth Beacon	Yes	No	No	No
More information	Data sheet Ordering guide	Data sheet Ordering guide	Data sheet Ordering guide	Data sheet Ordering guide

Table 3. Specialized 802.11ac APs summary

Indoor 802.11ac APs	205H AP	228 AP	270 Series
Positioning	Hospitality Includes 3 GbE access ports, PoE out and a USB host interface	Extreme indoor environments: Warehouse Industrial freezer	Outdoors Extreme high and low temperatures, persistent moisture and precipitation
Models	205H AP	228 AP	AP-275, AP-274, AP 277
Max data rate 5GHz band	867	1.300 Mbps	1.300 Mbps
Max data rate 2.4 GHz band	400	600 Mbps	600 Mbps
Integrated omnidirectional antennas	4	n/a	AP-275: 3
RP-SMA connectors for external dual-band antennas	n/a	6	AP-274: 3
Integrated 80° H x 80° V antennas	n/a	n/a	AP-277: 3
MIMO streams	2x2:2	3x3:3	3x3:3
Operating modes	All	All	All
ClientMatch technology	Yes	Yes	Yes
Advanced Cellular Coexistence (ACC)	Yes	Yes	Yes
Integrated Bluetooth Beacon	Yes	No	No
More information	Data sheet Ordering guide	Data sheet Ordering guide	Data sheet Ordering guide

Wired infrastructure

HPE offers a variety of switches for the access layer that support SDN and SDN applications. Depending on the network requirements, different switches can be chosen.

Table 4. Mobile-first campus switches

Type	Product series
Stackable access switches	Aruba 2920 Switch Series
Advanced stackable access switches	Aruba 3800 Switch Series
Advanced modular access/aggregation/small core switches	Aruba 5400R zl2 Switch Series
Large core and aggregation switches	HPE FlexNetwork 10500 Switch Series

The following are some of the factors to take into account when choosing the right access switches.

- Form factor: modular or stackable switches
- Stack size: up to 4 or up to 10
- Uplinks: Access switches need to be connected to both members of a switch pair in the next layer—aggregation or core. However, in many cases, having two uplinks per access switch may not be necessary. A stack of access switches can share the uplinks and make better use of them

The Aruba 5400R zl2 switch series is an excellent solution for the core of a small campus and large branches.

The HPE FlexNetwork 10500 switch series offers enterprise class capacity, performance and features ideal for the core and aggregation layers of large campus networks.

Aruba 2920 Switch Series

The HPE 2920 Switch Series consists of four switches: the HPE 2920-24G and 2920-24G-PoE+ Switches with 24 10/100/1000 ports, and the HPE 2920-48G and 2920-48G-PoE+ Switches with 48 10/100/1000 ports. Each switch has four dual-personality ports for 10/100/1000 or SFP connectivity.

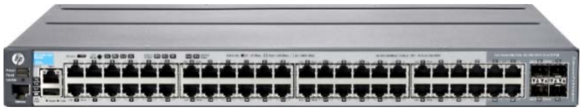


Figure 12. Aruba 2920 switch

The HPE 2920 switch series consist of 5 switches with a number of accessories, stacking module, and stacking cables:

- HPE 2920-24G switch
- HPE 2920-48G switch
- HPE 2920-24G-PoE+ switch
- HPE 2920-48G-PoE+ switch
- HPE 2920-48G-PoE+ 740W switch

The 2920 series has the following main features:

- Support for OpenFlow and SDN
- Support for basic routing: static and RIP
- Stacking
  The HPE 2920 switch stacking technology ensures chassis like scalability and resiliency in a flexible stackable form factor with plug and play functionality and the stack appears as a single switch entity simplifying stack management. This

technology allows simple software updates by updating a single stack switch and all other stack switches will be upgraded automatically. The 2920 stacking technology supports chain and ring topologies of up to 4 switches.

Aruba 3800 Switch Series

The HPE 3800 switch is a high-performance, low-latency campus access switch solution that is fully managed and supports a rich layer 2-4 feature set to ensure a high quality converged application delivery. Utilizing the HPE 3800 FlexChassis Mesh technology and dual redundant power supplies a highly resilient solution can be achieved. The HPE 3800 switch is covered by a lifetime warranty.

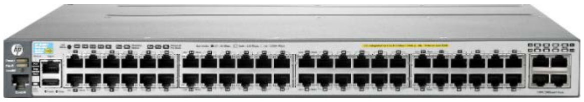


Figure 13. Aruba 3800 switch

The HPE 3800 switch series consist of 9 switches with a number of accessories, including power supplies, fan tray, stacking module, and stacking cables. There are five 24 port products and four 48 port products:

- HPE 3800-24G-2XG Switch
- HPE 3800-24G-2SFP+ Switch
- HPE 3800-24G-PoE+-2XG Switch
- HPE 3800-24G-PoE+-2SFP+ Switch
- HPE 3800-48G-4XG Switch
- HPE 3800-48G-4SFP+ Switch
- HPE 3800-48G-PoE+-4XG Switch
- HPE 3800-48G-PoE+-4SFP+ Switch

The 3800 series has the following main features:

- Support for OpenFlow and SDN
- Support for advanced routing: OSPF and BGP
- Meshed stacking
  The HPE 3800 switch mesh stacking technology ensures chassis like scalability and resiliency in a flexible stackable form factor with plug and play functionality and the stack appears as a single switch entity simplifying stack management. This technology allows simple software updates by updating a single stack switch and all other stack switches will be upgraded automatically. The FlexChassis Mesh technology supports the following topologies:
  - chain and ring topologies: up to 10 switches
  - fully meshed topology: up to 5 switches.

Aruba 5400R Switch Series

The 5400R switch series offers a set of features that positions it as a next generation campus product. The 5400R v3 zl2 modules this product line are based on the HPE Networking 6th Generation ASIC, a programmable device that allows for the development of new features using the same hardware.

This product series includes two chassis: 5406R and 5412R.

The 5400R has the following features:

- SmartRate 1/2.5/5/10Gbps Ethernet ports
  Enables the next generation of 802.11ac Wave 2 APs with 2.5GbE / PoE+ connections and investment protection for future 5Gbps APs.

Figure 14. Aruba 5400 switch

- Up to 288 PoE+ ports
  288 PoE+ 1GbE ports providing at 30W/port on a single 12 slot chassis
- MACsec
  Hardware-supported on all v3 modules except for 40GbE SFP+ ports. Available in the next software version
- 40GbE modules (Line rate)
- 2 PORT 40GbE QSFP+
- 20 GbE port + 1 40GbE QSFP+ port
- Fully-flexible OpenFlow
  FFOF allows for the development of new SDN features

HPE FlexNetwork 10500 Switch Series

This product series includes four chassis: 10504, 10508, 10508V and 10512.

The following are some of the advantages of the 10500 series

- Independent fabric modules
  The 10500 switch fabric modules are independent from the chassis management modules. Up to four fabric modules located in the back of the chassis offer high bandwidth for inter line card traffic.

Figure 15. HPE 10500 switch

- Performance and capacity

A 10512 chassis has a maximum capacity of 576 10GbE ports, 96 40 GBE ports, or 16 100GbE ports operating at line rate.

- Intelligent Resilient Framework (IRF)
  Up to 4 HPE 10500 chassis can be aggregated to form a single IRF-fabric.
  When IRF is deployed at the core and/or aggregation layers, it simplifies the design, installation, configuration, maintenance, and troubleshooting of the whole network.

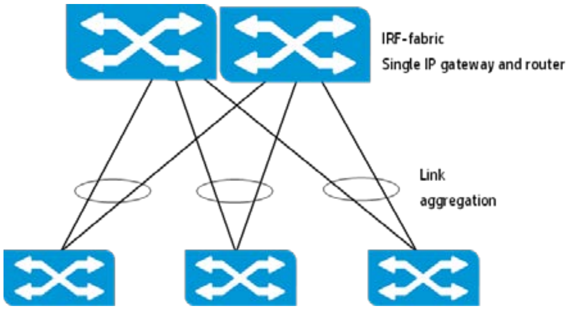


Figure 16. Optimized core/aggregation layer

In a traditional design for a 2-tier LAN, for example, to support switch-level redundancy at the core there is a need to include complex redundancy technologies like either the combination of MSTP and VRRP. MSTP offers Layer 2 (link) redundancy and loop protection while VRRP offers Layer 3 gateway redundancy. An alternative solution is to deploy a routing protocol at the access layer.

- Orthogonal chassis architectures

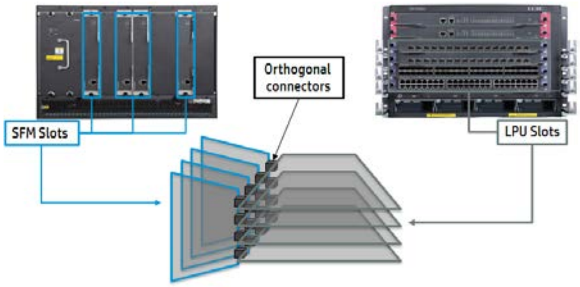


Figure 17: Orthogonal architecture

The 10500 orthogonal architecture offers direct connections between each line card and the fabric modules. Each connection operates at 40Gbps for a total capacity of 160 Gbps per line card slot.

MOBILE-FIRST CONTROLLER-BASED BRANCH

The mobile-first branch can be implemented by deploying a new family of mobility controllers: Aruba 7000 Cloud Controllers. These can run in both master and local mode as the 7200 controllers described in the data center and campus sections of this document. However, the cost of sending an engineer to deploy the controller the each branch is too high for many enterprises.

To address this issue, Aruba has created a third operation mode for the 7000 controllers: branch mode. This mode greatly simplifies the deployment of the whole branch. The controller can be connected directly to the router and automatically receive its full configuration from the master controller in the data center. The controller, once configured, can establish a tunnel to the master controller in the data center, for example for employees to access the corporate applications and data. Additionally the controller becomes the DHCP server for the whole branch.

Reference design

Figure 12 shows the recommended layout of a mobile-first controller-based branch. In this model, a switch stack is connected to the controller while the controller acts as the gateway for the whole branch.

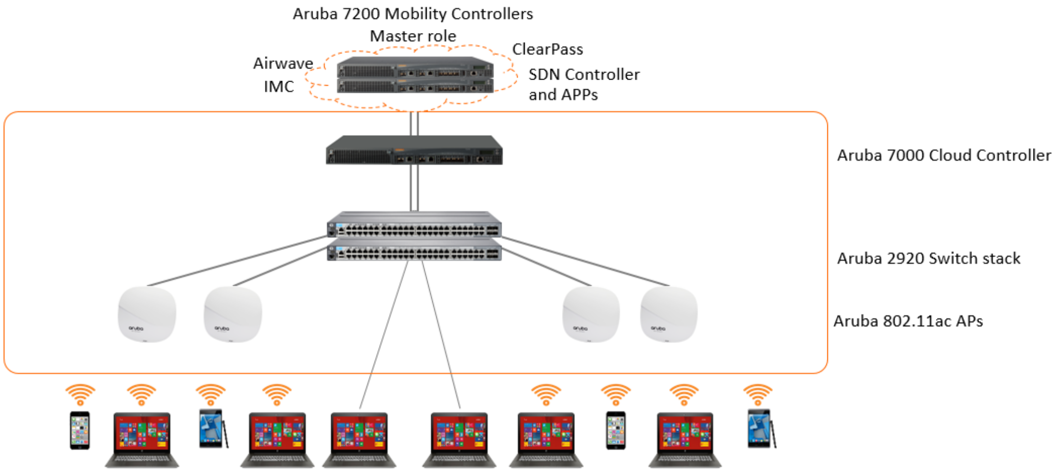


Figure 18. Mobile-first controller-based branch

Important: Only Aruba 7200 Mobility Controllers can adopt, configure and manage a branch controller and only Aruba 7000 Cloud Service Controllers can operate in branch mode.

Zero-touch deployment

One of the most interesting features of Aruba 7000 controllers is the provisioning function. In the case of a controller provisioning refers to the process of its adoption by the master controller in the data center. Branch controllers can be provisioned in three ways

- ZTP or Zero Touch Provisioning
  This provisioning method does not require the intervention of an administrator to facilitate the adoption by the master controller. There are two methods for ZTP: DHCP or Aruba Activate.
- ZTP via DHCP
  In order to use ZTP the last port of the 7000 series controller is configured on VLAN 4094 with DHCP Client (while in factory default state). The Aruba Branch Controller on boot-up in from factory default state sends a DHCP request on the last port with Option 60 set to "ArubaMC" Assuming the DHCP server is configured to respond to the Option 60. it will send a DHCP Response back with Option 43 set to the master controller's IP and country code for the Branch.

- ZTP via Activate
  Activate is a provisioning service for Aruba devices located in the public cloud.
  If the DHCP server cannot be configured with Option 43, an alternative method can be used i.e. Activate. The Branch controller in its factory default state is configured to communicate with Activate if DHCP options are not available. The controller will try and resolve "device.arubanetworks.com" over HTTPS 443.
  Note: the firewall should be configured to permit HTTPS 443.
- Mini-setup – This is done over the serial console of the controller
  If DHCP Options is not available and the cloud-based Activate service is not an option, the admin can use the mini-setup mode. This will require the admin to use the serial console of the controller and thus will be touching every controller. When using mini-setup, it is assumed that the controller is in branch mode. The process asks only for two parameters. The Master IP and Country Code.
- Full-setup – If the admin would like to use a different port, VLAN, Static IP etc. for the controller, then the manual or full-setup mode can be used. In this mode the admin has the flexibility to configure the controller the way he/she likes.
  After the branch controller has been provisioned, it is ready to receive its configuration. Aruba 72xx series controllers have a specific profile type called Branch Config Group. This profile has all the information needed configure a remote branch controller.

VPN

The branch controller can be used to configure a VPN to the master controller and provide a simple way of connecting the branch to the data center. Selected VLANs can be bound to this VPN to route their traffic to the data center, while traffic on other VLANs is routed by the switches and the branch router for local and Internet connectivity.

Branch wired network

HPE offers a variety of enterprise class switches for the branch that support SDN and SDN applications. Depending on the network requirements, different switches can be chosen. They can be summarized in 3 categories: layer 2 stackable, layer 3 stackable, and layer 3 modular. The product lines recommended in each case are:

- layer 2 stackable: Aruba 2920 Switch Series
- layer 3 stackable: Aruba 3800 Switch Series
- layer 3 modular: Aruba 5400R Switch Series

The first option is optimal in terms of cost, while the third can be required in those cases in which MultiGig Ethernet/Aruba SmartRate ports are required. Finally, if routing is required in the access layer, the second and the third options are recommended.

MOBILE-FIRST INSTANT BRANCH

Aruba offers a very effective solution for small to medium size branches called Aruba Instant. In the Instant solution there is no physical controller, instead the first Instant AP (IAP) that comes up becomes a virtual controller for itself and the rest of the IAPs. The IAP running the virtual controller is called the master AP. Up to 128 IAPs connected to the same VLAN form an Instant Cluster managed by the virtual controller on the master AP.

There are two fundamental difference between the Instant and the controller-based solutions.

1. By default, the client traffic is forwarded to the wired LAN directly out of each IAP
2. Master controllers cannot manage Instant Clusters. The Virtual Controller can be configured via its web interface, by Aruba Airwave in the data center, or by Aruba Central in the public cloud.

Additionally, to provide a direct and secure path to the corporate applications, the master AP can establish a VPN with the master controller.

Reference design

Figure 13 shows the typical design for an Instant branch.

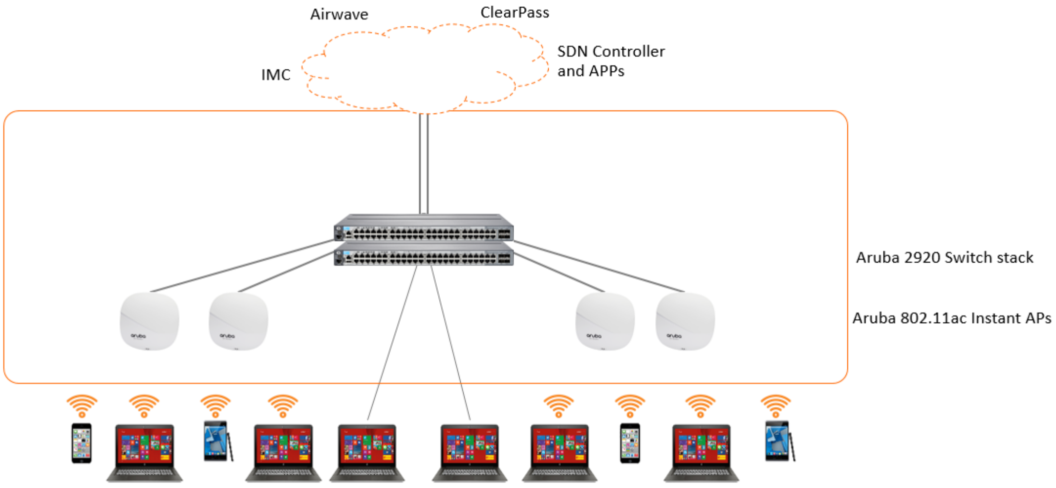


Figure 19. Mobile-first Instant branch

WLAN

Aruba Instant consists of a family of high-performance controller-less Instant Access Points (IAPs) that run the Aruba InstantOS to provide a distributed WLAN system. In an Instant deployment, all IAPs on the same Layer 2 domain form a cluster with one dynamically-elected AP that functions as the master. The master AP assumes the role of virtual controller (VC) within a cluster. Aruba Instant is a distributed WLAN system with a completely distributed control and data plane. However, certain network functions, such as monitoring, firmware management, and source Network Address Translation (NAT) require a central entity within a cluster. The VC within a cluster functions as this central entity. In an Aruba Instant cluster, if the master fails, another AP is elected as the master and assumes the role of VC.

In general, you can divide the functions of a WLAN system into three planes: the management plane, control plane, and data plane. Each Aruba Instant cluster handles the management, control, and data plane functions:

- Management plane – centralized
  Aruba Instant has a centralized management plane. At a cluster level, the self-elected VC functions as the single point of configuration for an IAP cluster. The graphical user interface (GUI) to the VC provides local configuration and monitoring

of an IAP cluster. Centralized configuration and management for multi-cluster networks are available using AirWave® or Aruba Central™ (public cloud).

- Control plane - distributed
  The control plane in an Aruba Instant cluster is completely distributed and handled by the individual IAPs. The distributed control plane functions include:
  - Adaptive Radio Management (ARM)
  - Auto Channel/Power assignment
  - Intrusion detection system (IDS)/ intrusion prevention system (IPS)
  - Client handover

  The VC is not responsible for any of these functions. For example, the client database is entirely maintained in the AP to which the client is connected. When a client roams, the new AP determines the last associated AP for the client and requests all client information from that AP. The other IAPs send updates to the VC IAP periodically, only for management plane reporting.
- Data Plane - distributed
  The data plane in an Aruba Instant cluster is also fully distributed, with a few exceptions. Each individual IAP handles the traffic for the clients that are associated to that IAP. Firewall policies and bandwidth control are also applied on a per-IAP basis. The flow of user traffic is not centralized to the VC. An exception to this rule is a magic VLAN (also known as a VC-assigned VLAN). On an SSID that uses a magic VLAN for its clients, all IAPs forward the traffic on that SSID to the VC, which performs NAT for the traffic. This process allows Layer 2 mobility for the VC-assigned VLAN. Similarly, any traffic that must be source NATed by the Aruba Instant cluster also flows through the VC. It is common to source NAT user traffic in remote deployments that have split-tunnel or bridging requirements.

Virtual controller

Aruba IAPs on the same Layer 2 domain form a cluster by electing one AP as the master AP, which functions as the virtual controller (VC).

If an AP is selected as the master and it assumes the virtual controller role, the master AP performs the VC function in addition to all the regular functions that are also performed by the member APs in the cluster. These functions are the VC functions of a master AP in an Aruba Instant cluster:

- Management plane functions of a virtual controller
  - Cluster configuration synching
    In an IAP cluster, only the master AP that functions as the VC needs to be configured. All other APs in the cluster download their configuration from the master AP. Any configuration change that is pushed from the management platform or configured over the GUI of the VC is synchronized to the other APs in the cluster.
  - Cluster monitoring
    In an IAP cluster, the VC assumes the monitoring role. All APs in the cluster periodically update the VC with their status. The VC consolidates all of this monitoring data, presents the data on its local WebUI, and pushes the data to management platforms, such as AirWave and Aruba Central.
  - Firmware image management
    The VC handles the image management in an IAP cluster. The VC ensures that all APs in the cluster are upgraded to the correct image version before rebooting the cluster.
  - Communication with management platforms
    Management platforms, such as AirWave and Aruba Central, communicate only with the VC of the cluster. The VC sends periodic updates of cluster monitoring data to the management platforms. Management platforms also push cluster

configuration changes to the VC, which, in turn, updates the other APs in the cluster.

- Control plane functions of a virtual controller
  - Dynamic RADIUS proxy (DRP)
    In an Aruba Instant cluster, the initial client authentication is handled by the AP to which the client is connecting to and not by the master AP. This means that you must add each AP in an Aruba Instant as a NAS client on a RADIUS server. In certain environments, you might not want to add each AP as a NAS client. DRP makes the VC the proxy for RADIUS exchanges. When you enable DRP, all APs in a cluster forward RADIUS exchange messages to the VC, which acts as a RADIUS proxy. For more information, see Dynamic RADIUS Proxy.
  - Handling Change of Authorization (CoA)
    The RADIUS protocol, which is defined in RFC 2865, does not support unsolicited messages that are sent from a RADIUS server to a network access server (NAS). However, in certain circumstances, session characteristics might need to be changed without requiring the NAS to initiate the exchange. The extensions that are defined in RFC 3576 allow a RADIUS server to send unsolicited disconnect or CoA messages to a NAS. In an Aruba Instant cluster, the RADIUS server sends RFC 3576 compliant messages to the VC, which then performs the necessary action.
  - DHCP server for client VLANs
    When you configure the Aruba Instant cluster as the DHCP server for a specific client VLAN, the DCHPE server functions are handled by the VC.
- Data plane functions of a virtual controller
  - Handling traffic for magic VLANs and VLANs that are local to the Aruba Instant cluster
    When you set up an SSID on an Aruba Instant network, client IP address assignment can be set to the VCassigned option. (This configuration is also referred to as a magic VLAN.) If you select this option, the client obtains its IP address from the magic VLAN of the master AP (that is, the VC). A magic VLAN is a private subnet that is created on the master AP for client IP address assignment. A magic VLAN differs from a traditional VLAN. The client traffic on a magic VLAN is always source NATed by the master AP and the master AP functions as the DHCP server for magic VLAN.
  - Handling traffic for VLANs that are local to the Aruba Instant cluster
    The Aruba Instant cluster lets you define VLANs such as local, centralized Layer 2, distributed Layer 2, centralized Layer 3, and distributed Layer 3 VLANs. (For more information, see Understanding InstantVPN Modes and Configuring VLANs for Layer 2 Modes.) The DHCP definitions for these VLANs reside on the Aruba Instant cluster. The client traffic on these VLANs flows through the VC of the cluster. For more information about the traffic flow for these VLANs, see Traffic Flows in an Aruba Instant Cluster.
  - Handling traffic when source NATing is required
    In an Aruba Instant network, the VC performs source NATing of any client traffic that requires it.

Instant Access Points

The Aruba AP product line includes the traditional controlled-based APs, Aruba Instant APs (IAPs), and remote APs (RAPs). Aruba controller-based APs start with part number AP-xxx, the IAPs with part number IAP-xxx, and RAPs with part number RAP-xxx. A controller-based AP that has the same model number (that is, the xxx in the part number) as an Instant-based AP has the same hardware specifications. For example, the controller-based AP with part number AP-135 has the same hardware specifications as the Instant-based AP with part number IAP-135. The key difference with an IAP is that it ships with Aruba InstantOS and, if needed, can be converted to a controller-based AP. All new RAP models also ship with Aruba InstantOS and, if needed, can be converted to controller-based RAPs.

Important: Controlled-based AP (for example, the AP-135) cannot be converted to an Instant-based AP.

Aruba Instant provisioning

As stated above, Aruba Instant has a centralized management plane. At a cluster level, the self-elected VC functions as the single point of configuration for an IAP cluster. The graphical user interface (GUI) to the VC provides local configuration and monitoring of an IAP cluster. Centralized configuration and management for multi-cluster networks are available using AirWave® or Aruba Central™ (public cloud).

To provision a cluster administrators can choose between Aruba Activate service or DHCP Options. Through these options the cluster vc receives the necessary parameters to connect to either Aruba Central or to Airwave.

Aruba Instant VPN

The virtual controller or master AP can be used to configure a VPN to the master controller and provide a simple way of connecting the branch to the data center. Selected VLANs can be bound to this VPN to route their traffic to the data center, while traffic on other VLANs is routed by the switches and the branch router for local and Internet connectivity.

Branch wired network

HPE offers a variety of enterprise class switches for the branch that support SDN and SDN applications. Depending on the network requirements, different switches can be chosen. They can be summarized in 3 categories: layer 2 stackable, layer 3 stackable, and layer 3 modular. The product lines recommended in each case are:

- layer 2 stackable: Aruba 2920 Switch Series
- layer 3 stackable: Aruba 3800 Switch Series
- layer 3 modular: Aruba 5400R Switch Series

The first option is optimal in terms of cost, while the third can be required in those cases in which MultiGig Ethernet/Aruba SmartRate ports are required. Finally, if routing is required in the access layer, the second and the third options are recommended.

MOBILE-FIRST REMOTE OFFICE

A remote office is a working environment in which a single AP is enough to satisfy the connectivity needs. An additional switch can be required to connect certain devices as printers and IP phones.

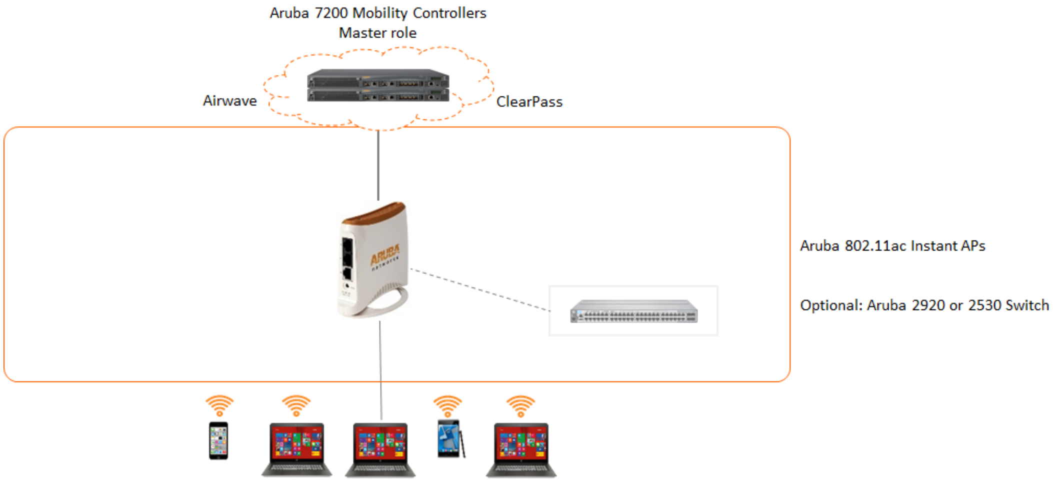

Aruba 7200 Mobility Controllers
Master role
Airwave
ClearPass
Aruba 802.11ac Instant APs
Optional: Aruba 2920 or 2530 Switch

Figure 20: Mobile-first remote office

WLAN

An Aruba Remote AP (RAP) extends the corporate LAN to any remote location by enabling seamless wired or wireless data and voice wherever a user finds an Internet-enabled Ethernet port or 3G cellular connection. RAPs are ideally suited for micro remote offices, home offices, telecommuters, mobile executives, and for business continuity applications.

Aruba RAPs typically terminate on the master mobility controllers in the network demilitarized zone (DMZ). Similar to the way that campus based APs and air monitors (AMs) are terminated, the mobility controllers terminate these remote devices coming in over the Internet with IPsec-protected sessions. This solution is designed to provide high availability. Redundancy may be configured at the controller, at the RAP, or in both places.

This solution assumes that a single RAP is necessary. If more APs are required, other solution should be considered: to deploy a branch controller or Aruba Instant.

Wired LAN

On any Aruba RAP that offers at least two Ethernet ports –and most of them do, the additional port can be configured for bridging or secure jack operation. This configuration provides maximum flexibility and allows for local wired access at remote sites. Just like a wireless SSID, the additional Ethernet ports on a RAP can be configured for all the authentication types and forwarding modes available. In a WLAN, a single SSID cannot be configured to provide 802.1X and MAC authentication simultaneously, but this limitation does not apply to a wired port. A wired port can be configured to provide 802.1X authentication and MAC authentication simultaneously, which allows better utilization of the available wired ports.

MOBILE-FIRST REMOTE CLIENT

Aruba Virtual Intranet Access (VIA)

VIA has two primary purposes:

- to provide secure corporate access to employee laptops and smartphones from anywhere
- to provide ease-of-use for the end users and network administrators

The ease-of-use is what differentiates VIA from other VPN solutions. VIA offers a zero-touch end-user experience and removes the complexity that is associated with configuring VPN clients on end-user devices. VIA provides ease-of-use not only for end users, but it also simplifies configuration and management for the IT team.

The Aruba VIA client that is available for Microsoft Windows computers (Windows XP, Vista, and Windows 7), Apple Mac OS X, Linux PCs, Apple iOS, and Android devices. It is a hybrid Internet Protocol Security (IPsec)/Secure Sockets Layer (SSL) VPN client.

If the user is connected to an untrusted network, the Aruba VIA client scans network connections and automatically establishes a secure connection back to the corporate network. Some additional features include Content Security Services (CSS), single-logon, SSL fallback when IPsec is blocked, and the ability to configure Wireless Local Area Network (WLAN) settings using the supplicant provided by the operating system.

NETWORK SOLUTIONS: WLAN ANALYTICS WITH ARUBA ALE

There are rich sources of client data on the network that are typically inaccessible to analytics engines that could derive meaningful business intelligence from seemingly random network activity. The data produced by these sources is worthless to the networking infrastructure, which consequently discards them. However it is priceless from the business point of view.

When a Wi-Fi enabled device comes within range of a wireless network it sends a message, called a “probe request,” asking for services available on the network. Probe requests are discarded by most Wi-Fi networks if the client device does not connect (associate) to the network. And yet, these simple transactions from unassociated client devices can yield important, business-relevant information. Broadly classified as “presence” information, probe requests can show how many people are near your network, how long they dwell there, and, if they leave and return, how recently, frequency, and timing of their visits.

Instead of discarding probe request and other context- and location-related information, it is essential to make them available to applications that can extract meaning and value. As a rule, the value of business intelligence is directly related to the infrastructure required to extract it. The higher the value, the more sophisticated the infrastructure that’s required to mine it.

The business intelligence derived from the Wi-Fi networks allows customers in verticals such as Retail, Hospitality, Transportation etc. to monetize their network using analytics and location tracking applications. The following are some common use cases of network monetization using business intelligence:

- Use dwell times and customer traffic insights (associated and un-associated clients) to feed into business intelligence and marketing decisions. E.g.: Determine "busy time" of the day for the store or a particular section and use that to make staffing decisions. Use traffic patterns to determine the impact of a particular promotion.
- Send push notifications to customers based on location for specific promotions and customer engagement. Eg: You enter a mall and get pushed notification of "Happy Hour" in a restaurant close to you or exclusive 20% off promotion in a specific store.
- Implement wayfinding to help customers find your store/restaurant/ or specific area for increased customer satisfaction and revenue opportunity. Eg: Improve patient satisfaction using wayfinding in hospitals to make it easier to look for a specific department or lab.

Public venues such as Airports, shopping centers and shopping malls can monetize the network by providing analytics and way finding services to their tenants.

The Aruba Analytics and Location Engine (ALE) works with Aruba WLANs to collect data about mobile devices presence data while protecting personal privacy. This data is then integrated with third-party analytics solutions that translate it into actionable business intelligence.

The solution only requires the deployment of the ALE server along with Airwave. In summary its components are:

- Aruba Access Points
- Controller (AOS 6.4.2.0) or Instant APs (6.4.2.0-4.1.1.0_46028)
- AirWave (v8.0.4)
- ALE (v1.3.0.0, build 46786)
- Analytics partner to integrate with ALE

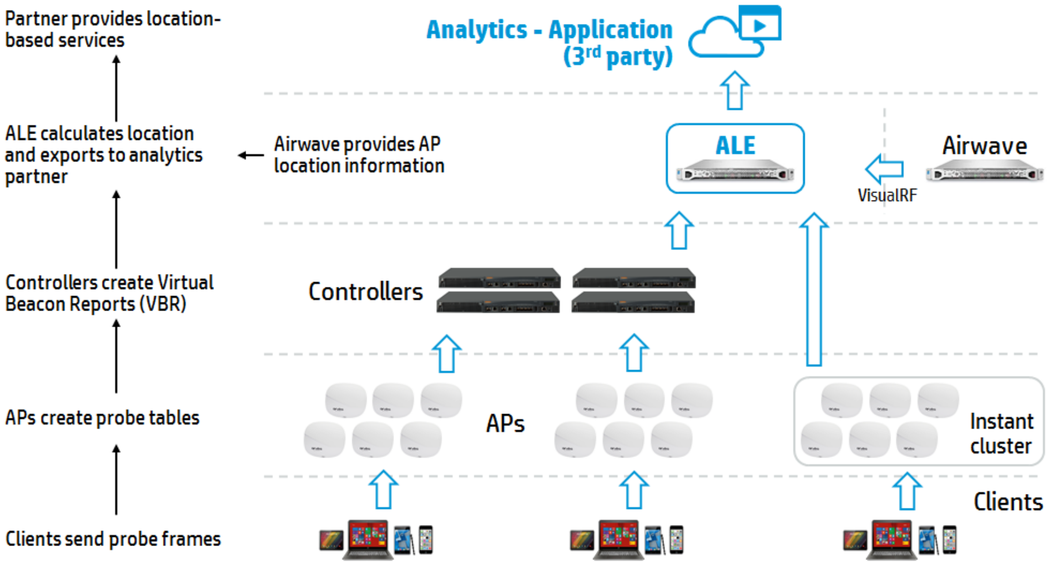

Partner provides location-based services
ALE calculates location and exports to analytics partner
Airwave provides AP location information
Controllers create Virtual Beacon Reports (VBR)
APs create probe tables
Clients send probe frames
Analytics - Application (3rd party)
ALE
Airwave
VisualRF
Controllers
APs
Instant cluster
Clients

Figure 21. ALE analytics architecture and process

Ale and privacy

One of the possible concern for customers who adopt analytics and other such applications is user privacy. User privacy is one of the most controversial topics and privacy restriction vary from country to country. So the ability for a system to support data anonymization is becoming more critical to avoid any possible legal issues.

ALE supports data anonymization. Anonymization is performed using a one-way hash of user media access control (MAC) address. Other Personally Identifiable Information (PII) such as IP address are nulled. Data anonymization is enabled by default on ALE. However, there are often applications/services such as Meridian that might not work with data anonymization. So, anonymization might have to be disabled for such applications/services. Applications/services that require non-anonymous data from ALE can provide anonymization after processing the non-anonymized data from ALE. In this case, the data anonymization if provided by the third party application/service rather than ALE.

Anonymization is enabled by default but can be disabled.

NETWORK SOLUTIONS: CUSTOMER ENGAGEMENT WITH ARUBA MERIDIAN

Unlike a hardware-only approach, the Aruba Networks Mobile Engagement Solution integrates best-in-class enterprise Wi-Fi and Aruba Location Services with self-service device onboarding and mobile app platforms into one integrated solution that's quick and easy to deploy.

- Aruba gigabit Wi-Fi – controller-managed and controllerless wireless LANs provide connection to all types of client devices
- ClearPass Guest securely connects visitors to Wi-Fi with a custom-branded device onboarding portal that offers targeted in-browser branding and advertising and encourages mobile app downloads
- Aruba's Meridian mobile app platform enables venues to quickly and easily create mobile apps or improve existing apps with features such as turn-by-turn directions within venues
- Aruba Location Services powered by Aruba Beacons integrate with the Meridian mobile app platform to enhance the visitor experience with location-aware features like a glowing blue dot on an indoor map and relevant push notifications based on a user's real-time location

The Aruba Mobile Engagement Solution leverages user, location, device and other contextual data to engage guests in a more meaningful way. This enables enterprise venues to deliver compelling, personalized information to their mobile devices while protecting their privacy.

Visitors who connect to a venue's Wi-Fi can specify their preferences so enterprise businesses know how they want to be engaged. And when they download a venue's custom-branded Meridian mobile app, they can opt-in to get personalized, location-relevant push notifications.

Meridian content management

In addition to delivering the back-end technology for guest mobile engagement, the Meridian platform includes the Meridian Editor content management system, which gives venues a quick and simple way to create and improve their own customized mobile apps.

A highly visual, cloud-based content management system, the Meridian Editor makes it easy to enter location-specific information like places of interest on a map, directions, onsite events, and services. This content encourages mobile-app users to explore and discover the venue.

With the Meridian Editor, enterprise venues can dramatically reduce the time and effort it takes to develop and maintain engaging, world-class apps for their guest's mobile devices.

Meridian powered client app

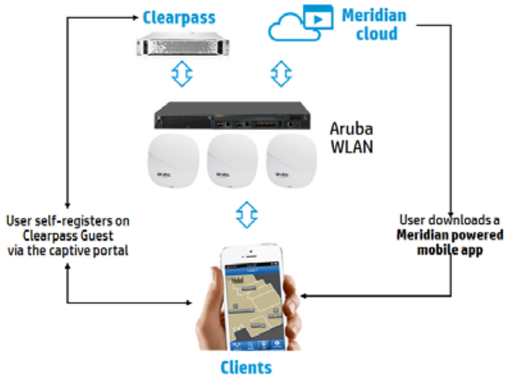

Clearpass
Meridian cloud
Aruba WLAN
User self-registers on Clearpass Guest via the captive portal
User downloads a Meridian powered mobile app
Clients

Figure 22. Aruba client registration and configuration

Once the app is available, when a visitor arrives at the venue and connects to Wi-Fi, a ClearPass self-registration portal page is presented on the mobile device. As part of the self-registration process, the visitor downloads the mobile app. The visitor now has access to both up-to date information on special offers, venue maps and a step-by step blue-dot navigation service.

Aruba Location Services powered by Aruba Beacons

Aruba Beacons are small Bluetooth devices that transmit beacons containing their ID at regular intervals. Aruba Beacons identify a visitor's location at a venue and work with Meridian-powered mobile apps to deliver many location-aware services to guest mobile devices, including:

- A glowing blue dot that shows the client's location on a map of the venue.
- Turn-by-turn directions to nearby amenities on the property.
- Push notifications with relevant content based on personal preferences.

One of the Bay Area's newest and largest sports stadiums leverages Aruba Beacons to dispatch location services to their customized mobile app so fans can get turn-by-turn directions to the nearest concessions, their seats and other places of interest.

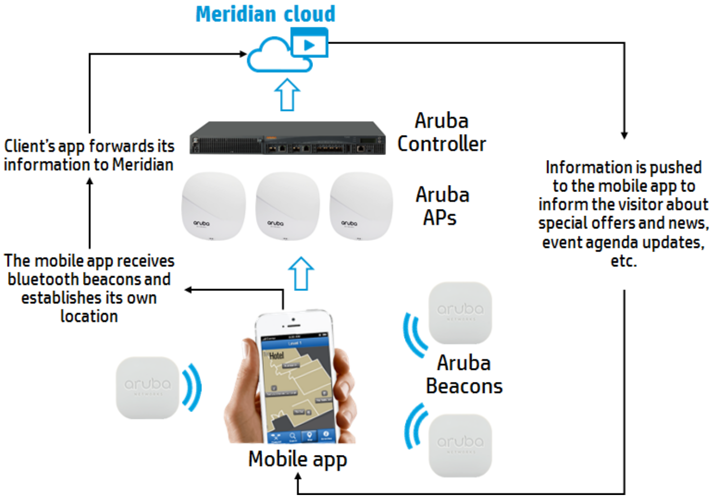

Meridian cloud
Aruba Controller
Client's app forwards its information to Meridian
Aruba APs
Information is pushed to the mobile app to inform the visitor about special offers and news, event agenda updates, etc.
The mobile app receives bluetooth beacons and establishes its own location
Aruba Beacons
Mobile app

Figure 23. Meridian location with Aruba Beacons

Aruba Beacons can be battery powered, low energy, devices or USB devices that can be connected to Aruba APs. In some new Aruba AP models, the USB beacon is integrated.

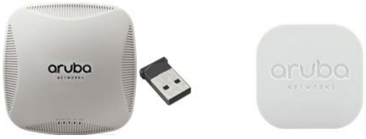


Figure 24. Aruba beacon types

One common application of the USB beacon is to transmit configuration updates to the standalone beacons.

NETWORK SOLUTIONS: CONTROLLING THE NETWORK WITH SDN

HPE Networking is leading the way in simplifying and transforming the network to meet your organization's needs for mobility, virtualization, high-definition video, rich-media collaboration tools, and cloud computing.

By embracing a software-defined network, it is possible to reap the full value of your network investment. SDN, delivered through our market-leading solutions, will help users and organizations experience applications as never before. It will free your IT administrators from the drudgery of manual network configuration and reconfiguration because the network will be automatically tuned to application and business needs.

The IT staff can focus more on the quality of the business experience, and spend less time managing the details of the underlying networking infrastructure.

HPE Virtual Application Networks (VAN) SDN Controller

HPE Virtual Application Networks (VAN) SDN Controller Software provides a unified control point in an OpenFlow-enabled network, simplifying management, provisioning, and orchestration. This enables delivery of a new generation of application-based network services. It also provides open application program interfaces (APIs) to allow third-party developers to deliver innovative solutions to dynamically link business requirements to network infrastructure via either custom Java programs or general-purpose RESTful control interfaces.

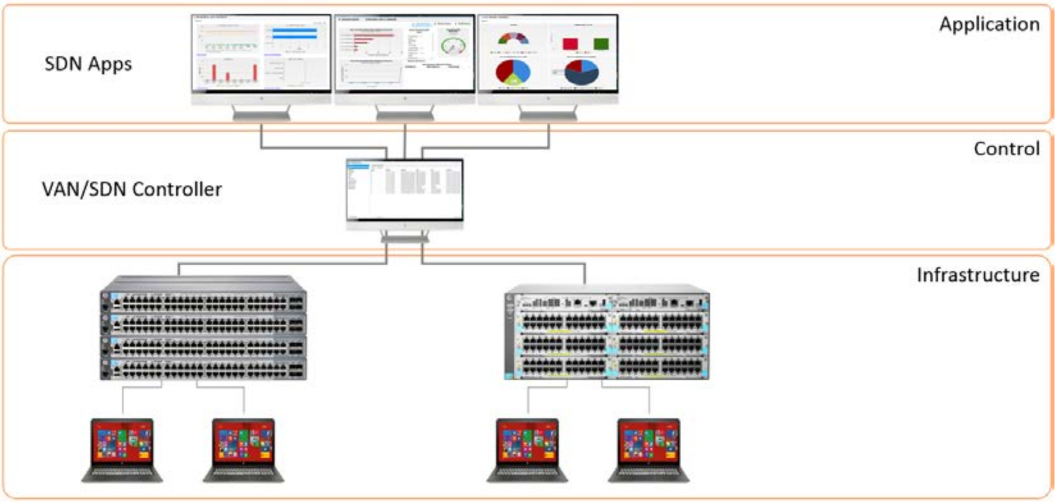


Figure 25. SDN architecture

The VAN/SDN Controller is designed to operate in campus, data center, and service provider environments. It offers:

- Enterprise-class platform for the delivery of a broad range of network innovations
- Compliant with OpenFlow 1.0 and 1.3 protocols
- Support for over 50 OpenFlow-enabled HPE switch models
- Open APIs to enable third-party SDN application development
- Extensible, scalable, resilient controller architecture

There are three campus specific HPE SDN apps available: SDN Network Protector, SDN Network Optimizer, and SDN Network Visualizer. As the SDN controller is an open environment several vendors have created their own applications.

With this solution, it is possible to get the benefits of SDN without re-architecting and existing network. This is accomplished with a hybrid deployment where SDN is used to provide enhancements while allowing traditional technologies and protocols to forward traffic throughout the network. The benefit of this is that it is only necessary to deploy OpenFlow enabled switches at the edge or access of a network.

Integrating Aruba WLAN and HPE VAN/SDN solutions

To provide an additional level of control, customers may want to deploy the HPE VAN/SDN solution in their networks. This OpenFlow based solution allows networks to react to traffic conditions and application access requests in real time, by deploying new or adjusting existing security and QoS policies.

The mobile-first network architecture allows to deploy the SDN solution combined with Aruba WLANs. To enable such a combination, the following network building block has been defined and it is the basis for mobile-first campus network designs. APs can be connected to the access switches or directly to the aggregation switch. This second topology takes advantage of the SmartRate ports of the 5400R switch and is ready for the next generation of APs with 2.5 GbE ports.

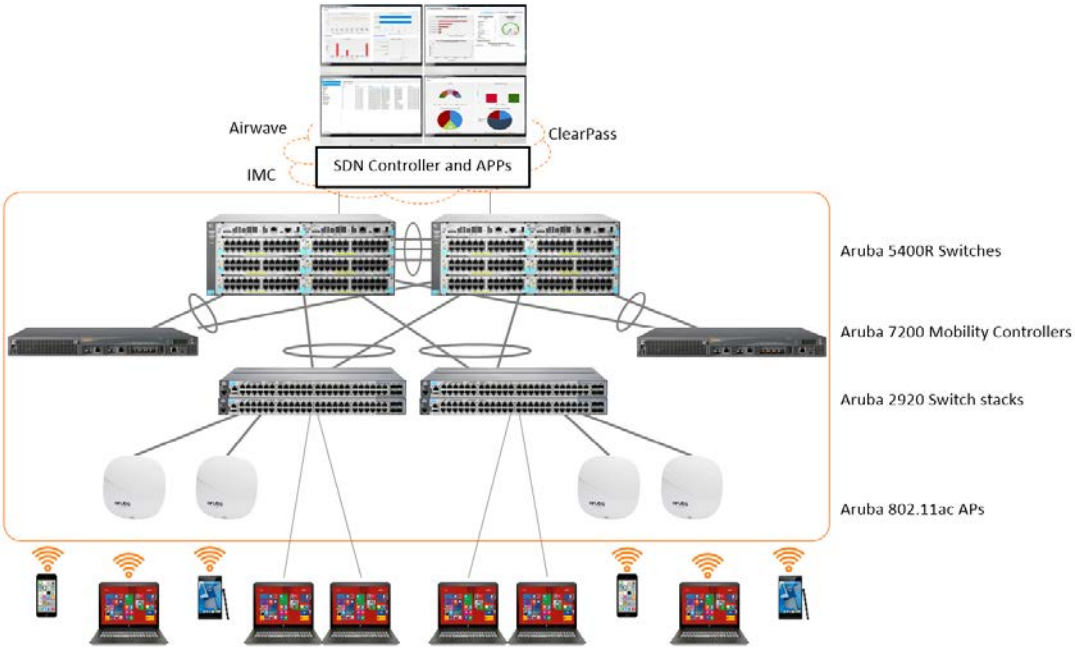


Figure 26. Mobile-first campus building block

The benefits of this design are:

- Scalability: as the local controller are connected to the aggregation/distribution switches, they would manage a smaller number of APs and clients than if connected directly to the core.
  Depending on the geographical distribution, each block can provide connection up to over 1000 clients.
- Support for future SmartRate APs: APs can be directly connected to 5400R zl2 v3 SmartRate ports, supporting 1/2.5/5Gbps Ethernet links.
- SDN support: In both cases, the wired and wireless client traffic converges on one or two HPE 5400R zl2 switches with v3 modules. This switching platform is the optimal SDN enforcement device due to its latest generation ASIC and the support of Fully Flexible OpenFlow.

HPE Network Protector SDN Application

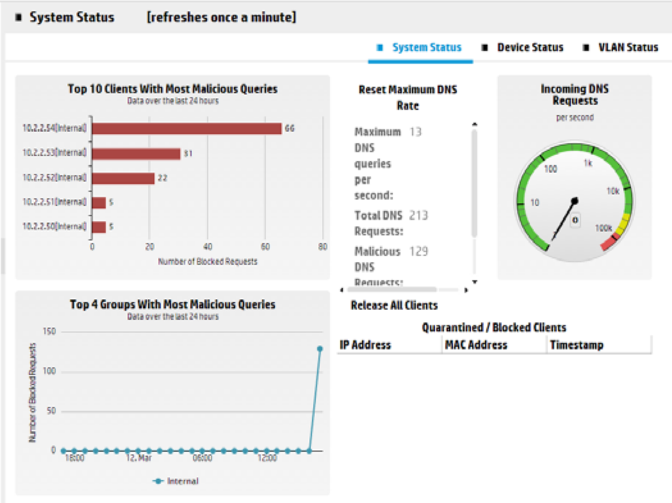
Network Protector was developed out of the continued need to enhance network security.

The HPE Network Protector SDN Application stops threats at the network access layer before they can cause damage. Network Protector can be used in any network environment where security is a concern, including the BYOD, data center and cloud computing environments. HPE envisions a network where Network Protector can be implemented on any network device anywhere in the network for unprecedented network visibility, event correlation accuracy, and security control.

HPE Network Protector features include:

- Runs on HPE Virtual Application Networks (VAN) SDN Controller
- Consumes real-time reputation security intelligence from the HPE TippingPoint DVLabs cloud service
- Protects from over 1,000,000 botnets, malware, and spyware malicious sites
- Provides native integration for improved visibility and accuracy with ArcSight solutions
- Uses OpenFlow-enabled switches to detect malware and botnets
- Has the ability to implement a custom whitelist and blacklist
- Has dynamic switch learning with HPE OpenFlow-enabled switches, which distributes detection into the switch infrastructure
- Provides security enforcement decision feedback with the HPE Intelligent Management Center

The value of the HPE Network Protector SDN Application is in pushing security to the access layer of a network without requiring additional hardware. It is not economically feasible to deploy an IPS between every access layer edge port and every network host. It is also desirable to block malicious traffic as close to the source as possible. Network Protector solves each of these issues.



Maximum DNS queries per second: 13

Total DNS Requests: 213

Malicious DNS Requests:129

Quarantined / Blocked Clients

IP Address	MAC Address	Timestamp

Figure 27. SDN Network Protector dashboard

HPE Network Optimizer SDN Application

Deploying trusted and granular quality of service (QoS) can be extremely complex and require implementing tedious and time-intensive manual configurations on a device-by-device basis. In fact, it is nearly impossible to implement traffic policy using deep packet inspection (DPI) for soft clients with legacy networks because of because of SIP TLS encryption and dynamic application ports used by UC&C applications, resulting in poor application traffic visibility.

The HPE Network Optimizer SDN application will automate policy deployment dynamically on a per-connection basis for voice, video, and application sharing to deliver a better user experience and reduce operational costs. When a desktop sharing, voice, or video connection is initiated using the Microsoft® Lync client in the campus or branch office, the Lync Server in the data center provides the HPE Network Protector SDN Application with call details such as source and destination IP address, protocol type, application ports, and bandwidth requirements at the start and end of every call. Network Optimizer then uses these per-connection application details to dynamically provision the end-to-end network path and QoS policy via the HPE Virtual Application Networks (VAN) SDN Controller using OpenFlow.

Once the QoS policies and path are programmed via OpenFlow, the call is connected to the destination client. The HPE Network Optimizer SDN Application uses the intelligence from Lync Server and the Lync SDN API, along with the robust capabilities of the HPE VAN SDN controller, to implement consistent QoS across the network. All of this is done dynamically through a central point of control; eliminating the need for manual, device-by-device configuration via the CLI, which greatly simplifies policy deployment and reduce the likelihood of human errors.

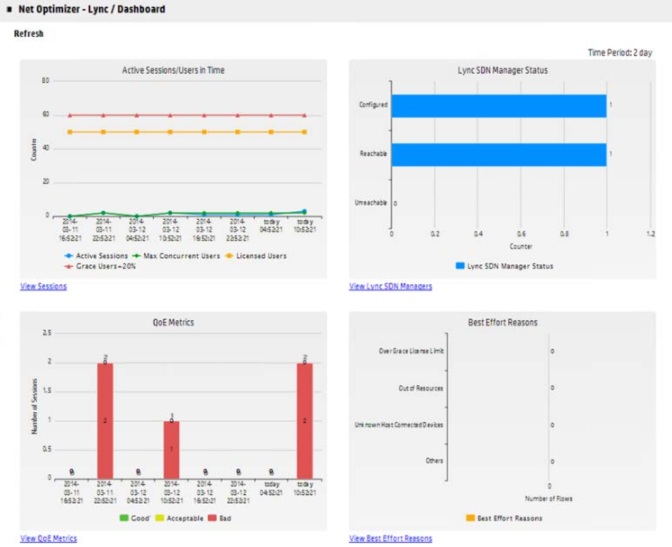


Figure 28. SDN Network Optimizer dashboard

HPE Network Visualizer SDN Application

Networks are growing in complexity to meet customer and user expectations for BYOD, high performance, resiliency, and flexibility. Often the methods used to investigate issues are disruptive, time-consuming, and have unintended consequences.

The HPE Network Visualizer SDN Application utilizes HPE VAN SDN Controller software to provide dynamic traffic capture with real-time, detailed network monitoring, allowing for fast network diagnosis and verification, and a rapid transition from incident to fix.

Some of the features benefits of this SDN app are:

- Active Directory integration
- Allows you to use user ID or user group as part of the traffic selection criteria
- Custom traffic selection criteria
- Gives the user the ability to precisely identify the traffic to be captured
- Real-time traffic capture
- Enables issue identification and investigation with live traffic
- Automated mirror session deployment
- Follows the user to ensure traffic capture regardless of connection location
- Multiple traffic capture destinations
- Support remote and local capture locations

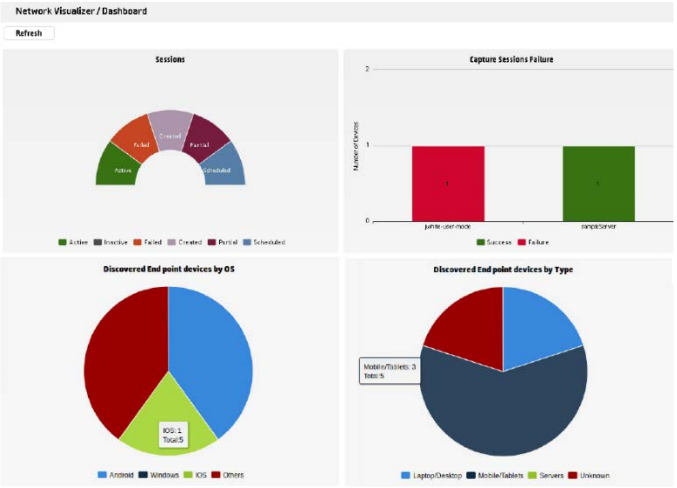


Figure 29. SDN Network Visualizer dashboard

APPENDIX A. ARUBA 7200 MOBILITY CONTROLLERS SPECIFICATIONS

Table 5. Aruba 7200 Mobility Controller specifications

	7240	7220	7210	7205
Maximum campus AP licenses	2,048	1,024	512	256
Maximum remote AP licenses	2,048	1,024	512	256
Maximum concurrent users/devices	32,768	24,576	16,384	8,192
Maximum VLANs	4,094	4,094	4,094	2,048
Active firewall sessions	2,015,291	2,015,291	2,015,291	1,000,000
Concurrent GRE tunnels (system BSSIDs)	32,768	16,384	8,192	8,192
Concurrent IPsec sessions	32,768	24,576	16,384	4,096
Concurrent SSL fallback sessions	8,192	8,192	8,192	4,096
Mobility Access Switch Tunneled Node ports	16,384	12,288	8,192	4,096
Firewall throughput	40 Gbps	40 Gbps	20 Gbps	12 Gbps
Encrypted throughput (3DES, AES-CBC)	40 Gbps	30 Gbps	10 Gbps	6 Gbps
10/100/1000Base-T ports	2 RJ-45 / 2 SFP (combo)	2 RJ-45 / 2 SFP (combo)	2 RJ-45 / 2 SFP (combo)	4 RJ-45 / 4 SFP (combo)
10 Gigabit Ethernet ports (SFP+)	4	4	4	2
10 Gigabit Ethernet ports (XFP)	N/A	N/A	N/A	N/A
Management ports, Console, USB	MGT: 1, CON: mUSB+RJ45, USB: 1			
Power-over-Ethernet ports (802.3af/802.3at)	Hot swappable dual redundant AC or DC power options			No
Power Options				Integrated AC power supply
Redundant power	Yes			No
Maximum power consumption	165 watts	125 watts	110 watts	75.2 watts
Wi-Fi standards support	802.11 a/b/g/n/ac			
Encryption types	WEP, TKIP, DES, AES-CCMP, 3DES, AES CBC			
Authentication types	WPA-Enterprise, WPA-PSK, WPA2-Enterprise, WPA2-PSK, 802.1X, MAC address, captive portal			
Hardware warranty	One year	One year	One year	One year
Software warranty	90 days	90 days	90 days	90 days
Minimum ArubaOS version	6.2.0.0	6.2.0.0	6.2.0.0	6.4.3.0

a Hewlett Packard
Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | info@arubanetworks.com

www.arubanetworks.com