Design reference guide

Aruba Mobile First campus reference architecture

Campus solution deep dive
Contents

Introduction ........................................................................................................................................ 5
Mobile First campus architecture ....................................................................................................... 5
Mobile First access reference design ............................................................................................... 6
Mobile First access components ....................................................................................................... 6
Mobility controller system in ArubaOS 6.x ....................................................................................... 9
   Controller roles ............................................................................................................................ 9
   Hierarchy ...................................................................................................................................... 9
   Master controller ........................................................................................................................ 9
   Local controller .......................................................................................................................... 11
Mobility controller system in ArubaOS 8.x ....................................................................................... 12
   Controller Hierarchy .................................................................................................................. 12
   Mobility Master ......................................................................................................................... 12
   Controller Cluster ...................................................................................................................... 12
Wired Technologies .......................................................................................................................... 13
   Smart Rate .................................................................................................................................. 13
   PoE (Power over Ethernet) .......................................................................................................... 14
   Stacking ...................................................................................................................................... 14
   High bandwidth uplinks .............................................................................................................. 14
   Authentication and authorization ................................................................................................. 15
   Network management and control with AirWave ........................................................................ 15
Scaling considerations ....................................................................................................................... 15
Centralized Mobile First access reference design ........................................................................... 16
   Hybrid design ............................................................................................................................ 16
   Components and technologies .................................................................................................. 17
   Use cases .................................................................................................................................... 17
   Scaling considerations .............................................................................................................. 17
Distributed access reference design ................................................................................................ 18
   Components and technologies: Aruba Instant ........................................................................... 18
      Management Plane .................................................................................................................. 19
      Control Plane ......................................................................................................................... 19
      Data Plane ............................................................................................................................. 19
      Virtual Controller .................................................................................................................. 19
IP Overlay and segmentation - VRF-lite and GRE .......................................................... 34
Single VLAN for WLAN clients.................................................................................. 35
  Traditional VLAN strategy for enterprise WLAN ......................................................... 35
  VLAN Pooling on Enterprise WLAN ........................................................................ 35
  Single VLAN design ................................................................................................. 36
  Concerns with Single VLAN design .......................................................................... 36
  Single VLAN design and the wired network ............................................................. 37
Introduction

Aruba understands that rigid, static enterprise networks do not satisfy the needs of today's enterprises. Users move, have more than one device, access video and audio interactive applications as much as they access databases and use office applications.

The Aruba Mobile First network is designed to allow people to move while connected, and to allow enterprises to innovate without being tied to an old infrastructure. It combines the best-of-breed wireless product line, a wired infrastructure ready to support mobility and IoT, end to end network management, and multi-vendor access control.

Mobile First campus architecture

This document describes the Mobile First network architecture for campus networks, including reference designs, technologies, and hardware and software components. Historically, documents on campus network architectures, described wired and wireless networks as separate entities, one running on top of the other but with minor or no interaction between them.

This guide takes a different approach, it first describes the access as a single system that integrates APs, mobility controllers, access switches, network management and access and traffic control. In a second part, it describes the network backbone: the switching system that transport all the traffic between the access system and the services and applications.

For the access system, three reference designs are presented:

- A traditional design that can be used in a vast majority of the cases, integrating controller-based wireless access and local forwarding access switching
- A centralized design in which wireless and wired traffic is tunneled to the mobility controllers to completely unify policy enforcement
- A distributed design in which traffic from wireless and wired clients is forwarded locally at the access layer using Aruba Instant technology

For the backbone, the two main designs are presented:

- A single node (collapsed core) backbone design mainly used for single building and small campuses
- A hierarchical backbone design for typically used in multi-building campuses
Mobile First access reference design

The most common campus access design is based on a traditional access switching infrastructure and a controller-based mobility system. This design satisfies the requirements of most campuses and can scale to tens of thousands of clients.

Mobile First access components

The components for this design are Aruba switches, Aruba APs, Aruba Mobility Controllers, AirWave and ClearPass Policy Manager. These components form an integrated access system.

Aruba APs provide connectivity to wireless clients and other endpoints.

Aruba access switches connect APs, wired clients and other endpoints like printers, cameras, etc. to the network. These switches on their own or working with ClearPass Policy Manager provide an access control service including authentication, authorization and accounting.
Aruba mobility controllers perform different functions for the APs. Several controllers can work together to provide a hierarchical and redundant mobility system with the APs.

The mobility controller system provides:

- AP tunnel termination and translational bridging
- Each AP establishes a GRE tunnel to a mobility controller
- All traffic to and from the AP's wireless clients is transported inside this tunnel
- In other words, the controller provides a virtual connection point to all the wireless clients
- Traffic arriving from a wireless client is translated from 802.11 to 802.3 frame format and traffic destined to a wireless client is translated from 802.3 to 802.11 frame format
- The frame translation function includes encryption and decryption of wireless traffic
- The controller can implement quality of service (QoS) by marking or remarking traffic and by providing traffic prioritization.

**Access control and policy enforcement**

- Working alone or in conjunction with ClearPass, the controller acts as the authenticator for wireless clients, in other words, it is the controller that rejects or authorizes mobile clients, and authorized clients are allowed to access only a certain set of services and resources
- The controller includes a stateful firewall that can be configured to filter wireless traffic including multicast and broadcast control

**Network management and visibility**

- Aruba Mobility Controllers are deeply integrated with AirWave and together, these two platforms provide granular visibility into the wireless network, allowing the network administrator to detect and troubleshoot connection and performance issues

**Aruba AirWave** is a network management platform for wired and wireless networks. AirWave is especially suited to manage Aruba mobility including:

- The Aruba AppRF feature provides deep visibility into performance and usage of mobile and web apps. Reputation reports allow network administrators to quickly take action against high risk sites and control Wi-Fi usage by app category and user role, device type and location specific insights allows them to make quick decisions to protect business critical apps
- AirWave uses VisualRF to allow for time-lapse mining of Wi-Fi coverage – enabling wireless network engineers to record and replay 24 hours of RF heat mapping. VisualRF also powers location specific, visual analytics on mobile and web app usage, mobile device performance, mobile UC voice and video quality, and more

AirWave also manages Aruba switches providing CPU, memory and interface monitoring, configuration management, firmware upgrades and more.

AirWave can be used to implement zero-touch provisioning for Aruba Instant APs (IAP), Aruba switches and branch controllers.

**Aruba ClearPass Policy Manager** solves today's security challenges across any multi-vendor wired or wireless network by replacing outdated legacy AAA with context-aware policies. It delivers visibility, policy control and workflow automation in one cohesive solution.

- ClearPass Universal Profiler provides granular visibility into all connected devices, even controllers and switches including a customizable dashboard to display categories and families of devices and individual attributes for everything connected.
• **ClearPass Guest** allows network administrators to give customers, contractors, and other visitors secure guest access to wireless and wired networks including customizing a guest access portal,

• **ClearPass Onboard** lets BYOD and IT-issued devices connect safely to the corporate network in compliance with security mandates. Flexible policies and unique certificates enable full and limited access based on roles, device type, and security posture

• **ClearPass OnGuard** performs vital endpoint health checks and posture assessments automatically to ensure that all laptops are fully compliant with industry and internal requirements before they connect to wired and wireless networks

**Mobility controller system in ArubaOS 6.0**

**Controller roles**

Aruba mobility controllers can assume different roles in the mobility system:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master active</td>
<td>It is the single point of policy configuration and coordination for the WLAN in smaller deployments (see details below). Deployed in the data center to be reachable from all the organization's sites.</td>
</tr>
<tr>
<td>Master standby</td>
<td>Is the backup of the master mobility controller and provides high availability.</td>
</tr>
<tr>
<td>Local</td>
<td>Local controller require a Master controller. Manages logically attached APs and handles user sessions on the network. One or more local controllers can be deployed in a campus and connected to the master controller in the data center. Local controllers can provide load balancing and high availability. Local controllers are the core of the mobility forwarding plane. GRE tunnels are created between the APs and the local controllers. One of these tunnels is used for AP management and control and the other transports client traffic to and from the AP. The controller provides security and visualization in the form of an internal stateless firewall. Also terminates wired client tunnels - see Centralized Reference Design section. Configuration of local controllers is split across the master and the local itself.</td>
</tr>
<tr>
<td>Branch</td>
<td>Aruba 70xx controllers can operate in Branch mode. Controllers in this mode require a Master controller and they are fully configured by it. A VPN can be configured between the branch and the master controller to provide secure communication with corporate resources and services</td>
</tr>
<tr>
<td>Standalone</td>
<td>A standalone controller is ideal for a single site that does not require high availability. It performs both master and local controller functions.</td>
</tr>
</tbody>
</table>

**Hierarchy**

Aruba 7200 Mobility Controllers are capable of assuming two roles in the campus mobility hierarchy: 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.

**Master controller**

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.

<table>
<thead>
<tr>
<th>ArubaOS 6.x</th>
<th>Location</th>
<th>ArubaOS 8.x</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master / master standby controllers</td>
<td>Data center</td>
<td>Mobility master</td>
</tr>
<tr>
<td>Local controllers</td>
<td>Campus core</td>
<td>Managed node</td>
</tr>
<tr>
<td>APs</td>
<td>Campus access</td>
<td>APs</td>
</tr>
</tbody>
</table>

Figure 6. Mobility controller hierarchy for the campus in ArubaOS 6.x and 8.x

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

**Local controller**

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, and 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 its 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.

**Mobility controller system in ArubaOS 8.x**

**Controller Hierarchy**

The mobility controller hierarchy in ArubaOS 8.x is similar to the previous 6.x version. The master role is performed by a virtual controller called Mobility Master and the local and branch roles are performed by a Managed Device (MD) or Managed Nodes (MN). The MDs can be controller appliances: 72xx and 70xx series controllers, or a virtual managed controller (VMC).

**Mobility Master**

In the ArubaOS 8.x release the mobility master can only be an ESXI VM and is deployed as an OVA. Later releases offer support for 7200 mobility controller series appliances and other hypervisors.

A mobility master supports up to 1,000 managed devices, 10,000 APs and 100,000 clients.

**Controller Cluster**

Controller clusters is an aggregation of MDs and requires an MM for configuration. The following conditions must be met to form a cluster:

- All MDs need to run the same software
- Up to 12 nodes in a cluster when using 72xx devices
- Up to 4 nodes in a cluster when using 70xx devices
- Up to 4 nodes in a cluster when using VMC devices
- Mix of VMC and hardware based controllers not supported
- Mix of 72xx and 70xx is not recommended

A cluster can be formed over a layer 2 or layer 3 network:
- L2-Connected: Cluster members sharing same user VLANs (recommended)
- L3-Connected: Cluster members NOT sharing same user VLANs

MDs in the cluster form a full mesh of IPsec VPNs that provides secure communication and synchronization. One of the cluster members is assigned the role of the Cluster Leader. This MD:
- Computes which client is mapped to which cluster member
- Dynamically Load Balance clients on increasing load or member addition
- Identify Standby MDs for Clients and APs to ensure hitless failover

APs create management and control connections to two MDs assigned by the cluster leader:
- AAC: AP anchor controller – establishes an active tunnel with the AP
- S-AAC: Standby AAC – establishes a standby tunnel with the AP

In a failover the S-AAC becomes AAC and a new S-AAC is assigned by the cluster leader (if available)

APs create a load balancing and high availability system for the clients by assigning to each one:
- UAC: User anchor controller
- S-UAC: Standby UAC

The AP establishes and active tunnel to the UAC and a standby tunnel to the S-UAC.

A MAC-address based hashing algorithm is used to map clients to UACs and S-UACs, providing a client-based load balancing. The hashing algorithm is the same for all AP, so, when a user roams it is assigned the same pair of UAC / S-UAC.

**Wired Technologies**

Aruba offers a variety of access switches with different features and options.

**Smart Rate**

Smart Rate is a multi-rate-gigabit Ethernet technology that allows a port to operate at 1, 2.5 and 5 Gbps with PoE+ or at 10 Gbps without PoE+.

This technology is especially important when 802.11ac Wave 2 APs are deployed. 802.11ac's multi-user MIMO (MuMIMO) allows network administrators to create WiFi cells of up to 1.7 Gbps. The **Aruba AP-330** series is one of the first mobility
products to offer the MuMIMO feature and includes a two Ethernet ports, one of them is Smart Rate capable and the other is a standard GbE port. If these APs are chosen, the perfect match is one of the following switches:

- Aruba 3810M 40G 8 HPE Smart Rate PoE+ 1-slot Switch - JL076A
- Aruba 5400R 20-port GbE PoE+ / 4-port Smart Rate PoE+ MACsec v3 zl2 Module - J9991A
- Aruba 5400R 8-port Smart Rate PoE+ MACsec v3 zl2 Module - J9995A

**PoE (Power over Ethernet)**

Depending on the number of devices to be powered and their power requirements, different products may be selected

<table>
<thead>
<tr>
<th>Switch Series</th>
<th>PoE budget per unit / slot</th>
<th>Field replaceable PSU</th>
<th>Redundant PSUs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aruba 5400R</td>
<td>720W</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Aruba 3810</td>
<td>1080W</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Aruba 2920</td>
<td>740W w/internal PSU</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>1440W w/RPS 640</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aruba 2930F</td>
<td>370W (24/48 PoE+ port models)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>125W (8 port model)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aruba 2540</td>
<td>370W</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Stacking**

Aggregating access switches to form a stack allows for the optimization of the uplinks, reducing the number of ports, cables and transceivers required. Instead of two uplinks per unit, a single stack wiring closet may have only 2 uplinks. More uplinks may be required, depending on bandwidth requirements

- **Backplane stacking**: this technology is based on dedicated stacking hardware and is available on the 3810 and 2920 switch series
- **Front-plane stacking**: this technology uses standard 1GbE, 10GbE, or 40GbE ports to interconnect the stack and is available on the 5400R and 2930F switch series. VSF (Virtual Switching Framework) and IRF (Intelligent Resilient Framework) are two front-plane stacking technologies

<table>
<thead>
<tr>
<th>Switch Series</th>
<th>Stacking technology</th>
<th>Max size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aruba 5400R</td>
<td>VSF</td>
<td>2 chassis (same model)</td>
</tr>
<tr>
<td>Aruba 3810</td>
<td>Backplane</td>
<td>5 in a full mesh, 10 in a ring</td>
</tr>
<tr>
<td>Aruba 2920</td>
<td>Backplane</td>
<td>4 in a ring</td>
</tr>
<tr>
<td>Aruba 2930F</td>
<td>VSF</td>
<td>4 in a ring</td>
</tr>
<tr>
<td>Aruba 2540</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>

**High bandwidth uplinks**

Many campuses require a high density of APs. In those cases, the number of APs connected to a single access switch (standalone or stack) is higher and the switch acts both as an access devices for wired clients and IoT devices and as an AP aggregator.

The traffic pattern of an AP differs from a typical wired client, for example a PC. In the case of a PC, the traffic is basically a sequence of traffic bursts, when the user accesses a web page, opens a file from a server, etc. separated by moments of very low activity. As an average the bandwidth utilization on the port is very low, typically between 1 and 3%.
A similar traffic pattern is created by a wireless client. Because the traffic between the AP and the access switch is the aggregation of all the traffic from the AP’s associated clients, its pattern is the sum of all their traffic bursts, and the bandwidth utilization, depending on the number of clients, can be consistently above a 10% and reach up to 60%.

This factor must be considered when analyzing the bandwidth requirements of the access switch’s uplinks. The other requirement to consider is the redundancy level: the minimum number of uplinks is 2 per stack or standalone switch.

<table>
<thead>
<tr>
<th>Switch Series</th>
<th>Max number of SFP uplinks / unit</th>
<th>Max number of SFP+ uplinks / unit</th>
<th>Max number of 10GBASE-T uplinks / unit</th>
<th>Max number of 40GbE uplinks / unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aruba 5400R</td>
<td>n/a</td>
<td>8 / module</td>
<td>8 per module (Smart Rate)</td>
<td>2 per module</td>
</tr>
<tr>
<td>Aruba 3810</td>
<td>n/a</td>
<td>4 (8 – )</td>
<td>8 (Smart Rate)</td>
<td>2</td>
</tr>
<tr>
<td>Aruba 2920</td>
<td>n/a</td>
<td>4 (modular)</td>
<td>4 (modular)</td>
<td>n/a</td>
</tr>
<tr>
<td>Aruba 2930F</td>
<td>4 (1 Gig uplink models)</td>
<td>4 (fixed)</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Aruba 2540</td>
<td>n/a</td>
<td>4</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>

Authentication and authorization
As stated above, authentication and authorization for wireless clients is enforced at the controller. For wired clients, this function is provided by the access switch. Switches and mobility controllers support 802.1X, MAC and Web portal authentication. In conjunction with ClearPass, Aruba devices provide role-based access control. Clients are assigned roles based on identity, device type, etc.; and through a role, the device applies different policies: VLANs, ACLs, etc.

Network management and control with AirWave
Aruba mobility controllers reach their maximum potential when the AirWave network management platform is deployed. The different Aruba wireless solutions and incorporates some important switching management and monitoring features.

Scaling considerations
The Mobile First access design is the main option for the campus access layer. It allows network architects to build an access system for campuses of all sizes, scaling to tens of thousands of devices.
Centralized Mobile First access reference design

This second access design takes advantage of the mobility controllers located at the core to centralize, not just wireless client traffic but also wired client traffic.

The design is based on an ArubaOS-switch feature called Tunneled Node. The current version of tunneled node is deployed in a per-port basis. A switch or a stack of switches with tunneled node enabled, creates a single layer 2 GRE tunnel to a primary controller. A secondary controller can be configured for redundancy. Ports can be configured in tunneled “mode”, and in those cases, all the traffic to and from these ports is encapsulated within the GRE tunnel. For clients connected to these ports, the switch acts as an access point and they share is a virtual access port at the controller.

Hybrid design

It is important to notice that in most cases only some ports will need to be configured in tunneled mode, while the rest works as standard access ports. In these cases, the resulting design is a mix of the designs described in first and second place in this document.
Components and technologies
The components and technologies for this design are the same as for the previous one except for the addition of Tunneled Node. Tunneled node is supported on the following Aruba switch series: 5400R, 3810, 2920, and 2930 and all Aruba mobility controllers.

Use cases
There are two main use cases for tunneled node:

- **Critical client protection**: some clients need to be protected from potential intruders and using the mobility controller’s firewall is a simple way to do it. By using tunneled node for these clients, the firewall controls access to the endpoint device. An important case is IP-based wired payment card readers.

- **Unified policy enforcement**: converging both wired and wireless client traffic on the controller, enables the network administrator to implement the same policies (user and traffic) for both wired and wireless clients. Unifying policies at the controller level has the benefit of providing deep visibility into the traffic, allowing administrators to

Scaling considerations
The maximum bandwidth of the GRE tunnel between a switch (or switch stack) and a controller is 10Gbps – minus overhead. This restriction is due to the fact that even when the link between the controller and the core switch can offer more than 10Gbps this is achieved by implementing link aggregation and all the packets on a certain GRE tunnel have the same source and destination addresses in the external IP and MAC header, so a single 10GbE port is used for all the tunneled traffic from that access switch.
Distributed access reference design
The first two access designs had in common the presence of mobility controllers. This third design presents a fully distributed solution based on Aruba Instant APs (IAPs).

A group of IAPs connected to the same VLAN forms an Instant Cluster. Instant clusters implement a distributed mobility controller function with a controller node located inside each APs. Even when the feature richness of a mobility controller is not fully implemented on an instant cluster, these sets of APs can perform most of those functions including AppRF.

Figure 11. Distributed access reference design
The main characteristic of this design is its simplicity. All authentication, policy enforcement and traffic forwarding is performed locally at the access layer.

Components and technologies: Aruba Instant
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 as described in the following sections.
Management Plane
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
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
- Deep Packet Inspection

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
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 requires source NAT to be provided 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). The master election is based on a master election protocol. The election process to select a master AP/VC is simple; the first IAP that comes online on the network is elected as the master AP/VC. If a master AP/VC fails, a new AP is re-elected as the master AP of the cluster. The master-re-election algorithm uses these conditions during a VC failover:

1. An IAP with an alternative uplink (3G or 4G only) receives preference.
2. If an IAP with an alternative uplink is not available, an IAP with the more capable hardware/a newer model receives preference in the following descending order:
   \[ \text{IAP225 & all the other newer models} > \text{IAP134/5 = RAP155} > \text{IAP104/5 = IAP175 = RAP108/9 = RAP3} \]
   This rule is being used to distinguish only between older models & newer models.
3. If both of the previous considerations are not applicable, an IAP with the longest uptime receives preference.
In an Aruba Instant cluster, the master AP/VC failover time varies from 13 seconds to 100 seconds because the VC election algorithm also takes the CPU load on the IAPs in the network into account.

**Network management**
Aruba AirWave or Central can be used to manage both the wired and wireless infrastructure in this design.
One additional advantage of this design is that both the Aruba IAPs and switches support zero-touch provisioning using either AirWave or Central.

**Scaling considerations**
Instant clusters are limited to 128 APs and up to 2000 simultaneous clients.
Because of this limit, the distributed campus access design can be applied to:

- Single building campus requiring less than 120 APs and with less than 1500 clients (reserving space for growth)
- Multi-building campus in which a single cluster provides adequate coverage for any individual building and in which RF continuity between buildings is not critical.

**Use cases**
The distributed design is recommended for a small to medium size (less than 1500 wireless clients) that requires less than 120 APs.

![Figure 12. Distributed policy enforcement using ClearPass and SDN apps](image)

An important use case is the situation in which HPE SDN Network Visualizer and other SDN apps need to be deployed. Because all traffic is forwarded locally at the access switch, SDN can be implemented for all traffic. SDN apps and ClearPass complete a fully distributed policy enforcement infrastructure.
Aruba switches integration features summary

As stated in the introduction, Aruba offers an integrated access system that includes switches, APs, mobility controllers, AirWave or Central, and ClearPass. From the point of view of the switches, there is a set of features that makes that integration possible.

<table>
<thead>
<tr>
<th>Network management</th>
<th>ZTP AirWave</th>
<th>IPsec to AirWave</th>
<th>Device/Interface monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch + AirWave + Central</td>
<td></td>
<td></td>
<td>Configuration management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Firmware upgrade</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Control</th>
<th>Tunneled node</th>
<th>802.1X / MAC / Portal</th>
<th>Internal captive portal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch + ClearPass + mobility controllers</td>
<td>SDN (controllers)</td>
<td>RBAC: RADIUS/TACACS</td>
<td>Local user role</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Infrastructure</th>
<th>Smart Rate (2.5/5Gbps)</th>
<th>Auto AP detection</th>
<th>VSF / BPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch + AP</td>
<td>10/40GbE uplinks</td>
<td>Rogue AP isolation</td>
<td>Full PoE+</td>
</tr>
</tbody>
</table>

Figure 13. Aruba access switches integration features

**Switch – AP integration**

**Smart Rate ports**: satisfies the bandwidth requirements of 802.11ac Wave 2 APs by providing a 2.5Gbps link with PoE+.

**10/40GbE uplinks**: satisfies a variety of uplink bandwidth requirements of access switches and stacks acting as AP aggregators, especially when Smart Rate ports are operating at 2.5Gbps.

**Auto AP detection**: simplifies AP deployment by automatically detecting Aruba APs and automatically applying a preconfigured profile to the corresponding port. The configuration profile includes: a VLAN list (untagged and tagged), a CoS value, ingress and egress bandwidth limit utilization limit, PoE priority and maximum power, and speed and duplex mode.

Figure 14. Auto AP detection

**Rogue AP isolation** (IAPs only): when deployed with IAPs, Aruba switches can isolate APs that do not belong to the cluster.

Figure 15. Rogue AP isolation with IAPs
Stacking – VSF/BPS: even when stacking does not relate specifically to the AP integration, when paired with 10GbE or 40GbE uplinks, it optimizes the number of links between the access and the aggregation layer, reducing the number of cables and the number of ports on the aggregation switch.

Full PoE+ and redundant power: depending on the APs model and quantity, and other PoE devices connected to the switch, the PoE budget plays an important role. And in many cases, redundant power can also be a requirement.

The 5400R and 3810 Switch series offer both 30W per port and redundant power supplies.

ClearPass integration
Aruba switches integrate with ClearPass Policy Manager to provide a secure access environment, including RADIUS and TACACS device access control and 802.1X, MAC and captive portal based network access control. RADIUS CoA, local user roles and captive portal are part of this integration.

Switch-controller integration
The tunneled node technology allows network administrators to integrate switches and mobility controllers. For details on this technology, its advantages, limitations and use cases see the Centralized Campus Access Reference Design section.

Switch-network management integration
AirWave offers the following Aruba switch management features:

• CPU, memory and interface monitoring:

![CPU Utilization](image1)

![Memory Utilization](image2)

- ![Firmware Upgrade Options](image3)
- ![Template-based configuration management including: Zero-touch provisioning and Configuration auditing](image4)
Figure 18. AirWave switch configuration template

- CDP/LLDP Neighbors table

<table>
<thead>
<tr>
<th>NAME</th>
<th>NEIGHBOR-PORT</th>
<th>LOCAL-PORT</th>
<th>ADDRESS TYPE</th>
<th>ADDRESS</th>
<th>PORT-DIR</th>
<th>CAPABILITIES</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>V2</td>
<td>V1</td>
<td>ip</td>
<td>10.188.21.100</td>
<td></td>
<td>ArubaOS (MODEL 2)</td>
<td></td>
</tr>
<tr>
<td>eth0</td>
<td>V4</td>
<td>V4</td>
<td>ip</td>
<td>10.188.21.100</td>
<td></td>
<td>ArubaOS (MODEL 2)</td>
<td></td>
</tr>
<tr>
<td>701</td>
<td>06</td>
<td>05</td>
<td>AF</td>
<td>7C4</td>
<td>V40</td>
<td>ip</td>
<td>10.188.32.1</td>
</tr>
<tr>
<td>701</td>
<td>06</td>
<td>06</td>
<td>AF</td>
<td>7C4</td>
<td>V41</td>
<td>ip</td>
<td>10.188.32.1</td>
</tr>
<tr>
<td>703</td>
<td>51</td>
<td>51</td>
<td>GE</td>
<td>E-4A1</td>
<td>GiGabitEthernet0/1</td>
<td>V1</td>
<td>ip</td>
</tr>
<tr>
<td>84A</td>
<td>40</td>
<td>15</td>
<td>51</td>
<td>4B1</td>
<td>GiGabitEthernet0/1</td>
<td>V2</td>
<td>ip</td>
</tr>
<tr>
<td>84A</td>
<td>40</td>
<td>15</td>
<td>51</td>
<td>4B1</td>
<td>GiGabitEthernet0/1</td>
<td>V3</td>
<td>ip</td>
</tr>
<tr>
<td>84A</td>
<td>40</td>
<td>15</td>
<td>51</td>
<td>4B1</td>
<td>GiGabitEthernet0/1</td>
<td>V4</td>
<td>ip</td>
</tr>
<tr>
<td>84A</td>
<td>40</td>
<td>15</td>
<td>51</td>
<td>4B1</td>
<td>GiGabitEthernet0/1</td>
<td>V5</td>
<td>ip</td>
</tr>
<tr>
<td>84A</td>
<td>40</td>
<td>15</td>
<td>51</td>
<td>4B1</td>
<td>GiGabitEthernet0/1</td>
<td>V6</td>
<td>ip</td>
</tr>
</tbody>
</table>

Figure 19. AirWave switch neighbor list

- Zero touch provisioning

Aruba switches can be automatically configured via the following methods

- **DHCP + AirWave**: By means of DHCP options, the switch receives the parameters necessary to contact AirWave: Server IP address, secret key, device group and folder. Using this information, the switch self-registers into AirWave and AirWave applies the template for that device groups/folder.

- **Activate + AirWave**: If the switch does not receive the options from DHCP, it contacts Activate. If the device has been registered in Activate, the switch receives the parameters necessary to contact AirWave: Server IP address, secret key, device group and folder. Using this information, the switch self-registers into AirWave and AirWave applies the template for that device groups/folder.

- **Activate + Central**: If the switch does not receive the options from DHCP, it contacts Activate. If the device has been registered in Activate, the switch’s connection is forwarded to Aruba Central from which it receives its configuration.
- CLI show commands

**CLI show commands**

- Troubleshooting
- L2 Loop Prevention
- Link Aggregation
- Loop Detection
- Slashing
- Media Access
- Routing and other L3 Protocols
- Security and Traffic Shaping
- Management

---

**Figure 20. AirWave switch CLI show command**

**Alternate access switches**

The recommended option for the campus access layer are the Aruba switches. These switch series – 2540, 2930F, 2920, 3810, and 5400R offer excellent integration with the Aruba mobility solution.

There are, however, some cases in which Hewlett Packard Enterprise FlexNetwork access switches may me a better fit. These switches are based on the Comware operating system.

**FlexNetwork**

---

**Aruba**

- 5400R
- 3810
- 2920
- 2930F

---

**Figure 21. FlexNetwork access switches positioning**

**End-to-end Comware operating system and IMC network management**: This solution is attractive when mobility or wired-wireless integration are not the priority and Comware has already been deployed in the data center and the campus core and aggregation.
If VRF (MPLS L3VPN) or VRF lite (MCE) are required at the edge of the network and cannot be terminated in the aggregation layer, the HPE 5510HI and 7500 switch series are the best options.

If layer 3 VXLAN with EVPN is required at the edge of the network and cannot be terminated in the aggregation layer, the HPE 7500 switch series is the best option.

<table>
<thead>
<tr>
<th>Switch Series</th>
<th>5130 EI</th>
<th>5130 HI</th>
<th>5510 HI</th>
<th>7500</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form factor</td>
<td>Stackable</td>
<td>Stackable</td>
<td>Stackable</td>
<td>Modular</td>
</tr>
<tr>
<td>Stacking</td>
<td>IRF Up to 9 units</td>
<td>IRF Up to 9 units</td>
<td>IRF up to 9 units</td>
<td>IRF up to 4 units</td>
</tr>
<tr>
<td>Operating system</td>
<td>Comware v7</td>
<td>Comware v7</td>
<td>Comware v7</td>
<td>Comware v7</td>
</tr>
<tr>
<td>Routing</td>
<td>Static, RIP</td>
<td>Static, RIP</td>
<td>Static, RIP, OSPF, BGP, IS-IS</td>
<td></td>
</tr>
<tr>
<td>Network virtualization</td>
<td>No</td>
<td>No</td>
<td>GRE, MPLS L3VPN, MPLS L2VPN, VPLS, IPv6 over IPv6</td>
<td></td>
</tr>
<tr>
<td>VXLAN</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes (L3)</td>
</tr>
</tbody>
</table>

In general, however, it is recommended to implement layer 2 switching in the access layer terminate VXLAN, VRF, VRF-lite, GRE tunnels at the aggregation layer and extend these tunnels using VLANs to the edge.
**Campus backbone**

To connect the access system to the different network services and applications in the campus, network designers have to choose between a single tier (collapsed) and a hierarchical backbone.

In a single tier backbone, access switches are connected directly to a single core switching node.

![Collapsed campus backbone with a single node](image)

In a hierarchical backbone, on the other hand, access switches are connected to aggregation switching nodes (also called distribution switching nodes), and the aggregation switching nodes are all connected to a core node.

![Hierarchical campus backbone with core and aggregation nodes](image)

Historically, campus networks were designed using a hierarchical backbone for several reasons:

- To multiply the capacity of the different tables: MAC, ARP, routing, etc.
- To multiply the layer 3 forwarding capacity and improve performance
- To reduce the port density per node
- To simplify the cabling plant especially in multi-building campuses
With the evolution of the switching technology, the first three items are no longer an issue. However in large, multi-building campuses the cabling plant can be extremely complex if all access switches are connected directly to the core node, the cost of running multiple fiber optics cables between buildings may be higher than that of an aggregation switch. Today, this is the main reason behind the choice of a hierarchical backbone.

**Backbone nodes**

Because the network backbone is critical, the best practice is to deploy backbone nodes in pairs of identical, interconnected devices.

![Typical campus backbone node](image)

**Access-aggregation triangles:**

In this scheme, all adjacent nodes or neighbors are connected to both devices using the same type of link (speed, medium, etc.), forming triangles. These device triangles, have the advantage of providing link-level as well as device-level redundancy. However, special technologies need to be used to prevent these triangle from becoming traffic loops.

![Access-aggregation triangle = potential loop](image)

To prevent loops between the access switches and the redundant aggregation nodes, there have been, historically two solutions:

- If the access switch forwards in layer 2, a combination of MSTP and VRRP is used. MSTP handles layer 2 redundancy by blocking traffic from different VLANs on different links, avoiding loops and distributing the load. VRRP on the other hand, handles layer 3 redundancy by allowing the aggregation switch to act as a single IP node with a virtual IP address for each VLAN, which is used by the clients as its default gateway.
- As the combination of MSTP and VRRP requires some complex configuration and is difficult to troubleshoot, many network administrators preferred to deploy layer 3 technologies at the access layer and use IP routing to control traffic in the redundant triangle, for example configuring OSPF everywhere.

**VSF and IRF**

Aruba core and aggregation switches offer the alternative of configuring both devices in the node, as a single logical entity. In Aruba switches, this technology is called Virtual Switching Framework (VSF) and in Comware OS-based switches it is called Intelligent Resilient Framework (IRF).
With VSF or IRF a pair of backbone switches behaves as a single device and there is no need to configure MSTP and VRRP or to configure routing in the access layer.

Layer 2 redundancy is implemented by deploying link aggregation between neighbors and layer 3 redundancy is embedded in the VSF/IRF technology.

**Switching and routing**

**VSF/IRF in the aggregation layer**

When the aggregation switching node is a VSF or IRF fabric implementing layer 2 switching in the access layer is the best practice. The following figure shows the different protocols implemented at each layer for unicast, multicast and segmentation.
Pair of standalone switches in the aggregation layer

In some cases, network administrators or designers prefer to avoid creating a single control plane in the aggregation and core layers and choose the traditional dual switch configuration. In that case, layer 3 access is the best practice.

The next figure shows the different protocols implemented at each layer for unicast, multicast and segmentation.

Figure 29. Protocol mapping with dual switch aggregation nodes

Other backbone technologies: overlays

In some cases, the traditional routing scheme is not enough to address the different requirements of a campus and an overlay network or a set of different routing domains needs to be implemented.

- VXLAN extends VLANs across a standard IP routed network even across WAN links and VPNs, to create single layer 2 domains that can span the entire enterprise including data centers, campuses, and branches. The IP network is called the “underlay” and the set of VXLAN tunnels is called an “overlay”. VXLAN tunnels encapsulate and transport Ethernet frames between VXLAN endpoints called VTEPs.

Originally, VTEPs were layer 2 functions and mapped tunnel termination points to VLANs. Today, some switches support an extended version called layer 3 VTEPs that can map a tunnel termination point to a layer 3 interface or that can route between VXLAN tunnels.

One of the challenges of VXLAN is the handling of broadcast, unknown unicast and multicast (sometimes called BUUM traffic). The simplest solution is for the VTEP to forward copies of these frames through all the tunnels of that VXLAN (flooding).

Flooding will always be necessary for broadcast. However, unknown unicast and multicast traffic may require a more sophisticated solution.

The standard solution for multicast is to take advantage of the multicast routing capabilities of the underlay. In that case, the VTEPs act as an IGMP and PIM router and use the PIM tree to forward multicast properly to those VTEPs that have receivers (multicast group members).

In the case of unicast, a control protocol can be added so VTEP can share MAC address table information from their local VLANs. Today, the standard control protocol is EVPN, which is based on Multiprotocol BGP (MP-BGP).

- GRE creates point to point layer 3 tunnels between routers or layer 3 switches. A GRE tunnel can transport IPv4 over IPv4, IPv4 over IPv6, IPv6 over IPv4, and IPv6 over IPv6.

- VRF-Lite creates multiple virtual routing domains across the same infrastructure, isolating routing tables and processes, and allowing for the reuse of IP addresses. VRF-lite is also called MCE or multi-VPN-instance customer edge.

In some cases, network administrators combine VRF-lite with GRE to create a new virtual routing domain.
• **VRF or MPLS L3VPN**: VRF or virtual routing forwarding, creates multipoint IP VPNs on top of an MPLS backbone network.

• **PW or MPLS L2VPN**: PW or pseudo-wire creates a point to point Layer 2 VPN between to MPLS PE (provider edge) devices.

• **VPLS**: VPLS or Virtual Private LAN Service creates a multipoint Layer 2 VPN over an MPLS backbone network.

In most cases, the campus aggregation nodes are the termination points of these overlays and virtual domains. On these nodes, tunnels and VRFs are mapped to VLANs connecting to the access switches. The main advantages of this approach are:

• Access switches are not required to support these technologies (avoiding the associated cost)

• Clients can be mapped to VLANs through the authentication and authorization process, for example by ClearPass, and their traffic can be inserted in the appropriate virtual network at the aggregation layer.

**Aruba aggregation and core switches**

Aruba offers different switch series that can function in these roles.

---

### Figure 30. Core/aggregation switches

To select the right platform for each particular case, at least the following characteristics must be considered:

• Port density: there must be enough 10GbE or 40GbE ports to connect all access switches, mobility controllers, routers, server farm switches, etc.

• Feature set: MPLS L3VPN (VRF) or MCE (VRF-lite), VXLAN, GRE and/or IPv6 tunnels

• Table sizes (see Scaling considerations below)

<table>
<thead>
<tr>
<th></th>
<th>5400R v3</th>
<th>5940</th>
<th>7500</th>
<th>10500</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Form factor</strong></td>
<td>Modular</td>
<td>Stackable</td>
<td>Modular</td>
<td></td>
</tr>
<tr>
<td><strong>Device aggregation</strong></td>
<td>VSF - Up to 2 chassis</td>
<td>IRF - Up to 9 units</td>
<td>IRF - Up to 4 chassis</td>
<td></td>
</tr>
<tr>
<td><strong>Device virtualization</strong></td>
<td>No</td>
<td>No</td>
<td>MDC – Up to 8 non-default contexts</td>
<td></td>
</tr>
<tr>
<td><strong>Port density (Max)</strong></td>
<td>96x 10GbE, 24x 40GbE</td>
<td>48 10GbE + 6x 40GbE, 32x 40GbE</td>
<td>120x 10GbE, 40x 40GbE</td>
<td>576 10GbE, 96 40GbE</td>
</tr>
<tr>
<td><strong>Operating system</strong></td>
<td>ArubaOS-Switch</td>
<td>Comware v7</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Routing</strong></td>
<td>Static, RIP, OSPF, BGP, PBR</td>
<td>Static, RIP, OSPF, BGP, IS-IS, PBR</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Overlays</strong></td>
<td>VXLAN (L2)</td>
<td>GRE, MCE (VRF-Lite), L3 VXLAN w/EVPN</td>
<td>GRE, MPLS L3VPN (VRF), MPLS L2VPN, VPLS, MCE (VRF-Lite), L3 VXLAN w/EVPN</td>
<td></td>
</tr>
</tbody>
</table>
**Single-building campus reference design**

In a campus consisting of a single building, the network is a combination of one of the three access designs and a single core node. In this design the core switching node connects directly to:

- All access switches (or stacks)
- Local mobility controllers (if a controller-based access solution is deployed)
- Campus edge routers
- Local server farm switches (if present)

![Diagram of single building campus reference design]

Figure 31. Single building campus reference design

**Components**

**Access system**

Any of the three access reference designs described above can be used in a single building campus. If managed APs and mobility controller are being deployed (as opposed to IAPs), the recommendation is to connect controllers directly to the core.

**Core (Collapsed aggregation/core)**

Depending on the particular requirements one of the switch series listed in the previous section, can be deployed at the core.

**Technologies / protocols (HA, unicast-multicast routing, overlays, QoS, etc.)**

For redundancy reasons, the best practice is:

- To deploy two identical – interconnected - core switches
- To connect all access switches with the same type of link to both of them
- To connect each local mobility controller to both of them
- To connect both edge routers to both of them

**Scaling considerations**

One important consideration when designing the core for a controller-based wireless network is that:

- Controllers are directly connected to the core
- Controllers are usually configured to forward in layer 2
- The core switching system is the default gateway for all the wireless clients
- If access switches are also configured to forward in layer 2, the core switching system is the default gateway also for all the wired clients
Under these conditions, as the number of clients grow beyond 5000, the size of the ARP table needs to be considered. For example, in a professional sports stadium, the number of clients can reach 20 to 30 thousand devices. Additionally, if IPv6 is deployed, each device will require more than one entry in the ARP table.

**Multi-building campus reference design**

In a multi-building campus consists of an access system, an aggregation switching system per building and a central core switching system.

**Components**

**Access system**

Any of the three access reference designs described above can be used in a single building campus. If managed APs and mobility controller are being deployed (as opposed to IAPs), these controllers must be connected to the core.

**Core and aggregation switching systems**

The switches offered by Aruba for these two roles are the same described above for the single-building core.

**Technologies / protocols (HA, unicast-multicast routing, overlays, QoS, etc.)**

For redundancy reasons, the best practice is:

- To deploy two identical – interconnected – switches both at the core and aggregation layer
- To connect all access switches with the same type of link to both aggregation switches
- To connect all aggregation switches to both core switches
- To connect each local mobility controller to both core switches
- To connect both edge routers to both of them

**Campus network infrastructure management with IMC**

Aruba AirWave is an excellent network management application for the access system. However, for complex campus networks, Hewlett Packard Enterprise offers another network management platform: Intelligent Management Center (IMC).

IMC can manage large LAN and WAN infrastructures, including VLANs, QoS, ACLs, IPsec and MPLS VPNs, and VXLAN management, configuration and software upgrade management, and more.

**Campus edge routing**

Hewlett Packard Enterprise offers three router product lines (HSR, VSR, MSR) that can be deployed at the edge of a campus to connect it to remote datacenters, other campuses, and branches.

**HPE HSR6800 Router Series**

The HPE HSR6800 Router Series is a family of high-performance, multiservice routers designed for data center interconnection, enterprise WAN core, campus WAN edge, and high-speed WAN aggregation services.

![Figure 34. HSR6800 Router Series](image)

It runs the Comware operating system and features an advanced multi-core, distributed service processing hardware architecture that scales up to 420 Mpps forwarding and up to 2 Tbps switching capacity. The router delivers robust routing, multicast, MPLS, IPv6, security, quality of service, carrier-level high-availability features, and high-density 10GbE and 1GbE interface options.

**HPE HSR6600 Router Series**

The HPE HSR6600 Router Series are high-performance service WAN routers, ideal for small-to-medium campus WAN edge and aggregation and high-end branch deployments.

![Figure 35. HSR6600 Router Series](image)

These routers are built with a high-performance multi-core networking processor that delivers, in a 2RU form factor, up to 15 Mpps IP forwarding, robust routing, QoS, MPLS, IP VPN, security, and modular WAN and LAN interface options, integrated into
a single compact powerful routing platform. In addition, these routers feature robust carrier class reliability capabilities to reduce disruption from network or system failures.

**HPE VSR1000 Router Series**

The HPE FlexNetwork VSR1000 Virtual Services Router Series is a virtualized application which provides similar functionality as a physical enterprise router. It runs in a virtual machine on an x86-based server, enabling significant TCO savings given its agility and ease of deployment. It is available in one, four and eight virtual CPU versions. Robust routing and high-performance services like firewall, crypto VPN, QoS and MPLS are provided without additional feature licenses. A variety of deployment models are supported including enterprise virtual CPE at POP or on premise, and vPC gateway.

**HPE MSR Router Series**

The MSR Router product line is targeted at branches of all sizes. It encompasses 5 router series: MSR93X/95X, MSR1000, MSR2000, MSR3000 and MSR4000.

**Use cases**

To illustrate these designs several use cases are presented in this section.

**IP Overlay and segmentation - VRF-lite and GRE**

In several different situations, network administrators need to segregate traffic from different clients. The main options used to achieve this goal are VRF-lite and VRF.

- **VRF-lite** is a technology that allows for the creation of independent routing domains that extend along the same set of devices, switches and routers. At the device level, VRF-lite creates independent routing tables. Between devices, each VRF instance runs its own routing protocol instance (for example OSPF 2, OSPF 3, etc.).

- With **VRF** these routing domains are extended along the same set of devices, switches and routers by means of a set of MPLS L3 VPNs.

- The termination point of both **VRF** and VRF-lite is the same: VLAN interfaces are bound to VRF instances.

Because of its inherent simplicity, VRF-lite is usually preferred over VRF for traffic isolation.

---

**Design reference guide**

**Aruba Mobile First campus reference architecture**

---

Figure 36. Campus reference design for VRF-lite and GRE
The reference design for VRF-lite in a 3-tier Mobile-first campus is composed of:

- **Access**:  
  - Aruba 3810 / 5400R / 2930F / 2920 switch series  
  - Configuration: L2 switching  
  - Isolation: Ports assigned to different access VLANs. ClearPass can be used to map ports to VLANs based on client context  

- **Aggregation - VRF-lite and GRE tunnel termination**:  
  - HPE FlexNetwork 5940 or 7500 switch series  
  - Configuration: IRF for L2-L7 redundancy, L3 switching (MPLS PE function for full VRF)  
  - Isolation: access VLAN interfaces mapped to VRF instances  

- **Core**:  
  - HPE FlexNetwork 10500 switch series  
  - Configuration: L3 switching  
  - Isolation: VRF routing (not necessary if VRFs are mapped to GRE tunnels – see Campus 1 in reference design diagram)  

The reference design for VRF-lite in a 2-tier Mobile-first campus is the same as the 3-tier, but the core and aggregation functions run on the same devices. In other words, VRF instances are terminated at the core (see Campus 2 in reference design diagram.).

There may be situations in which routing is the preferred choice for the access layer. In those cases VRF and/or VRF-lite need to be supported at the access and the HPE 5510 HI switches and the HPE 7500 switches are the options.

**Single VLAN for WLAN clients**

**Traditional VLAN strategy for enterprise WLAN**

VLAN has been a popular concept in the field of networking and there have been multiple reasons for network administrators to use VLANs. Here are a few common ones:

- Limit broadcast domains by reducing the size of the subnet.  
- Segregate traffic for security - Not a very elegant way to provide security but sometimes that is the best option.  
- Quality of Service (QoS) - Really a way to segregate traffic, so that it can be queued properly even if not tagged.  
- Non-contiguous Internet Protocol (IP) space – Mostly the case where IPv4 public addresses are used for wireless clients.  
- Simpler administration – Looking at the IPv4 address can provide information about user, user’s group (employee, contractor, or guest), location etc. However, IPv6 can be tricky.

**VLAN Pooling on Enterprise WLAN**

Due to the Bring Your Own Device (BYOD) trend, large numbers of consumer mobile devices are connecting to enterprise WLAN. Network administrators need to ensure that there are enough IP addresses available to support these clients. As the clients are always roaming across the campus, these clients are always roaming throughout the campus. Thus, when they roam from one part of the campus to other, and as far as RF is contiguous, they are not going to renew their IP address. To support these needs, VLAN Pooling is widely used.
While VLAN Pooling has been a popular feature for enterprise WLAN for many years, these are some of its challenges:

- **802.11 Frames do not Identify VLAN Tags**: when a single SSID is mapped to a VLAN pool, broadcasts on any VLAN reach all clients on the SSID.

- **IPv6 SLAAC Breaks**: An IPv6 client can receive an IPv6 router advertisement from a different VLAN in the same VLAN pool.

- **Inconsistent Utilization of VLANs from VLAN Pool**: Most of the vendors use hash algorithms to assign a VLAN from the VLAN pool to the wireless client. As this hash algorithm is mainly based on the client's MAC-address and number of VLANs in the pool, over the years of study, there have been many situations where some VLANs from the VLAN pool are completely exhausted due to large number of clients in them, while other VLANs are quite empty.

### Single VLAN design

The Single VLAN design refers to one large subnet to serve all the clients connecting to an SSID in the campus environment with contiguous RF. Controller and tunnelled APs make it possible to scale to larger subnets in the range of /22 to /16.

It can greatly reduce the complexity of the WLAN design, and it addresses the IPv6, DHCP, and roaming challenges seen with VLAN pooling. All of the requirements of the wireless LAN can be met by using the Single VLAN design. Large universities can use the maximum advantage of this design with their thousands of wireless clients across a large campus with contiguous RF followed by large enterprises with multiple buildings at a location.

The Single VLAN design recommends to use the same VLAN throughout the campus with contiguous RF. If there are multiple buildings in different locations (for example, school districts or corporate branches spread across different cities or towns), different VLANs and subnets should be used.

The Single VLAN architecture recommends using one large subnet for all the clients connecting to an SSID. However, separate VLANs can be used for clients connecting to separate SSIDs. Ideally, in a campus WLAN, separate VLANs for employee and guest SSIDs should be used.

Lastly, wired and wireless clients should not be sharing the same VLAN. Use separate VLANs for wired clients and, if needed, use multiple smaller subnets to restrict broadcast domain for wired devices. The Single VLAN architecture is for wireless LAN only, as the controller has a lot of visibility and control over wireless users, but none for wired devices. The obvious problems related to large VLANs on wired networks still apply.

### Concerns with Single VLAN design

The single VLAN design brings up several concerns: broadcast and multicast traffic, ARP and DHCP traffic. Aruba mobility controllers have several functions that can be enabled to eliminate these issues:

- **Convert Broadcast ARP to Unicast**: Converts broadcast ARP and DHCP packets to unicast before sending to wireless clients.

- **Suppress ARP**: Stops flooding of unknown ARP request to wireless clients.

- **Optimize Duplicate Address Detection**: Controls the flooding of Gratuitous ARP and IPv6 Duplicate Address Detection frames to wireless clients.

- **Drop Broadcast and Multicast Traffic**: Stops flooding of broadcast and multicast traffic to wireless clients.

- **AirGroup**: Allows mdns and upnp traffic by converting them to unicast.

- **IGMP Snooping and Dynamic Multicast Optimization**: Keeps track of clients subscribed to multicast stream and converts multicast packets to unicast before sending it to wireless clients.
Single VLAN design and the wired network

In the single VLAN design, all wireless client traffic is forwarded between the APs and local controllers through GRE tunnels. The client VLAN traffic being addresses in this design as the Single VLAN spans between the tunnel termination inside the local controllers and the IP gateway. The scope of this VLAN should be restricted to this area.

![Single VLAN design and the wired network](image)

In other words, this VLAN is dedicated exclusively to transport wireless clients traffic (PCs, tablets, smartphones) between the mobility controllers and the IP gateway or between controllers for east-west traffic.

For all other nodes on the network (other wired or wireless devices: surveillance cameras, building management system sensors, wired clients, printers, etc.) the traditional VLAN and subnet design methodology applies.

**Core layer challenges:** In a single VLAN design, the IP interface for the wireless client VLAN resides in the core switching system, so this system becomes the IP gateway for all wireless clients. In this situation the core switching system provides routing to an unusually large IP subnet in which as many as 15,000 to 65,000 clients reside (/17, /16 subnet masks).

The IP gateway of any subnet, to perform correctly, needs to be able to store the MAC addresses and the ARP entries for all the other IP nodes connected to that subnet. Additionally, as the gateway is only one of the IP interfaces of a routing entity, the switch be able to store all MAC-addresses and ARP entries of all the other IP interfaces, along with IP routes, MPLS label-forwarding information, and ACL/QoS rules.

As stated above, the most critical features of the core layer in this particular architecture are:

- MAC-address table capacity
- ARP table capacity

Aruba, as a Hewlett Packard Enterprise company offers a variety of switch series targeted at the core of networks of different sizes and feature requirement levels. The choices for the core are the following:

- Aruba 5400R zl2 Switch Series with v3 modules: small deployments of up to 10,000 clients
- HPE 10500 Switch Series with EC modules: large deployments of up to 100,000 clients
Figure 38. Main core options for a single VLAN WLAN design

<table>
<thead>
<tr>
<th>Switch Series</th>
<th>MAC address</th>
<th>ARP</th>
<th>Operating System*</th>
<th>Module type**</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aruba 5400R</td>
<td>64K</td>
<td>25K</td>
<td>AOS-S 16.01 or later</td>
<td>v3</td>
</tr>
<tr>
<td>HPE 10500</td>
<td>288K</td>
<td>80K</td>
<td>710-R7179 or later</td>
<td>SG</td>
</tr>
<tr>
<td></td>
<td>256K</td>
<td>128K</td>
<td></td>
<td>EC</td>
</tr>
</tbody>
</table>
For more information

Aruba networks

HPE information library