



**The Aruba Mobile Virtual Enterprise
A Mobility-Centric Network Access Architecture**

Table of Contents

Executive summary	3
The mobile enterprise has arrived	4
Yesterday's network is mismatched for today's users	5
Policy control: VLANs are obsolete, context is key	5
No more silos – roaming requires unified access	6
WLANs built for coverage now need capacity	6
MOVE: Context-aware access architecture for the mobility era	6
A context-aware network and services	7
MOVE with unified access	8
WLANs built for tomorrow's traffic	9
MOVE with scalable deployments	10
Embrace the mobility era with MOVE	12
About Aruba Networks	12

Executive summary

Enterprise mobility has come to the mainstream along with many other attributes of the socialized consumer Internet experience: multimedia content, heavy use of rich collaboration technologies and cloud-based applications.

Users are embracing these changes as an integral part of how work gets done, blurring the lines between corporate-owned and bring-your-own devices, local and remote services, even the wireless network and cellular access.

But for IT, these new mobility realities are overwhelming a network whose legacy design dates back to the client-server era. As a result, enterprises face:

- Access control based on a virtual LAN infrastructure that's obsolete and doesn't scale.
- Network services that are fragmented by an access infrastructure consisting of siloed wireless, wired and virtual private networks;
- A wireless infrastructure built for coverage, not the capacity needed to support a high density of users and rich, multimedia applications.

To deliver the services users are demanding in a secure, cost-effective manner, enterprises need a network access architecture engineered for mobility. The Aruba Networks® Mobile Virtual Enterprise (MOVE) architecture delivers just that.

Aruba MOVE™ unifies disparate, wireless, wired and remote access methods into one cohesive access solution – for traveling business professionals, remote office workers, corporate headquarters employees and guests.

It unifies network access services and provides context-aware access controls based on user, device, application and location, enabling IT to embrace mobility and BYOD cost effectively with an architecture that supports a variety of deployment options based on an enterprise's size, needs and budget.

With Aruba MOVE, the entire mobile enterprise workforce has consistent, secure access to the appropriate network resources based on who they are, where they are, what device they're using, and how they're connected.

Because MOVE securely unifies disparate networks and eliminates redundant services, it provides capital and operational cost savings that free up IT dollars so enterprises can embrace the influx of mobile devices and deliver secure mobile access to applications and other new business initiatives.

MOVE consists of a set of network services, such as identity management and context-based policy enforcement, coupled with affordable access modes that utilize these services across all locations and access methods.

Collectively, these services and access modes deliver:

- A unified services architecture that gives IT a common set of network services for managing security, policy and network performance across the entire access infrastructure, ensuring service consistency while reducing duplicate infrastructure;
- A context-aware security model for both corporate-owned and personally-owned devices, eliminating the need to support VLANs at the network edge and enabling BYOD;
- Simple, self-provisioned access for mobile devices, freeing up IT time and resources;
- Application-aware networking, ensuring that business-critical applications get the quality of service they need to operate effectively; and
- Deployment options designed to address organizations of all sizes.

With Aruba MOVE, IT can fully enable the mobile enterprise. MOVE delivers a unified access network architecture designed to support increasing numbers of mobile devices and users, to improve service delivery, and to meet the deployment needs of enterprises both large and small.

The mobile enterprise has arrived

Mobile devices – from Apple’s iPhone, iPad, and iPod Touch to Android-based devices and those running Windows Mobile 7 – have become the application and Internet platform of choice for millions of users, displacing PCs as the default computing platform.

Research firm Gartner Inc. estimates that the combined installed base of smartphones and browser-equipped enhanced phones, for example, will exceed 1.82 billion units by 2013. From 2013 onward, this combined installed base will be greater than the installed base for PCs.¹

Increasingly, users are bringing personal smartphones, tablets and laptops to work and putting pressure on IT to provide anytime, anywhere access to corporate applications, data, and other resources.

In other cases, employers are moving away from corporate-provided devices and encouraging employees to purchase their own. As part of this broad BYOD trend, users and IT staff demand the ability to connect to the enterprise network from any location using any (and all) of their mobile devices.

Additionally, the dynamic social networking experience that originated on the consumer Internet has unleashed a wave of business-critical applications across the enterprise. Users are employing smart phone apps that let them chat with an expert on another continent, for example, conduct virtual whiteboard sessions with remote colleagues and videoconference easily.

Users have come to expect the same rich, interactive media experience in their work tools and applications, including audio, streaming live content, and high-definition video on-demand, that they get from Facebook and YouTube.

Cloud computing has reduced the resources IT needs to support end-user desktops and local servers. Many applications no longer reside on users’ desktops; they run in the cloud from data centers hundreds, even thousands, of miles away.

However, the combined nature, volume, and diversity of today’s applications and user devices have increased the importance of managing quality of service (QoS) across the network. IT needs to ensure, for example, that the engineering team’s multi-country videoconference isn’t dragged down by an employee trying to download a video from YouTube.

All of these new mobile devices rely on a wireless network (Wi-Fi in the enterprise, LTE outside) that is reliable, secure, and high performance. Industry adoption of 802.11n has led to dramatic increases in wireless LAN (WLAN) speed and reliability, making it possible to support an array of data, voice and video applications over mobile devices. But WLANs are only a part of network access.

Mobile devices are the new laptop. To accommodate this new reality, enterprises need a unified access network architecture that’s optimized for mobility.

¹ Gartner, Inc., Top Predictions for IT Organizations and Users, 2011 and Beyond: IT’s Growing Transparency, 23 November 2010, ID: G00208367

Yesterday's network is mismatched for today's users

Existing enterprise networks were not designed to handle the demands of today's mobile users. Conceived when access was confined to corporate campuses, legacy infrastructure designs depend on a plethora of network devices and security appliances to protect physical assets within the walls of the enterprise.

This approach made sense when the same person connected to the same port and used the same client device and accessed the same applications. But that assumption is no longer true.

In today's mobile enterprise, users want to connect to the network from anywhere, anytime, using any device, even personally-owned devices – very few of which have Ethernet ports. And they want to roam freely between office, conference room, car, home, and virtually any other location.

However, legacy network infrastructure is woefully mismatched to these mobility requirements in three key areas:

Policy control: VLANs are obsolete, context is key

Mobility requires a new way of thinking about and managing network services, such as authentication, authorization, quality of service (QoS), and policy definition and enforcement. Consider the process of identifying a user and determining if that user should have access to a particular application. How does this process change based on that user's location?

- If the user connects to a port in a conference room, a network access control (NAC) solution and virtual LAN (VLAN) might control access.
- On the wireless LAN, a separate access control system and VLANs might be required.
- From a home office, a user will require a VPN connection.

What happens if a security policy changes? Or a new application comes online? Or an employee with a personal smartphone that's configured to access the WLAN quits?

To manage services and policies, must understand the underlying technologies for a multitude of devices and services, and resolve the inevitable changes in the network. The fragmented infrastructure leads to fragmented policies, which leaves the enterprise vulnerable to numerous security risks.

In addition, many organizations traditionally rely on VLANs to segment the network for traffic control; for example, to isolate specific user populations, such as guests, and to constrain access.

However, VLANs operate at the port level, so are only visible at the network edge. To support mobility, IT needs visibility and control beyond the port level to define security, QoS, and other policies based on contextual information, including who the user is, how and where they're connecting to the network, with what device, and for what purpose.

This contextual information is crucial to ensuring that the right policy is applied at the right time. For example, an enterprise may want to provide a sales manager with limited access to order information via a smartphone, but full access when using a laptop.

Similarly, IT may want to use QoS policies to expedite a surgeon's request for a patient's medical records while throttling pod-cast downloads by visitors in the hospital waiting room.

VLANs cannot scale to the number of pieces of context needed to secure the mobile enterprise. IT would potentially need to create a separate VLAN/SSID for an employee using an iPad at headquarters, a separate VLAN/SSID for when he uses his iPad at a branch office, and separate VPN rules for using his iPad on the road, for example.

In the mobility era, VLANs are obsolete. What enterprises need is a context-aware network that allows IT to manage a single set of services across the organization, and the flexibility to define policies based on who the user is, where they are located, the device in use, and where they want to go on the network.

No more silos – roaming requires unified access

Today's IT organizations support three distinct networks:

- The traditional wired network;
- The rapidly growing WLAN, functioning as an overlay to the wired network; and
- VPNs for secure connectivity from branch and home offices.

These networks have separate infrastructures, including separate technologies, devices, management platforms, and security appliances, which results in duplicate functions.

As a result, IT is burdened with ensuring that services, such as authentication and policy enforcement, as well as application performance are consistent across networks. This complexity drives up security risk along with operations costs.

Siloed networks inhibit consistent policy definition and enforcement, which impedes user mobility. They make roaming impractical by requiring users to login each time they change location.

What the mobile enterprise needs is a unified access architecture that lets IT manage and secure the wireless, wired and remote access infrastructures as if they are one single network; apply a consistent set of policies; and enables users to roam with their mobile devices without having to re-authenticate when they move location.

WLANs built for coverage now need capacity

Up to now, the wired network has been users' primary mode of accessing enterprise applications and resources. Because relatively few user devices were wireless, organizations built their WLANs simply to provide adequate coverage across the campus, and then built mobility support on top.

As the mobility trend gains momentum, however, many enterprises find themselves with an over-built wired infrastructure and under-sized WLAN.

The influx of mobile devices and the rise in multimedia applications is driving the enterprise need for a high-performance, highly reliable WLAN that can support a high density of users and traffic.

Enterprises need a standards-based WLAN solution that can cost-effectively deliver the capacity and characteristics, such as auto-configuration, needed to support rising numbers of mobile devices and user mobility.

MOVE: Context-aware access architecture for the mobility era

Aruba Networks knows that the next generation of access networks must focus squarely on mobile users, their devices and their applications – not on infrastructure or ports.

Consequently, the Aruba Mobile Virtual Enterprise (MOVE) architecture is designed to unify disparate wireless, wired, and VPN networks and services, including identity management, security, and network configuration, enabling IT organizations to fully support the mobile enterprise.

The Aruba MOVE architecture addresses the needs of the mobile enterprise by providing:

A context-aware network and services

Aruba designed MOVE as a context-aware access network that collects four attributes for each session:

- User identity and role, such as employee, contractor, guest, student, faculty;
- Device identity, including type (laptop, tablet, smartphone, etc.) and ownership (corporate vs. personally owned);
- Application fingerprint, including type (data, video, voice) and its location (in the cloud, data center, etc.); and
- Location, including the user's location (headquarters, branch office, remote, etc.), time of day, and access medium (wireless, wired, cellular).

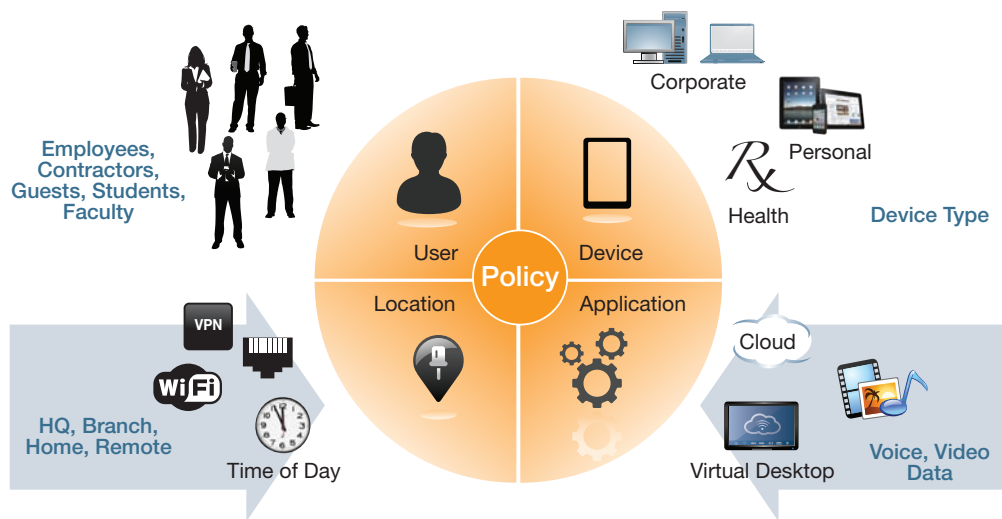


Figure 1. Context-aware network

The Aruba MOVE architecture provides concurrent visibility into the identity of all users, their devices and their locations on both wired and wireless networks. Consequently, it is easier for IT organizations to quickly identify and mitigate potential threats.

For example, an Aruba retail customer with stores located in busy shopping areas captures 20,000 potential rogue APs each day. If the retailer had to investigate each individual event, it would be unable to find any actual rogues until after damage had been done. Aruba's ability to correlate wireless and wired events enables the IT security team to prioritize its threat-mitigation effort.

MOVE's context-based approach to network access eliminates the need to maintain VLANs at the network edge. Context-aware access policies allow IT to control users and devices so that employees can switch effortlessly between desktops, laptops, tablets, smartphones and other mobile devices and have a single, consistent way to access the appropriate corporate resources.

In addition, MOVE provides a common set of network services that include:

- Identity management
- Device profiling and configuration
- Device posture check
- Guest access
- Context-based policy enforcement
- Application traffic management
- Content security
- Network configuration
- RF and spectrum management
- Compliance enforcement and reporting

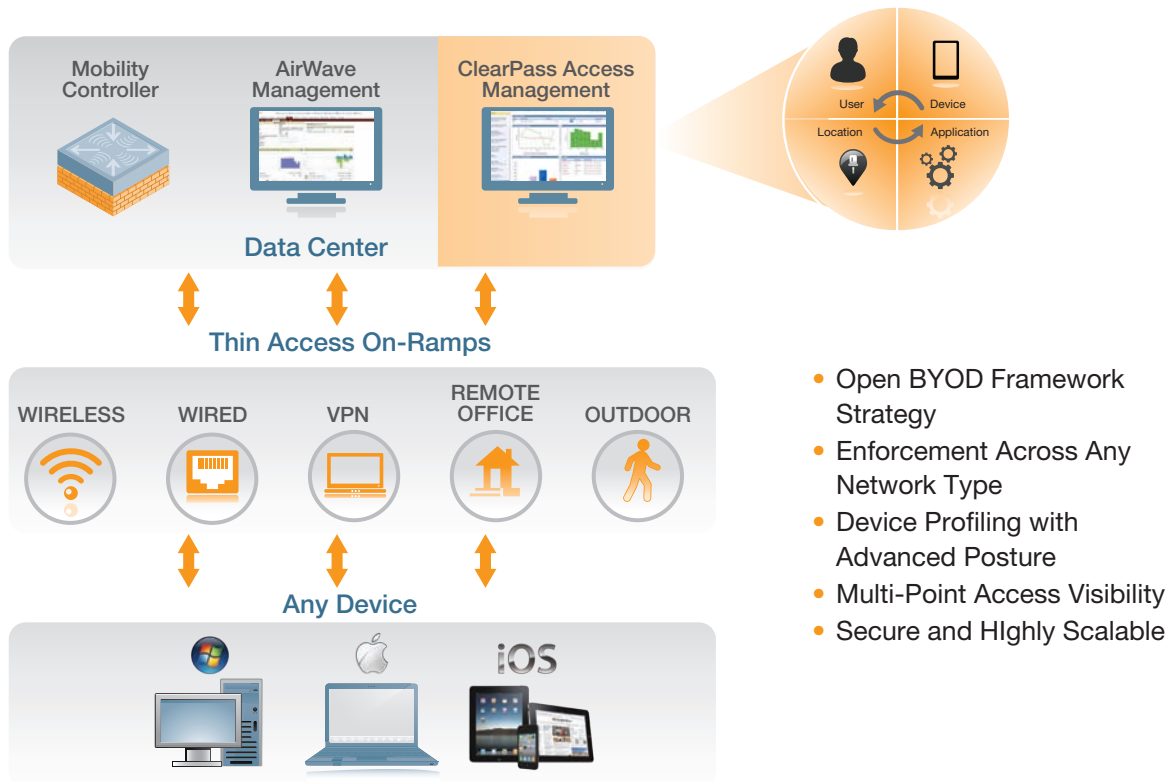
Aruba MOVE network services consolidate the functions of multiple independent management tools, configuration servers, location servers, NAC systems, VPNs, spectrum analyzers, and wireless intrusion detection systems.

This enables IT to define services once, via an Aruba Mobility Controller, eliminating the need to touch a profusion of wiring closets, firewalls, NAC solutions, management systems and reporting tools that operate in separate domains.

MOVE ensures that network operations are consistent across the entire enterprise, as is the user's experience, regardless of user role, location, access method, mobile device or applications.

Why Aruba?

Aruba customer BAA, one of the world's largest commercial airport operators, deployed a single, unified network infrastructure at Heathrow Airport's Terminal 5 to provide public Wi-Fi access for 80,000 people every day, support key staff functions like baggage reconciliation, and run point-of-sale and other applications for airport retailers. "In our view, Aruba had the only architecture that could guarantee the level of security we required," said Kevin Fallon, commercial leader of Terminal 5 systems at BAA.



- Open BYOD Framework Strategy
- Enforcement Across Any Network Type
- Device Profiling with Advanced Posture
- Multi-Point Access Visibility
- Secure and Highly Scalable

Figure 2. Expanded MOVE architecture

MOVE with unified access

Aruba MOVE unifies the wireless, wired, and VPN infrastructure, providing a consistent set of services and access controls while lowering support costs. Aruba Mobility Access Switches and wireless APs are self-installing and self-configuring via predefined parameters created in the Aruba Mobility Controller.

This zero-touch approach eliminates hundreds of hours of manual work; instead of spending a half hour to configure every device, the Mobility Controller pushes out configurations to all devices.

As a result, IT can more easily remote locations without on-site IT staff, as well as make additions, moves and changes more quickly.

Based on joint estimates with customers across a number of industries, companies can save as much as two person-days per week by adopting the Aruba MOVE architecture.² That's 40 percent of a network engineer's time that is now available for new projects, such supporting the deployment of iPads, tablets and other mobile devices.

Aruba MOVE supports a wide range of network access modes that leverage its common set of network services to deliver consistent, reliable and secure context-aware access to users. These access modes include:

- **Wireless access points (APs):** Aruba 802.11n APs support distributed and centralized traffic forwarding modes, while providing best-in-class RF management through Adaptive Radio Management (ARM) technology.

All Aruba APs offer RF management and monitoring capabilities without requiring dedicated modes of operation. For example, the Aruba AP-134 and AP-135 set the standard for Wi-Fi coverage in business environments with extremely high concentrations of mobile devices.

- **Mobility Access Switch:** Aruba has extended the user-centric, services-based approach of the MOVE architecture to a new class of wired APs. Designed to provide network access in wiring closets, Aruba S3500 Mobility Access Switches connect wired Ethernet devices such as virtual desktops, IP phones, videophones, video surveillance cameras and 802.11 APs.
- **Remote APs:** Aruba Remote APs (RAPs) automatically extend corporate enterprise resources to branch and home office networks using site-to-site VPN tunnels to the central data center. Using zero-touch configuration, employees at branch and home offices can easily set up their own RAPs with no IT assistance.
- **Outdoor:** Aruba wireless mesh routers combine a unique multi-radio, multi-frequency architecture and adaptive Layer 3 routing to bring high-performance networking to outdoor environments.

They deliver unparalleled speed, scale, and reliability as well as low latency and seamless handoffs for voice, video and other latency-sensitive applications across multiple hops in the wireless mesh network.

- **Virtual Intranet Access (VIA) client:** This Aruba software client provides secure remote network connectivity for Apple iOS, Mac OS X and Windows mobile devices and laptops.

WLANs built for tomorrow's traffic

Aruba makes it easy for enterprises to build a cost-effective, standards-based wireless infrastructure with the capacity and reliability necessary to handle increasing numbers of mobile devices and multimedia applications.

For starters, Aruba offers an extensive portfolio of devices that support the IEEE 802.11n standard, including single- and dual-radio indoor and outdoor 802.11n access points with external or integrated antennas.

Designed for high-performance, 802.11n technology delivers up to 300 Mbps of link speed for Wi-Fi radios compared to 54 Mbps with legacy 802.11a/b/g. This means increased bandwidth for users, faster performance for enterprise applications, and the ability to support high densities of mobile devices.

² Aruba Networks calculations. Please contact us for details.

In addition, 802.11n was designed for reliability. Whereas older 802.11a/b/g technologies use only one to transmit and one antenna to receive, 802.11n uses multiple antennas to transmit and receive signals, which boosts the signal quality and reliability on both ends of the Wi-Fi connection.

To further increase performance and reliability, Aruba developed its signature Adaptive Radio Management (ARM), which automatically manages the WLAN's 2.4-GHz and 5-GHz radio bands to optimize Wi-Fi client performance and mitigate RF interference. Key ARM features include:

- **Band steering**, which actively guides faster 802.11a/n clients, such as iPads, to the best available wireless channel in the 802.11 5GHz frequency band, resulting in a performance boost for applications due to better immunity from noise, fewer sources of interference, and more available channels.
- **Spectrum load balancing**, which dynamically shifts Wi-Fi clients to available 802.11 channels instead of individual AP radios, helps prevent network performance from degrading due to oversubscription of 802.11 channels.
- **Co-channel interference mitigation**, which operates across all APs and wireless clients on the same 802.11 channel, addresses the challenges of densely populated deployments, such as lecture halls and airport lounges.
- **Airtime fairness** gives all Wi-Fi clients on the same AP radio equal opportunity to transmit and receive, which is essential for dense client deployments.

In addition, ARM's auto application-detection capabilities can distinguish voice and video from data traffic and automatically apply the appropriate QoS mechanisms. Aruba WLANs also let IT organizations implement application-aware traffic filtering to further improve overall network performance; IT can use this capability, for example, to limit Apple iPad users' access to Bonjour and iTunes.

MOVE with scalable deployments

Aruba recognizes that enterprises come in many sizes and shapes. That's why MOVE is designed to support a variety of deployment options, allowing IT to implement the architecture that best suits their environment and easily grow their deployment as needs change.

With MOVE, mobility services such as authentication, authorization, policy definition and enforcement can be handled in a variety of devices depending on size and complexity of the network:

- **Start small:** A small enterprise that needs a reliable, secure and hi-performance WLAN can build a MOVE network that relies on Aruba Instant APs to deliver a full set of mobility services. If the organization also needs BYOD or guest services, IT can add that functionality with Aruba's ClearPass guest and device management appliances.

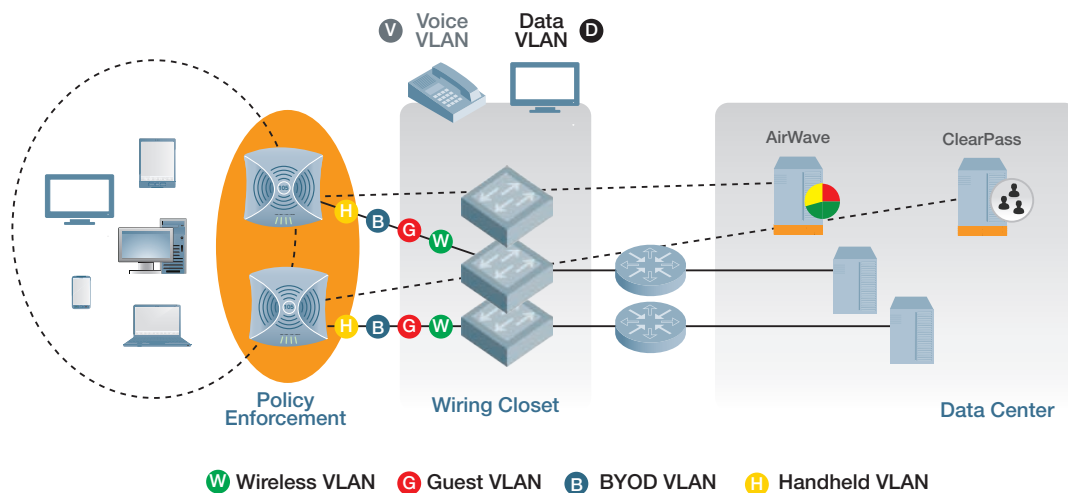


Figure 3. Start small

Grow the WLAN: As the WLAN – or size of the enterprise – grows, IT may opt to have the mobility services running in a wiring closet, with the policy enforcement also taking place there. Aruba’s S3500 Mobility Access Switch is capable of acting as a WLAN Mobility Controller, defining and enforcing policy from attached APs.

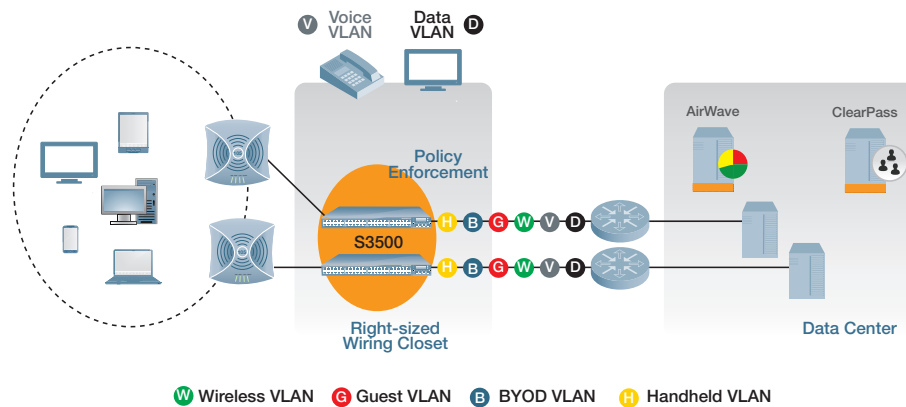


Figure 4. Grow the WLAN

Large environments: Enterprises with multiple wiring closets and a large WLAN infrastructure may want MOVE services centralized in a specialized appliance, such as the Mobility Controller, located in the data center. Aruba offers a range of Mobility Controllers to scale to even the largest of customer environments.

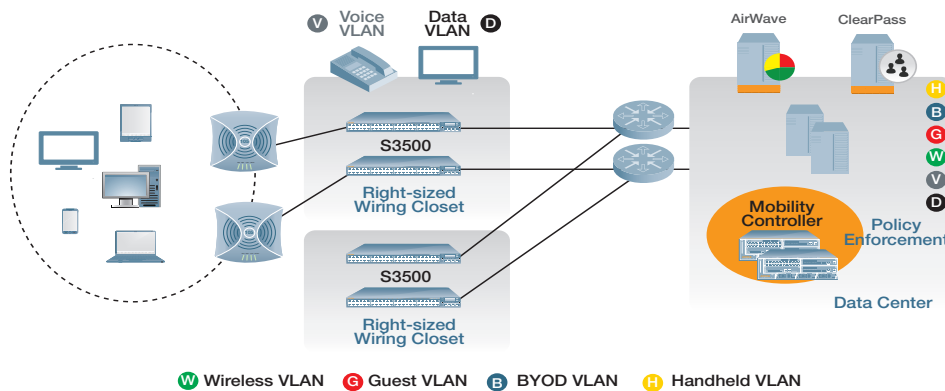


Figure 5. Large environments

Extend mobility to branch offices and teleworkers: Enterprises that want to provide users working from branch offices, home offices, and other remote sites can utilize Aruba Remote Access Points as well as the Virtual Internet Access (VIA) client in those locations to provide a consistent set of mobility services that treats remote users as if they were in the headquarters.

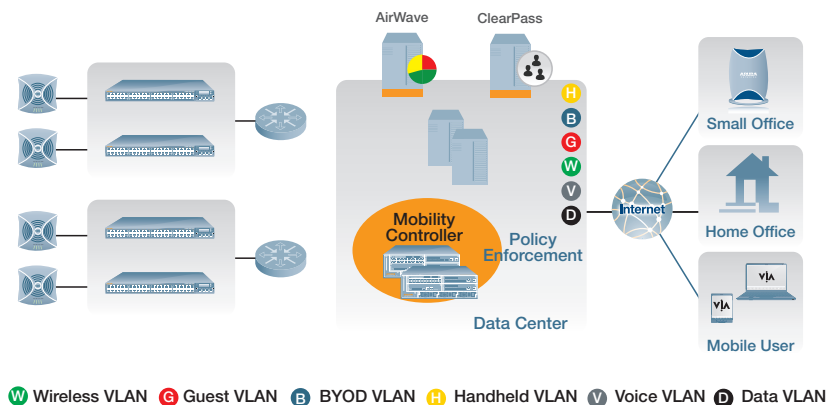


Figure 6. Extend mobility to branch offices and teleworkers

Embrace the mobility era with MOVE

By providing a mobility-centric architecture, Aruba's MOVE transforms an enterprise's legacy network into a flexible infrastructure for mobile users. It does so by unifying disparate wireless and wired infrastructures into one seamless network access solution – for traveling business professionals, remote workers, corporate headquarters employees, guests and other users.

With Aruba MOVE, access privileges are linked to a user's context. That means the enterprise workforce has consistent, secure access to network resources based on who they are, where they are, what devices they're using, and how they're connected. It's an architecture that's driven by mobility and the proliferation of Wi-Fi-enabled mobile devices, designed to support BYOD access.

MOVE eliminates the cost and complexity of managing separate wireless and wired access policies and VLANs at the edge. With Aruba, enterprises can unify their access infrastructure, boost WLAN capacity, and improve service delivery for the growing number of mobile users and devices.

About Aruba Networks

Aruba is the global leader in distributed enterprise networks. Its award-winning portfolio of campus, branch/teleworker, and mobile solutions simplify operations and secure access to all corporate applications and services – regardless of the user's device, location, or network. This dramatically improves productivity and lowers capital and operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at www.arubanetworks.com. For real-time news updates follow Aruba on [Twitter](#), [Facebook](#), or the Green Island News Blog.



www.arubanetworks.com

1344 Crossman Avenue. Sunnyvale, CA 94089

1-866-55-ARUBA | Tel. +1 408.227.4500 | Fax. +1 408.227.4550 | info@arubanetworks.com