The Aruba MOVE Architecture: Integrating Access Management, Network Infrastructure and Mobility Applications
Table of Contents

User freedom has become IT’s burden 3
The MOVE architecture 4
Access management with MOVE 4
The ClearPass access management system 5
  Network access control (NAC) 6
  Device onboarding and management 6
  Mobile application management 7
BYOD and guest self-service portals 7
  WorkSpace mobile app 8
  Guest portal 8
Mobility Controllers 9
Mobility Controller deployment options 10
AirWave management system 10
Network infrastructure 11
  WLAN APs 11
  Mobility Access Switches 12
  Remote APs 12
  Virtual Intranet Access (VIA) client software 13
Mobility applications 13
  Access management apps for employees and guests 13
  Meridian mobile app for visitor engagement 14
  Open APIs for third-party applications 14
MOVE – A complete mobility and BYOD solution 14
About Aruba Networks, Inc. 15
The number of mobile devices will soon equal the number of people on the planet, whose islands of Wi-Fi in homes, offices and hotspots are blending into a continuous ocean, bringing bandwidth everywhere, to everybody.

The combination of instant access and mobility is shaping numerous facets of everyday life, including the next-generation workplace.

Employees, contractors, guests, and even customers now expect access to multimedia content, collaboration technologies and cloud-based applications from any location, with any device.

Users have blurred the lines between corporate-owned and bring-your-own devices (BYOD) and are downloading new mobile applications at an astonishing rate of 130 per minute, according to Gartner.

User freedom has become IT’s burden

So it's no surprise that supporting mobile users and their devices has become a fact of life for IT departments in enterprises of all sizes. What seems easy to a user – getting network access via a personal device – is quite complex for IT.

IT staff members in different functional areas must make changes to separate network, security, and management systems.

This takes time because today’s network and supporting system designs are fixed and port-centric, relying on policies that are tied to a user’s role, with no regard for the multiple devices and applications in use.

Local area networks (LANs) are separated from wide area networks (WANs) with different access rights, but both are available in the same office. Each wiring closet has a separate configuration and so does the wireless LAN (WLAN).

Coordinating changes across these silos takes time and leads to access problems, poor performance, and security risks – all of which slows business responsiveness and leads to user frustration.

The Aruba Networks® Mobile Virtual Enterprise (MOVE) architecture addresses these challenges by unifying all things mobility – access management, the network infrastructure and mobility applications – into one cohesive and manageable system that strengthens security and simplifies bring-your-own-device initiatives.

MOVE is software-centric so it can adapt to the dynamics of mobility. This enables IT to manage traffic flows on any wired, wireless and remote network and control how devices and work applications are used. Whether away or at work, MOVE gives users consistent, secure access to the appropriate corporate resources based on who they are, where they are and what device they’re using.

The result is a rightsized network infrastructure that saves IT time, reduces capital and operating expenses, speeds-up service delivery, and provides every user with the highest-quality mobility experience.
The MOVE architecture

A complete BYOD and mobility infrastructure solution, MOVE leverages contextual data – user roles, device types, application flows, location and time-of-day – and extends this intelligence across the network to devices and apps.

The MOVE architecture encompasses three major components:

- **Access management.** This encompasses the ClearPass Access Management System™ for application, device and network usage controls; AirWave management for wired, wireless and remote networks; and Mobility Controllers for flow-based traffic management.
- **Network infrastructure.** This comprises 802.11ac WLAN access points (APs), Mobility Access Switches, Remote Access Points™ (RAPs), and Virtual Intranet Access™ VPN client software.
- **Mobility applications infrastructure.** These end-user tools include the Aruba WorkSpace mobile app for BYOD; Aruba APIs for location and analytics applications; and Meridian apps for visitor engagement.

MOVE can be deployed in various ways, including cloud or on-premises with centralized or branch options, based on an enterprise’s size, needs and budget. This flexible approach enables IT to support mobility and BYOD cost effectively for any business or organization.

![Figure 1. The mobility-centric MOVE architecture.](image)

**Access management with MOVE**

With MOVE, Aruba brings access management into the mobility era. Using the ClearPass Access Management System, MOVE combines access policies for networks, devices, and applications into a single policy-definition point.

With ClearPass can centrally define policies, which are then enforced across any vendor’s network and multiple vendors’ mobile device management (MDM) agents, as well as the Aruba WorkSpace mobile app for BYOD.
The result is a significant time savings for IT and a dramatic reduction in errors associated with correlating security policies across multiple systems. Enterprises benefit from policies that are consistently applied, no matter where users connect or what devices they use.

MOVE also centralizes wired, wireless and remote network management with the AirWave management system. Regardless of how people connect, AirWave consolidates usage information on all users, devices and apps into intuitive dashboards and workflows. Whether it is a real-time RF troubleshooting task or historical forensics for regulatory compliance, AirWave addresses critical needs of managing a modern, multi-faceted mobility network.

Finally, MOVE makes access management more dynamic with both controller-based and controllerless options. Legacy systems that require IT to use manually configured, static access – based on VLANs, ACLs, SSIDs, routes, and other mechanisms – create high overhead for IT and thwart mobility. With MOVE, Aruba Mobility Controllers and controllerless APs replace these old, fixed controls with programmable flow-based traffic management.

Mobility Controllers and controllerless APs employ a context-aware firewall that can distinguish one traffic flow from another and automatically adjusts how traffic is handled based on the mix of users, devices, applications and their location.

MOVE is unique in that access management is a software-defined layer that sits above the access network infrastructure. As a result, enterprises can easily monitor and improve mobile access without upgrading and reconfiguring their existing networks.

The ClearPass Access Management System

![ClearPass diagram](image)

*Figure 2. ClearPass gives you one place to manage all things BYOD.*

The ClearPass Access Management System integrates network, device and application policy management into a single comprehensive software platform.

With ClearPass, IT can manage role-based access policies, onboard and profile devices, distribute and secure mobile applications, and admit guest users – all from a single user interface.

By unifying access policies, ClearPass gives IT the ability to enforce security policies on all devices, applications and networks from one system.
IT can now control who can access what, when, where, and how, across wired and wireless, and extend those same policies to devices and work apps – even when they are not connected to the company network.

In today’s BYOD and mobile workforce world, IT can’t afford the time or risks involved in configuring controls for every network, device and application. ClearPass eliminates these silos and gives IT a platform where network, device and application policies build on each other.

IT can now define more comprehensive security policies than ever before to protect company data and prevent unauthorized access to resources. For example, IT can use ClearPass to write a policy that will wipe and lock confidential applications if a device is detected as jailbroken.

Such a policy isn’t possible without ClearPass because the system that detects a jailbroken device is typically different from one that distributes and manages mobile applications.

Likewise, IT can now define a policy that leverages application and device visibility to enforce network policies. That means a device running Microsoft Lync video conferencing can get priority treatment while the wired and wireless networks automatically forward AirPlay traffic across subnets for guests who wants to use their own device to project to an AppleTV in a conference room.

ClearPass provides three main policy definition and enforcement capabilities – network access control, device onboarding and management and mobile application management (MAM).

**Network access control (NAC)**

ClearPass provides NAC for wired, Wi-Fi and remote access networks. Within ClearPass, IT can define multiple network usage restrictions – including BYOD and guest policies – that extend across any existing infrastructure.

Using the RADIUS protocol, ClearPass policies are downloaded on-demand at the time a user connects – whether through wireless, wired, VPNs or a branch network – and remain in force for as long as the user is connected.

ClearPass gives IT the flexibility to write policies for different types of networks, devices and users.

For instance, IT can write a BYOD policy that gives an authorized employee access, via a personal smartphone, to email and the Internet but not internal financial applications that contain confidential data.

Similarly, a guest access policy can limit guests to Wi-Fi Internet access in the lobby with limited bandwidth, between the hours of 9 and 5.

**Device onboarding and management**

To speed-up device deployments, ClearPass forces every new device to go through a self-configuration wizard, which prompts users to download device credentials as well as network and security settings.

ClearPass can then provision its OnGuard NAC agent for laptops and desktops, Aruba WorkSpace MDM/MAM agent for smartphones and tablets, or alternatively support third-party NAC and MDM agents. The ClearPass Policy Manager lets IT implement a wide range of device policies, which are enforced by these agents.
For example, IT can define security policies that require users to employ a strong password, download a unique credential, check if their devices have up-to-date antivirus software, and check if their devices are jailbroken – before accessing the network.

**Mobile application management**

ClearPass lets IT define a variety of application policies. For example, a security policy may require a device on company premises to encrypt data for specific finance applications and require a VPN connection if the data is in motion.

IT can additionally define a policy that restricts application use based on location or time-of-day. This type of policy can be useful in retail by limiting employee use of point-of-sale applications on certain mobile devices to specific hours and at specific stores.

Motion-sensitive policies can also be defined. For example, to prevent liability issues, IT can create a policy that prevents access to corporate email and other business applications while a user is in motion, which could result in distracted driving.

To ensure application policies defined with ClearPass are enforced on any private or public network, the Aruba WorkSpace mobile app adds a policy enforcement wrapper for business applications installed on user devices.

**BYOD and guest self-service portals**

ClearPass empowers mobile users and streamlines IT operations through employee and guest access portal applications.

The Aruba WorkSpace mobile app lets employees personalize their BYOD experience while enforcing IT-defined security policies on personal devices. Similarly, the Aruba guest web portal enables guests to self-register and get access to Wi-Fi networks in an automated fashion.
WorkSpace mobile app

As part of ClearPass, the WorkSpace mobile app lets IT push a customized work environment to every employee’s mobile device, automatically creating a corporate workspace that’s based on the user’s unique identity and device type.

Employees can use this personalized portal to access and manage their work apps and onboarded devices, provision Wi-Fi access for their own guests, and even share AirPrint and AirPlay devices with other users and groups – all without help desk assistance.

With WorkSpace, an employee’s work apps are available through a single sign-on. Users can view the policy status of these apps and download optional productivity apps from an enterprise app store or disable unused apps.

The WorkSpace mobile app acts as a policy enforcement agent on personal devices that references policies defined in ClearPass.

For example, WorkSpace can require application data to be encrypted on the device and over the network. IT can also prevent data leakage by restricting cloud backups, active directory authentication, and cut-and-paste between work and personal applications.

Furthermore, if an employee loses a device or the device is stolen, IT can securely lock or wipe the company applications and data on that device, while leaving personal applications and data untouched.

Guest portal

With Aruba’s guest web portal, IT can collect any information it needs about a guest, and optionally route guest access requests to a sponsor within the company, who is required to accept the request before the guest account is created.

Guest accounts can be set to expire automatically after a specified number of hours or days. And IT can use customizable templates to create guest access usage reports to satisfy compliance and auditing requirements.
Using customizable web skins, enterprises can also create uniquely branded guest login and device registration portals as well as push messages, advertisements, event notifications and other useful information to guests.

In addition, Aruba’s guest portal application easily integrates with third-party lobby, customer relationship management (CRM) and patient check-in systems, so users don’t have to enter information in multiple places.

**Mobility Controllers**

Network policies are only effective if the underlying network is intelligent enough to have visibility into traffic and can control it. Aruba brings intelligence to the network with its Mobility Controllers, which provide flow-based traffic management.

Aruba Mobility Controllers employ an integrated context-aware firewall to recognize who is connected, what devices and applications are being used, and in what location, and automatically adjusts traffic flows across the network.

Flow-based traffic controls make it much easier for IT to manage today’s influx of multimedia and cloud-based applications as well as software-based services like voice-over-WLANs and unified communication.

Network-wide flow-based controls simplify the management of cloud-based applications and software services because they are applied only to the underlying user traffic instead of the protocol carrying user traffic.

As a result, IT can optimize video and voice streams or assign bandwidth to business-critical applications while restricting the performance of personal applications, even though all apps run on a web browser and appear as HTTP/HTTPS traffic.

Policy enforcement actions with a Mobility Controller include:

- **Steer traffic based on visibility into user role, devices and apps.** If an employee wants to use AirPlay in a conference room or AirPrint to a nearby network printer, Mobility Controllers recognize these flows and show the Apple TVs and printers closest to and allowed for that user. There’s no need to manually-configure VLANs and ACLs, which is virtually impossible in a large campus.

- **Track and prioritize flows for encrypted traffic.** Mobility Controllers can differentiate an encrypted Microsoft Lync video conferencing session from a file download and respond appropriately by prioritizing the video flow.

- **Control bandwidth use by time of day, location and other metrics.** The context engine in Mobility Controllers discerns work apps from personal apps, even if they’re web- and cloud-based. Personal apps get less bandwidth while work apps get all the bandwidth they need.

- **Optimize WLAN bandwidth for video.** When a user launches a latency-sensitive application like Microsoft Lync video, Mobility Controllers automatically increase the bandwidth and quality of service (QoS) to optimize the user’s experience.
Mobility Controller deployment options

To accommodate enterprises of various sizes and organizational structures, Aruba offers three deployment options for Mobility Controllers.

1. In the network core. Ideal for campuses, APs and Mobility Access Switches tunnel all traffic to a Mobility Controller in the core, where it performs flow-based traffic management. This acts as a single touch-point for VLANs and IP addresses and speeds-up Layer 3 roaming.

2. DMZ Mobility Controller. Ideal for small branch offices and teleworkers, a remotely-located AP or Mobility Access Switch sets up a VPN tunnel to the data center. Enterprise apps and traffic are selectively forwarded to a Mobility Controller in the DMZ, where traffic flows are managed. Web and non-critical traffic go directly to the Internet from the remote site.

3. Controllerless deployment: Ideal for branch networks, Aruba Instant™ performs flow-based traffic management in software inside APs. One dynamically-elected Aruba Instant AP performs all the functions that a hardware-based Mobility Controller does.

Aruba Instant APs bring enterprise-grade security, resiliency and scale to branch networks. Configuration is a snap. Just power-up one Instant AP, configure it wirelessly, and it automatically distributes the network configuration to other Instant APs in the WLAN.

Despite its enduring enterprise-class capabilities, the Aruba controllerless WLAN solution is extremely economical and eliminates the overhead of forwarding enterprise traffic back to headquarters.

AirWave management system

In addition to providing centralized management, AirWave gives IT complete visibility into multivendor wireless, wired and remote networks across multiple locations. It actually shows devices and applications on the network and automatically tracks the location of every user and device.
With AirWave, IT can perform real-time monitoring, manage RF coverage and wireless security, troubleshoot problems and perform forensic analysis, log incidents, run custom and historical reports, and demonstrate regulatory compliance.

IT benefits from being able to manage wired and wireless network devices, RF coverage, users and their devices, and application behavior through a single pane, with convenient dashboards for at-a-glance visibility into all network activity.

In contrast to the challenge of correlating events across multiple siloed management systems, AirWave’s centralized approach makes it easier for IT to troubleshoot and resolve problems quickly while maximizing network uptime and IT resources.

AirWave offers full visibility into network security to satisfy reporting and compliance requirements. The network is automatically audited for configuration errors that result in policy violations and full reports can be generated so IT can easily correct improper configurations.

For rogue detection, AirWave aggregates, correlates, alerts and logs IDS attacks to improve network security and compliance. It also provides the full roaming history of users and complete audit logs of AirWave administrative access, including actions taken and by whom.

Network infrastructure

The second component of the MOVE architecture is Aruba’s industry-leading network infrastructure solution, which includes WLAN APs, Mobility Access Switches, Remote APs, and Virtual Intranet Access™ VPN client software.

WLAN APs

Aruba’s purpose-built 802.11ac and 802.11n APs support Mobility Controller-managed and controllerless operating modes, while featuring integrated Adaptive Radio Management™ (ARM), ClientMatch™, AppRF and airtime fairness technologies.

All Aruba APs automatically select the right channel and transmit power for a device. In addition, APs leverage unique application-awareness in conjunction with patented algorithms for airtime fairness, which ensures that all devices have equal access to the WLAN.

Aruba APs also support zero-touch cloud provisioning with Aruba Activate™, which enables APs to get their configurations automatically from a cloud-based provisioning system. No manual intervention is required. APs can use Aruba Mobility Access Switches or the existing wired network for power-over-Ethernet (PoE) and backhaul.
To maximize client performance, patented ClientMatch technology continually monitors each device’s capabilities and WLAN connection and matches it to the best radio on the best AP. This occurs at the time of connection, as clients roam and as network conditions change.

If a client moves to another AP’s coverage area or interference causes performance to drop, ClientMatch will automatically steer the device to an AP or channel that delivers better performance.

For outdoor environments, Aruba wireless mesh routers deliver high-performance Wi-Fi client access and data backhaul and feature a unique multi-radio, multi-frequency architecture that supports adaptive Layer 3 routing. In addition to speed, scale, and reliability, they offer seamless handoffs for voice, video and other latency-sensitive apps across multiple hops.

**Mobility Access Switches**

Designed to provide network access in wiring closets and branch offices, Mobility Access Switches connect wired Ethernet devices such as virtual desktops, IP phones, videophones, video surveillance cameras and 802.11 APs.

Multiple models are available with a variety of port configurations, modular components and physical footprints. Mobility Access Switches feature ArubaStack technology, which enables up to eight switches across multiple wiring closets to operate as one virtual stack or cluster.

Mobility Access Switches are ideal companions to Aruba APs because they work together as one system. Mobility Access Switches reserve port PoE power for APs, automatically learn VLAN configurations, and shut down a port that’s classified as a rogue AP.

Leveraging a Mobility Controller, Mobility Access Switches also support a common policy framework across the entire wired and wireless network. In branch offices, Mobility Access Switches can use Mobility Controller tunnels for site-to-site VPNs.

**Remote APs**

Aruba RAPs™ extend corporate enterprise resources to branch and home offices by establishing VPN tunnels to a central data center.
Offering wired and wireless connectivity, single- and dual-radio RAPs perform role-based access control, policy-based forwarding, air monitoring, and wireless intrusion protection. Zero-touch configuration makes it easy for employees to set up their own RAPs with no IT assistance.

Virtual Intranet Access (VIA) client software
VIA™ VPN client software provides secure Wi-Fi connectivity for Android, iOS, Mac OS X and Windows mobile devices and laptops. Unlike legacy IPsec VPNs, VIA chooses the best enterprise network connection and configures mobile device settings to ensure a simple, zero-touch wireless experience.

Mobility applications
The third cornerstone of the MOVE architecture encompasses an extensive range of enterprise mobility application infrastructures for IT, employees and guests, including the WorkSpace mobile app for BYOD and Meridian mobile app for visitor engagement. Aruba also supports a rich ecosystem of app developers through open APIs.

Access management apps for employees and guests
As mentioned earlier, the Aruba WorkSpace mobile app empowers employees to personalize their BYOD experience while reducing demands on IT resources. And the fully automated Aruba guest web portal app makes it easy for visitors to self-register for network access.
Meridian mobile app for visitor engagement

Meridian-powered custom and consumer mobile apps leverage location over Wi-Fi information to deliver indoor GPS services to casinos, hospitals and large public venues. Many retailers and resort hotels use Meridian to engage customers with targeted location-based messaging.

Open APIs for third-party applications

Using access and network infrastructure APIs, third-party app developers can leverage contextual data about users, devices, applications and policies to create rich applications for unified communications, MDM, location, analytics, security, and content services.

Third-party app developers can also leverage these Aruba APIs to push context-specific information out to users. Meridian Apps is a noteworthy example of a developer whose enterprise mobility apps are enabled by the Aruba MOVE architecture.

MOVE – A complete mobility and BYOD solution

By consolidating access management, network infrastructure and mobility applications into a single MOVE architectural framework, there’s no longer a need for IT to purchase, deploy, configure and manage multiple, siloed mobility and BYOD systems.

MOVE ensures that every policy that IT creates is extended across the entire enterprise network to every device and application – even when users are not connected to the company network.
Additionally, MOVE lets enterprises rightsize their networks in preparation for the next-generation workplace. Flow-based traffic controls ensure network reliability and usability for the influx of rich multimedia applications that are populating mobile devices.

In Aruba’s vision of the next-generation workplace, IT organizations will reduce their reliance on fixed networks and legacy equipment, which will also dramatically reduce the capital costs of a refresh and ongoing operating expenses.

The MOVE architecture is software-based and designed for multivendor network environments. That means enterprises can implement the MOVE architecture on any network infrastructure with no upgrades whatsoever.

MOVE provides IT with a single, cohesive system that is responsive and adaptive to the dynamics of business and technology. The result is improved operational efficiency across IT boundaries, exceptional application performance, stronger security, and a mobile experience everyone can rely on.

About Aruba Networks, Inc.

Aruba Networks is a leading provider of next-generation network access solutions for the mobile enterprise. The company’s Mobile Virtual Enterprise (MOVE) architecture unifies wired and wireless network infrastructures into one seamless access solution for corporate headquarters, mobile business professionals, remote workers and guests. This unified approach to access networks enables IT organizations and users to securely address the Bring Your Own Device (BYOD) phenomenon, dramatically improving productivity and lowering 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, Africa and Asia Pacific regions. To learn more, visit Aruba at www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook, and for the latest technical discussions on mobility and Aruba products visit Airheads Social at http://community.arubanetworks.com.