The Next Generation Network Access Architecture for Mobile Technology
# Table of Contents

- Government agencies recognize the benefits of mobility ........................................... 3
- MOVE: A user-centric, role-based access architecture for wired, wireless and remote access .......................................................... 3
- Introducing Aruba MOVE for Government ................................................................. 4
- Access from a wide range of network on-ramps ......................................................... 5
- The benefits of simplified management ........................................................................ 6
- The business case for Aruba ........................................................................................ 6
- Conclusion ..................................................................................................................... 7
- About Aruba Networks, Inc. ......................................................................................... 7
Government agencies recognize the benefits of mobility

Government agencies are experiencing tremendous pressure from their end users to support commercial, consumer-grade mobile devices – smartphones, tablets and laptops. Just as in the corporate world, workers in the public sector have become accustomed to the productivity enhancements that these mobile devices bring to their lives and understand the value they can offer in the workplace. A variety of mobile devices like Android and Windows based smartphones and tablets, Blackberrys, iPhones, and iPads have been fielded by the end users themselves. These users want wireless LAN (WLAN) access when on-site, and they want 3G/4G support for global field mobility. Some end users, in attempts to fulfill their communication requirements, utilize these commercial-grade devices in an unsecure manner to conduct voice and data communications – which can put their agencies at risk.

MOVE: A user-centric, role-based access architecture for wired, wireless and remote access

The next generation of access networks must focus squarely on users, their devices and their applications – not infrastructure or ports. Users should have simple, secure network access regardless of where they work or roam, which devices and applications they are using, or how they want to connect.

Access to government data using these mobile devices needs to be secured as well. This is especially true in the event that the data resides on the mobile device itself. Even sensitive but unclassified data needs to be protected when being accessed through the use of commercial mobile devices. There are alternatives available to help secure this data. Among them are:

- **Virtual Desktop Infrastructure** separates a personal computer desktop environment from a physical machine using a client-server model of computing. For example, the actual computer desktop, its operating system, programs, applications, processes and data are stored on a server that is centrally run and located. Mobile devices can authenticate and access these centrally virtual machines through an application that runs on the mobile device. Only screenshot data of the virtual machine is transmitted between the mobile device and remote central server, while the data is protected centrally and never resides on the mobile device.

- **Mobile Device Management** solutions provide the ability to manage mobile devices while providing options to enforce security policies and access. This enables administrators the ability to require the use of passwords, detect and deny access to jailbroken or rooted devices, and even remove sensitive data from the device. In addition, applications such as email and IM can be utilized within a “sandbox” protected area on the mobile device. Government data that resides on a mobile device can be separated from the user’s personal data. The separated government data is encrypted so that it cannot be accessed in the event that the device is lost or stolen. Encryption applied to this data must adhere to government validations (i.e. FIPS-140) and certifications.

While processes are still evolving, DoD based documents currently exist that allow the use of mobile devices such as Android and Windows 7 tablets, iPads, iPhones, and Blackberrys, as long as they are configured and adhere to the policies outlined within the security guides published by DISA.
In addition, the National Security Agency recently announced the first release of SE Android, which is a security enhanced version of the Android operating system. It provides mandatory access control within the operating system for controlling access and security policies.

These efforts allow for the use of commercial mobile devices within government networks. Aruba Networks’ MOVE for Government works in conjunction with these efforts to provide secure mobility solutions for unclassified and classified government networks.

Introducing Aruba MOVE for Government

In the past, an access network to support mobility was built on many different disparate technologies: wired for local access, wireless for mobile devices, VPN clients and concentrators for remote access, and separate systems for outdoor. However, none of these technologies were unified or designed to work together, leading to high operational costs. Aruba Networks® now offers government agencies a significantly improved approach. Leveraging its next-generation Mobile Virtual Enterprise (MOVE) architecture, Aruba securely unifies disparate computing infrastructures into one seamless network access solution – for government employees, contractors, visitors, and military personnel in garrison or in deployment. Authorized users get access to network resources wherever they need them, with automatic access policy enforcement based on who they are – no matter where they are, what devices they use and how they connect.

Aruba’s MOVE for Government architecture combines advanced WLAN technology with government validated and policy compliant mobile device software supporting stringent government security regulations such as Common Criteria Certification, FIPS 140-2 Validation, DoD directives 8100.2 and 8420.1 Compliance. The solution provides this policy compliant and validated technology that all US government agencies are required to utilize. All at no extra cost compared to other commercial solutions.

MOVE for Government provides a common set of network services that manage security, policy, and network performance for every user and device on the network, regardless of method of access. These services include:

• Identity management
• Guest access
• Role-based policy enforcement
• Application traffic management
• Content security
• Device and network configuration
• RF and spectrum management
• Compliance

With Aruba MOVE for Government, services are defined once via a centralized Aruba Mobility Controller in the data center. This eliminates the need to keep up with a profusion of wiring closets, firewalls, NAC solutions, management systems and reporting tools that operate in separate domains.

“Field force automation is also considered a critical issue for federal agencies that are trying to do more with less, and smartphones and PDAs are being picked up by federal field services officers as a strong productivity aid.”

Source: 1105 Government Information Group
As a result, network operations are consistent across the entire organization, regardless of user location, access method, mobile device or applications. Aruba MOVE easily accommodates users with multiple devices, whether government-owned or user-owned.

This user-centric approach to network access makes it easier for government agencies to accommodate the deluge of smartphones, tablets and other personal mobile devices that employees are bringing to work. Aruba MOVE also eliminates the need to maintain VLAN at the edge and manually configure user additions and changes.

Figure 2: The Aruba MOVE architecture for government deployments.

Access from a wide range of network on-ramps

Aruba MOVE for Government offers a wide range of network on-ramps that leverage a common set of network services to deliver consistent, reliable and secure access to users:

- **Wireless APs.** Aruba 802.11n APs provide high-performance connectivity to mobile and fixed wireless devices, while providing best-in-class RF control using Adaptive Radio Management (ARM) technology.

- **Mobility Access Switches.** Aruba has extended the user-centric, services-based approach of the MOVE architecture to a new class of access switches. Designed to provide network access in wiring closets, Aruba S3500 Mobility Access Switches connect wired Ethernet devices such as virtual desktops, video surveillance cameras and 802.11 APs.

- **Remote APs.** An alternative operating mode for Aruba APs, Aruba Remote APs (RAPs™) automatically extend centralized resources to branch and remote locations using site-to-site VPN tunnels to the central data center. Using zero-touch configuration, personnel at these sites can easily set up their own RAPs with no IT assistance.

- **Outdoor APs.** Aruba outdoor APs combine a unique multi-radio, multi-frequency architecture, Adaptive Radio Management and hardened enclosures to bring high-performance networking to outdoor or deployable environments. Using the ArubaOS mesh features, they can connect to the backbone network wirelessly as an alternative to a wired AP connection.
The benefits of simplified management

With the Aruba solution, services are defined once via a centralized Aruba Mobility Controller in the data center. This eliminates the need to keep up with a profusion of wiring closets, firewalls, network access control (NAC) solutions, management systems and reporting tools that operate in separate domains.

As a result, network operations are consistent across the entire organization, regardless of user location, access method, mobile device or applications. Aruba MOVE for Government easily accommodates users with multiple devices, including both legacy devices and commercial mobile technology, including smartphones, tablets and laptops. With its user-centric approach, the Aruba solution also eliminates the need to maintain VLANs at the edge and manually configure user additions and changes.

The business case for Aruba

With tight budgets and mobility at a critical juncture, the Aruba MOVE architecture presents a very compelling business case for government, civilian and military agencies:

- Significantly lower purchase costs compared to proprietary solutions. Additional operational savings come from:
  - Eliminating cumbersome CCI checkout and handling processes.
  - Accelerating the move from wired to near-gigabit 802.11n, thereby reducing the number of Ethernet switches needed in favor of more cost-effective Wi-Fi access.
  - Moving to thin on-ramps at the edge that are easier to install and operate.
  - Reducing cellular carrier data package charges for 3G/4G communications as they can become expensive, especially when users exceed data limits. Implementing 802.11 WiFi solutions for mobile communications not only minimize cellular data plan costs, device and data security can be achieved in a compliant manner to protect valuable unclassified and classified government data.
- Easier support for both local and remote users. Because it utilizes a single architecture and network design for local (using WLAN, WLAN mesh and wired) and remote (using remote wired and WLAN) access, it is simpler to manage. Instead of employing well over a dozen steps to configure network access using a legacy approach, employees can configure the Aruba solution in just three simple steps.
- Improved security by supporting all access modes. Aruba Mobility Controllers manage classified WLAN users and classified wired users to simplify network design and strengthen the overall security posture by adding access control and user firewalling.
- A higher performance network. Aruba 6000 Mobility Controllers with M3 controller modules support 4 Gbps of AES-256 encrypted throughput for thousands of concurrent users. Up to four M3 controller modules can be installed in a single 6000 Mobility Controller chassis for 16 Gbps of encrypted traffic throughput.
- Lower end-user support costs and higher satisfaction. Aruba gives the entire workforce – employees with and without clearance as well as contractors and guests – a single, consistent way to access the appropriate agency resources.

Role-based access policies allow IT to control users and devices, so that personnel can switch effortlessly between desktops, laptops, tablets, smartphones and other mobile devices. By cutting down on the confusion and saving time for users, Aruba reduces IT service desk calls and increases user satisfaction.
Conclusion

The Aruba MOVE architecture gives government IT organizations the technology they need to realize their vision to embrace mobility in a meaningful way. It does so by securely unifying disparate computing infrastructures into one seamless network access solution – for government employees, contractors, visitors, and military personnel in garrison or in deployment.

It is an architecture that’s driven by mobility and the proliferation of Wi-Fi-enabled mobile devices. These devices – which have no Ethernet port – are connecting to enterprise networks in unprecedented numbers and will quickly surpass desktop connections.

Aruba MOVE eliminates the cost and complexity of managing separate wired and wireless access policies and VLANs at the edge. In fact, with Aruba you’ll need fewer ports and consequently less equipment in the wiring closet – effectively rightsizing your access infrastructure.

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 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 updates and to read the latest news and opinions from Aruba, visit our Communities page.

“The vision we’re looking at is, every soldier is issued a phone.”

*Michael McCarthy,*
*Director of Operations at the Brigade Modernization Command Mission Command Complex, U.S. Army*

*Source: Network World*