WHITE PAPER

SECURE AND EFFORTLESS MOBILITY FOR THE PUBLIC SECTOR

BROCADE HYPEREDGE AND ARUBA MOBILITY-DEFINED NETWORKS™ COMBINE TO PROVIDE A FEDERALLY CERTIFIED, SECURE, AND COST-EFFICIENT MOBILITY SOLUTION.

TABLE OF CONTENTS

Like their enterprise counterparts—37 percent of which are expected to be mobile by 2015[1]—Federal workers are on the move. A recent Meritalk survey[2] of Federal workers found that 54 percent connect remotely at least once a day, and mobility has increased their efficiency, availability, and engagement. Yet, according to same Meritalk study, all the potential of an engaged mobile workforce is lost due to cumbersome security procedures (57 percent), slow connections (65 percent), and limited access (43 percent).

Supporting mobile users, their devices, and their organizational expectations is increasingly challenging for government IT departments. Getting network access and using sophisticated applications securely via a personal device appears easy to a user, but it is quite a complex task for the IT department. For that reason, Brocade and Aruba Networks have partnered together to provide agencies with a secure, optimized mobile user solution that is effortless to maintain and that cuts Total Cost of Ownership (TCO) 46 percent compared to the comparable Cisco solutions. The combined solution from Brocade and Aruba delivers an open standards-based unified network solution that reduces complexity and meets all Federal security and compliance standards—to better support secure mobility and Bring Your Own Device (BYOD) initiatives.

NEW APPLICATIONS, DEVICES, AND EXPECTATIONS ADD NEW STRESSES

Whether an organization is enterprise or public sector, today's applications and devices continue to increase in sophistication. They provide more services, a rich multimedia user experience, and increased mobility. But they also create security concerns and place immense pressure on the network—a network that was not originally designed to handle such technology.

Applications: Video, Unified Communications (UC), and other sophisticated applications all have a significant impact on user productivity and on the network.

Video: Today, users expect real-time access to streaming video for agency trainings, remote meetings, and even video calls using FaceTime, Lync, and Skype. This "video-on-demand" expectation requires the network to deliver high bandwidth with low latency and jitter. It also requires constant monitoring to restrict applications for personal use and ensure they do not interfere with the bandwidth needed for agency applications.

UC: UC brings all forms of employee communication to a single device—whether a desktop/laptop computer, tablet, iPad, or smartphone—that delivers real-time collaboration. Human collaboration is dynamic. For example, a low-bandwidth text message can instantly transform into a shared desktop that enables joint editing of documents, and—with a mouse click—can expand to a video chat, before disappearing again at the end of the collaboration. The network has to monitor and prioritize the application used and adjust traffic flow dynamically. This includes providing better support for peer-to-peer (that is, East-West) traffic patterns—now increasingly common with applications such as Lync)—while ensuring consistent security policies to deliver an optimized user experience.

New Devices and Expectations: Gartner predicts that by 2016, 78 percent of all enterprises will embrace BYOD; 38 percent will stop providing corporate devices to their employees altogether, while 40 percent will allow a mix of BYOD and corporate-supplied devices. While BYOD adoption by government agencies may remain lower for the foreseeable future, the explosion of smartphones, tablet computers, and iPads sets an expectation that access to the data and applications users rely on in their personal lives will be available when they are at work. BYOD has a positive impact on IT budgets when users purchase and maintain their own devices, yet it creates concerns about securing access to sensitive data, especially for government organizations with stricter security requirements. BYOD also creates issues with easily maintaining an optimized and productive mobile user experience. As mentioned previously, a Meritalk study found that 57 percent of Federal mobile workers think cumbersome security policies are a major barrier to achieving greater productivity and engagement. User expectations of high-quality anywhere, anytime access require easily implemented and consistently applied security and application usage policies across both wired and wireless networks and user devices.

The impact of these applications and devices on the network creates a need for higher bandwidth, lower latency, and secure, pervasive, and reliable wireless access. Incremental improvements to networking protocols such as Quality of Service (QoS), rate limiting, and traffic prioritization, as well as implementation of network access control appliances, helps to maintain the quality experience. Yet it also adds management complexity that impedes an organization's ability to quickly deploy new applications and rapidly respond to mission—or user—requests.

[1] IDC, Worldwide Mobile Worker Population 2011-2015 Forecast, 2012.
[2] Meritalk, Feds on the Go: Network Needs for Maximum Mobility, August 19, 2013.

Friction Points: Agency and User Expectations Confront Network Realities

Every network in the enterprise or public sector, whether it is the data center or the wiring closet, must be designed to meet agency expectations that are balanced with technology choices. This is not easy, with IT budgets and personnel remaining flat (or shrinking), while application sophistication, data, security requirements, and user devices continue to grow rapidly. And with the increased pace of today's business, government leaders, agencies, managers, and users are demanding use of new applications and technology in days rather than weeks.

To keep pace with these changes, agency administrators need an intelligent and secure infrastructure that meets appropriate certification levels such as Federal Information Processing Standards (FIPS) and Suite B encryption. Such an infrastructure also needs to show which users are connecting, when they are connecting, and the type of applications and devices they are using. It then has to work seamlessly with the wired and wireless infrastructure to effortlessly and cost-efficiently ensure an optimized and secure user experience (see Figure 1).

Brocade HyperEdge Architecture and Aruba Combine to Make Mobility Secure and Effortless

For an organization to meet mission objectives, it must be agile—able to adapt to changing conditions quickly. Mobility meets that challenge by allowing enterprise users to use sophisticated applications and collaborate with anyone, anywhere, at any time. However, user freedom places two significant burdens on IT. First, the legacy local area network (LAN) and its rigid, Spanning Tree Protocol-based 3-tier design was not designed for mobility. Second, securing mobile devices and ensuring an optimized user experience—especially on devices supplied by users, which have disparate platforms and operating systems—becomes a labor-intensive operation.

Brocade and Aruba have combined two innovative architectures to eliminate these burdens and deliver a secure and effortless mobile user experience.

Brocade HyperEdge Architecture and Aruba Mobility-Defined Networks make optimized and secure mobility effortless.

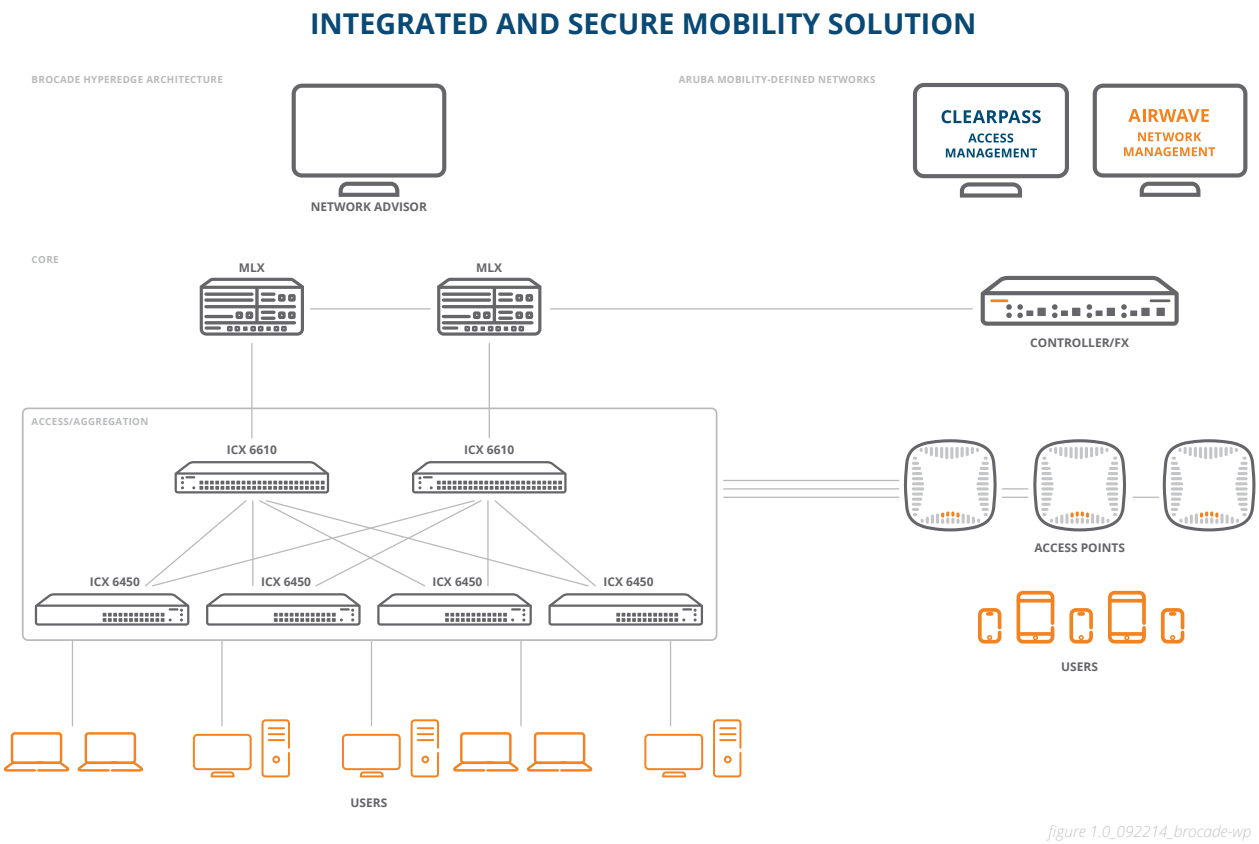

Figure 1: The Brocade HyperEdge and Aruba Mobility-Defined Networks architectures make optimized and secure mobility effortless.

Brocade HyperEdge Architecture

Brocade® HyperEdge™ Architecture integrates innovative new wired features, such as Distributed Services, with application-aware access management technology from Aruba's MOVE architecture to secure and optimize mobility using a wired TCO that is 52 percent lower than comparable Cisco solutions. Here's how these unique innovations combine to deliver an unparalleled solution.

Brocade Mixed Stacking with HyperEdge Distributed Services

A significant innovation underpinning HyperEdge Architecture is Distributed Services. When combined with mixed stacking, administrators have the ability to combine premium and entry-level switches in the same stack, manage all switches as a single virtual switch and, most importantly, extend premium services to all ports in the stack—including ports from entry-level switches. This capability provides two distinct advantages: significant per-port cost reduction and long-term investment protection. (See Figure 2.)

Per-Port Cost Reduction: With premium services available to all switches and ports within a mixed stack, organizations no longer need to buy an entire stack of premium switches to provide these services. Adding just one Brocade ICX® 6610 Switch to a stack of Brocade ICX 6450 Switches reduces the aggregate per-port acquisition costs by nearly 50 percent, as compared to an equivalent stack of Cisco premium switches. For a more detailed cost comparison, go to www.brocade.com/CampusTCO.

Long-Term Investment Protection: With mixed stacking enabling HyperEdge Distributed Services, organizations no longer need to rip-and-replace entire stacks of switches to meet new service demands. Using Brocade mixed stacking and Distributed Services, organizations can initially deploy a stack of Brocade ICX 6450s to inexpensively provide Layer 2 and some Layer 3 services. As the need for more comprehensive advanced Layer 3 services increases, organizations can simply add one Brocade ICX 6610 (or two for high availability) to the stack of Brocade ICX 6450s, and HyperEdge Distributed Services extends the premium services to all switches in the stack. This eliminates the need to replace the entire stack of switches, as is the case with other vendors' solutions.

Unified Wired/Wireless Management with Brocade Network Advisor

Brocade Network Advisor (BNA) network management software provides visibility from the Data Center to the Campus Access Network. With visibility to Storage Area Networks (SAN) and Data Center and Campus LANs, including Aruba wireless networks, BNA helps proactively manage end-to-end network health, performance and aids troubleshooting. Administrators can quickly identify network issues with customizable dashboards and drill-down to isolate and fix problems whether on the wired or wireless network.

MIXED STACKING WITH HYPEREDGE DISTRIBUTED SERVICES

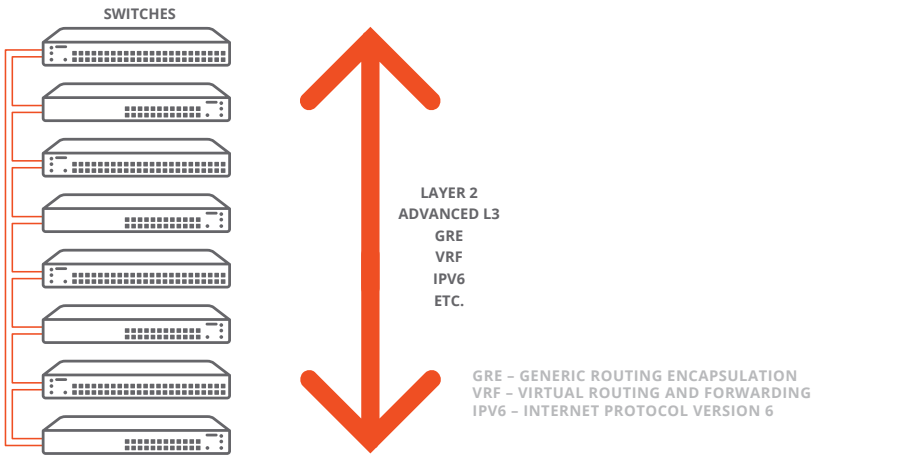

Figure 2

Aruba Mobility-Defined Networks

The Aruba Mobility-Defined Networks architecture completes the BYOD and mobility infrastructure solution. It uses standards-based protocols to work seamlessly with Brocade HyperEdge Architecture. Mobility-Defined Networks correlate real-time data about users, device, applications and locations—and extends this intelligence across the wired and wireless network to automate infrastructure-wide performance optimization and security actions.

The primary components of Aruba Mobility-Defined Networks are:

- 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 Federally-certified and Suite B-compliant Mobility Controllers for flow-based security and traffic management.
- Wireless Network Infrastructure: This comprises indoor and outdoor 802.11ac WLAN Access Points (APs), Remote Access Points (RAPs), and Virtual Intranet Access VPN client software.
- Mobility Applications Infrastructure: These end-user tools include Aruba APIs for location and analytics applications and Meridian apps for visitor engagement.

Access Management

Using the ClearPass Access Management System, Aruba Mobility-Defined Networks combines Suite B-compliant wireless controllers and FIPS-compliant APs with access control policies for wired networks, devices, and applications into a single policy-definition point. Administrators can centrally define policies, which then work seamlessly with Brocade wired and Aruba wireless networks and multiple vendors' Mobile Device Management (MDM) agents for BYOD. The result ensures a secure and compliant environment, a significant time savings for IT, and a dramatic reduction in errors associated with correlating security policies across multiple systems. Agencies and organizations benefit from policies that are consistently applied, no matter where users connect or the devices they use.

Mobility-Defined Networks also centralizes wired, wireless, and remote network management with the AirWave management system. Regardless of how users connect, AirWave consolidates usage information on all users, devices, and applications into intuitive dashboards and workflows. Additionally, AirWave provides end-to-end Brocade and Aruba network infrastructure visibility, monitoring, and management. Whether you have a real-time RF troubleshooting task or need historical forensics for regulatory compliance, AirWave addresses the critical needs of managing a modern, multifaceted, multivendor mobility network.

THE ARUBA MOBILITY-DEFINED NETWORKS ARCHITECTURE

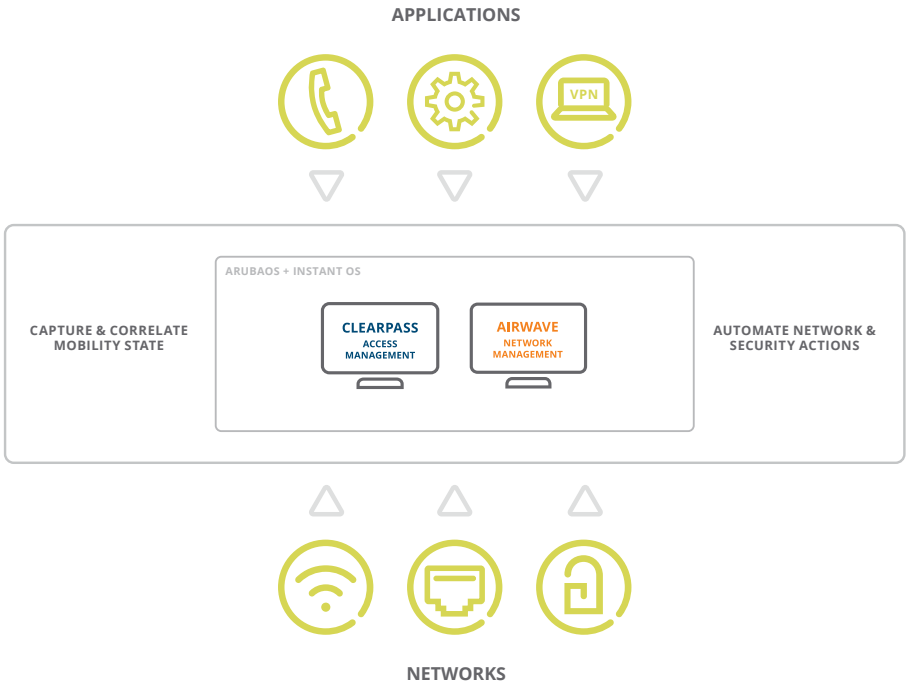

figure 3.0_092214_brocade-wp

Figure 3

Finally, the Mobility-Defined Networks architecture makes access management more dynamic with Federally-certified Mobility Controllers that employ a context-aware firewall which can distinguish one traffic flow from another and automatically adjust how traffic is handled, based on the mix of users, devices, and applications and their location.

Wireless Network Infrastructure

The second component of the Aruba Mobility-Defined Networks architecture is Aruba's industry-leading WLAN APs, RAPs, and Virtual Intranet Access VPN client software. Aruba's purpose-built 802.11ac APs work with Aruba's Mobility Controllers and feature integrated Adaptive Radio Management (ARM), ClientMatch™, AppRF™, and airtime fairness technologies.

Aruba APs leverage unique application awareness in conjunction with patented algorithms for airtime fairness, which ensures all devices have equal access to the WLAN. To further maximize client performance, the patented ClientMatch technology continually monitors device capabilities and WLAN health to match poor performing devices to the best radio on the best AP. Also, to keep deployment and management costs to a minimum, Aruba APs support zero-touch provisioning with Aruba Activate, which enables APs to get their configurations automatically from a cloud-based provisioning system. No manual intervention is required.

Mobility Applications Infrastructure

The third cornerstone of the Mobility-Defined Networks architecture encompasses the 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.

HYPEREDGE AND MOBILITY-DEFINED NETWORKS ARCHITECTURES DELIVER SECURE AND OPTIMIZED MOBILITY EFFORTLESSLY

By combining Brocade HyperEdge Architecture with Aruba Mobility-Defined Networks, today's organizations get an unparalleled mobility solution. With Brocade HyperEdge Architecture and its mixed stacking with Distributed Services technology, agencies extend taxpayer dollars by getting premium features without paying a premium price. With the Aruba Mobility-Defined Networks architecture and the patented ClientMatch technology that works seamlessly with Brocade wired and Aruba's innovative wireless technology, organizations get a certified, secure, and optimized mobile user experience.

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.

aruba NETWORKS

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com