



**WHITE PAPER**

**Enterprise Network Mobility: A TCO Analysis**

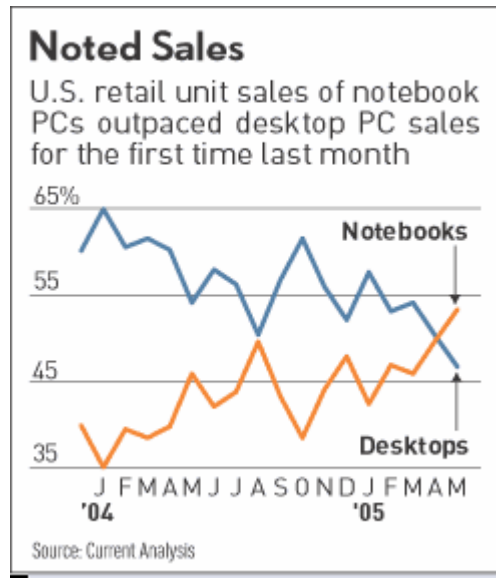
By:  
Nicholas John Lippis III  
President  
Lippis Consulting

*Distributed Courtesy of:*



**The Mobile Enterprise:**

In May 2005, the sales of laptops outstripped desktop machines for the first time, and so the requirement for laptop connectivity into corporate networks will only continue to increase. Notebooks or laptops make up 33% of total PC sales worldwide today. That's up from 20% in 1999, according to IDC. And since these laptops are mobile by definition the ability to protect them from exploits is more difficult. Employees using laptops at home may become contaminated. Once that employee plugs his/her laptop into the corporate network, it has the potential to infect the entire corporate network, disrupting business process.



**Employees required to plug into their business process while at a customer's site**

In certain industry sectors, especially professional and financial services, there has been an increased need for employees to work at their customer's office(s). Employees often are required to link back to their corporate business process while plugged into a customer's network. While the network will provide connectivity, security concerns for both companies often limit the practice, thus creating a discontinuity in business process. The concerns usually center around the potential for exploit contamination on both networks or the extraction of sensitive information.

**Competitors working together for a common client sharing resources**

Business process driven by competitive pressures is creating odd bed fellows. It's not uncommon that competitors are often forced to work together to service a common client. During this type of arrangement competitors often share resources, both IT and physical office space, thus creating high security concerns.

**Collaborating employees from different companies sharing resources**

As the global economy evolves and the links between economies and businesses strengthen so too will the level of collaboration. But increased collaboration between employees from different companies is not just for global concerns; regional

companies are also increasingly being linked together as firms focus on their core competency.

**Customers requiring deeper access and communications with their suppliers**

Gone are the days when a customer representative would service a client's communications needs. Customers have since bypassed this single point of contact approach requiring wider and deeper access to its suppliers to obtain information. For many firms, especially during complex projects, it is not uncommon that a matrix of communication flows such as IM, e-mail, voice communications, video/audio conferencing, etc., between companies occurs to satisfy customer requirements.

**Traditional desktops & laptops plugging into LANs and WLANs**

In addition to the above-mentioned new ways of extending business process, the traditional methods of connecting computers and IP phones into local area networks, be they wired or wireless, and extending that connectivity over wide area networks need to be maintained and refreshed. In short, the increasing web of business process and associated links are additive to existing network infrastructure.

These highly collaborative and mobile working arrangements are driving businesses straight into a security vulnerability abyss. Mobile solutions require controllable network security that challenges access, quarantines infected end points and contains exploits before they propagate through the mobile enterprise.

In order to address the above new norm of doing business, the mobile enterprise is incorporating Wireless LAN or WLAN technologies, internal network security and converged voice and data networks to increase collaboration. A recent Forrester study revealed that 60% of all enterprises were either deploying or upgrading WLAN infrastructure in 2005. WLAN technology is the enabler for mobility within the enterprise. WLANs have transitioned from a special access technology to a general purpose status. Due to necessity, WLAN vendors had to solve the network access security and transmission speed problems and they have. WLANs are more secure than wired LANs. With WLANs being now general purpose and a critical component of an architected enterprise network framework, WLANs are solving the network access security problem and incorporating converged networks by supporting VoIP over WLANs or VoWLAN. WLANs provide not only mobility, but also the ability for broad network expansion in a manner that is not only more rapid, but also more flexible than traditional wired LANs. The result is a mobile enterprise that supports all facets of corporate computing, including office connectivity, remote access and telecommuting.

---

**Overlay versus Integrated**

There are two architectural approaches to deliver the mobile enterprise. Simply put it's a question of overlay versus integrated.

An overlay WLAN network is placed over the existing wired network infrastructure of Ethernet switches and routers. Wireless access points communicate directly with controllers through the wired infrastructure. This wired infrastructure could be local or remote. Access points may be placed at remote offices offering mobility services

to knowledge workers within that building but much of the intelligence resides in a controller that is located in a regional or headquarters office connected to a LAN and WAN. Network security, quality of service, VoIP, roaming, location services, guest hot spot et al services are provided by the controller. In short the access points and controllers are plugged into an existing wired infrastructure to provide mobility services over or on top of a wired network.

The network integrated approach is based on placing WLAN functionality such as AAA, network access control, intrusion detection services, roaming, location services etc within Ethernet switches and routers. Access points are distributed throughout the work space and communicate to various modules, blades, software and appliances within Ethernet switches.

---

Each approach has associated pros and cons, attributes and cost. Every design be it a house, car, building, network or mobile enterprise has cost implications and consequences. This paper quantifies the Total Cost of Ownership (TCO) differences between overlay and integrated WLAN deployments so the reader can choose which approach best suites their mobile enterprise needs. Included in this paper are the capital expenditures associated with each deployment strategy, as well as deployment and ongoing operational costs over a one-year period for a 1000 person deployment.

## **EVOLUTION OF WLAN ARCHITECTURES**

---

The rapid proliferation of enterprise WLANs has spawned a wide range of product categories, architectures and deployment models. Initial enterprise WLAN deployments typically followed the "rogue" model, with employees adding simple SOHO access points to the enterprise network for convenience. Such deployments fall outside of the enterprise network management and security realm, exposing the enterprise to significant risk. Further, all MAC-layer intelligence, including authentication, encryption, etc., is concentrated into the access point itself. This "Fat AP" approach results in a series of discrete network elements that must be individually managed and maintained.

Second-generation enterprise WLANs added a control plane that was tightly integrated with the LAN switching fabric. While this strategy enabled better traffic integration with the wired LAN, the majority of the intelligence remained distributed at the fat AP.

Third-generation enterprise WLAN architectures implemented a centralized management layer in the form of the WLAN controller. The WLAN controller offloads the MAC-layer intelligence from the access point, managing authentication, encryption, NAT, etc. from a single point. This "overlay" approach relegates the AP to a simple radio transmitter that is a slave to the controller. The overlay approach has gained favor in the enterprise, enabling centralization of management and maintenance tasks rather than managing each AP as a discrete network element.

Next-generation WLAN architectures also employ the thin AP approach, though there are two key differences:

1. While the bulk of MAC-layer intelligence is stripped from the AP, functionality that is best deployed in a distributed manner is integrated into the AP. This includes RF monitor features, which enable optimization of the WLAN infrastructure through signal coverage and connection speed analysis, as well as rogue AP detection.
2. The controller layer is now focused on not only providing all of the authentication, authorization, accounting, encryption RF management, QoS functionality, but is now also providing a collapsed WLAN backbone overlay above the traditional wired LAN.

This new overlay approach to enterprise WLAN architecture greatly simplifies the WLAN, as all network services are provided from the intelligent controller layer. Additionally, there is no need to re-engineer the wired network to accommodate the wireless traffic (VLANs, QoS, security, VoIP, etc.), as the WLAN operates as an independent overlay.

### **ENTERPRISE WLAN TOTAL COST OF OWNERSHIP (TCO) – ONE-YEAR STUDY**

---

This paper quantifies the total cost of ownership (TCO) savings achieved by deploying a centrally managed overlay WLAN solution versus a network integrated WLAN solution. The model takes into consideration the capital and operational expenses associated with ground-up deployments of each approach over a one-year period for 1000 users.

The cost model for a typical network integrated WLAN architecture is based on discounted list pricing from a leading network equipment vendor, as well as the associated integration and management costs. The cost model for the centralized WLAN overlay approach is based on the “Mobile Edge” architecture of Aruba Networks, one of the leaders in overlay WLAN deployments. As the study shows, there are significant capital and operational cost benefits to deploying a centralized WLAN overlay network.

### **ASSUMPTIONS**

---

The following total cost of ownership model is based upon a common large enterprise WLAN deployment. This assumes:

- **Environment**
  - 1000 enterprise end users
  - 100 access points (10:1 user to access point ratio)
  - No existing WLAN infrastructure
- **Infrastructure Elements**
  - 802.11 a/b/g access points
  - Secure VPN connectivity between AP's and control plane
  - WLAN firewall
  - Intrusion detection/prevention technology for the WLAN
- **Deployment Costs**
  - Skilled labor at \$150/hour

- **Operational Costs**
  - IT manager with \$100,000/year salary
  - Annual support/maintenance cost of 18% of Capital Expenditure
- **Timeline**
  - 1 Year

**NETWORK INTEGRATED APPROACH**

---

The network integrated approach examined in this study is based upon a WLAN architecture that is tightly integrated with the wired LAN switching fabric.

**Capital Expenditures**

A series of 100 intelligent access points is deployed across the enterprise campus. The core of the distributed WLAN is based upon a mid-sized modular LAN switch chassis. Baseline requirements for the chassis include WLAN supervisor switching fabric, redundant power supplies, and a 48-port Power over Ethernet (PoE) line card to provide power to the distributed access points. In addition, a 150 access point WLAN service module license is required to manage user roaming, access point/user authentication (ACL's, 802.1xx, etc.), WLAN segmentation, and incorporation of wired LAN access policies.

Description	List Price	Qty.	Total
<b>Switch Chassis</b>			
9slot, LAN Switch Chassis	\$ 9,500	1	\$ 9,500
WLAN Supervisor Switch Fabric	\$ 28,000	1	\$ 28,000
WLAN Service Module w/150 Access Point License	\$ 45,995	1	\$ 45,995
PoE 802.3af 10/100, 48 port(RJ45) line card	\$ 7,995	1	\$ 7,995
2500W AC Power Supply	\$ 3,000	1	\$ 3,000
<b>Gigabit Ethernet Switch</b>			
8-port GE , Enhanced QoS (Req. GBICs)	\$ 9,995	1	\$ 9,995
Redundant 3000W AC power supply	\$ 3,000	1	\$ 3,000
<b>Access Points</b>			
Dual Radio a/b/g access point (approx. 10 users per access point)	\$ 599	100	\$ 59,900
<b>Security Components</b>			
Secure Authentication Server	\$ 11,995	1	\$ 11,995
Firewall and VPN Security System	\$ 96,000	1	\$ 96,000
WLAN Access Control Server (500 Users)	\$ 20,995	2	\$ 41,990
WLAN Guest Access Platform	\$ 7,000	1	\$ 7,000

**Enterprise Network Mobility: A TCO Comparison**

---

WLAN Location Appliance	\$	14,995	1	\$	14,995
WLAN IDS Device	\$	6,000	1	\$	6,000
Wireless Sensors for Rouge AP Detection (approx. 25% the no. of AP)	\$	700	25	\$	17,500
				<b>Capex</b>	<b>\$ 362,865</b>
				<b>Discount</b>	<b>40%</b>
				<b>Net Capex</b>	<b>\$ 217,719</b>

WLAN security is the largest capital cost spend, by a factor of two, in the integrated WLAN architecture. Securing the network integrated WLAN requires that an access control server is also deployed to manage AAA services, including Extensible Authentication Protocol (EAP), Protected EAP (PEAP), RADIUS, LDAP and VPN authentication. An integrated VPN/stateful firewall device must also be deployed to secure the wireless perimeter and data transmission. A WLAN-specific intrusion detection system (IDS) must also be deployed to detect anomalies, as well as rogue AP detection probes. Typically, an enterprise will deploy 1 probe per 4AP's, totaling 25 in this implementation. To keep track of WLAN end points a location server is required and to provide WLAN guest access a specific security appliance is required.

In order to effectively interconnect the WLAN with the wired LAN backbone, an 8-port Gigabit Ethernet switch must be deployed upstream from the LAN switch chassis. This GigE switch requires enhanced QoS to manage traffic prioritization onto the wired LAN, as well as redundant power supply.

A 40% discount factor is applied to the network integrated WLAN equipment. Depending on relationship, this discount could be as much as 50% if other projects or purchases are being funded at time of acquisition.

**Deployment Costs**

A new plenum cable drop is required to provide Ethernet-based power to each access point. When the AP's are powered and operational, a site survey must be conducted to determine ideal AP placement, connection speed, signal strength and bandwidth to optimize the WLAN. A networking professional will be required to configure VLAN's, install new blades and supervisor control modules in Ethernet switches, add appliances and update RADIUS authentication policies for the introduction of WLAN traffic onto the wired LAN, as well as update the Layer 2 switching OS.

To add security to the integrated network approach 802.1x would have to be configured at the LAN edge, new blades, and firewall, VPN, IDS and captive portal appliances would also have to be configured and installed. Then network access control to protect exploits from propagating throughout the enterprise would be installed driving upgrades in switches and routers. The configuration and set-up of a layer 2/3 network integrated WLAN approach is a non trivial task and in fact represents an additional 75% mark-up on capital cost.

## Enterprise Network Mobility: A TCO Comparison

Deployment Costs				
Power and Cable	New plenum drops for access points	\$ 1,500	100	\$150,000
Site Survey	Site survey before deployment	\$ 5,000	1	\$ 5,000
Wired Network Adjustments	VLAN configurations, RADIUS updates (40 skilled man hours @ \$150/hr.)	\$ 150	40	\$ 6,000
Layer 2 OS Upgrades	Upgrades for existing layer 2 infrastructure (20 skilled man hours @ \$150/hr.)	\$ 150	20	\$ 3,000
<b>Deployment</b>				<b>\$164,000</b>

### **Operational Expenses**

Once the network integrated WLAN is deployed, a range of technical expertise is required to manage and maintain the discrete network elements. This skill set includes understanding of APs, security infrastructure and policies (VPN, IDS, RADIUS, firewall, network access control, location management), as well as the Layer 2 switching environment and VLAN configuration.

Operational Costs				
Loaded yearly cost of 1 Network Manager (VLAN, RADIUS, IOS)	\$ 100,000	1	\$	100,000
Site survey for optimization	\$ 5,000	1	\$	5,000
Approx. 12% of CAPEX	\$ 43,544	1	\$	43,544
<b>OPEX</b>				<b>\$ 148,544</b>

As the WLAN intelligence is integrated into layer 2 and 3 devices and access points, additional site surveys must periodically be performed to optimize the AP connection to the network core. This typically requires a one-time fee from an experienced network professional. Ongoing support and maintenance costs at 12% of the capital expenditure top off the annual operational expenses.

## **THE OVERLAY APPROACH**

The centrally managed, overlay approach, as leveraged by Aruba Networks' Mobile Edge Solution, focuses on collapsing the network, security, and AP intelligence layers into the mobility controller; creating a WLAN overlay above the existing enterprise wired LAN infrastructure.

### **Capital Expenditures**

The core of the overlay architecture is based upon the Aruba 5000 Mobility Controller, a modular, vertically-integrated WLAN controller. The Aruba 5000 incorporates an 8Gbps total throughput (7.2Gbps encrypted) WLAN switch with add-on modules to the Aruba Supervisor Card to provide the requisite authentication, encryption, traffic management and AP control services. All AP's are configured and managed by the Mobility Controller. In this instance, a single Aruba 5000 chassis is deployed with an Aruba Supervisor Card with support for up to 128 AP's for WLAN management and AAA services. A 2-port GigE/24-port FE SPoE line card is added to provide power to the access points. Integrated into the 5000 is a wireless intrusion protection, secure wireless connectivity and integrated location services, all features which are either modules or appliances in the network integrated approach.

100 Aruba 70 Access Points are deployed across the enterprise campus. The access points provide not only radio for wire conversion, but also provide RF monitor

services. This enables WLAN site surveys to be conducted by the AP's, allowing for dynamic self-optimization.

Description	List Price	Qty.	Total
<b>Switch Chassis</b>			
Aruba 5000 Base System (SPOE Power)	\$ 3,995.00	1	\$ 3,995
Aruba Supervisor Card I (128 AP Support)	\$ 15,000	1	\$ 15,000
Aruba 2xGE/24 FE Line Card SPOE	\$ 7,000	2	\$ 14,000
<b>Access Points</b>			
Aruba 70 Wireless Access Point	\$ 595	100	\$ 59,500
<b>Security Components</b>			
Policy Enforcement Firewall Module for Aruba Supervisor Card I (128 AP)	\$ 8,000	1	\$ 8,000
VPN Server Module for Aruba Supervisor Card I (128 AP)	\$ 8,000	1	\$ 8,000
Client Integrity Module (128 AP)	\$ 8,000	1	\$ 8,000
External Services Interface Module (128 AP)	\$ 8,000	1	\$ 8,000
Fortinet Anti-Virus Platform	\$ 9,995	1	\$ 9,995
Wireless Intrusion Protection Module for Aruba Supervisor Card I (128 AP)	\$ 8,000	1	\$ 8,000
		<b>CAPEX</b>	<b>\$ 142,490</b>
		<b>Discount</b>	<b>25%</b>
		<b>Net Capex</b>	<b>\$ 106,868</b>

The WLAN perimeter security layer is achieved by adding the Aruba Policy Enforcement Firewall Module, an ICSA-compliant stateful firewall that can apply policy down to the individual user level. Transmission security and secure roaming is provided by adding the Aruba VPN Server Module. The VPN Server Module utilizes a hardware-based encryption module to maximize performance and efficiency. The VPN Server Module also allows for emulation of other enterprise VPN servers, enabling users to leverage existing VPN clients and configurations; or, the Aruba VPN client can be deployed, installed and configured to end users with no intervention required. An Aruba Wireless Intrusion Protection (WIP) Module is added to provide an additional layer of security, offering Denial of Service (DoS) prevention, Rogue AP detection, and network intrusion detection (NIDS) services. Each Aruba Supervisor Card Module in this implementation supports up to 128 access points.

The external services interface (ESI) software module enables communications and traffic direction to external appliances/services thus extending mobility features of the mobility controller. In this configuration the Fortinet network based anti-virus protection platform is added to the mobility controller though ESI. To provide internal network security defenses, network access control is implemented with Fortinet anti-virus protection and Aruba's Client Integrity Module which defends the network at the edge/access by automatically detecting, quarantining, and repairing infected or misconfigured devices before network access is granted.

This overlay approach provides VoIP-aware adaptive radio management including call admission control, automatic voice prioritization quality of service, and a voice

protocol aware stateful firewall supporting all the major protocols such as SIP, Spectralink, Vocera, Cisco's Skinny as well as fast roaming capabilities. As dual mode phones (GSM/WiFi) become increasingly popular, so too will the requirement to layer VoIP over the WLAN infrastructure. A conservative 25% discount factor is applied to the overlay WLAN approach.

**Deployment Costs**

Aruba's Mobile Edge overlay architecture operates independent of the wired LAN, requiring little or no change to the underlying wired infrastructure. No Layer 2 OS or policy updates are necessary, nor is the configuration of VLANs for WLAN traffic integration and management. This eliminates both the software and professional services costs associated with these updates. Additionally, Aruba's SPoE solution delivers power over Ethernet to the Aruba 70 access points over the existing category 5 wiring infrastructure, eliminating the expense of new plenum cable drops. RF monitor services provide by the AP's also remove the site survey requirement for WLAN optimization. In short, the mobile edge overlay architecture avoids the \$164K deployment cost.

Deployment Costs			
Power and Cable	Use existing infrastructure to deploy AP. No special cable run needed	\$	-
Site Survey	No site survey needed with Aruba's self configuring architecture (RF Live)	\$	-
Wired Network Adjustments	No adjustment to wired network needed with Aruba's overlay architecture	\$	-
Layer 2 OS Upgrades	No upgrades to OS on existing equipment forced by Aruba's WLAN deployments	\$	-

**Operational Expenses**

The collapsed nature of the Aruba Mobile Edge deployment centralizes all WLAN management functionality into the Mobile Controller, versus requiring the management of multiple discrete, distributed network appliances. As such, only approximately 25% of an IT manager's full time employment or FTE is required to manage and maintain the WLAN on an ongoing basis. Expertise for the WLAN switching, security, optimization and traffic management functions is achieved in a single environment through a common management console. The RF monitor and self-correcting features of the Aruba 70 Access Points eliminate the need for periodic site surveys. Ongoing support and maintenance costs are lower than the network integrated WLAN approach at 14% of the list price for controllers and OS software where applications are maintenance cost are 4%.

Operational Cost				
Loaded yearly cost of 0.25 Network Manager (Integrated Aruba System)	\$	25,000	1	\$ 25,000
No ongoing site surveys needed. System optimizes automatically	\$	-	0	\$ -
14% of List Price for Controllers/Software & 4% for Aps	\$	19,949	1	\$ 19,949
			<b>OPEX</b>	<b>\$ 44,949</b>

**FINDINGS**

---

The findings of this study suggest that there are significant capital, deployment, and operational savings achieved by deploying a centralized, mobile edge overlay WLAN solution versus a distributed network integrated WLAN solution for a 1000 user/100 access point implementation.

	<b>Integrated</b>	<b>Overlay</b>	<b>Savings</b>
<b>Capital Costs</b>	\$217,719	\$106,868	51%
<b>Deployment Costs</b>	\$164,000		100%
<b>Operational Costs</b>	\$148,544	\$ 44,949	70%
<b>Year One TCO</b>	<b>\$530,263</b>	<b>\$151,816</b>	<b>71%</b>

The centralized, overlay approach offered first by such firms as Aruba Networks offers a 71% 1 year total cost of ownership savings, and a 70% savings on ongoing operational costs associated with supporting the WLAN. Put another way the cost of an integrated approach is \$530/user versus \$151/user for the overlay approach. The largest contributor of capital cost difference between the two approaches is network security while deployment cost is significantly different. The bottom line is that it's just easier to deploy an overlay WLAN network.

Note that we sum capital cost and operational expense to arrive at a single TCO number while CFOs and accountants would not. The result would be the same; however the numbers would be different as every firm has their own calculation approach to IRR, depreciation schedules, asset utilization et al.

**CONCLUSION**

---

The study reveals that there is a clear and substantial cost benefit to deploying centrally managed mobile edge overlay WLAN architecture. It's clear that there are significant capital savings that stem from the collapse and integration of multiple discrete network elements into a centralized Mobility Controller, especially in the area of network security and VoIP support. Focusing all WLAN switching, AAA services, access control, network security and AP management into a common platform eliminates the complex integration of individual appliances that each contributes only a component of the overall WLAN architecture. Additionally, the implementation of a WLAN as an overlay to the existing enterprise wired LAN offers increased cost efficiencies by eliminating disruption of the LAN infrastructure, alleviating the requirement for Layer 2 switching upgrades and traffic engineering. The ability to utilize the existing LAN wiring infrastructure to deliver Power over Ethernet to the campus access points also greatly reduces the TCO, as well as the implementation timeline, by not requiring that new physical cable media be deployed.

The most striking TCO benefit is the 70% operational savings delivered by the Aruba Networks solution for ongoing support and management. The delivery of all WLAN services through a single, vertically-integrated platform allows for centralized management and control of the entire WLAN, allowing IT managers to easily manage the solution from a single, familiar management console. The overlay strategy enables the enterprise to manage the WLAN independent of the underlying wired LAN, alleviating the challenge of attempting to manage WLAN traffic and services in the context of wired LAN policies. Finally, the Mobility Controller enables simple, centralized ongoing management and maintenance of the radio access infrastructure, further contributing to operational savings.

The way business is being done is changing. It's becoming more mobile and collaborative. To support the new norms of business process a secure mobile

enterprise is fundamental. An overlay WLAN approach delivers the attributes needed to economically support mobile enterprise needs.

### **About Aruba Networks, Inc.**

Aruba Networks provides an enterprise mobility solution that enables secure access to data, voice and video applications across wireless and wireline enterprise networks. The Aruba Mobile Edge Architecture allows end-users to roam to different locations within an enterprise campus or office building, as well as to remote locations such as branch and home offices, while maintaining secure and consistent access to all of their network resources. Using the Aruba Mobile Edge Architecture, IT departments can manage user-based network access and enforce application delivery policies from a single integrated point of control in a consistent manner. Aruba's user-centric enterprise mobility solution integrates the ArubaOS operating system, optional value-added software modules, a centralized mobility management system, high-performance programmable mobility controllers, and wired and wireless access points. Based in Sunnyvale, California, Aruba has operations in the United States, Europe, the Middle East and Asia Pacific, and employs staff around the world. To learn more, visit Aruba at <http://www.arubanetworks.com>.

© 2007 Aruba Networks, Inc. All rights reserved. Aruba Networks and Aruba Mobile Edge Architecture are trademarks of Aruba Networks, Inc. All other trademarks or registered trademarks are the property of their respective holders. Specifications are subject to change without notice.