

ARUBA™

The Mobile Edge Company



**The Aruba Mobile Edge
Product Line**



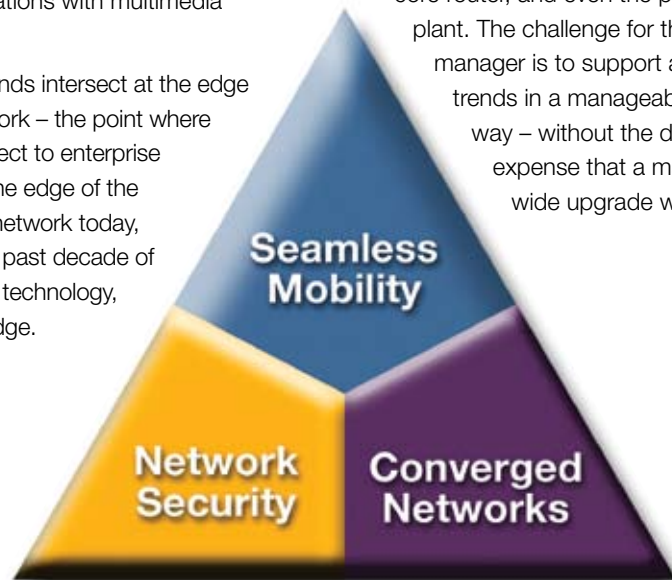
The Challenge

Network managers today are faced with three major IT trends that they must address: mobility, security, and convergence. Mobility is heavily driven by users through technologies such as Wireless LANs, cellular phones and VPNs to conduct business in the office, on the road and at home. Network security, protecting information assets against unauthorized disclosure, alteration, or destruction, has become increasingly important in the age of Internet worms, viruses, and spyware. Security has taken on increased importance in the United States, the European Union, Asia Pacific, and other locations with the introduction of new government regulations related to privacy, confidentiality, and integrity of financial results. Finally, converged networks that support both data and voice offer significant financial benefits and support richer enterprise communications with multimedia integration.

All three trends intersect at the edge of the network – the point where users connect to enterprise services. The edge of the enterprise network today, built on the past decade of networking technology, is a fixed edge.

It was designed for a time when users and devices were not mobile, and for a time when wireless was a point product used only in the warehouse and factory. The edge of today's network is highly reliable and extremely simple. When users connect to a port, the network is there to provide them with instant high-speed access. But this simplicity does not lend itself to security – the network does not differentiate between authorized and unauthorized users, and it cannot make decisions about which people get which type of access. Today's network was built for best-effort data delivery. It was built before Power over Ethernet existed to supply power to desktop phones, and before application aware quality of service policies were needed to ensure high voice quality.

Today's network can be upgraded to address mobility, security, and convergence. The upgrade is a massive one, involving every closet switch, branch office router, core router, and even the physical cable plant. The challenge for the network manager is to support all three trends in a manageable, reliable way – without the disruption and expense that a massive network-wide upgrade would entail.



The Solution

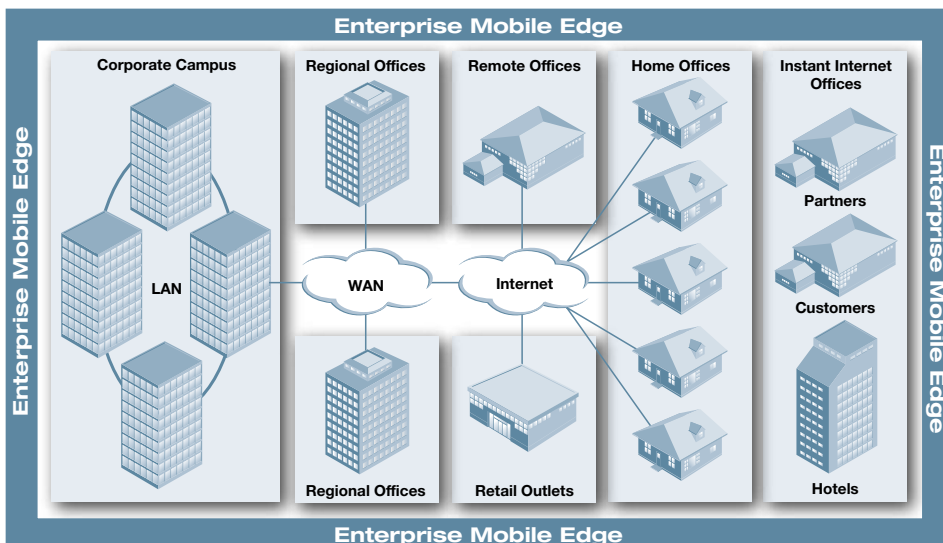
Aruba's Mobile Edge System enables a new type of edge for the enterprise network – the mobile edge. The mobile edge allows users and devices to connect over the air and across any network, to securely gain access to enterprise resources. It is a new layer in the network that logically sits on top of existing fixed networks and fulfills the requirements of security, mobility and convergence without requiring major upgrades to the existing network. The mobile edge is architected to securely work over existing IP network facilities, and extends across both private enterprise networks as well as the public Internet.

The mobile edge by definition supports true mobility where users can seamlessly and securely roam across multiple locations. In addition, it delivers voice convergence through multimedia mobile devices and Voice over Wireless LAN (VoWLAN) handsets with high quality and reliability. This eliminates the significant expense of adding powered VoIP ports to the fixed edge. Further, the mobile edge is built on the notion of identity-based security. Mobile users and devices, by definition, do not connect to the network through a fixed port. For this reason, the network must identify every user and device that joins the network. Once this identity is known, custom security policies may be applied to the network so that only access appropriate to the business needs of the user or device

is provided. This drastically improves network security by eliminating excess privilege on the network while providing identity-based auditing.

The mobile edge not only solves today's challenges around mobility, security and convergence but provides a roadmap to reduce overall costs of the network infrastructure. The natural long-term evolution of the enterprise network edge is to become predominately mobile. When this happens, a radical transformation of enterprise network economics will be realized when the costs of cabling infrastructure and the operational expense of moves, adds and changes are eliminated. This introduces a dilemma for incumbent networking vendors. The incumbent vendors, in order to continue their growth, must entice customers to spend more on their networks. The mobile edge, by drastically reducing networking costs, runs directly counter to the needs of the incumbent vendors. The 'incumbent's dilemma' develops whenever major turning points in technology develop – the incumbent cannot grow business by offering a solution that allows customer to spend less.

The mobile edge is not based on this incumbent's dilemma. It is an evolutionary new architecture that delivers mobility, security and convergence for today's networks and builds on a vision where the enterprise network will ultimately have far fewer ports than today.





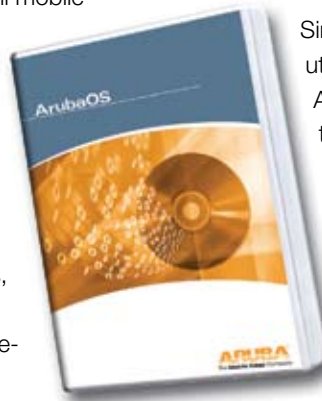
The Products

Aruba's Mobile Edge System consists of three components:

1. ArubaOS system software which provides all the intelligence for the Mobile Edge
2. Mobility controllers which are centralized service delivery platforms for the Mobile Edge
3. Controlled access points (APs) which tunnel wired and wireless user traffic to mobility controllers over the LAN, WAN and the Internet

ArubaOS System Software

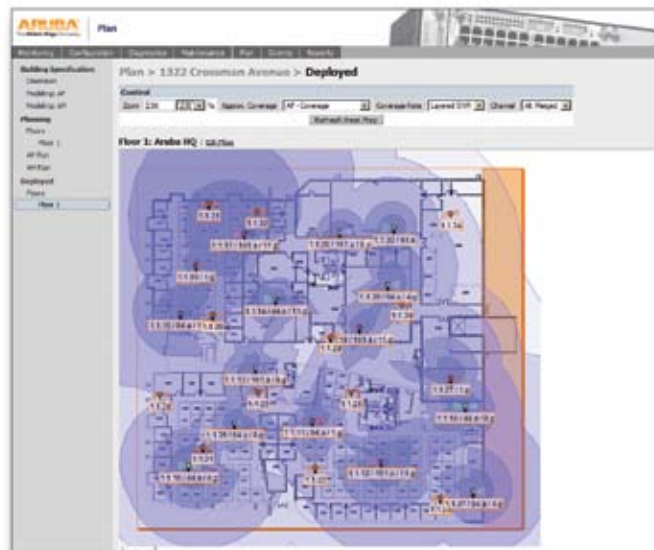
A robust and sophisticated suite of system software that powers the mobile edge, ArubaOS coordinates all mobile edge operations with advanced capabilities that include seamless mobility, identity-based security, non-disruptive integration into existing networks, mobile VoIP capabilities, adaptive radio management, enterprise-class resiliency, open APIs, end-to-end QoS and centralized management.



ArubaOS is fully modular software that runs on all Aruba mobility controllers and controlled access points, allowing them to work seamlessly in delivering services to users on the mobile edge. The base feature set of ArubaOS comes standard with every mobility controller and includes sophisticated authentication and encryption, seamless mobility with fast roaming, RF management and analysis tools, centralized configuration, location tracking and more.

ArubaOS gives administrators a single point of control from which to locate and shut down rogue APs, identify and thwart malicious attacks and impersonations, load-balance traffic, detect coverage holes and interference and create stateful role-based security policies that follow individuals as they move across the mobile edge.

Since all Aruba mobility controllers utilize the same hardware architecture, ArubaOS is fully portable across the entire range, offering identical features but with differing price and performance points, depending on the underlying mobility controller. ArubaOS is entirely modular, with particular emphasis on reliability features such as automatic process restarts to minimize the impact of software failures and full VRRP redundancy across processors and chassis to minimize the impact of hardware failures.



ArubaOS includes the following optional software modules:

Wireless Intrusion Protection module provides patented classification technology that identifies and protects against malicious attacks such as denial of service, vulnerabilities such as rogue APs and ad-hoc networks, client and AP impersonation, and man-in-the-middle attacks.

Policy Enforcement Firewall module delivers user and group policy enforcement through an integrated ICASA-certified stateful firewall. Security policies can be centrally defined and enforced on a per-user or per-group basis, following users as they move. Policies are enforced dynamically, taking into account a variety of metrics such as user location, time-of-day, device type, authentication method and others.

VPN Server module provides integration support for a variety of virtual private network implementations, eliminating the need for discrete, external VPN concentrators. Hardware acceleration provides LAN-speed VPN connectivity. Supported VPN protocols include L2TP/IPsec, IPsec/XAUTH and PPTP. Both client termination as well as site-to-site VPNs are supported.

Client Integrity module provides wired and wireless network integration for client integrity enforcement, protecting the network against infection from malware such as viruses and worms that take advantage of mobile devices. The Client Integrity Module integrates software from Sygate Technologies™ for host integrity, virtual desktop with file and cache cleaner and safe guest access with protection against 'zero-day' threats.

Remote AP module lets network managers securely extend corporate wireless functionality to any location with an Internet connection. Remote APs allow seamless corporate-like WLAN connectivity at home, a remote office, or anywhere a mobile worker chooses to work.

External Services Interface module enables any Aruba mobility controller to communicate with external service devices. The ESI module selectively redirects network traffic, based on policy, to devices providing inline network services such as anti-virus, network intrusion detection, content filtering, content transformation and usage auditing. Full load balancing and health checking are supported.

Advanced AAA module extends authentication and authorization features of standard ArubaOS, including domain- and realm-based selection of authentication server, dynamic authentication and authorization using RFC 3576 and an XML API for building external portal and authentication systems.

xSec module provides termination of highly secure xSec client sessions, offering link-layer 256-bit AES-CBC encryption with complete header obscuration for highly sensitive environments. The xSec module also enables the encryption of trunk ports between Aruba mobility controllers based on the same strong encryption standard.





Mobility Controllers

Mobility controllers are high-performance networking platforms built specifically to run centralized ArubaOS functions such as controlled access point management, 802.11 station management, 802.11x authentication and encryption, site-to-site and client VPNs using IPsec/3DES encryption, stateful policy enforcement firewalls, L1-L7 intrusion protection, endpoint integrity checking, and seamless user roaming between access points and across mobility controllers.

All mobility controllers share a common hardware architecture which includes a dedicated control plane CPU, a high-performance programmable data plane network processor unit, and a unique programmable encryption engine for centralized L2 and L3 encryption. They aggregate traffic from the mobile edge, inspect and police it and deliver it to the core enterprise network. Mobility controllers are typically positioned in data centers, for a controlled environment and access to the high-speed core network, since they handle traffic from hundreds of APs and thousands of users.

Aruba's line of mobility controllers includes multiple models, sized and priced to support the varying requirements of different sized mobile networks.



The Aruba 6000 is the only modular mobility controller on the market. The four-slot modular chassis supports up to 8 Gbps of cleartext (7.2 Gbps of encrypted) throughput, up to 72 10/100 Mbps ports, 8000 simultaneous users and from 4 to 512 controlled APs. Hot-swappable line card slots support multiple connectivity options including a 24 port Fast Ethernet + 2 port Gigabit Ethernet line card as well as a 2 port Gigabit Ethernet line card.



The Aruba 2400 is a stackable, 24-port mobility controller that supports 48 APs. Designed for regional headquarters or dense building deployments, the Aruba 2400 supports up to 512 simultaneous users and delivers up to 400 Mbps of encrypted throughput.



The Aruba 800 is a fixed configuration mobility controller designed for small and branch office applications. The Aruba 800 provides eight 10/100 Mbps user ports and one copper or fiber gigabit uplink. Programmable hardware-based encryption supports 200 Mbps of full-duplex encrypted traffic.

Controlled Access Points

Centrally controlled by ArubaOS software, Aruba's line of wired and wireless APs serve as distributed traffic collectors tunneling wired and wireless traffic to mobility controllers over IP networks. Wireless APs provide radio coverage and user connectivity services while simultaneously serving as surveillance devices that constantly monitor the air for radio-based security threats. They also perform intrusion protection functions when wireless threats are detected. Wireless APs also run distributed ArubaOS functions such as adaptive radio management, distributed encryption for local forwarding of Wireless LAN traffic, wireless intrusion detection and protection, rogue AP detection and containment among others. Wired APs simply serve as traffic collectors and tunnel wired user traffic across a LAN or a WAN to an Aruba mobility controller.

Aruba offers a wide range of controlled APs including indoor and outdoor 802.11a/b/g single-radio access points, 802.11a/b/g dual-radio access points, 802.3 wired access points and hybrid wired/wireless access points. WLAN APs come equipped with integral antennas or options for a wide variety of external antennas. All controlled APs work with all Aruba mobility controllers to provide a high-performance, secure mobile edge.

Controlled APs can be connected to an existing IP network and will automatically discover an Aruba mobility controller, configure themselves, and begin operation. The mobility controller is responsible for downloading software images, configuring, and coordinating all controlled APs. APs are powered through 802.3af Power over Ethernet (PoE), eliminating extra wiring requirements. They also come equipped with DC power jacks that work with AC power adapters if PoE is not available.

All APs can simultaneously provide wireless service as well as monitor the air. They continuously scan the RF environment, locating and tracking all wireless clients to provide warning of intrusion or interference. This dual functionality eliminates the need

for a separate overlay of RF sensors to troubleshoot and optimize the wireless environment.

Aruba's controlled APs are available in a wide variety of form factors and capabilities.

The Aruba 41 is a low-cost single-radio AP designed for the telecommuter or home office. With a single integral antenna and 802.3af Power over Ethernet, the Aruba 41 is an ideal AP for deployment where antenna diversity and plenum installation are not factors.



The Aruba 60 and

61 are single radio, 802.11a or b/g APs designed for dense wireless deployments in the corporate office. Plenum rated and powered by 802.3af Power over Ethernet or through an external AC adapter, the Aruba 60 and 61 deliver superior capacity, performance, and coverage. The Aruba 61 features an integrated 802.11a/b/g omnidirectional antenna while the Aruba 60 features dual external antenna connectors. The Aruba 60 and 61 are the perfect APs for highly dense "Wireless Grid" deployments.



The Aruba 65 is a dual-radio 802.11a/b/g AP designed for the mobile enterprise worker or road warrior. With integral diversity antennas, 802.3af Power over Ethernet, an external power adapter, and a compact design, the Aruba 65 fits easily in a briefcase and connects wherever a mobile user travels.



The Aruba 70 is the industry's first dual-radio 'hybrid' access point that provides concurrent operation of 802.11a and 802.11b/g services, as well as secure wired access through an additional Ethernet port. The Aruba 70 is a multi-purpose device that can function both as an access point and as an RF monitor – either independently or concurrently – across the 2.4 GHz and 5 GHz bands. Ideally suited for plenum or workspace deployment, the Aruba 70 can be securely wall-mounted, ceiling-mounted, or desk-mounted.



The Aruba 80 is the industry's first controlled outdoor access point. With support for 802.11a, 802.11b/g, and wireless bridging, the Aruba 80 handles all outdoor wireless applications. The Aruba 80 is rated for extreme outdoor environments, with an operating temperature range of -30 to 55 degrees Celsius and an integral lightning arrester and ground point.





The Applications

The mobile edge is an enabling technology for new applications that can deliver increased productivity, cost savings, security improvements, and faster access to information that ultimately leads to better decision making. The mobile edge enables several major applications in the areas of mobility, security, and convergence.

Mobility

Guest Access – Provides controlled Internet access, both wired and wireless, to authorized visitors while keeping the internal network secure.

Internal WLAN Hotspots – Wireless LAN access for employee and visitor convenience in strategic locations such as conference rooms, lobbies, cafeterias, and auditoriums.

Enterprise-wide WLAN – Pervasive, highly-available, high-performance wireless LAN access throughout an entire enterprise building, campus, or extended enterprise.

Remote/Branch Office Access
– Secure extensions of the mobile edge to remote and branch offices using the Internet or enterprise WAN as transport.

Small Office, Home Office, and Road Warrior Access – Extends the mobile edge anywhere a user travels through portable, personal remote access points.

Secure Mobility for Legacy WLANs
– Extends the life of existing wireless LAN deployments through enhanced security, roaming, and management.

Location Tracking – Uses an enterprise-wide WLAN deployment to provide precise location tracking of any Wi-Fi device in the facility.

Security

Identity-based Security – Enhances security by identifying the business role of the user and then allowing only network access appropriate to that role.

WLAN Intrusion Prevention – Prevents radio-based security breaches by identifying threats to the network from attackers and uncontrolled wireless devices.

Endpoint Integrity – Ensures a defined level of client security, such as anti-virus, anti-spyware, or personal firewall software is present before network access is granted.

External Security Services – Integrates best-of-breed security appliances, such as anti-virus, content filtering, and IDS as interior network services that are client-independent.

L2 Security for Wired LANs – Delivers mobile edge solutions such as encryption, mobility, and identity-based security to legacy wired LANs.

Convergence

Telephony Solutions – Provides the cost advantages of Voice over IP with the mobility benefits of cellular voice.

Voice Instant Messaging – Enables hands-free voice communication through an innovative new class of voice instant messaging devices, enhanced with proximity sensing.

Converged Mobile Devices – Delivers quality of service and access control to unified communications messaging devices integrating multi-media services such as voice, data, email, and fax.

Fixed-Mobile Convergence – Unifies public and private voice networks by providing seamless handoffs between networks for dual-mode cellular/Wi-Fi voice devices.

The Aruba Difference

Aruba's mobile edge architecture provides superior features and benefits to competing wired and Wireless LAN solutions. With Aruba's mobile edge solution, enterprises can transform the network into a competitive advantage through a highly mobilized workforce with instant access to information. At the same time, the reduced infrastructure costs, increased security, and increased flexibility provide a powerful economic advantage.

Only Aruba delivers:

1. Identity-based security to protect the network and mobile users

The mobile edge is, by definition, mobile. On the mobile edge any user can appear in any place at any time, so the network must recognize the user or device by identity. Identity-based security solves security problems by applying rules to people rather than to ports on the network, only permitting access appropriate to the business role of the user.

2. Non-disruptive integration into existing networks

The mobile edge must be cost-effective in order to enjoy widespread adoption. Deployment of the mobile edge cannot force large scale upgrades or changes to the existing infrastructure, nor can it force network downtime. The mobile edge must integrate into existing management tools, security monitoring systems, and auditing procedures.

3. Secure convergence for mobile VoIP and data services

The mobile edge must be multi-service. On the mobile edge, voice is a critical service. Voice over wireless LAN (VoWLAN) provides all the mobility benefits of cellular with the cost savings of VoIP and does not require expensive power upgrades to wiring closets. Newer dual-mode voice handsets operate over the enterprise Wireless LAN wherever it is available, and over the public cellular network everywhere else, providing true cost-effective voice mobility to users.

4. Adaptive radio management for self-configuring WLANs

The mobile edge requires adaptive control of the air. Radio frequency (RF) transmission is an inherent part of wireless, and one with which many network administrators are not familiar. The goal of any wireless deployment is to provide the required coverage while guaranteeing maximum performance. With the pervasive nature of wireless on the mobile edge, RF tuning cannot be a manual task that the network administrator must perform. RF management must be entirely automatic, reliable, and adaptable.

5. Remote extensions for instant enterprise hotspots

The mobile edge moves with the user. Users move outside the walls of the enterprise facility, yet still need access to enterprise voice and data networks. Left to their own devices, users will create their own version of the mobile edge wherever they need to – using DSL or cable connections at home, using open wireless networks at public hotspots, plugging into Ethernet jacks in hotel rooms, or connecting over public wireless networks such as GSM or EVDO. To avoid the support and security problems

caused by this approach, the mobile edge must extend on-demand enterprise voice and data connectivity over the Internet to create secure personal hotspots wherever users need to work. These hotspots move with the user, but control and configuration remains with the network administrator.

6. Enterprise-grade scalability, reliability and performance

The mobile edge must be dependable. To realize the full benefits of the mobile edge, it must provide predictable, consistent performance and high reliability. The system should gracefully recover from all component failures with no network outage noticeable to the user. Performance should meet all requirements of mobile applications, and should remain high even in challenging RF environments. Finally, the mobile edge should grow with the enterprise without requiring additional people to manage it.

7. Open mobility platform for application development and integration

The mobile edge is a business-enabler. New mobile applications will create business opportunities and enhance existing ones, creating competitive advantages for users of the technology. Applications such as voice, location tracking, and sensor networks are the first purely mobile applications and more are being developed as mobile networks become more prevalent. In addition to mobile applications, new services are continually being developed for security, such as network-based spyware blocking, and convergence, such as fixed-mobile handoff and emergency call location tracking. The mobile edge must be flexible, extensible, and open to application development by best-of-breed vendors.





ARUBA[™]
The Mobile Edge Company

1322 Crossman Avenue • Sunnyvale, California 94089 • Tel: 408.227.4500 • Fax: 408.227.4550