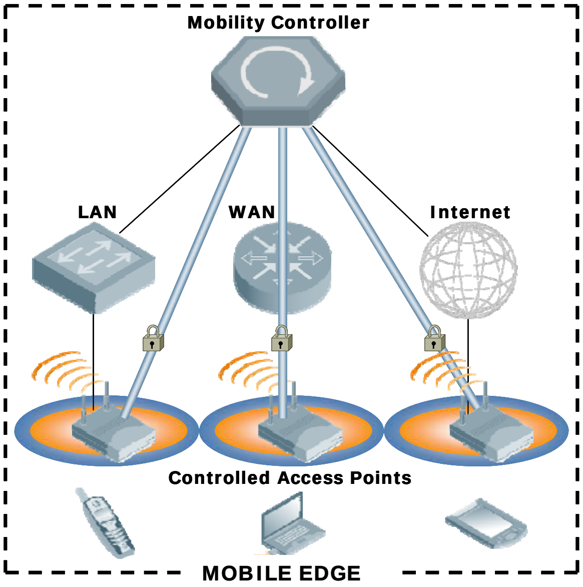
ARUBA™
The Mobile Edge Company

Aruba Networks – Response to Network Computing's Enterprise WLAN Infrastructure Request for Information

Architecture

Aruba Networks' mobility architecture is known as the "Mobile Edge." The Mobile Edge is a recognition that network users move, and the network services must follow to be available wherever the users need to do business. The Mobile Edge is built using centralized mobility controllers at the core and a series of wired and wireless access points at the edge. Between the two components is a reliable, high-speed transport network – the corporate LAN, the corporate WAN, and the Internet. Aruba mobility controllers and access points communicate with each other using standard IP protocols such as IPSec and GRE. This means that wired and wireless APs can be deployed anywhere, and connected to any IP network, as long as a mobility controller is reachable from that network. The existing wired network is known as the "no touch zone" since no modification to any portion of the transport network is required in order to deploy an Aruba solution.

The figure below illustrates Aruba's overlay deployment model. As shown in the diagram, Aruba controlled APs are deployed and connected to existing wired networks. APs obtain an IP address from the local DHCP server, dynamically locate a mobility controller, and finally establish either GRE or IPSec tunnels to a mobility controller. All wireless client traffic, in encrypted 802.11 format, is delivered to the mobility controller through these tunnels. The tunneling mechanism ensures that the assigned subnet of the wireless clients does not depend on the subnet where the AP is deployed, thus avoiding "VLAN explosion" at the edge of the network.



Aruba's architecture differs from other offerings in the market in two major ways:

- Secure transport is not required. Aruba APs establish encrypted IPSec tunnels to the mobility controller and may be deployed across hostile networks such as the Internet. Competing products that offer "remote office" modes of operation require a secure link between the AP and the controller.
- Centralized encryption. Aruba APs do not decrypt wireless traffic. Instead, this traffic is brought back to the mobility controller in native over-the-air format. This provides much stronger security, allows the APs to be deployed in non-secure locations, and aids in RF management and troubleshooting since 802.11 headers are available to the controller. In sensitive security environments such as government deployments where FIPS 140-2 is required, centralized encryption also establishes the cryptographic boundary at the mobility controller itself, rather than requiring a cryptographic boundary to be drawn around the entire network.

Wired-Wireless Integration

Customers are often tempted to buy their wireless LAN from the same vendor that provides their wired LAN. While there are some benefits that can result from this approach in terms of streamlining purchasing, there is ultimately no benefit in terms of technology or support. Vendors who claim "integration" have in fact integrated almost nothing, and often have an ulterior motive of upgrading existing equipment and selling additional equipment where it is not needed. The lack of true integration in these products leaves customers confused, since they expect an "integrated" product to operate using common configuration, common management infrastructure, and common troubleshooting techniques. Unfortunately, most "integrated" products are simply blades for a large chassis that share the same power supply and backplane.

Aruba understands that enterprise networks are made up of a variety of equipment – in the LAN and WAN, in the corporate and branch office, and on the desktop. Aruba designed its products based on standards to provide the greatest interoperability possible while not requiring anything but fast, reliable transport from the underlying network. Aruba has been deployed in enterprises that use Cisco routers and Nortel Ethernet switches in the corporate office with Netgear consumer-grade equipment in branch offices connecting to business-class DSL lines. These networks are managed by a collection of tools such as NetCool, mrtg, and custom Perl scripts. By providing a wireless LAN that operates as a pure overlay, Aruba is able to install in such environments and provide support to these customers, where other "integrated" vendors would require massive equipment swap-outs in order to "guarantee interoperability." Likewise with client interoperability, Aruba does not have the luxury of promulgating proprietary client drivers. Instead, Aruba works to achieve interoperability with all clients, and when problems are found Aruba proactively works with client manufacturers to address these problems. Aruba's technical support engineers have never told a customer, "You'll need to buy wireless cards that support our proprietary driver shim in order for us to guarantee the best performance."

Security

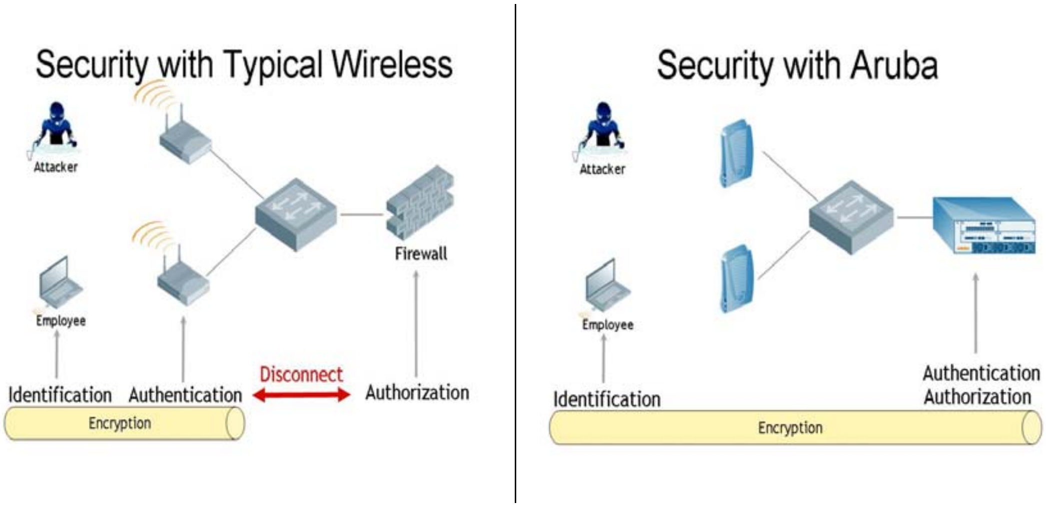
Although the standardization of WPA2 was a great step forward in wireless security, it is not the end. Even using WPA2, a single compromised username/password combination could potentially breach the entire network. In order to provide the greatest degree of protection, a multi-layered approach to security is needed. In an Aruba deployment, a multi-layer security system is built from the following integrated components:

- Encryption – Aruba is the only vendor in the industry to support centralized encryption at gigabit rates. All encryption in an Aruba network, whether for WEP, VPN or WPA2 is performed by a dedicated programmable encryption engine located in the Aruba mobility controller. The result for customers is greater security without a performance impact. Most other vendors claiming "thin" access points (APs) do not have the required encryption performance in the controller and thus perform this function in the AP, using encryption routines built into radio chipsets. This sacrifices security for customers, because sensitive encryption keys must be distributed to APs across potentially hostile networks. Performing encryption in the AP also means that traffic leaving the AP is plaintext – a weak point for an attacker to tap in and monitor confidential transactions. Aruba suffers from no such security weakness – wireless data remains encrypted until it reaches the mobility controller, usually located in a data center or other secure facility. Because encryption keys never leave the controller, and because user data is encrypted until reaching the controller, data protection is maintained.

- Authentication – Because there are no physical ports in a wireless network, it is essential to ensure that only authorized parties are permitted access to the network. In addition, for accountability and auditing, each user of the network should be uniquely identified. Strong authentication is the best way to accomplish this. Aruba recommends 802.1x-based protocols such as WPA and WPA2 to provide authentication, with IPSec as an alternate. A variety of authentication credentials can be supported. Aruba recommends certificate-based authentication, smart card authentication, or token authentication such as SecureID. Username/password authentication may be used, but only in the presence of a strong password policy backed up with password auditing.

- Role-based authorization – The Aruba mobility controller contains a full ICSA-certified stateful firewall. Like standard firewalls, the Aruba firewall can make permit/deny decisions based on ingress interface, egress interface, source address, destination address, protocol, port number, and application-layer state. Unlike traditional firewalls, the Aruba firewall is also identity-aware and can make permit/deny decisions based on identity of the user or device. Identity awareness comes through authenticating users and devices joining the network. Identity is mapped to a business role – in a retail environment, for examples, roles may include "handheld scanner", "store associate", or "store manager." Once the role of the user is learned, appropriate rules may be applied that control what that user or device is permitted to do on the network. Through identity-based security, privilege escalation attacks are prevented, such as an attacker cracking the WEP key on the scanner network and using it as a gateway to access credit card information or financial data.

  Combining encryption, authentication, and access control in a single device provides a powerful security advantage. Because wireless devices authenticate to the network, identity is learned. Because encryption from those wireless devices terminates at the mobility controller, the system can ensure that network traffic was not forged by an intruder or tampered with in transit. And finally, because access control is done through the Aruba firewall, policy can be tightly tied to the identity and role of the user rather than to an arbitrary parameter such as IP address. This means that even a malicious insider cannot alter a MAC address or IP address to "become" someone else – access control decisions are made on the basis of user identity, not network address. The figure below illustrates the difference between an integrated identity-aware firewall and a traditional external firewall.



- Intrusion Protection – Aruba's Wireless Intrusion Protection feature set protects against threats *from* wireless as well as threats *to* wireless. Threats *from* wireless come in the form of Windows XP laptops that have enabled bridging between a wireless and wired interface, rogue APs installed by employees into the network, unsecured wireless bridges, and ad-hoc networks. Threats *to* wireless include denial of service attacks, impersonation attacks, and man-in-the-middle attacks. Aruba's WIP system detects and blocks such threats, while pinpointing the physical location of the threat on a building floor plan so the administrator may take proper action.

- Client integrity – Mobile clients leave the building, and thus the protection of the corporate firewall/IDS. When those clients return to the network, any malicious software they may be carrying is let into the network behind the external security perimeter. Client integrity protection is a method of ensuring that clients meet a minimum level of security requirements, such as anti-virus software, before allowing network access. For *managed* clients, controlled by the IT department, Aruba integrates seamlessly with a number of popular software packages including Microsoft NAP, Symantec Secure Enterprise, and Cisco NAC. For *unmanaged* clients, such as visitors at a corporate office or students on a university campus, Aruba provides integrated client integrity protection through the Client Integrity Module for ArubaOS. Finally, for *unmanageable* clients such as cellphones, PDAs, and non-standard operating systems, Aruba is able to provide protection services - such as anti-virus scanning, content inspection, and intrusion detection – inside the interior of the network through controlled forwarding of traffic through best-of-breed security appliances.

- Auditing – Aruba provides the capability of logging any and all access to the network, on a per-session basis or even a per-packet basis if required. Using these logs, a detailed record of "who did what, and when" can be constructed. Additionally, ArubaOS allows the definition of "trigger events" that cause the system to place users into "watch lists". Once on a watch list, all activity related to a user is logged, including physical location, signal strength, authentication activity, and all data traffic. This information can be stored in a format suitable for forensic use in a court of law.

- FIPS Validated – Aruba has achieved Federal Information Processing Standards (FIPS) validation for 802.11i-based wireless LAN systems, which makes the company the first to be able to provide secure WLANs meeting this requirement to the U.S. federal government. 802.11i is the latest standard in wireless security widely acknowledged to be the safest available standards-based mechanism for wireless data transmission. While vendors other than Aruba can offer FIPS-validated systems that are proprietary or partial, Aruba is the first vendor to offer a complete and integrated system for the Federal marketplace approximately eight months ahead of competitors.

Government agencies can now easily and securely deploy standards-based commercial off-the-shelf (COTS) wireless fidelity (Wi-Fi) across their organization without having to install different FIPS-validated wireless security products, each of which adds significant complexity and cost. Other wireless systems distribute security in different devices such as access points (APs), controllers and firewalls, meaning each device must obtain FIPS-validation and re-validation in the event of any security change. In addition, these devices prohibit some of the primary benefits of mobility, such as roaming between access points and high availability through failover. Other vendors' progress towards FIPS validation can be viewed at http://csrc.nist.gov/cryptval/preval.htm

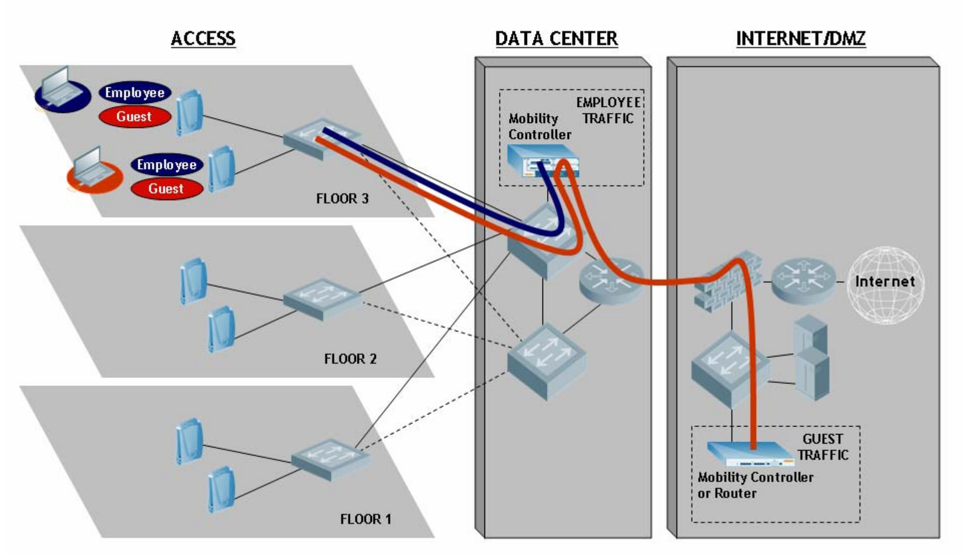
Guest Access

Guest access is a requirement from a majority of enterprise customers today. Guest access is a productivity-enhancing tool for the visitor and the employee alike, meaning that there are solid business reasons for its deployment. There are three main challenges when deploying guest access: First, ensuring that only legitimate company guests have access to the network. Second, minimizing IT resources needed to support the solution. And third, controlling the guest traffic so that only approved services are used and so that guest traffic is kept off the internal corporate LAN.

The Aruba guest experience begins at the receptionist desk when checking in. A receptionist is able to use a simple web browser interface to the Aruba controller or management system in order to provision a guest account. A username and password is generated, and the receptionist is able to specify an account expiration date and time or a session length. This happens without giving the receptionist administrative privileges on the system and without the need to install an external guest management system.

Next the visitor connects to the guest SSID and is given an IP address. During this time, the Aruba integrated firewall ensures that the visitor is completely quarantined from the rest of the network, including other guest clients on the same SSID. The user launches a web browser and is taken to Aruba's integrated captive portal website where he or she is prompted for a username and password. Entering the username and password provided by the receptionist, the guest is granted access. The visitor is able to run a set of administrator-defined applications such as VPN, web browsing, and POP3 email. The administrator has blocked SMTP, peer to peer file sharing, port scanning, and other non-approved services. Additionally, the administrator has specified a bandwidth limit for the guest user so that visitors are not able to consume excessive amounts of network bandwidth.

The biggest challenge when deploying guest access is ensuring with absolute certainty that guest traffic cannot cross the boundary into the internal corporate network. Only Aruba, through the use of an integrated stateful firewall, can provide this level of assurance. Competing solutions use VLANs for traffic separation, a technique that will not pass security audits because of the risk of "VLAN hopping" or crafted packet attacks. In a basic single-controller Aruba solution, the guest user is placed into a guest role with a set of firewall policies applied that limit where the guest user may send traffic. In a more advanced guest access solution, such as that shown in the figure below, guest traffic is actually tunneled over GRE or IPSec to a second mobility controller located outside the firewall – or even off the enterprise network altogether. By terminating the employee SSID inside the corporate network and the guest SSID outside the corporate network, complete separation is maintained.



Performance and Scalability

Aruba offers four different models of mobility controllers to meet the needs of different sized deployments. A remote location such as a small clinic or retail store can install the Aruba 200 mobility controller or Aruba Remote AP to support a small network, while a large corporate office, university campus, or military base can install one or more Aruba 6000 mobility controllers to support a much larger network. All devices in the local or extended network can be controlled and maintained from a single management console. The table below summarizes the performance and capacity characteristics of Aruba's family of mobility controllers.

	Aruba 6000	Aruba 2400	Aruba 800	Aruba 200
Deployment	Large Campus	Branch Office	Remote Office	Branch Office
Size	3RU	1RU	1RU	Desktop
Access Points	512	48	4 or 16	6
Users	8000	768	256	100
Plaintext Throughput	8 Gb/s	2 Gb/s	1 Gb/s	1 Gb/s
Encrypted Throughput	7.2 Gb/s	400 Mb/s	200 Mb/s	200 Mb/s

Availability

Availability of a wireless system consists of three different areas:

- Availability of the RF. If the client and AP cannot communicate reliably or with high enough performance over the wireless link, users will not be able to use wireless as their primary connection. Aruba's Adaptive Radio Management (ARM) constantly monitors the RF environment to ensure that APs are operating on their optimal channel and are providing sufficient RF coverage to service all clients. Aruba APs monitor other Aruba APs and feed information back to the mobility controller for processing. By self-tuning and automatically avoiding interference, ARM ensures that the radio signal is as clear as possible.
- Availability of the AP. Failure of an AP is first dealt with by placing multiple APs within range of all areas of a building such that the failure of a single AP or even multiple APs will be treated as a simple roaming event by clients. Second, Aruba APs may be physically dual-homed by using both Ethernet ports so that failure of an entire closet switch does not take down the AP.
- Availability of the controller. In a centralized architecture, the controller must not be a single point of failure. Aruba supports "active-active" redundancy, whereby two controllers each service half of the APs in a given location. The failure of a single controller will cause that group of APs to reconnect to the operational controller. During the failover interval, the remaining operational APs are able to take the load. Aruba also supports "active-standby" redundancy using industry-standard VRRP. In this type of deployment, all APs connect to a virtual IP address that is shared between the two controllers. If the active controller fails, the standby controller immediately takes over the virtual IP address. APs do not notice that a failure has taken place.

VoIP Support

Aruba has consistently outperformed the competition in independent voice over WLAN bakeoff testing. Aruba provides the highest voice quality measured through R-values, the lowest latency and jitter, the fastest roaming, and the strongest security. Aruba also provides voice management features that enable real-life deployments that work outside of lab environments. Aruba's architecture is uniquely suited for supporting voice over Wi-Fi.

- Aruba provides protocol-aware QoS to ensure voice traffic is prioritized properly. Other WLAN solutions require that voice traffic be placed on a separate SSID from data traffic, and all QoS is mapped to the SSID. In an Aruba solution, converged devices that support simultaneous voice and data can be supported because the Aruba system identifies voice flows and gives them priority while providing best-effort service to data traffic.
- Aruba provides flow-based Call Admission Control (CAC) that guarantees voice priority while preventing queue starvation for data traffic. Flow-based CAC requires a stateful flow classification engine which understands voice protocols such as SIP, SVP, and Cisco Skinny. When a voice call is placed over the network, the Aruba system recognizes the off-hook condition and checks to see how many other active voice calls are present. If a given AP has a full load of voice calls, the system will load balance the new client to a less-utilized access point, and if none is available, will prevent the call from proceeding – resulting in a fast busy signal. This function is critical for voice devices that do not yet support 802.11e-based call admission control using T-SPEC.
- To secure the voice traffic, Aruba's stateful firewall provides for:
    - Stateful recognition of traffic flows (e.g., SIP) via the built in flow classifier to offer the ability to prioritize flows from a VoIP client app versus data on the same device.

- Rules allow for enabling of VoIP traffic to not become a backdoor mechanism to attack the internal network by limiting the traffic to specific ports and IP addresses. In addition, the firewall is stateful for voice protocols such as SIP and H.323, allowing it to selectively open ports for calls based on information in the control channel.
- Traffic is priority tagged in the Aruba GRE header for prioritization via DSCP (DiffServ Control Point) to take advantage of wired QoS mechanisms.
- Bandwidth control per-role (e.g. guests can be limited to specific throughput levels) to prevent VoIP traffic from being overrun by data.

Aruba Networks has partnered with the premier VoIP solutions providers, including Avaya, Alcatel, Spectralink and Vocera. Aruba is routinely involved in extensive interoperability testing and configuration with these partners to ensure compatibility as new voice over Wi-Fi standards evolve.

Design and Deployment

Wireless APs are a shared medium, where each client must contend for bandwidth and access to the medium with all other clients attached to the same access point. Wireless "best practices" from just a few years ago made this problem more acute by deploying access points for maximum range rather than maximum performance. With greater range, a larger number of clients were associated to each AP, leading to higher contention for the available bandwidth. With greater range, clients could also be far away from the AP, resulting in lower speed.

Aruba offers a deployment option, known as the "Wireless Grid," that can ease deployment and planning headaches. Aruba's Wireless Grid deployment architecture solves the performance problems of past-generation wireless by creating numerous small "cells" within the RF environment, with each cell containing only a small number of clients. The Wireless Grid is built upon the following principles:

1. Where possible, APs should be deployed in user space – not above ceiling tiles. The RF obstructions present in user space help to reduce range – thus increasing performance. APs may be connected using existing Cat5 cabling. In many hospitals and buildings with asbestos, exposing the ceiling for AP or wiring repair creates potential health hazards. Particularly in these environments, putting APs in user space is far more cost effective and easier to maintain than APs in-ceiling.
2. Access points today are inexpensive and the prices will keep falling. Once factors such as installation cost and site survey cost are taken into account it is far less costly to deploy a large number of inexpensive APs in user space than to deploy a small number of APs above the ceiling
3. In order to prevent interference between closely-spaced APs, advanced RF management is required. Aruba's Adaptive Radio Management (ARM) is optimized to automatically maximize performance while minimizing interference.

For those customers who desire a more traditional wireless deployment with a smaller number of APs, Aruba offers a planning tool known as "RF Plan" that allows import of building dimensions, floor plan drawings in JPEG or AutoCAD format, and desired coverage parameters. The tool then builds a 3D predictive model of RF coverage and plans out the optimal location of APs.

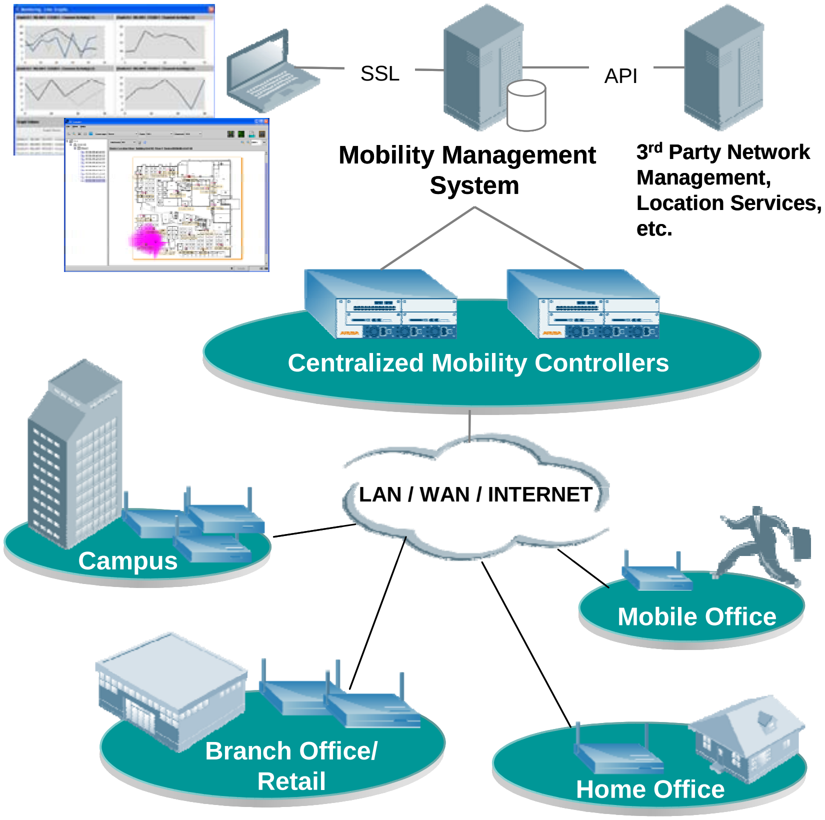
Monitoring and Management

Aruba systems are a single interface point for management of the entire wireless LAN. The system contains an integral network management system (NMS) that configures, controls, and operates all mobility controllers and access points in the entire network. In addition, integrated troubleshooting tools make it possible to diagnose and fix client problems from a central location.

Aruba devices can be configured in a master-slave relationship, where a single controller or pair of controllers acts as a network management system for all controllers and APs in the network. All configuration and monitoring is done from the master controller, which automatically pushes configuration changes to and pulls statistics from other controllers in the network. The integrated management system is an advantage in smaller networks, because no dedicated servers need to be purchased to run a standalone NMS.

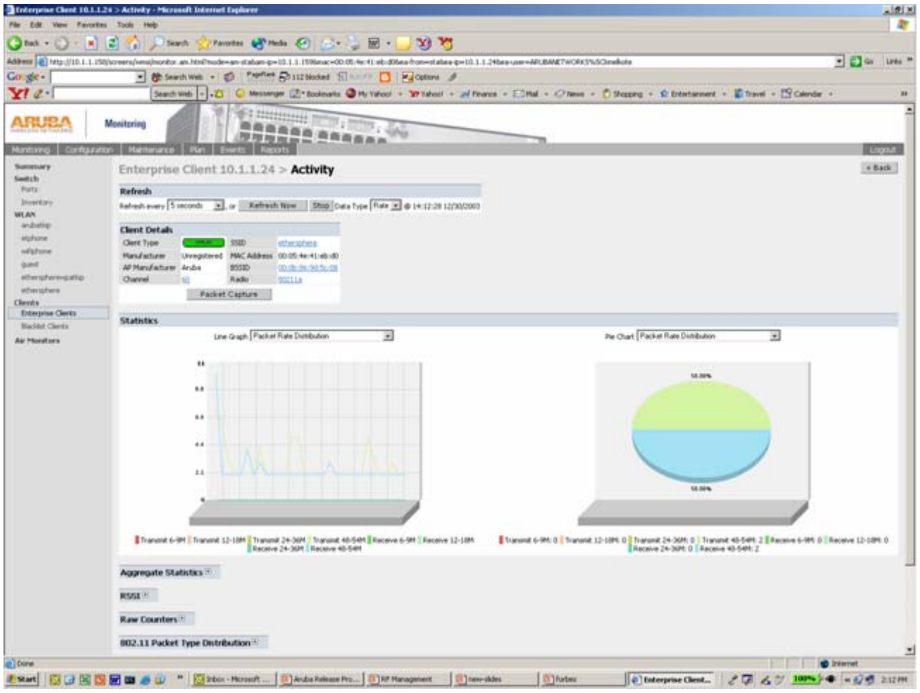
For larger networks, or in networks where extensive logging and reporting is not available through an existing network management system, Aruba offers its Mobility Management System (MMS), a stand-alone network management product that runs either as an appliance or on a customer's own PC-based hardware. This system supports hundreds of switches and contains all the same capabilities of the integrated NMS, with the added benefit of hard disk storage for long-term log and report archiving.

The Aruba Mobility Management System provides a comprehensive suite of applications for planning, monitoring, fault management, reporting, RF coverage and location visualization for the Mobile Edge of enterprise networks. The client centric management model allows IT administrators to rapidly scope and visualize all objects related to any given network user in real time and serves as a key differentiator of the Mobility Management System.


SSL
API
Mobility Management System
3rd Party Network Management, Location Services, etc.
Centralized Mobility Controllers
LAN / WAN / INTERNET
Campus
Mobile Office
Branch Office/ Retail
Home Office

Client Troubleshooting

Aruba includes the unique ability to monitor any combination of L1-L4 parameters for any client on the network. Statistics may be displayed and graphed, as shown in the figure below, for such parameters as bandwidth utilization, packet size breakdown, retransmit frame rate, interference, signal strength, transmit/receive rate, and a host of others. Often, analysis of this display is sufficient to determine the cause of a client issue.



Enterprise Client 10.1.1.24 > **Activity**

Refresh

Refresh every 5 seconds, or Data Type Rate @ 14:12:28 12/30/2003

Client Details

Client Type	[illegible]	SSID	ethersphere
Manufacturer	Unregistered	MAC Address	00:05:4e:41:eb:d0
AP Manufacturer	Aruba	BSSID	[illegible]
Channel	[illegible]	Radio	802.11a

Statistics

Line Graph: Packet Rate Distribution

Pie Chart: Packet Rate Distribution

Transmit 6-9M: 0 Transmit 12-18M: 0 Transmit 24-36M: 0 Transmit 48-54M: 2 Receive 6-9M: 0 Receive 12-18M: 0 Receive 24-36M: 0 Receive 48-54M: 2

When statistical analysis is not sufficient to troubleshoot a client problem, Aruba offers integrated packet capture ability. An 802.11-level packet capture, with full wireless headers, can be done from any Aruba AP with results sent back to a central console for analysis. This means that a network administrator never has to leave his or her desk to troubleshoot wireless problems. This can be particularly important in campus environments, where long distances may be involved, and in healthcare, where IT staff may not have ready access to all areas of a building. One Aruba healthcare customer commented, "The fact that I don't have to send staff with handheld wireless sniffers into a live trauma center anymore is huge for us."

Advanced Services

The Aruba Mobile Edge Architecture enables a number of current and future advanced services. Today, location-based services are popular for wireless LANs. Using Aruba's location-based service, the physical location of any 802.11 radio can be tracked, recorded, and plotted on a map of a building or campus. One Aruba customer – a large sports arena – uses this capability to locate mobile assets such as golf carts and plasma televisions on wheels within a large area. The arena deployed an Aruba WLAN system primarily for a mobile point-of-sale application for concessions, but found they could use the same infrastructure for location-based services. The arena uses asset tracking tags from PanGo – an Aruba partner – to track valuable equipment as it moves around the arena. In an effort to standardize location-based services, Aruba has submitted a proposal to the IEEE 802.11 Task Group V that was unanimously approved by the group. This proposal would standardize how Wi-Fi asset tags communicate with wireless infrastructure equipment. To get location information back out of the Aruba system, Aruba provides a location API built into each mobility controller. Unlike competing vendors who sell separate location appliances, Aruba also provides the location API as a standard feature on the Mobility Management System.

Distribution Model and Partnerships

Aruba approaches the worldwide market with a combination of direct sales, OEM, reseller and service partnerships, and VAR relationships. Within North America, Aruba uses a mixture of all of these, though a significant majority of sales come via channels. Internationally, the company sells exclusively through channel partners. This model holds true for large as well as small-medium enterprises.

Aruba has worldwide strategic OEM, reseller and service partnerships with Alcatel, AT&T, IBM Corporation, Hewlett-Packard Corporation and NCR Corporation. Additionally, Aruba has a large network of domestic and international local and regional value-added resellers.

Our objective is to identify a limited number of value-add partners focused on enterprise mobility, and assist them in profitably growing their business.

The VAR relationships are carefully managed to avoid conflict. The program is structured to foster a collaborative environment; Aruba's direct sales team is the same group that supports the channel. This cooperative approach ultimately benefits the customer.

The Aruba Partner Program has three levels of partnership – Solution Provider, Enterprise Solution Provider, and Strategic Solution Provider – aimed at different customer sizes and segments. Aruba Partners receive access to inside sales and field resources, joint marketing funds, partner website access, sales tools, training tools, demo equipment discount, and deal registration.

Aruba also offers a formal support certification program focused on the requisite technologies essential to building and deploying secure enterprise-class 802.11 wireless LAN environments. Through a combination of written and practical (lab) exams, candidates can achieve certification as an either an Aruba Certified Associate (ACA) or Aruba Certified Expert (ACE) - credentials that signify mastery of the skills necessary to deploy and manage the most advanced wireless LAN networks in the world.

Cost

Aruba Networks' North American list price for key products is as follows:

- Access Points: Range from $195 to $595 depending on model
- Mobility Controllers: Starting prices from $1,795 to 17,995, including including ArubaOS and RF management, depending on model and capacity
- Mobility Management System Software: from $3,995
- Support Pricing: Lists at 14% of list for systems and software and 4% of list for APs