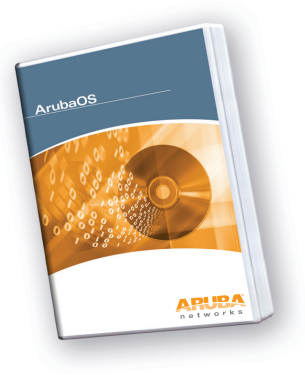
ARUBAOS OPERATING SYSTEM SOFTWARE

Designed for Scalable Performance



ArubaOS® is the operating system and application engine for all Aruba Mobility Controllers and wireless LAN (WLAN) access devices. The software architecture of ArubaOS is designed for scalable performance, and is built using three core components.

First, a hardened, multicore, multithreaded supervisory kernel manages administration, authentication, logging and other system operation functions. Second, an embedded real-time operating system powers dedicated packet-processing hardware, implementing all routing, switching and firewall functions. Third, a programmable encryption/decryption engine built on dedicated hardware delivers client-to-core encryption for wireless user data traffic and software VPN clients.

ArubaOS comes with an extensive set of capabilities. Aruba's Adaptive Radio Management (ARM) technology employs infrastructure-based controls to optimize Wi-Fi client behavior and automatically ensures that Aruba access points (APs) stay clear of interference, resulting in a more reliable, higher performance WLAN infrastructure.

To protect wired network resources from wireless threats, ArubaOS delivers the industry's leading integrated rogue AP classification and containment solution.

Optional software modules are also available for added functionality and are enabled through license keys. Optional modules include the Aruba Policy Enforcement Firewall (PEF), RFProtect™ wireless security and spectrum analysis capabilities, Advanced Cryptography for military-grade Suite B encryption and xSec advanced Layer 2 encryption. Aruba's Virtual Intranet Access (VIA) software client enables secure IPSec VPN connectivity back to corporate resources for road-warriors when they are away from the office.

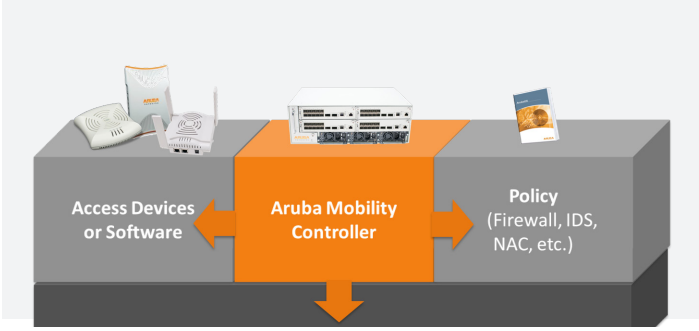
ENABLING A UNIFIED ACCESS ARCHITECTURE

Access layer networks of the past fifteen years were not built for the mobility and security requirements of today's distributed enterprises. Traditionally, networks were built with a focus on Ethernet ports and physical locations, rather than the user or device connecting to the network. Consequently, the addition of secure mobility to such networks becomes overly complex and costly, often requiring large-scale equipment upgrades.

Aruba's Mobile Virtual Enterprise (MOVE) architecture allows any user, regardless of physical location, whether wired or wireless, to securely access the enterprise network with an always-on, consistent experience. Uniform security and access control policies are applied to users in headquarters, branch offices, home offices, or on the road. Users and devices join the enterprise network through simple lightweight access devices or software, which securely and automatically connect to an Aruba Mobility Controller installed in the enterprise network core. The Mobility Controller, powered by ArubaOS, directly controls Aruba access devices and access software, managing their software image, configuration, user connection state, and policy enforcement. The entire network is managed by Aruba AirWave®, which provides IT staff with unmatched visibility and control of network users and infrastructure.

FLEXIBLE AND ADAPTABLE ARCHITECTURE

Network design with Aruba is not a "one size fits all" approach. Some organizations need pervasive Wi-Fi, while some are purely wired. Branch offices have different requirements than corporate headquarters. And even within a corporate campus, some organizations value a centralized traffic forwarding model where all network traffic flows to the data center, while other organizations need a more distributed approach. The unparalleled flexibility enabled by ArubaOS permits all these permutations and more, adapting the network to the requirements of the organization rather than dictating rigid design specifications.



Unified Access Architecture

ARUBA networks

User Connectivity Method	• Enterprise-grade secure Wi-Fi • Wired Ethernet • VPN remote access
Access Point Connection Method	• Private or public IP cloud - Ethernet - Wireless WAN (EVDO, HSDPA, etc.) • Wi-Fi mesh (point-to-point or point-to-multipoint)
Traffic Forwarding	• Centralized – All user traffic flows to Mobility Controller • Locally bridged – All user traffic bridged by access device to local LAN segment • Policy-routed – User traffic selectively forwarded to Mobility Controller or bridged locally, depending on traffic type/policy
Wi-Fi Encryption	• Centralized – All user traffic encrypted between client device and Mobility Controller • Distributed – User traffic encrypted between client device and access point • Open – No encryption
Integration with Existing Networks	• L2 or L3 integration – Mobility Controllers can switch or route traffic on a per-VLAN basis • Rapid Spanning Tree – enables fast L2 convergence • OSPF – enables simple integration with existing routing topologies

ENTERPRISE SECURITY FRAMEWORK

To secure the enterprise network, ArubaOS performs authentication, access control, and encryption for users and devices. Network authentication delivers greater access security, but retrofitting authentication onto existing wired networks is often extremely complex and expensive. In Aruba's MOVE architecture, authentication is a standard component and can be implemented for both wired and wireless networks. For wired networks, 802.1X is the industry-standard method of authentication. For wireless networks, 802.1X authentication is one component of the WPA2 and 802.11i protocols widely recognized as state-of-the-art for wireless security.

ArubaOS uniquely supports AAA FastConnect, which allows the encrypted portions of 802.1X authentication exchanges to be terminated on the controller where Aruba's hardware encryption engine dramatically increases scalability and performance. Supporting PEAP-MSCHAPv2, PEAP-GTC, and EAP-TLS, AAA FastConnect removes the requirement for external authentication servers to be 802.1X-capable and increases authentication server scalability by permitting hundreds of authentication requests per second.

For clients without WPA, VPN, or other security software, Aruba supports a Web-based captive portal that provides secure browser-based authentication. Captive portal authentication is encrypted using Secure Sockets Layer (SSL), and can support both registered users with a login and password or guest users who supply only an email address.

The optional ArubaOS Policy Enforcement Firewall (PEF) license may be added for enhanced user-centric security. Without the PEF license, a user or device may be mapped to a particular VLAN based on the port or wireless SSID from which a user connects to the network. Once the user has been mapped to a particular VLAN, external firewall systems or routers are typically used to provide basic access controls. PEF enhances access security by adding full identity-based security with integrated firewall controls applied on a per-user basis. This allows ArubaOS to create a security perimeter around each user or device, tightly controlling how that user or device may access enterprise network resources.

Governments and other organizations that require additional security may add the optional ArubaOS Advanced Cryptography (ACR) module. ACR brings military-grade Suite B cryptography to Aruba Mobility Controllers, enabling user mobility and secure access to networks that handle classified information. Approved by the U.S. National Security Agency (NSA), Suite B improves performance, eliminates unwieldy workflows and strict handling requirements, allows interoperability, and supports commercially available devices — all at a fraction of the cost of previous-generation cryptographic methods.

Authentication Types	• IEEE 802.1X (EAP, LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, EAP-POTP, EAP-GTC, EAP-TLV, EAP-AKA, EAP-Experimental, EAP-MD5) • RFC 2548 Microsoft Vendor-Specific RADIUS Attributes • RFC 2716 PPP EAP-TLS • RFC 2865 RADIUS Authentication • RFC 3579 RADIUS Support for EAP • RFC 3580 IEEE 802.1X RADIUS Guidelines • RFC 3748 Extensible Authentication Protocol • MAC Address authentication • Web-based captive portal authentication
Authentication Servers	• Internal database • LDAP/ SSL Secure LDAP • RADIUS • TACACS+ • Authentication Server Tested Interoperability: Microsoft Active Directory, Microsoft IAS RADIUS Server, Microsoft NPS RADIUS Server, Cisco ACS Server, Juniper/ Funk Steel Belted RADIUS Server, RSA ACEserver, Infoblox, Interlink RADIUS Server, FreeRADIUS
Encryption Protocols	• CCMP/AES • WEP: 64 and 128 bit • TKIP • Secure Sockets Layer (SSL) and TLS: RC4 128-bit and RSA 1024- and 2048-bit • L2TP/IPsec (RFC 3193) • XAUTH/IPsec • PPTP (RFC 2637)
Programmable Encryption Engine	Yes – permits future encryption standards to be supported through software updates
Web-based Captive Portal (SSL)	Yes
Integrated Guest Access Management	Yes
Site-to-Site VPN	Yes – IPsec tunnel establishment between Mobility Controllers and other IPsec-compliant devices. Authentication support for X.509 PKI, IKEv2, IKE PSK, IKE aggressive mode.

AN ARCHITECTURE FOR SEAMLESS MOBILITY

Enterprise users increasingly require network access while moving from location to location, whether from a classroom to a library, a cubicle to a conference room, from headquarters to a branch office, or from the office to a user's home. Mobility should be a seamless experience for the user, whether it is Wi-Fi roaming without loss of voice sessions or roaming from the office to home with no change in logon procedures or access experience. When the access network is unified under Aruba's MOVE architecture, users experience consistent network services that "just work."

For Wi-Fi networks, ArubaOS provides seamless connectivity as users move throughout the network. With roaming handoff times of 2-3 milliseconds, delay-sensitive and persistent applications such as voice and video experience uninterrupted performance. ArubaOS integrates proxy Mobile IP and proxy DHCP functions letting users roam between subnets, ports, APs, and controllers without special client software. And with VLAN pooling, user membership of VLANs is load-balanced to maintain optimal network performance as large groups of users move about the network.

Aruba's unified access architecture also extends the enterprise to remote locations, over private WANs or using the public Internet, giving users the same access experience regardless of location. And to address users who are away from enterprise network infrastructure, Aruba Mobility Controllers also operate as standard VPN concentrators, linking remote users into the same access and security framework as other enterprise users. With Aruba, there is no longer any need to build separate access networks for each work location – a unified access architecture treats all locations the same.

Fast Roaming	2-3 msec intra-controller 10-15 msec inter-controller
Roaming Across Subnets and VLANs	Sessions do not drop as clients roam throughout the network
Proxy Mobile IP	Establishes home agent/foreign agent relationship between controllers automatically
Proxy DHCP	Prevents clients from changing IP address when roaming
VLAN Pooling	Load balances clients across multiple available VLANs automatically

ENTERPRISE-GRADE ADAPTIVE WIRELESS LANS

Aruba's ARM technology takes the guesswork out of AP deployments. Once APs are brought up, they immediately begin monitoring their local environment for interference, noise, and signals being received from other Aruba APs. This information is reported back to the controller, which is then able to control the optimal channel assignment and power levels for each AP in the network – even where 802.11n has been deployed with mixed HT20 and HT40 channel types.

Advanced ARM features dynamically adapt the infrastructure to ensure optimal network performance in today's challenging heterogeneous client environments. With 802.11n in widespread use, users have an expectation of high performance, even in crowded areas such as lecture halls. ARM ensures high performance and multi-media QoS through techniques such as band steering, which moves dual-band clients out of the crowded 2.4 GHz band, and Airtime Performance Protection, which prevents slower clients from bringing down performance of the entire network. Where dense user populations exist, ARM's Airtime Fairness provides equal RF access across multiple client types and across multiple client operating systems. Finally, in areas with dense AP coverage, ARM ensures the optimal use of each channel through automatic channel load balancing and co-channel interference mitigation.

ARM can be used in conjunction with the optional Aruba RFProtect™ module spectrum analyzer. While ARM optimizes client behavior and ensures that APs stay clear of interference, the spectrum analyzer utilizes Aruba 802.11n APs to remotely identify and classify Wi-Fi and non-Wi-Fi sources of interference.

Using Aruba 802.11n APs to scan the spectral composition of 2.4-GHz and 5-GHz radio bands, the Aruba RFProtect spectrum analyzer remotely identifies RF interference, classifies its source and provides real-time analysis at the point of the problem.

Data collected by the Aruba RFProtect spectrum analyzer is used to quickly isolate packet transmission problems, ensure over-the-air QoS and mitigate traffic congestion caused by RF contention with other devices operating in the same band or channel. Appropriate remediation measures can then be put in place to optimize network performance.

Once the network is deployed, the Aruba system provides a real-time, color "heatmap" display of the RF environment showing signal strength, coverage and interference. Through tight integration with AirWave VisualRF, WLAN coverage and capacity planning can be automated, precluding the need for frequent and expensive manual site surveys.

ArubaOS collects aggregate and raw wireless statistics on a per station, per channel and per user basis. All statistics can be recorded and analyzed through AirWave, and are also available via SNMP for easy integration into third-party management or analysis applications. Live packet capture is available that can turn any Aruba AP or Air Monitor into a packet capture device, able to stream real-time 802.11 frames back to monitoring stations such as WireShark or WildPackets OmniPeek. With this detailed information, administrators can quickly troubleshoot user problems, determine top wireless talkers and diagnose congested APs.

To protect against unsanctioned wireless devices, Aruba's rogue AP classification algorithms allow the system to accurately differentiate between threatening rogue APs connected to the network and nearby interfering APs.

Once classified as rogue, these APs can be automatically disabled through the wireless and wired network. Administrators are also notified of the presence of rogue devices, along with their precise physical location on a floorplan, so they can be promptly removed from the network. Rogue AP classification and containment is available within base ArubaOS and does not require additional Mobility Controller licensing.

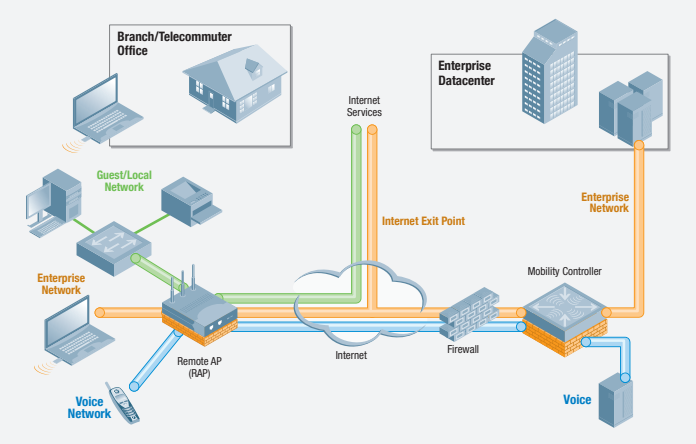
For comprehensive wireless intrusion protection (WIP), the RFProtect module for Aruba Mobility Controllers enables protection against ad hoc networks, man-in-the-middle attacks, denial-of-service (DoS) attacks and many other threats, while enabling wireless intrusion signature detection.

TotalWatch™, an essential part of the RFProtect WIP capability, delivers the industry's most effective WLAN threat mitigation. It provides visibility into all 802.11 Wi-Fi frequencies at 5-MHz increments, including in between channels, monitors the 4.9-GHz frequency band and automatically adapts wireless security scanning intervals on APs based on data availability.

Tarpit containment is another vital RFProtect WIP feature. With tarpit containment, Aruba APs respond to probe requests from rogue devices with fake BSSIDs or channels. The rogue device then associates with that fake info and fails to push any traffic. User interaction is then required to get the rogue device connected again.

ArubaOS includes advanced location visualization and tracking of 802.11 devices. RF signature-based location triangulation allows administrators to physically locate any 802.11 user or device within one meter of accuracy. With Aruba's real time location tracking (RTLS) capabilities, multiple devices can be continuously located and tracked simultaneously. The location of devices can be displayed on building floorplans to network administrators through the AirWave Management Platform, or linked to outside systems through a simple application programming interface (API).

Adaptive Radio Management (ARM)	Automatically manages all RF parameters to achieve maximum performance
802.11n HT20 and HT40 Support	Manages spectrum for all 802.11n networks
Client Band Steering	Keeps dual-band clients on optimal RF band
Self-Healing Around Failed APs	Automatically adjusts power levels to compensate for failed APs
Airtime Fairness	Guarantees performance in high-density environments
RF-Spectrum Load Balancing	Evenly distributes clients across all available channels
Airtime Performance Protection	Prevents low-speed clients from slowing down high-speed clients
Single-Channel Coordinated Access	Ensures optimal performance even with nearby APs on the same channel
RF Plan	Automatic pre-deployment modeling, planning and placement of APs and RF monitors based on capacity, coverage and security requirements
Coverage Hole and Interference Detection	Detects clients that cannot associate due to coverage gaps
Timer-Based AP Access Control	Shuts off APs outside of defined operating hours
Remote Wireless Packet Capture	Remotely captures raw 802.11 frames and streams to protocol analyzer
Plug-Ins for Third-Party Analysis Tools	WireShark, OmniPeek, Air Magnet
Rogue AP Detection and Containment	Detects unauthorized access points and automatically shuts them down
Real-Time Location Tracking and Monitoring	Yes
Location Tracking API for External Integration	Yes



Aruba RAPs are ideally suited for providing secure mobile connectivity to branch and home offices.

REMOTE NETWORKING FOR BRANCH OFFICES AND TELEWORKERS

Aruba's remote networking solutions provide a simple, secure, and cost-effective way to extend the corporate network to branch offices, clinics, SOHOs, stores and telecommuters. Traditional remote networking solutions replicate routing, switching, firewall, and other services at each remote location. Managing and controlling user access to network services, applications, and resources requires proliferating ports, subnets, and VLANs – effectively creating multiple networks at each site. This is costly and complex to deploy and maintain.

Whether supporting branch offices of one or one hundred users, Aruba's remote networking solution delivers full-service networking without compromises. As the head-end component of the remote networking solution, data center-based Aruba Mobility Controllers handle all complex configuration, management, software updates, authentication, intrusion detection, and remote site termination tasks. Branch office network services are virtualized in the data center controllers and then extended over any public or private IP network to affordable Remote Access Points (RAPs) that provide secure connectivity and services to end users.

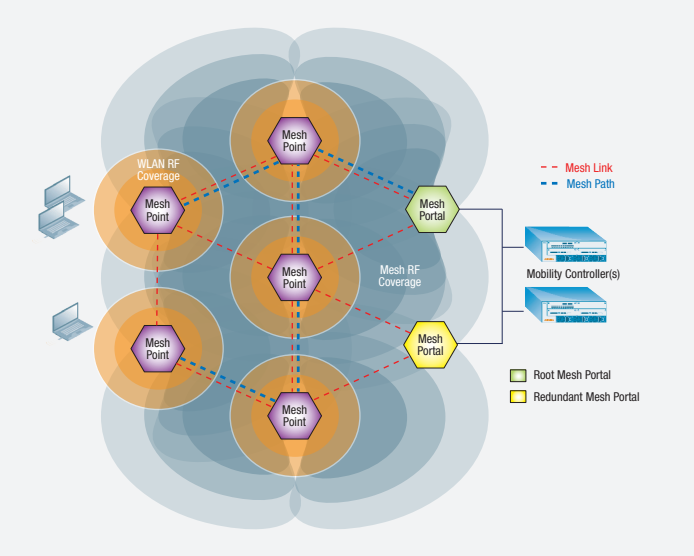
Zero-Touch Provisioning	Administrators can deploy RAPs without any pre-configuration. Simply ship it to the end user (RAP-2, RAP-5 series only)
Wired and Wireless	Users connect to RAPs via wired Ethernet, Wi-Fi, or both
Flexible Authentication	802.1X, Captive Portal, MAC address authentication per-port and per-user
Centralized Management	No local configuration is performed on APs – all configuration and management done by Mobility Controller
3G WWAN	RAP-5 series support USB wireless WAN adapters (EV-DO, HSDPA, etc.) for primary or backup Internet connection
FlexForward Traffic Forwarding	• Centralized – All user traffic flows to Mobility Controller • Locally bridged – All user traffic bridged by access device to local LAN segment • Policy-routed – User traffic selectively forwarded to Mobility Controller or bridged locally, depending on traffic type/policy (requires PEF license)
Enterprise-Grade Security	RAPs authenticate to to Mobility Controllers using X.509 certificates, then establish secure IPsec tunnels
Uplink Bandwidth Reservation	Defines reserved bandwidth for loss-sensitive application protocols such as voice
Local Diagnostics	In the event of a call to the help desk, local users can browse to a pre-defined URL to access full RAP diagnostics
Remote Mesh Portal	A RAP may also act as a mesh portal, providing wireless links to downstream Aruba access points (except RAP-2WG)
Supported Access Points	RAP-2WG, RAP-5WN, RAP-5, AP-105, AP-120/121, AP-124/125, AP-60/61, AP-65, AP-70, AP-85
Minimum Required Link Speed	64 kbps per SSID
Encryption Protocol (RAP to Mobility Controller)	AES-CBC-256 (inside IPsec ESP)

INTEGRATING ROAD WARRIORS INTO A SINGLE ACCESS ARCHITECTURE

Users who need access to enterprise resources while away from their office typically rely on VPN client software, which connects to a VPN concentrator located in an enterprise DMZ.

With Aruba, remote VPN users are treated just like any other user. They leverage the same access policies and service definitions used on a campus Wi-Fi network or a branch office RAP deployment. Because any Aruba Mobility Controller can act as a VPN concentrator, a parallel access infrastructure need not be deployed or maintained.

ArubaOS is compatible with several popular VPN clients and the VPN clients built into major client operating systems. In addition, ArubaOS also provides the optional Aruba VIA client, which can be installed on iOS, Mac OS X and Windows mobile devices and is ordered via the PEF-V license for the corresponding Aruba Mobility Controller. By merging access networks together, policy and access configuration is unified, the user experience is improved, helpdesk calls are reduced, and IT expenses are lowered.



Tested Client Support	Aruba VIA client on Windows Cisco, Nortel VPN clients OpenVPN, Apple/Windows native client
VPN Protocols	• L2TP/IPsec (RFC 3193) • XAUTH/IPsec • PPTP (RFC 2637)
Authentication	Username/password, X.509 PKI, RSA SecurID, Smart Card, Multi-factor

SECURE ENTERPRISE MESH

Aruba's Secure Enterprise Mesh solution provides a flexible, wire-free design allowing access points to be placed wherever they are needed – indoors and outdoors. The absence of fiber or cable runs significantly reduces network installation costs and requires fewer Ethernet ports. The solution fully integrates with the Aruba unified access architecture, enabling a single, enterprise-wide network wherever users may roam. Aruba's Secure Enterprise Mesh is based on programmable software and does not require specialized hardware; virtually any Aruba indoor or ruggedized outdoor access can function as a mesh access point.

The Aruba Secure Enterprise Mesh can support all enterprise wireless needs including Wi-Fi access, concurrent Wireless Intrusion Protection, wireless backhaul, LAN bridging, and point-to-multipoint connectivity, all with a single common infrastructure. Aruba's Secure Enterprise Mesh is an excellent solution for connectivity applications, including inter-building connectivity, outdoor campus mobility, wire-free offices, and wireline back-up; security applications, such as video and audio monitoring, alarms and duress signals, and industrial applications and sensor networks.

Through cooperative control technology, Aruba's mesh solution uses an intelligent link management algorithm to optimize traffic paths and links. Mesh access points communicate with their neighbors and advertise a number of RF and link attributes (e.g., link cost, path cost, node cost, loading) that allow them to make intelligent selection of the best path to take for the application. Mesh paths and links automatically adjust in the event of high-loads or interference. Further, application tags for voice and video traffic are shared to ensure latency sensitive traffic is prioritized over data. The cooperative control technology also provides self-healing functionality for the mesh network in the event of a blocked path or AP failure.

Broad Application Support	Wi-Fi access, concurrent wireless intrusion protection, wireless backhaul, LAN bridging, and point-to-multipoint connectivity
Unified Access Architecture	Integrates mesh networks with campus WLAN and branch office networks. Users seamlessly roam between campus Wi-Fi and mesh networks.
Cooperative Control	Intelligent RF link management determines optimal performance path and allows the network to self-organize
Self Healing	Resilient self-healing mesh automatically overcomes a block path or AP failure
Mesh Clustering	Supports scalability by allowing a large mesh to be segmented into highly available clusters
Centralized Encryption	Data encrypted end-to-end, from client to core, protecting the network even if a mesh access point is stolen
Centralized Management	All mesh nodes are configured and controlled centrally by Mobility Controllers. No local management required.
Extensive Graphical Support Tools	Full network visualization includes coverage heat maps, automatic link budget calculation, floorplans, and maps with network topology
Standards-Based Design	Secure Enterprise Mesh is designed using principles from draft IEEE 802.11s and will be able to easily migrate to this standard once it is ratified

NETWORK MANAGEMENT AND HIGH-AVAILABILITY

Controller configuration, management, and troubleshooting is provided through a browser-based GUI and a command line interface that will be familiar to any network administrator. ArubaOS also integrates seamlessly with the AirWave® Management Suite which eases management during all stages of the WLAN lifecycle – from planning and deploying to monitoring, analyzing and troubleshooting. AirWave provides long-term trending and analysis, help desk integration tools, and extensive customizable reporting.

All APs and controllers, even those distributed in branch or regional offices, can be centrally configured and managed from a single console. To ease configuration of common tasks, intuitive task-based wizards guide the network administrator through every step of the process.

Controllers can be deployed in 1:1 and 1:n VRRP based redundant configurations with redundant datacenter support. When deployed in Layer-3 topologies, the OSPF routing protocol enables automatic route learning and route distribution for fast convergence.

Web-Based Configuration	Allows any administrator with a standard web browser to manage the system
Command Line	Console, SSH
Syslog	Yes – supports multiple servers, multiple levels, and multiple facilities
SNMP v2c	Yes
SNMP v3	Yes – enhances standard SNMP with cryptographic security
Centralized Configuration of Controllers	A designated "master" controller can configure and manage several downstream "local" controllers
VRRP	Supports high availability between multiple controllers
Redundant Data Center Support	Yes – Access devices can be configured with IP addresses for backup controllers
OSPF	Yes – Stub mode support for learning default route or injecting local routes into an upstream router
Rapid Spanning Tree Protocol	Yes – Provides fast L2 convergence

ARUBAOS SUPPORT FOR IPV6

With the depletion of available IPv4 addresses, organizations are now planning for or have already begun deployments of IPv6 within their networks. While IPv4 and IPv6 both define how data is transmitted over networks, IPv6 adds a much larger address space than IPv4 and can support billions of unique IP addresses.

As organizations transition from IPv4 to IPv6, network equipment must support dual-stack interoperability of IPv6 within an IPv4 network or full deployments within a pure IPv6 environment. ArubaOS supports deploying Aruba Mobility Controllers and Access Points (APs) in today's IPv6 and dual-stack environments.

MANAGEMENT OVER IPV6

- SSH
- Telnet
- SCP
- WebUI
- FTP
- TFTP
- Syslog

Captive Portal over IPv6	Yes
Support IPv6 VLAN Interface Address on Mobility Controller	Yes
Support AP-Controller Communication over IPv6	Yes
ICSA IPv6 Certified Firewall	Yes
USGv6 Certified Firewall	Yes

CONTEXT AWARE CONTROLS FOR MISSION-CRITICAL NETWORKING

Support for 802.11e and Wi-Fi Multimedia (WMM) ensures wireless QoS for delay-sensitive applications with mapping between WMM tags and internal hardware queues. Mobility Controllers enable mapping of 802.1p and IP DiffServ tags to hardware queues for wired-side QoS and can be instructed to apply certain 802.1p and IP DiffServ tags to different applications on demand.

With the addition of the Aruba PEF module, voice-over-IP protocols – including SIP, SVP, Alcatel NOE, Vocera and SCCP – are followed within the Aruba Mobility Controller. Aruba's Application Fingerprinting technology enables Mobility Controllers to follow encrypted signaling protocols.

Once these streams are identified, Aruba WLANs can prioritize them for delivery on the wireless channel as well as trigger voice-related features such as postpone ARM scanning for the duration of a call and prioritize roaming for clients that are engaged in an active call. These capabilities are critical to enabling the large-scale deployment of enterprise voice communications over Wi-Fi.

Additionally, ArubaOS now includes Device Fingerprinting technology, allowing network administrators to assign network policies on device types in addition to applications and users. Device Fingerprinting delivers greater control over which devices are allowed to access the network and how these devices can be used. ArubaOS can accurately identify and classify mobile devices such as the Apple iPad, iPhone, or iPod as well as devices running the Android or BlackBerry operating systems. This information can be shared with the AirWave Management Platform for enhanced network visibility for all network users, regardless of location or mobile device.

802.1p Support	Yes
802.11e Support	Yes
T-SPEC/TCLAS	Yes
WMM	Yes
WMM Priority Mapping	Yes
U-APSD (Unscheduled Automatic Power Save Delivery)	Yes
802.11k	Improves call quality and rapid handoff for voice and other quality-sensitive devices
IGMP Snooping for Efficient Multicast Delivery	Yes
Application and Device Fingerprinting	Yes

CERTIFICATIONS

- Wi-Fi Alliance Certified (802.11a/b/g/n/d/h, WPA™ Personal, WPA™ Enterprise, WPA2™ Personal, WPA2™ Enterprise, WMM™, WMM Power Save)
- ICSA Firewall, Corporate v4.1 (with optional Policy Enforcement Firewall module), ICSA IPv6 Firewall
- FIPS 140-2 Validated (when operated in FIPS mode)
- Common Criteria EAL-2
- RSA Certified
- Polycom/Spectralink VIEW Certified
- USGv6 Firewall

STANDARDS SUPPORTED

General Switching and Routing

- RFC 1812 Requirements for IP Version 4 Routers
- RFC 1519 CIDR
- RFC 1256 IPv4 ICMP Router Discovery (IRDP)
- RFC 1122 Host Requirements
- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 894 IP over Ethernet
- RFC 1027 Proxy ARP
- RFC 2236 IGMPv2
- RFC 2328 OSPFv2
- RFC 2338 VRRP
- RFC 2460 Internet Protocol version 6 (IPv6)
- RFC 2516 Point-to-Point Protocol over Ethernet (PPPoE)
- RFC 3220 IP Mobility Support for IPv4 (partial support)
- RFC 4541 IGMP and MLD Snooping
- IEEE 802.1D-2004 – MAC Bridges
- IEEE 802.1Q – 1998 Virtual Bridged Local Area Networks
- IEEE 802.1w – Rapid Spanning Tree Protocol

Quality of Service and Policies

- IEEE 802.1D – 2004 (802.1p) Packet Priority
- IEEE 802.11e – Quality of Service Enhancements
- RFC 2474 Differentiated Services

Wireless

- IEEE 802.11a/b/g 5 GHz, 2.4 GHz
- IEEE 802.11d Additional Regulatory Domains
- IEEE 802.11e Quality of Service
- IEEE 802.11h Spectrum and TX Power Extensions for 5 GHz in Europe
- IEEE 802.11i MAC Security Enhancements
- IEEE 802.11k Radio Resource Management (partial support)
- IEEE 802.11n Enhancements for Higher Throughput
- IEEE 802.11v Wireless Network Management (partial support)

Management and Traffic Analysis

- RFC 2030 SNTP, Simple Network Time Protocol v4
- RFC 854 Telnet client and server
- RFC 783 TFTP Protocol (revision 2)
- RFC 951,1542 BootP
- RFC 2131 Dynamic Host Configuration Protocol
- RFC 1591 DNS (client operation)
- RFC 1155 Structure of Mgmt Information (SMIv1)
- RFC 1157 SNMPv1
- RFC 1212 Concise MIB definitions.
- RFC 1213 Management Information Base for Network Management of TCP/IP-based internets - MIB-II
- RFC 1215 Convention for defining traps for use with the SNMP
- RFC 1286 Bridge MIB
- RFC 3414 User-based Security Model (USM) for v.3 of the Simple Network Management
- RFC 1573 Evolution of Interface
- RFC 2011 SNMPv2 Management Information Base for the Internet Protocol using SMIv2
- RFC 2012 SNMPv2 Management Information
- RFC 2013 SNMPv2 Management Information
- RFC 2578 Structure of Management Information Version 2 (SMIv2)
- RFC 2579 Textual Conventions for SMIv2
- RFC 2863 The Interfaces Group MIB
- RFC 3418 Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
- RFC 959 File Transfer Protocol (FTP)
- RFC 2660 The Secure HyperText Transfer Protocol (HTTPS)
- RFC 1901 1908 SNMP v2c SMIv2 and Revised MIB-II
- RFC 2570, 2575 SNMPv3 user based security, encryption and authentication
- RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3
- RFC 2233 Interface MIB
- RFC 2251 Lightweight Directory Access Protocol (v3)
- RFC 1492 An Access Control Protocol, TACACS+
- RFC 2865 Remote Access Dial In User Service (RADIUS)
- RFC 2866 RADIUS Accounting
- RFC 2869 RADIUS Extensions
- RFC 3576 Dynamic Authorization Extensions to Remote RADIUS
- RFC 3579 RADUIS Support For Extensible Authentication Protocol (EAP)
- RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS)
- RFC 2548 Microsoft RADUIS Attributes
- RFC 1350 The TFTP Protocol (Revision 2)
- RFC 3164 BSD System Logging Protocol (Syslog)
- RFC 2819 Remote Network Monitoring (RMON) MIB

Security/Encryption

- IEEE 802.1X Port-Based Network Access Control
- RFC 1661 The Point-to-Point Protocol (PPP)
- RFC 2406 IP Encapsulating Security Payload (ESP)
- RFC 2661 Layer Two Tunneling Protocol “L2TP”
- RFC 3193 Securing L2TP using IPsec
- RFC 2451 The ESP CBC-Mode Cipher Algorithms
- RFC 2403 The Use of HMAC-MD5-96 within ESP and AH
- RFC 2401 Security Architecture for the Internet Protocol
- RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 The Internet Key Exchange (IKE)
- RFC 2405 ESP DES-CBC cipher algorithm with explicit IV
- RFC 2403 Use of HMAC-SHA1-96 with ESP and AH
- RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPsec
- RFC 4017 Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs
- RFC 3706 A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 3748, 5247 Extensible Authentication Protocol (EAP)
- RFC 3079 Deriving Keys for use with Microsoft Point-to-Point Encryption (MPPE)
- RFC 4137 State Machines for Extensible Authentication Protocol (EAP) Peer and Authenticator
- RFC 2716 PPP EAP TLS Authentication Protocol
- RFC 2246 The TLS Protocol (SSL)
- RFC 2407 Internet IP Security Domain of Interpretation for ISAKMP
- RFC 3948 UDP encapsulation of IPSec packets
- RFC 4793 EAP-POTP
- Internet Draft – draft-ietf-ipsec-nat-t-ike-00
- Internet Draft – draft-ietf-ipsec-nat-t-ike-01
- Internet Draft – draft-ietf-ipsec-nat-t-ike-02
- Internet Draft – EAP-TTLS
- Internet Draft – EAP-PEAPv0
- Internet Draft – XAuth for ISAKMP

ARUBA networks

www.arubanetworks.com

1344 Crossman Avenue. Sunnyvale, CA 94089

1-866-55-ARUBA | Tel. +1 408.227.4500 | Fax. +1 408.227.4550 | info@arubanetworks.com