

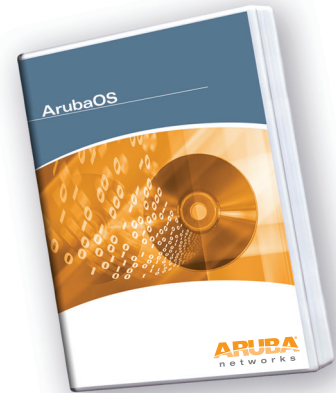


## ARUBAOS OPERATING SOFTWARE

The ArubaOS software suite serves as the operating system and application engine for all Aruba Controllers, enabling Aruba's unique adaptive wireless LAN, identity-based security, branch office networking, remote access, and wireless intrusion prevention services.

The software architecture of ArubaOS is designed for scalable performance, and is built using three core components. First, a hardened, multi-core, multi-threaded supervisory kernel manages administration, authentication, logging, and other overhead functions. Second, an embedded real-time operating system powers dedicated packet processing hardware, implementing all traffic forwarding and firewall functions. Third, a programmable encryption engine manages dedicated encryption/decryption hardware for high-speed crypto performance.

ArubaOS is offered as a base set of capabilities, with an additional series of optional software modules enabled through license keys. Optional modules include Wireless Intrusion Protection, Policy Enforcement Firewall, VPN Server, Remote Access Point, Voice Services Module, Secure Enterprise Outdoor Mesh, and xSec Advanced L2 Encryption.



### SECURE AUTHENTICATION, ENCRYPTION, AND ACCESS CONTROL

- 802.1X authentication with WPA, WPA2 and 802.11i
- AAA FastConnect for hardware-based acceleration and local processing of 802.1X authentication
- Programmable hardware-based centralized encryption engine for client-to-datacenter secured connections
- Web-based Captive Portal for SSL browser-based authentication
- Sophisticated guest access and guest credential management features enable secure guest access with minimal administrative overhead

### SEAMLESS MOBILITY

- User-centric networking manages wired and wireless users as they roam between ports or wireless APs
- Roaming times of 2-3 milliseconds enable ultra-fast handoffs for delay-sensitive applications
- Proxy mobile IP and proxy DHCP allow users to roam seamlessly between APs and controllers

### NETWORK MANAGEMENT AND HIGH-AVAILABILITY

- Seamless integration with the AirWave Wireless Management Suite allows unprecedented control and visibility over the entire network
- Intuitive configuration wizards complete common tasks in just a few mouse clicks
- Redundant controller arrays using VRRP
- Automatic RF fault tolerance avoids radio dead spots and provides AP back-up
- Rapid Spanning Tree for fast L2 convergence
- OSPF routing protocol enables high availability when L3 topologies change

### QOS, VOIP SUPPORT AND LOCATION TRACKING

- 802.11e, WMM and 802.1p support
- Automatic mapping of WMM priorities to 802.1p and IP DSCP
- Location of any 802.11 device with real-time display
- 802.11k support improves call quality and rapid handoff for voice and other quality-sensitive devices

### ENTERPRISE-GRADE WIRELESS LAN

- Dynamic Infrastructure Control with built-in Adaptive Radio Management (ARM)
- Automatic channel and power assignment (includes high-throughput 20MHz (HT20) and 40MHz (HT40) channels.
- Automatic band steering keeps dual-band clients on optimal RF band
- Airtime fairness guarantees performance in high-density environments
- Airtime performance protection prevents low-speed clients from slowing down high-speed clients
- Spectrum load balancing evenly distributes clients across all available channels
- Coordinated Access ensures optimal performance of nearby APs on the same channel
- RF-Live for real-time monitoring and display of RF coverage and interference
- Automatic pre-deployment modeling, planning and placement of APs and RF monitors based on capacity, coverage and security requirements
- Live packet capture tools provide detailed records of entire wireless environment
- Secure indoor wireless mesh connects access points without wires
- Automatic detection, classification, and containment of rogue access points

# ARUBAOS OPERATING SOFTWARE

## SECURE AUTHENTICATION, ENCRYPTION, AND ACCESS CONTROL

ArubaOS delivers industry-leading capabilities for securing devices, users and data on the enterprise network. A wide range of authentication methods are supported, including the industry-standard WPA2 and 802.11i protocols widely recognized as state-of-the-art for wireless security. ArubaOS provides the latest Layer 2 encryption technologies, and with its programmable hardware encryption processor the controller can be upgraded to support emerging encryption standards.

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. Supported for 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 several hundreds of authentication requests per second to be processed.

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 SSL (Secure Sockets Layer), and can support both registered users with a login and password or guest users who supply only an email address. Through Aruba's integrated GuestConnect system, front-desk reception staff can use a customized web portal page to issue and track authentication credentials for visitors. GuestConnect can also be extended to any user in an enterprise directory system, letting guest sponsors directly request network access credentials. Guest credentials can be printed, emailed, or sent to mobile phones through an SMS gateway.

## SEAMLESS MOBILITY

ArubaOS provides seamless connectivity as users move throughout the network. With roaming cutover 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. Aruba's mobility capabilities work with all third-party access points. 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.

## 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 Wireless Management Suite (AWMS) which eases management during all stages of the WLAN lifecycle – from planning and deploying to monitoring, analyzing and troubleshooting. AWMS 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.

## QOS, VOIP SUPPORT AND LOCATION TRACKING

Support for 802.11e and WMM ensures wireless QoS for delay-sensitive applications with mapping between WMM tags and internal hardware queues. Controllers also support mapping of 802.1p and IP DiffServ tags to hardware queues for wired-side QoS. Layer-2 QoS capabilities are easily enhanced to Layer-3+ flow management and DiffServ using the add-on Policy Enforcement Firewall module.

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 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 web-based GUI, or using the add-on External Services Interface, linked to outside systems through a simple application programming interface (API).

## ENTERPRISE-GRADE WIRELESS LAN

Aruba's Adaptive Radio Management (ARM) 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 perform dynamic infrastructure control to ensure 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 performance through techniques such as band steering (which moves dual-band clients out of the crowded 2.4GHz 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.

Once the network is deployed, Aruba's RF-Live feature provides a real-time, color display of the RF environment showing signal strength, coverage and interference. RF-Live enables WLAN coverage and capacity planning, and precludes 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 the AirWave Wireless Management Suite, 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 installed on the local network and nearby "interfering" APs. Once classified as rogue, these APs can be automatically disabled through both the wireless and wired networks. Administrators are also notified of the presence of rogue devices, along with their precise physical location on a floorplan, so that they may be removed from the network.

# ARUBAOS OPERATING SOFTWARE

## TECHNICAL SPECIFICATIONS

### SECURE AUTHENTICATION, ENCRYPTION, AND ACCESS CONTROL

Authentication types	<ul style="list-style-type: none"> <li>• IEEE 802.1X (EAP, LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, EAP-POTP, EAP-GTC, EAP-TLV, EAP-AKA, ZLXEAP, EAP-Experimental, EAP-MD5)</li> <li>• RFC 2548 Microsoft Vendor-Specific RADIUS Attributes</li> <li>• RFC 2716 PPP EAP-TLS</li> <li>• RFC 2865 RADIUS Authentication</li> <li>• RFC 3579 RADIUS Support for EAP</li> <li>• RFC 3580 IEEE 802.1X RADIUS Guidelines</li> <li>• RFC 3748 Extensible Authentication Protocol</li> <li>• MAC Address authentication</li> <li>• Web-based captive portal authentication</li> </ul>
Authentication servers	<ul style="list-style-type: none"> <li>• Internal database</li> <li>• LDAP/ SSL Secure LDAP</li> <li>• RADIUS</li> <li>• TACACS+</li> <li>• Third party Authentication Servers Tested Interoperability: Microsoft Active Directory, Microsoft IAS RADIUS Server, Microsoft NPS RADIUS Server, Cisco ACS Server, Funk Steel Belted RADIUS Server, RSA ACEserver, Infoblox, Interlink RADIUS Server, FreeRADIUS, A-10 Networks IDSentire</li> </ul>
Encryption types	<ul style="list-style-type: none"> <li>• WEP: 64 and 128 bit</li> <li>• WPA-TKIP, WPA-PSK-TKIP, WPA-AES, WPA-PSK-AES</li> <li>• WPA2/802.11i: WPA2-AES, WPA2-PSK-AES, WPA2-TKIP, WPA2-PSK-TKIP, WPA2-Mixed Mode</li> <li>• Secure Sockets Layer (SSL) and TLS: RC4 128-bit and RSA 1024- and 2048-bit</li> <li>• Programmable hardware upgradeable to new encryption mechanisms</li> </ul>
Rogue AP detection	Yes
Rogue AP classification	Yes
Rogue AP containment	Wired and wireless

### SEAMLESS MOBILITY

Fast roaming	2-3 msec intra-switch 10-15 msec inter-switch
Roaming across Subnets and VLANs	Yes
Mobile IP support	Yes
Proxy Mobile IP	Yes
Proxy DHCP	Yes
VLAN Pooling	Yes

### RF MANAGEMENT, PLANNING AND TROUBLESHOOTING

Adaptive Radio Management (ARM)	Yes
Multiple ESSIDs per AP	Yes
Automatic AP calibration	Yes
Self-healing around failed APs	Yes
Load balancing based on number of users	Yes
Load balancing based on utilization	Yes
Coverage hole and interference detection	Yes
Timer-based AP access control	Yes
RF Planning and Deployment Tool	Yes
Wireless RMON/ packet capture	Yes
Plug-ins for third-party analysis tools	WireShark, OmniPeek, Air Magnet
802.11h 5 GHz extensions for Europe	Yes
802.11d additional regulatory domains	Yes

### NETWORK MANAGEMENT AND HIGH AVAILABILITY

Web-based Configuration	Yes
Command Line	Console, telnet, SSH
Syslog	Yes
SNMP v2c	Yes
SNMP v3	Yes
Aruba private MIB	Yes
MIB-II	Yes
Centralized configuration of controllers	Yes
VRRP	Yes
Redundant datacenter support	Yes
OSPF	Yes
Rapid Spanning Tree Protocol	Yes

# ARUBAOS OPERATING SOFTWARE

## QUALITY OF SERVICE, VOIP SUPPORT AND LOCATION

802.1p support	Yes
802.11e support	Yes
T-SPEC/TCLAS	Yes
WMM	Yes
U-APSD (Unscheduled Automatic Power Save Delivery)	Yes
IGMP Snooping for efficient multicast delivery	Yes
Real-time location tracking and monitoring	Yes
Location tracking API for external integration	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 Wireless LAN v1.0
ICSA Firewall, Corporate v4.1 (with optional Policy Enforcement Firewall module)
FIPS 140-2 Validated (when operated in FIPS mode)
Common Criteria EAL-2
RSA Certified
Polycom/Spectralink VIEW Certified

## 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 5GHz, 2.4GHz  
IEEE 802.11d Additional Regulatory Domains  
IEEE 802.11e Quality of Service  
IEEE 802.11h Spectrum and TX Power Extensions for 5GHz in Europe  
IEEE 802.11i MAC Security Enhancements  
IEEE 802.11k Radio Resource Management (partial support)  
IEEE 802.11n Draft 2.0 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 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 RADIUS Support For Extensible Authentication Protocol (EAP)  
RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS)  
RFC 2548 Microsoft RADIUS Attributes  
RFC 1350 The TFTP Protocol (Revision 2)  
RFC 3164 BSD System Logging Protocol (Syslog)

## ARUBA OS OPERATING SOFTWARE

### 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 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 3947 Negotiation of NAT-Traversal in the IKE
- 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
- Internet Draft EAP-TTLS
- Internet Draft EAP-PEAPv0
- RFC 4793 EAP-POTP
- Internet Draft XAuth for ISAKMP



[WWW.ARUBANETWORKS.COM](http://WWW.ARUBANETWORKS.COM)

1344 Crossman Avenue, Sunnyvale, CA 94089 | Tel. +1 408.227.4500 | Fax. +1 408.227.4550