DATA SHEET

ARUBAOS

Enhanced network operating system for today's digital workplace

ArubaOS is the network operating system behind our industry-leading wireless solutions. Whether you are deploying wireless across a large campus solution, a mid-sized branch, or supporting remote workers, ArubaOS delivers the seamless connectivity, security, and reliability that your organization requires. It offers controller-based and controller-less options to meet enterprise demands across all types of industries and supports current standards and interoperability for Wi-Fi standards.

SIMPLIFIED DEPLOYMENT

Deploying and provisioning network devices is an important but often time-consuming activity for network administrators. With rapid growth in remote work, onboarding becomes a cumbersome activity to support across several disparate locations. ArubaOS simplifies and automates deployment with the following features:

- **Zero touch provisioning (ZTP):** Network configurations can be implemented and distributed from the Mobility Conductor through zero-touch provisioning (ZTP) to all Mobility Controllers or via Aruba Central in controller-less environments to eliminate the need for IT support on site.
- **Remote Access Points (RAPs):** Any AP can act as a RAP and can be deployed in disparate locations such as small offices/home offices (SOHO) or temporary work sites. RAPs can simply be shipped to the end-user and administrators can deploy them through zero touch provisioning without any local pre-configuration on the APs. Management, configuration and troubleshooting are provided through a browser-based GUI. Learn more about Aruba's Remote Access Solution. See Table 1 and Figure 1.
- **Multi-tenancy Wi-Fi support (MultiZone):** This is ideal for multi-tenancy requirements where multiple organizations are housed in a single office space or for a single organization that requires separate secure networks. MultiZone capabilities can also be used to segment traffic such as IoT or guest traffic within a single tenant for greater security.

KEY FEATURES

- Support for Wi-Fi 6 standards including WPA3, Enhanced Open, uplink MU-MIMO, OFDMA, and Target Wake Time
- Unified wired and wireless access policies with Dynamic Segmentation to provide secure access for users, applications, and devices.
- Live Upgrade and Seamless Failover to ensure business continuity and eliminate unnecessary downtime.
- Channel optimization and client roaming for seamless connectivity and improved user experience.
- SLA-grade application assurance to improve user experience for latency-sensitive voice and video applications.
- Automated deployment with zero touch provisioning to rapidly deploy without IT support.

Remote Access Points Benefits	
Zero-touch provisioning	Administrators can deploy RAPs without any preconfiguration. Simply ship it to the end user.
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 – Configuration and management are done by the Mobility Controller.
4G LTE WAN connection	RAPs support USB cellular LTE modems for primary or backup Internet connectivity.
FlexForward traffic forwarding	• Centralized – all user traffic flows to a 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 Mobility Controllers using X.509 certificates and 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 predefined URL to access full RAP diagnostics.
Remote mesh portal	A RAP may also act as a mesh portal, providing wireless links to downstream APs.
Minimum required link speed	64 kbps per SSID
Encryption protocol (RAP to Mobility Controller)	AES-CBC-256 (inside IPsec ESP)

Table 1: Remote Access Point Benefits

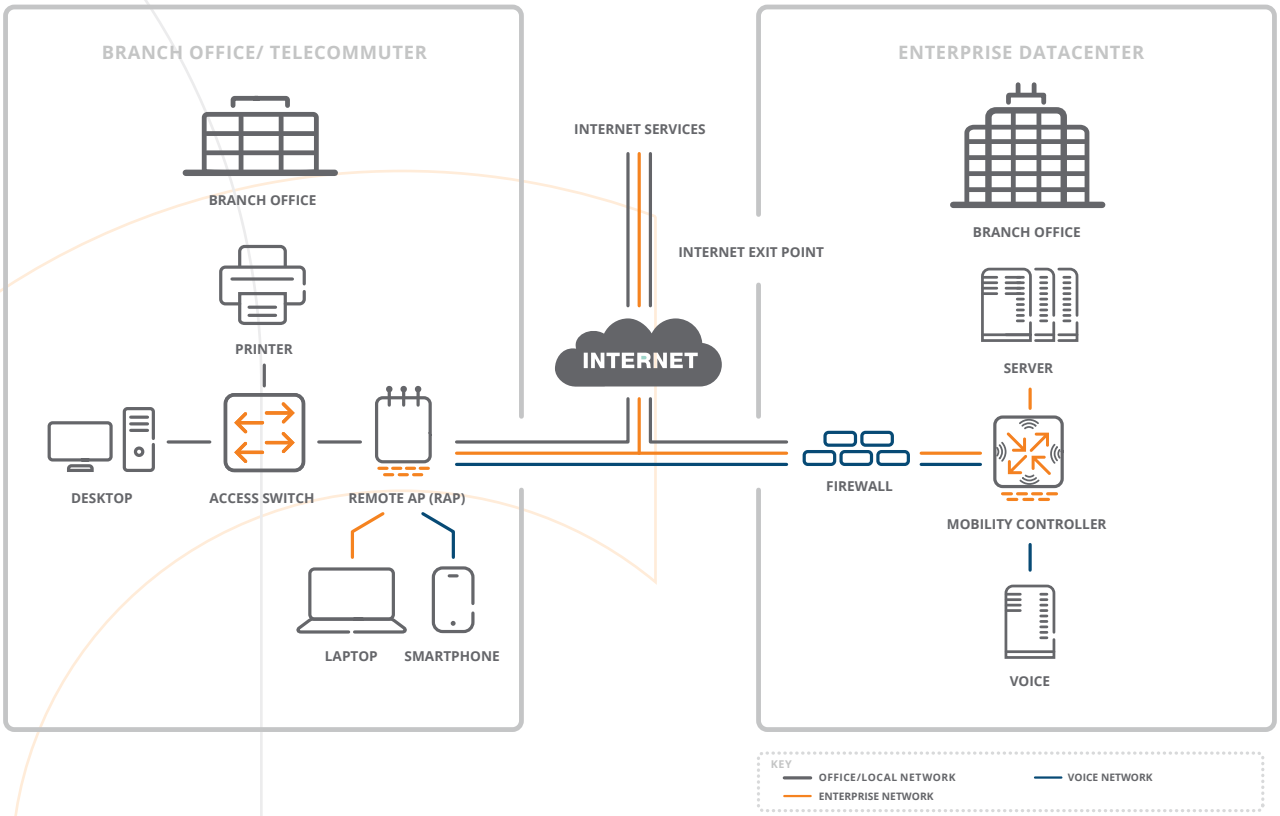

Figure 1: Aruba RAPs for secure mobile connectivity to micro-branch and small offices

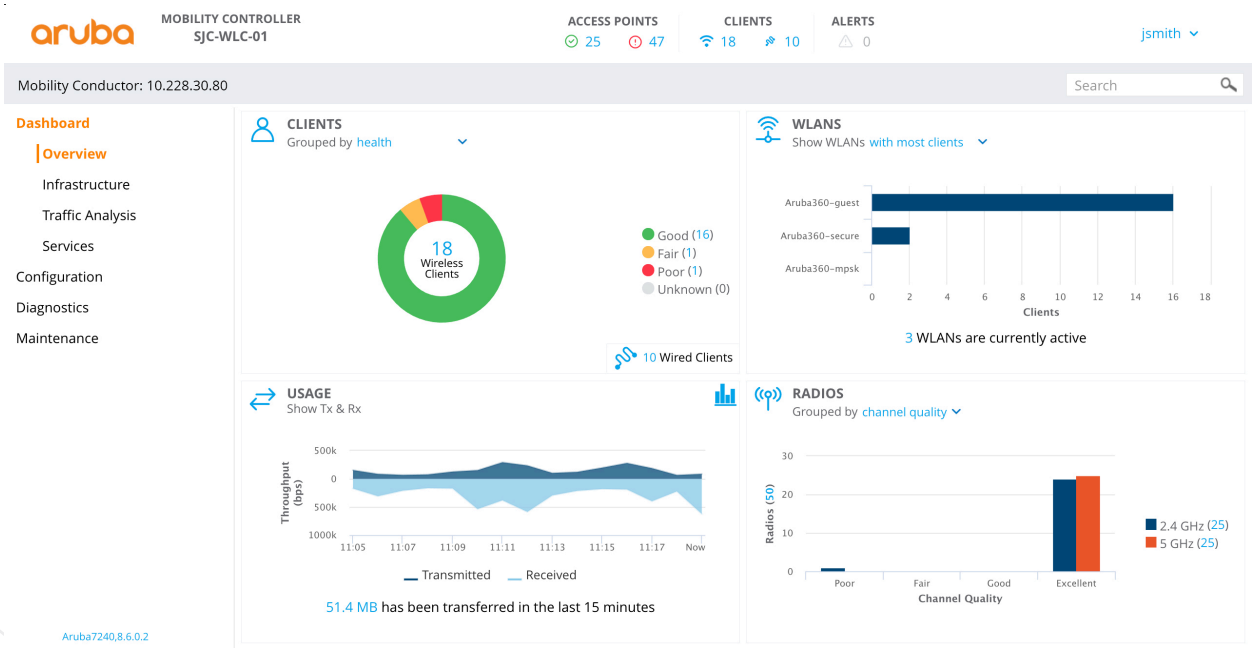

Figure 2: ArubaOS user interface with dashboards, configuration, diagnostics, and maintenance

RF OPTIMIZATION

Ensuring optimal network performance and seamless end-user experience is becoming increasingly difficult with the growth in bandwidth-intensive applications and latency-sensitive IoT deployments. ArubaOS employs AI and machine learning to optimize client, application, and operator activities. See Table 2. This includes:

- **Client optimization:** Clients that stubbornly remain connected to a single AP even when they roam to an area with APs that offer better connectivity can have a significant impact on the performance of the client and overall network health. Aruba's patented RF optimization technology, ClientMatch, scans APs in the neighborhood to ensure that client devices associate with the best-performing AP.
- **RF optimization:** Using machine learning algorithms, AirMatch automates RF channel assignment, channel width, and radio power assignments. It proactively learns and acclimates the network based on changing environmental conditions and system capacity. Machine learning makes dynamic channel assignment, width adjustment, and transmit power adjustment possible. AirMatch provides even distribution of radios across available channels to mitigate interference and maximize system capacity, dynamically adjusts between 20MHz, 40MHz, and 80MHz to match the density of your environment, and automatically adjusts the transmit power of APs across the entire network.
- **SLA-grade application assurance:** ArubaOS provides complete orchestration for Air Slice, an application assurance technology unique to Aruba Wi-Fi 6 access points. By allocating radio resources, such as time, frequency, and spatial streams and combined with intelligence gathered by Aruba's Policy Enforcement Firewall (PEF), APs provide guaranteed bandwidth and low latency for specific users and applications.

RF Optimization Features and Benefits	
Client band steering	Keeps dual-band clients on optimal RF band.
Sticky client mitigation	Ensure client devices associate with the best-performing AP in the neighbourhood to improve client performance and overall network health
Self-healing around failed APs	Automatically adjusts power levels to compensate for failed APs.
Airtime fairness	Manages client access to the air resources. Can be configured to provide fair access or to deliver preferred access to clients that connect using the latest 802.11 standard.
RF spectrum load-balancing	Evenly distributes clients across available channels.
Single-channel coordinated access	Ensures optimal performance even with nearby APs on the same channel.
RF planning	Automatic predeployment 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.
Plug-ins for third-party analysis tools	Wireshark, OmniPeek, AirMagnet.
Rogue AP detection and containment	Detects unauthorized APs and automatically shuts them down.

Table 2: Remote Access Point Benefits

SECURITY AND VISIBILITY

The previous approach of using manual and static configurations does not sufficiently meet the security requirements of highly dynamic mobile and IoT environments. To mitigate risk, ArubaOS provides network administrators enhanced levels of visibility and advanced features such as:

- **Dynamic Segmentation with Policy Enforcement Firewall:** To improve security and ease of management, IT can centrally configure and automatically enforce role-based policies that define proper access privileges for employees, guests, contractors, and other user groups– no matter where users connect on wired and WLANs. Dynamic Segmentation eliminates the time consuming and error-prone task of managing complex and static VLANs, ACLS, and subnets by dynamically assigning policies and keeping traffic secure and separated. Policies can be manually created within ArubaOS or centrally managed by Aruba ClearPass Policy Manager and applied to multiple networks simultaneously.
- **Deep Packet Inspection with AppRF 2.0:** ArubaOS provides extensive visibility and control into over 3,000 apps using AppRF 2.0 that allows for the configuration of security policies and bandwidth controls of applications and application categories. AppRF 2.0 supports Deep Packet Inspection (DPI) capabilities within the policy enforcement firewall for application classification. Optimizing and limiting traffic per application is simple, and intuitive via an easy-to-use dashboard. Unrecognized applications and categories can also be defined through application customization. Role-based policies also offer the flexibility to control exactly which users can run what applications and unwanted applications can be blocked to conserve bandwidth. Rate limits for applications or application categories permit non-essential traffic while preventing it from overwhelming mission critical applications.
- **Web classification (WebCC):** ArubaOS provides a cloud-based web content classification, policy, and reputation service for URL filtering, IP reputation and geolocation filtering, which helps enforce network acceptable use policies to block and rate-limit connections based on Aruba's identity-based controls. See Figure 3.
- **Enhanced Wi-Fi authentication security:** The addition of WPA3 support in the Wi-Fi 6 standard brings stronger encryption and authentication methods, plus Enhanced Open provides per user encryption on open networks. See Table 3.
- **Third-party integration:** REST-based APIs allow for integration with security vendors such as Palo Alto Networks and Check Point Software to ensure end-to-end security. Policies can be pre-defined for specific types of traffic and forwarded to an on-premises security firewall for additional inspection.
- **Virtual Internet Access (VIA) VPN support:** A VIA add-on license lets remote users securely connect to an Aruba network through a hybrid IPSec/SSL VPN software client without the need for a dedicated VPN Concentrator in the enterprise DMZ. User devices adhere to the same policies and service definitions used at headquarters or a branch. Learn more at Aruba VPN Services.

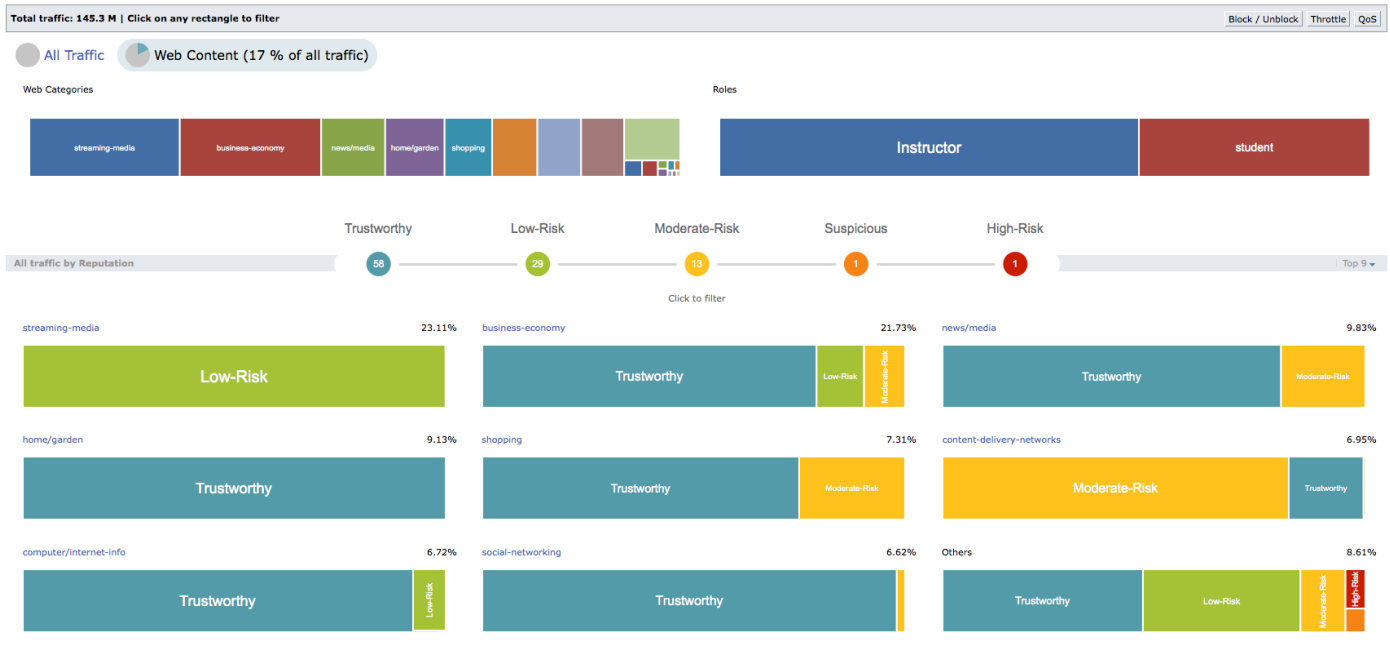

Figure 3: WebCC dashboard

ENTERPRISE SECURITY FRAMEWORK

Authentication types	1. 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) 2. RFC 2548 Microsoft vendor-specific RADIUS attributes 3. RFC 2716 PPP EAP-TLS 4. RFC 2865 RADIUS authentication 5. RFC 3579 RADIUS support for EAP 6. RFC 3580 IEEE 802.1X RADIUS guidelines 7. RFC 3748 extensible authentication protocol 8. MAC address authentication 9. Web-based captive portal authentication
Authentication servers	1. Internal database 2. LDAP/SSL secure LDAP 3. RADIUS 4. TACACS+ 5. Tested authentication server interoperability: • Microsoft Active Directory (AD) • Microsoft IAS and NPS RADIUS servers • Cisco ACS, ISE servers • Juniper Steel Belted RADIUS, Unified Access servers • RSA ACE/Server • Infoblox • Interlink RADIUS Server • FreeRADIUS

ENTERPRISE SECURITY FRAMEWORK	
Encryption protocols	1. CCMP/AES 2. TKIP 3. SSL and TLS: • RC4 128-bit • RSA 1024-bit • RSA 2048-bit 4. L2TP/IPsec (RFC 3193) 5. XAUTH/IPsec 6. PPTP (RFC 2637)
Integrated guest access management	Provides secure guest access options
Site-to-site VPN	IPsec tunnel is established between Mobility Controller and IPsec devices. Authentication support for X.509 PKI, IKEv2, IKE PSK, IKE aggressive mode.

Table 3. ArubaOS security framework.

MANAGEABILITY AND TROUBLESHOOTING

Using disparate network management tools makes troubleshooting inefficient and can impact business outcomes by slowing down root issue identification, analysis, and resolution. ArubaOS supports integrated dashboards and powerful visualizations of key health and performance metrics that provide IT operators visibility and insights for efficient troubleshooting. It also supports key third party integrations that enable Aruba APs to serve as IoT and location-ready gateways. Manageability and troubleshooting capabilities include:

- **Unified Communications and Collaboration:** UCC visibility and reporting provides network administrators a consolidated view of how media collaboration applications are performing with enhanced Wi-Fi troubleshooting capabilities. ArubaOS provides integrated dashboards for call quality metrics and prioritization of business-critical applications including Wi-Fi calling support. Call quality metrics for latency, jitter, and packet loss are available for a wide variety of applications including Microsoft Skype for Business/Lync, Microsoft Teams, Cisco Skinny Call Control Protocol (SCCP), Spectralink Voice Priority (SVP), SIP, Vocera, and more. See Figure 4.

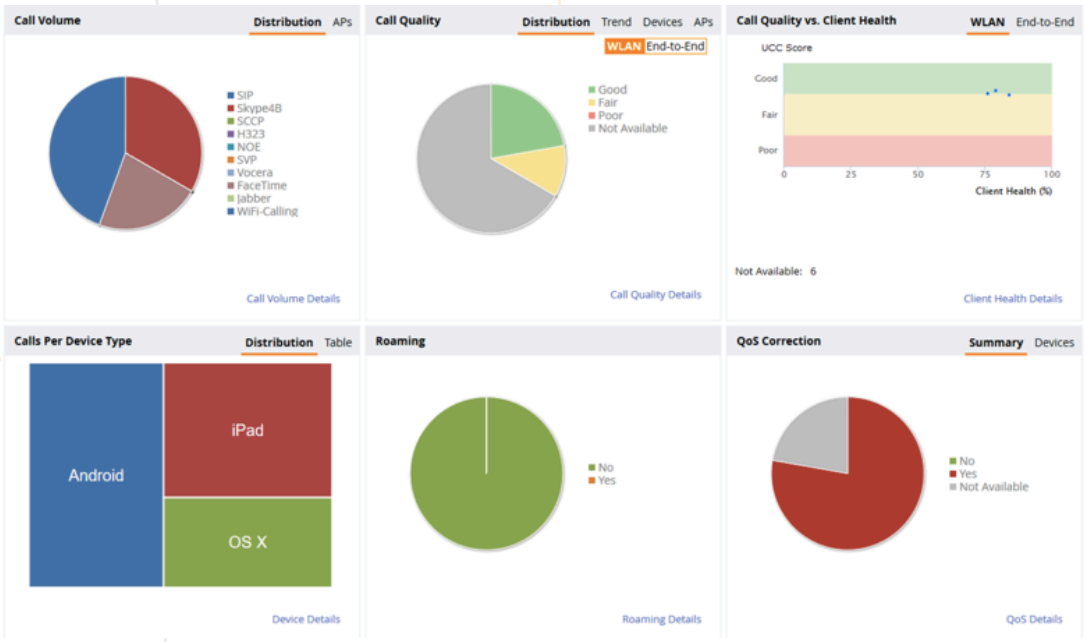

Figure 4: UCC dashboard to provide visibility into the performance of critical voice and video applications

Figure 5: WAN Dashboard

- **Integrated WLAN and WAN dashboards:** ArubaOS uses features such as policy-based routing, dynamic path steering and compression to improve WAN health with intelligence that spans WLAN and WAN. An integrated dashboard also helps visualize key WAN metrics such as latency, jitter, and packet loss across public and private uplinks. See Figure 5.
- **AirGroup support:** Aruba extends enterprise Wi-Fi capabilities to Apple, Google, and third-party devices (AppleTV, etc.) and services like AirPlay, AirPrint, and Google Cast through AirGroup, a unique capability that optimizes IP multicast traffic, prioritizes services, and adds policy controls. Simple configuration options ensure that these client devices are always accessible over WLAN, while advanced options provide access controls to devices based on physical location, time of day, and user/role-based details.
- **Mesh capabilities:** ArubaOS supports wireless mesh for AP uplinks in the absence of fiber or cable runs. Most commonly deployed for point-to-point wireless backhaul, security camera use cases, network access in on-premises locations, and to bridge the network at the furthest reaches of the coverage area, Aruba's wireless mesh provides the same enterprise network services as standard wire-based design. Aruba uses an intelligent link algorithm between each AP to automatically adjust and optimize traffic paths and links. Network managers can repurpose any indoor or outdoor AP or use 802.11ad Point-to-Point technology for high-performance gigabit-speed backhaul.
- **IPv6:** ArubaOS supports IPv6 environments as well as dual-stack interoperability of IPv6 within an IPv4 network. This is ideal for organizations that have nearly depleted available IPv4 addresses and need to transition from IPv4 to IPv6 (which adds a much larger address space).
- **IoT and location-ready wireless support:** By leveraging existing wireless infrastructure, Aruba greatly reduces system complexity and cost for transferring IoT data from sensors to IoT applications that can derive IT and business value. Each Aruba AP serves as an IoT and location-ready gateway with no additional software required. Aruba's solution includes integration with Aruba Meridian, ALE, and third-party Wi-Fi, BLE, Zigbee and USB-based vendor solutions. In addition, Aruba's IoT Transport for Azure provides secure, bidirectional integration with Azure to accelerate application development while minimizing cost and overhead.

Wi-Fi Network Management and Configuration	
Web-based configuration	Allows any administrator with a standard web browser to manage the system.
Command line	Console and SSH
Syslog	Supports multiple servers, multiple levels, and multiple facilities
SNMP v2c	Yes
SNMP v3	Enhances standard SNMP with cryptographic security.
Centralized configuration of Mobility Controllers	A designated conductor Mobility Controller can configure and manage several downstream local controllers.
VRRP	Supports high availability between multiple Mobility 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 Layer 2 convergence.

Table 4. Management and configuration details

24x7 RELIABILITY

AOS provides seamless wireless connectivity to ensure high availability 24x7 with controller clustering capabilities, hitless failover, and live upgrades without system downtime. Controller clustering, a unique capability managed by the Mobility Conductor, enables up to 12 Mobility Controllers in a cluster to act as a single virtual instance. This improves network capabilities by decoupling network requirements from the limitations on individual hardware – dramatically scaling performance and reliability. See Table 5 and Table 6.

To mitigate disruption to the network, user session information is shared across a cluster to maintain active voice calls, video streams, data transfers, roaming clients, as well as network management. Features such as live and in-service upgrades are used to eliminate maintenance windows as well as plan for unscheduled outages.

- **Centralized Tunneling:** To improve AP utilization for networks with complex Layer 2 and Layer 3 requirements, AP licenses enable individual APs to forward all traffic, policy, management and control decisions to a controller. ArubaOS 8 and later releases also allow Aruba access switches to mimic the role of an AP (e.g. wired AP).

High Availability Deployment Modes	
Active/Active (1:1)	Each Mobility Controller typically serves 50% of its rated capacity. The first acts as a standby for APs served by second controller and vice-versa. If a controller fails, its APs failover to the other controller, ensuring high-availability to all APs.
Active/Standby (1+1)	One Mobility Controller terminates all the APs, while the other controller acts as a standby. If the primary controller goes down, APs move to standby controller.
N+1	Multiple active Mobility Controllers are backed-up by single standby controller.

Table 5. Mobility Controller deployment mode options

Feature	Benefit
AP establish simultaneous communication channel with both active and standby Mobility Controller.	Instantaneous failover to redundant Mobility Controller when first fails.
During a failover, the APs do not turn their radios off and on.	SSID always available.
The solution works across Layer 3 networks	No special topologies needed.
Client state sync	Credentials are cached, eliminating need to reauthenticate and overload RADIUS server.
N+1 oversubscription	Simplifies configuration and reduces number of Mobility Controllers needed.

Table 6. Mobility Controller features and benefits

- **Hitless Failover:** Using Controller Clusters, user sessions and AP traffic are load balanced to optimize network utilization during peak periods and maximize availability during unplanned outages. This means that users will not notice any impact to voice calls, video streaming, or data transfers in an unlikely event that a controller loses connectivity.
- **Live Upgrade:** ArubaOS can be upgraded while supporting active user sessions – eliminating the need for planned maintenance windows or downtime. With the Mobility Conductor, each Controller Cluster or individual service modules can be selectively upgraded without impacting the rest of the network.
- **Seamless Layer 2:** ArubaOS includes proxy mobile IP/DHCP functions and automatically load balances clients across multiple VLANs to provide seamless connectivity as users move between floors, buildings or across the entire network – even while using video and voice applications. For better user experience, ArubaOS supports roaming across subnets and VLANs with handoff times of just 2-3 milliseconds without reauthentication, changes to IP addresses, or loss of firewall state.

SUMMARY

ArubaOS delivers optimized wireless connectivity and flexibility to meet the needs of small offices, mid-sized branches, and large campus environments. With unique AI and optimization capabilities such as ClientMatch, AppRF, and AirMatch, ArubaOS provides high levels of performance even in dense environments. It also offers built-in security including Dynamic Segmentation for robust security policy enforcement and MultiZone capabilities for secure multi-tenant environments as well as IoT and guest segmentation. For additional information on Aruba WLAN products and services, please refer to the Aruba wireless overview and our product warranty and support online.

CERTIFICATIONS

- Wi-Fi Alliance certified (802.11a/b/g/n/d/h/ac/ad/ax) WPA™
- Personal, WPA™ Enterprise, WPA2™ Personal, WPA2™
- Enterprise, WPA3™ Enterprise, WPA3™ Personal, Enhanced Open™, WMM™, WMM Power Save
- FIPS 140-2 validated (when operated in FIPS mode)
- Common Criteria certified
- RSA certified
- USGv6 firewall

STANDARDS SUPPORTED

General switching and routing

- 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 1058 Routing Information Protocol
- RFC 1122 Host Requirements
- RFC 1256 IPv4 ICMP Router Discovery (IRDP)
- RFC 1519 CIDR
- RFC 1812 Requirements for IP Version 4 Routers
- RFC 1997 BGP Communities Attribute
- RFC 2091 Triggered Extensions to RIP to Support Demand Circuits
- RFC 2236 IGMPv2
- RFC 2328 OSPFv2
- RFC 2338 VRRP
- RFC 2385 Protection of BGP Sessions via the TCP MD5 Signature Option
- RFC 2453 RIP Version 2
- RFC 2460 Internet Protocol version 6 (IPv6)
- RFC 2516 Point-to-Point Protocol over Ethernet (PPPoE)
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
- RFC 2918 Route Refresh Capability for BGP-4
- RFC 3220 IP Mobility Support for IPv4 (partial support)
- RFC 3376 IGMPv3 Internet Group Management Protocol, Version 3
- RFC 3736 DHCP Services for IPv6
- RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6
- RFC 4271 A Border Gateway Protocol 4 (BGP-4)
- RFC 4291 IP Version 6 (IPv6) Addressing Architecture
- RFC 4360 BGP Extended Communities Attribute
- RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- RFC 4541 IGMP and MLD Snooping
- RFC 4604 IGMPv3/MLDv2 for SSM
- RFC 4724 Graceful Restart Mechanism for BGP
- RFC 4760 Multiprotocol Extensions for BGP-4
- RFC 4822 RIPv2 Cryptographic Authentication
- RFC 4862 IPv6 Stateless Address Autoconfiguration (9xxx)
- RFC 4893 BGP Support for Four-octet AS Number Space
- RFC 5492 Capabilities Advertisement with BGP-4
- RFC 5668 4-Octet AS Specific BGP Extended Community

- RFC 5798 Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6
- RFC 6106 IPv6 Router Advertisement Options for DNS Configuration
- RFC 8201 Path MTU Discovery for IP version 6
- IEEE 802.1D-2004 – MAC Bridges
- IEEE 802.1Q – 1998 Virtual Bridged Local Area Networks
- IEEE 802.1w – Rapid Spanning Tree Protocol
- IEEE 802.1AB - Station and Media Access Control Connectivity DIscovery (LLDP specification)
- IEEE 802.3AD - Link Aggregation Control Protocol (LACP)

QoS and policies

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

Wireless

- IEEE 802.11a/b/g/n/ac/ax 5 GHz, 2.4 GHz
- IEEE 802.11d Additional Regulatory Domains
- IEEE 802.11e QoS
- 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
- IEEE 802.11ac Enhancements for Very High Throughput
- IEEE 802.11ax
- IEEE 802.11n Enhancements for Higher Throughput
- IEEE 802.11r Fast BSS Transition (FT)
- IEEE 802.11v Wireless Network Management (partial support)
- IEEE 802.11mc
- IEEE 802.11w

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 Bootstrap Protocol (BOOTP)
- RFC-1542 Clarifications and Extensions for the Bootstrap Protocol
- RFC 2131 Dynamic Host Configuration Protocol
- RFC 1591 DNS (client operation)
- RFC 2136 Dynamic Updates in the Domain Name System (DDNS)
- RFC 3007 Secure Domain Name System (DNS) Dynamic Updated (Supports the TSIG method).
- RFC 1155 Structure of Management Information (SMIv1)
- RFC 1157 SNMPv1
- RFC 1212 Concise MIB definitions
- RFC 1213 MIB 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 1901 1908 SNMP v2c SMIv2 and Revised MIB-II
- 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 SNMP
- RFC 959 File Transfer Protocol (FTP)
- RFC 2516 A method for Transmitting PPP over Ethernet (PPPoE)
- RFC 2570, 2575 SNMPv3 user based security, encryption and authentication
- RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3
- RFC 2660 Secure HyperText Transfer Protocol (HTTPS)
- 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
- RFC 5176 Dynamic Authorization Extension to Remote Authentication Dial In User Service (RADIUS)

Security and encryption

- IEEE 802.1X Port-Based Network Access Control
- RFC 1334 PPP Authentication Protocols (PAP and CHAP)
- RFC 1661 The Point-to-Point Protocol (PPP)
- RFC 2104 Keyed-Hashing for Message Authentication (HMAC)
- RFC 2131 Dynamic Host Configuration Protocol
- RFC 2246 The TLS Protocol (SSL)
- RFC 2401 Security Architecture for the Internet Protocol
- RFC 2403 The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2405 ESP DES-CBC cipher algorithm with explicit IV
- RFC 2406 IP Encapsulating Security Payload (ESP)
- RFC 2407 IP Security Domain of Interpretation for ISAKMP
- RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 Internet Key Exchange (IKE) v1
- RFC 2451 The ESP CBC-Mode Cipher Algorithms
- RFC 2661 Layer Two Tunneling Protocol "L2TP"
- RFC 2716 PPP EAP TLS Authentication Protocol
- RFC 3079 Deriving Keys for use with Microsoft Point-to-Point Encryption (MPPE) RFC 3162 Radius over IPv6
- RFC 3193 Securing L2TP using IPsec
- RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPsec
- RFC 3706 Dead Peer Detection (DPD)
- RFC 3748, 5247 Extensible Authentication Protocol (EAP)
- RFC 3947 Negotiation of NAT-Traversal in the IKE
- RFC 3948 UDP encapsulation of IPsec packets
- RFC 4017 EAP Method Requirements for Wireless LANs
- RFC 4106 GCM for IPSEC
- RFC 4137 State Machines for EAP Peer and Authenticator
- RFC 4306 Internet Key Exchange (IKE) v2
- RFC 4793 EAP-POTP
- RFC 5246 TLS1.2
- RFC 5247 EAP Key Management Framework
- RFC 5281 EAP-TTLS v0
- RFC 5430 Suite-B profile for TLS
- RFC 7030 Enrollment over Secure Transport
- RFC 7383 IKEv2 Message Fragmentation (Only responder side logic is implemented. AOS as a initiator does not propose this Fragmentation method)
- RFC 8201 Path MTU Discovery for IP version 6
- RFC 8110 Opportunistic Wireless Encryption
- IETF Draft RadSec – TLS encryption for RADIUS

SERVICE AND WARRANTY INFORMATION

- Access Points: Limited Lifetime Warranty
- Other Hardware: 1 year for parts/labor, can be extended with support contract
- Software: 90 days, can be extended with support contract

For additional information, please refer to the webpages:

- Aruba Access Points
- Aruba Gateways and Controllers
- Aruba VPN Services
- Aruba Support Portal
- Aruba Product Warranties

ORDERING INFORMATION*	
Part Number	**Description**
JW471AAE	Aruba LIC-ENT Enterprise (LIC-AP LIC-PEF LIC-RFP and LIC-AW) License Bundle E-LTU
JW472AAE	Aruba LIC-AP Controller per AP Capacity License E-LTU
JW473AAE	Aruba LIC-PEF Controller Policy Enforcement Firewall per AP License E-LTU
JW474AAE	Aruba LIC-RFP Controller RFProtect per AP License E-LTU
JZ148AAE	Aruba LIC-VIA per VIA Client License E-LTU This license enables firewall services on a per session basis for VPN termination from Aruba VIA VPN client
Q9B90AAE	Aruba LIC-ACR Controller Advanced Cryptography 1 Session License E-LTU
JY028AAE	Aruba Controller Web Content Classification 1 Year Subscription E-STU
JY029AAE	Aruba Controller Web Content Classification 3 Year Subscription E-STU
JY030AAE	Aruba Controller Web Content Classification 5 Year Subscription E-STU
JY031AAE	Aruba Controller Web Content Classification 7 Year Subscription E-STU
JY032AAE	Aruba Controller Web Content Classification 10 Year Subscription E-STU
JW495AAE	Aruba PEF VIA Lic for 7005 Cntrlr E-LTU
JY342AAE	Aruba PEF VIA Lic for 7008 Cntrlr E-LTU
JW496AAE	Aruba PEF VIA Lic for 7010 Cntrlr E-LTU
JW497AAE	Aruba PEF VIA Lic for 7024 Cntrlr E-LTU
JW498AAE	Aruba PEF VIA Lic for 7030 Cntrlr E-LTU
JW499AAE	Aruba PEF VIA Lic for 7205 Cntrlr E-LTU
JW500AAE	Aruba PEF VIA Lic for 7210 Cntrlr E-LTU
JW501AAE	Aruba PEF VIA Lic for 7220 Cntrlr E-LTU
JW502AAE	Aruba PEF VIA Lic for 7240 Cntrlr E-LTU

* Note: LIC-VIA license is per VIA user license and is not tied to any particular controller. It can be transferred from one controller to another. Unlike PEFV, LIC- VIA supports centralized licensing and can be managed by Mobility Conductor or a Conductor Controller in AOS 8.x deployment. Refer to the 7000 Series and 7200 Series ordering guides for more information.

MOBILITY CONTROLLER ORDERING INFORMATION

Large enterprises that require mission-critical reliability and availability can opt to deploy Mobility Controllers that are meant to centralize all control functionality for APs and enable high performance network access and resiliency. Mobility Controllers are made available as virtual or physical appliances and can be managed by Mobility Conductors to enable reliability and high scale – up to 100,000 clients, 10,000 access points (APs) and 1,000 controllers/gateways.

The Aruba 7200 Series can be deployed using Aruba Mobility Controller software licenses in a campus or branch access layer deployment. In this mode, the controllers cannot be simultaneously used for SD-WAN. In Mobility Controller mode, the 7200 Series can also participate in Aruba's Dynamic Segmentation framework, with, at minimum, an access point (AP) license and a Policy Enforcement Firewall (PEF) license for each Aruba access point and switch in the network.

MOBILITY CONTROLLER LICENSES

Part Number	Description
JW472AAE	Aruba LIC-AP Controller per AP Capacity License E-LTU
JW473AAE	Aruba LIC-PEF Controller Policy Enforcement Firewall per AP License E-LTU
JW474AAE	Aruba LIC-RFP Controller RFProtect per AP License E-LTU
JW471AAE	Aruba LIC-ENT Enterprise (LIC-AP LIC-PEF LIC-RFP and LIC-AW) License Bundle E-LTU
Q9B90AAE	Aruba LIC-ACR Controller Advanced Cryptography 1 Session License E-LTU
JY028AAE	Aruba Controller Web Content Classification 1 Year Subscription E-STU
JY029AAE	Aruba Controller Web Content Classification 3 Year Subscription E-STU
JY030AAE	Aruba Controller Web Content Classification 5 Year Subscription E-STU
JY031AAE	Aruba Controller Web Content Classification 7 Year Subscription E-STU
JY032AAE	Aruba Controller Web Content Classification 10 Year Subscription E-STU
Q9B90AAE	Aruba Adv Crypto 1 Session Lic E-LTU
JW499AAE	Aruba PEF VIA Lic for 7205 Cntrlr E-LTU
JW500AAE	Aruba PEF VIA Lic for 7210 Cntrlr E-LTU
JW501AAE	Aruba PEF VIA Lic for 7220 Cntrlr E-LTU
JW502AAE	Aruba PEF VIA Lic for 7240 Cntrlr E-LTU
JZ148AAE	Aruba LIC-VIA per VIA Client License E-LTU

For each AP attached to the controller the minimal configuration is 1 x LIC-AP per AP.

- LIC-ENT (JW471AAE) is equivalent to 1 each of LIC-AP, LIC-REF, LIC-RFP and LIC-AW.
- LIC-AW is a device license for AirWave Management system
- For Dynamic Segmentation, the per-AP license count must equal the sum of APs and switches that are tunneling traffic. For virtual switch stacks, one AP license will be consumed per stack.
- The PEFV license enables firewall services on a per-controller basis for VPN termination such as Aruba VIA, Aruba RAPs and IAP-VPN.

Note: PEFV license can also be used for VIA VPN termination. But PEFV is tied to a particular controller and the license capacity scales to the controller user capacity. On the other hand, LIC-VIA license is per VIA user license and is not tied to any particular controller. It can be transferred from one controller to another. Unlike PEFV, LIC-VIA supports centralized licensing and can be managed by Mobility Conductor or a Conductor Controller in AOS 8.x deployment.

The Aruba 9000 Series can alternatively be deployed using Aruba Mobility Controller software licenses, where the 9000 Series will perform just like a 7000 Series or 7200 Series Mobility Controller in a campus or branch access layer deployment. In this mode, the gateway cannot be simultaneously used for SD-WAN. In Mobility Controller mode, the 9000 Series can also participate in Aruba's Dynamic Segmentation framework, with, at minimum, an access point (AP) license and a Policy Enforcement Firewall (PEF) license for each Aruba access point and switch in the network.

MOBILITY CONTROLLER LICENSES	
Part Number	**Description**
JW472AAE	Aruba LIC-AP Controller per AP Capacity License E-LTU
JW473AAE	Aruba LIC-PEF Controller Policy Enforcement Firewall per AP License E-LTU
JW474AAE	Aruba LIC-RFP Controller RFProtect per AP License E-LTU
JW471AAE	Aruba LIC-ENT Enterprise (LIC-AP LIC-PEF LIC-RFP and LIC-AW) License Bundle E-LTU
Q9B90AAE	Aruba LIC-ACR Controller Advanced Cryptography 1 Session License E-LTU
JY028AAE	Aruba Controller Web Content Classification 1 Year Subscription E-STU
JY029AAE	Aruba Controller Web Content Classification 3 Year Subscription E-STU
JY030AAE	Aruba Controller Web Content Classification 5 Year Subscription E-STU
JY031AAE	Aruba Controller Web Content Classification 7 Year Subscription E-STU
JY032AAE	Aruba Controller Web Content Classification 10 Year Subscription E-STU
JZ148AAE	Aruba LIC-VIA per VIA Client License E-LTU

- A single 9000 Series Gateway cannot be simultaneously used for SD-WAN and Mobility Controller functionality.
- For each AP attached to the gateway, the minimal configuration is 1 x LIC-AP per AP.
- LIC-AW is a device license for the AirWave network management system.
- For Dynamic Segmentation, the per-AP license count must equal the sum of APs and switches that are tunneling traffic. For virtual switch stacks, one AP license will be consumed per stack.
- LIC-VIA license is a per-user session license that can be transferred from one gateway/controller to another.
- LIC-VIA supports centralized licensing and can be managed by Mobility Conductor or a Conductor Controller in an ArubaOS 8 deployment.

DS_ArubaOS_RVK_062521 a00073441enw