DATA SHEET

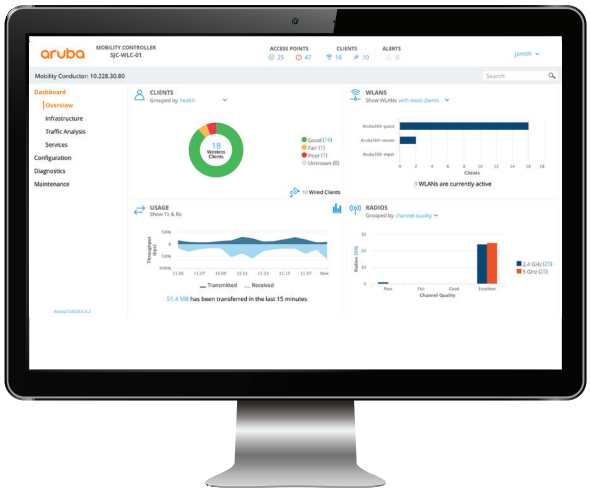
ARUBAOS

Enhanced network operating system for today's digital workplace

OVERVIEW

ArubaOS is the network operating system for Aruba Mobility Conductors, Mobility Controllers and controller-managed campus access points (APs). With industry-leading software innovation, ArubaOS is engineered to deliver enterprise-grade performance and mission-critical reliability for enterprise deployments of all sizes.

Aruba supports the latest Wi-Fi Alliance standards such as Wi-Fi 6 (802.11ax) and 802.11ad, as well as WPA3 and Enhanced Open security protocols. Also supported are all previous standards and protocols such as 802.11a/b/g/n/ac, which enables your network to satisfy today's and tomorrow's use cases (See Table 1).



SIMPLE AND SECURE ACCESS

ArubaOS also serves a key role in Dynamic Segmentation, enforcing policy based on user role, device type, application and location to simplify and secure wired and wireless network access. This feature can be enabled with the ArubaOS Policy Enforcement Firewall (PEF) license and eliminates the need to manually configure SSIDs, VLANs or ACLs for each new client on the network.

Refer to ArubaOS release notes for a list of detailed features.

ARUBA AIR SLICE

ArubaOS provides complete orchestration for Air Slice, an SLA-grade 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), AP's provide guaranteed bandwidth for specific users and applications. Learn more in the Air Slice tech brief.

KEY FEATURES

- Support for new Wi-Fi 6 (802.11ax), WPA3 and Enhanced Open – and all existing standards
- Advanced AI-powered closed-loop wireless/RF optimization
- Enhanced AP utilization and client roaming
- SLA-grade application assurance with Air Slice (ArubaOS 8.7+)
- Automated deployment with ZTP and hierarchical configuration
- Dynamic Segmentation enforces wired and wireless access policies to simplify and secure the network
- Application awareness for 3,000+ applications without additional hardware
- Live Upgrade and Seamless Failover

Enterprise security framework	
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+ • 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
Encryption protocols	• CCMP/AES • WEP 64- and 128-bit • TKIP • SSL and TLS: - RC4 128-bit - RSA 1024-bit - RSA 2048-bit • L2TP/IPsec (RFC 3193) • XAUTH/IPsec • PPTP (RFC 2637)
Programmable encryption engine	Permits future encryption standards to be supported through software updates
Web-based captive portal (SSL)	Allows flexibility in authentication methods
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 1

24x7 MISSION-CRITICAL NETWORKING

With the growth in cloud-based applications, services, IoT and mobile devices, end-users expect network resources to be available wherever and whenever they connect. Likewise, enterprise networks must extend beyond traditional security perimeters while delivering a seamless user experience. With the latest version of ArubaOS, controller clustering boosts network performance and ultimately helps organizations improve productivity by upwards of hundreds or even thousands of hours every year.

Controller clustering, a unique capability managed by 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.

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. Mobility Controllers in standalone, campus, or branch mode can also be deployed in traditional 1:1 or 1:N VRRP-based redundant configurations (See Table 2 and 3).

Management, configuration and troubleshooting are provided through a browser-based GUI (See Figure 1 and Table 4) or through CLI – familiar for any network manager. The Mobility Conductor can centrally configure and manage Mobility Controllers and APs in a large campus or distributed branch environments, and provide intuitive task-based wizards to ease configuration.

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 2

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 3

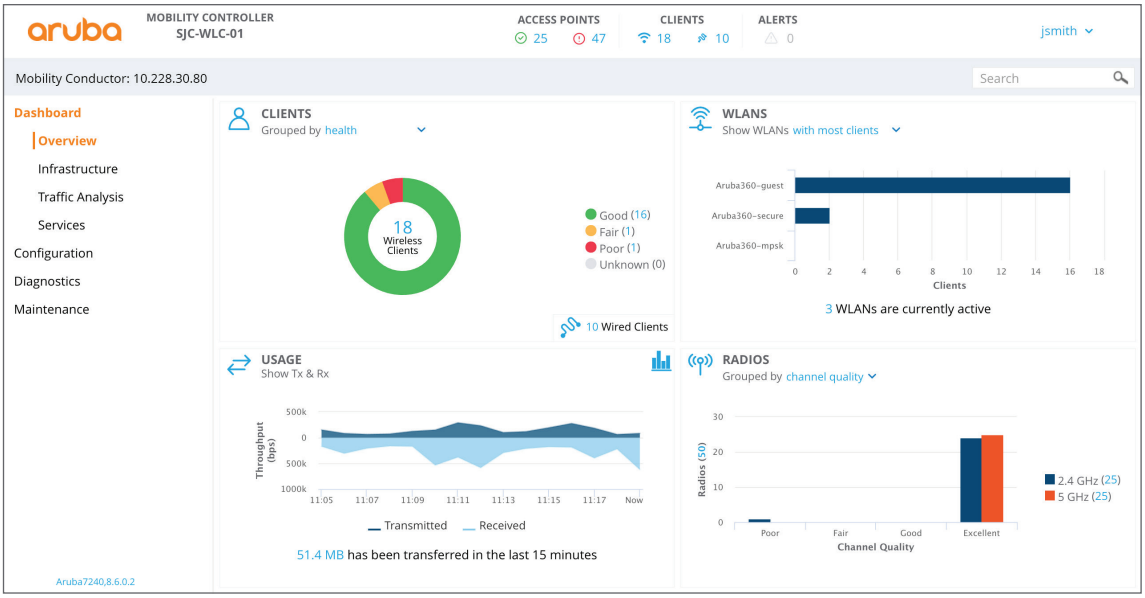


Figure 1: ArubaOS 8 user interface

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

PERFORMANCE

Adaptive Radio Management (ARM)

ARM maximizes an AP's Wi-Fi stability and predictability by dynamically choosing the best 802.11 channel and transmit power. This capability helps ensure optimal performance for all clients and applications, especially in environments with a large number of mobile users and performance-stringent applications that can cause network contention and interference. (See Table 5)

ClientMatch

A patented RF optimization technology, ClientMatch is a feature of ARM that boosts Wi-Fi client performance by alleviating sticky client issues. Client devices associate with the best-performing AP and can also be grouped based on its supported Wi-Fi standards (e.g. downlink or uplink MU-MIMO) to improve system capacity. This is ideal for environments with complex roaming requirements.

Centralized tunneling

To improve AP utilization (e.g. memory, processing and bandwidth) 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) – switch configuration and management is delivered through Aruba AirWave. (See Table 6)

Adaptive Radio Management Benefits	
Adaptive Radio Management (ARM)	Automatically manages all RF parameters to achieve maximum performance.
802.11ac VHT20, VHT40 and VHT80 support	Manages spectrum for all 802.11ac networks.
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	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.
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, AirMagnet.
Rogue AP detection and containment	Detects unauthorized APs and automatically shuts them down.

Table 5

Unified Access framework	
User connectivity method	• Secure enterprise-grade Wi-Fi • Wired Ethernet • VPN remote access
AP connection method	• Private or public IP cloud - Ethernet - Wireless WAN (EVDO, HSDPA) • Wi-Fi mesh (point-to-point and point-to-multipoint)
Traffic forwarding	• Centralized – All user traffic flows to a Mobility Controller • Policy-routed – User traffic is selectively forwarded to a Mobility Controller or bridged locally, depending on the traffic type and policy
Wi-Fi encryption	• Centralized – Traffic is encrypted between devices and the Mobility Controller • Distributed – Traffic is encrypted between the device and AP • Open – No encryption
Integration with existing networks	• Layer 2 and Layer 3 integration – Mobility Controllers can switch or route traffic on a per-VLAN basis • Rapid Spanning Tree – Enables fast Layer 2 convergence • OSPF – Simple integration with existing routing topologies

Table 6

Context-aware controls

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. ArubaOS also includes device fingerprinting, which allows network managers to assign policies based on device type and firmware (e.g. iPhone, Android, etc). This allows the network to regulate which devices are provided access to the network and how these devices can be used. (See Table 7)

Context Aware Control Network	
T-SPEC/TCLAS	Yes
WMM	Yes
WMM priority mapping	Yes
U-APSD (Unscheduled Automatic Power-Save Delivery)	Yes
IGMP snooping for efficient multicast delivery	Yes
Application and device fingerprinting	Yes

Table 7

Seamless Layer 2 and Layer 3 roaming

ArubaOS includes proxy mobile IP/DHCP functions to provide seamless connectivity as users move between floors, buildings or across the entire network – even while using video and voice applications. Roaming handoff times of just 2-3 milliseconds, without reauthentication, changes to IP addresses or loss of firewall state. When ArubaOS runs on Mobility Conductor, roaming is enabled through Controller Clustering. (See Table 8)

VLAN pooling

Instead of configuring VLANs on every network edge switch, something in ArubaOS centralized in Mobility Controllers and tunneled to APs. Major advantages include reduced network configuration complexity and max spanning tree diameter. User membership of VLANs is load-balanced to maintain optimal network performance as large groups of users move about the network.

SECURITY AND VISIBILITY

Dynamic Segmentation

For each wireless client, wired port or user on a wired port, traffic can be forwarded to a Mobility Controller or Gateway and then securely segmented based using the Policy Enforcement Firewall. Port-based Tunneling (PBT) can be used to forward all traffic from a wired port, while user-based tunneling (UBT) can forward role-specific traffic – completely eliminating the need for network administrators to locally configure ACLs, VLANs and subnets.

Policy Enforcement Firewall (PEF)

As a key component of Dynamic Segmentation, PEF is an ArubaOS license that enables user and application visibility. It delivers full policy enforcement based on user role, application, device and location awareness over WLAN, LAN and remote VPN connections for Remote APs, Instant APs and VIA VPN client services.

Policies can be manually created within ArubaOS, or centrally managed by Aruba ClearPass Policy Manager and applied to multiple networks simultaneously.

Application visibility and control

Application visibility is a feature within PEF that provides extensive visibility and control into over 3,000 apps using Deep Packet Inspection (DPI) for 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*. (See Figure 2 and Table 9)

Seamless roaming features	
Fast roaming	2-3 msec intra-controller 10-15 msec inter-controller
Roaming across subnets and VLANs	Sessions do not drop as clients roam on the network
Proxy mobile IP	Automatically establishes home agent/foreign agent relationship between Mobility Controllers
Proxy DHCP	Prevents clients from changing IP address when roaming
VLAN pooling	Automatically load balances clients across multiple VLANs

Table 8

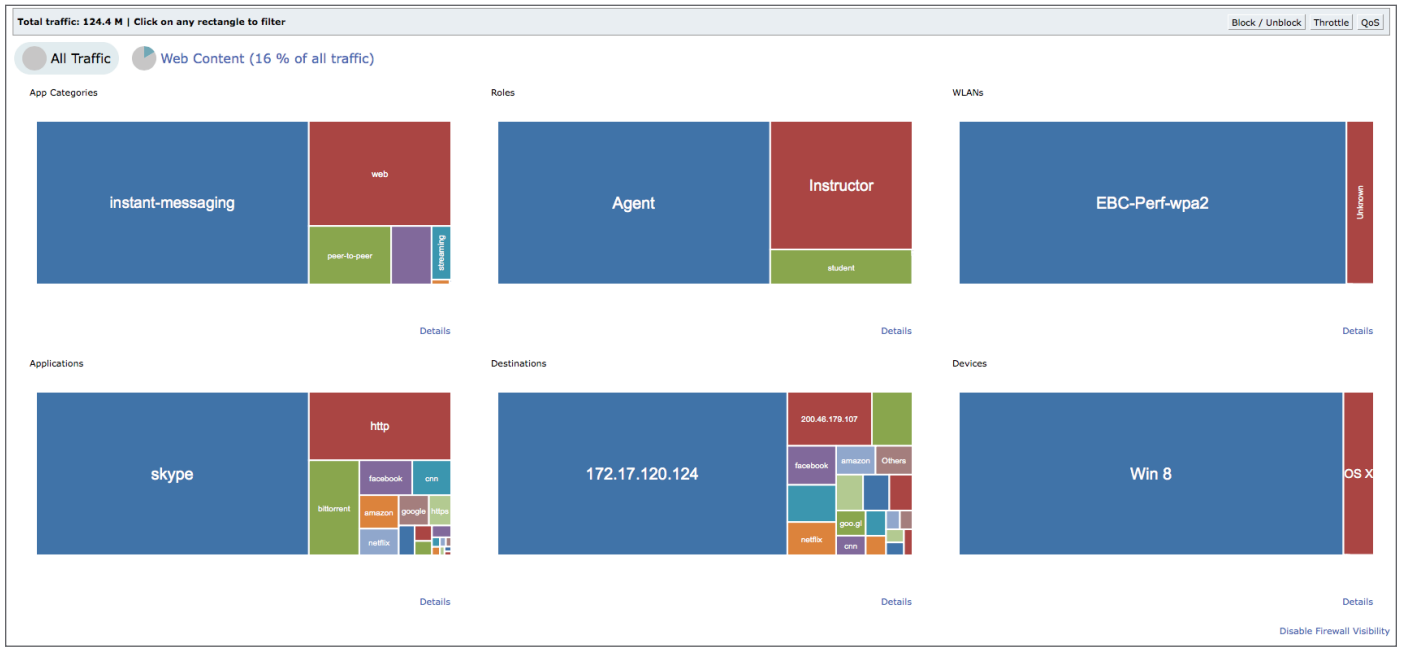


Figure 2: Application traffic analysis dashboard

Policy Enforcement Firewall with user and application visibility	
Feature	**Benefit**
Global or role-based policies	Simplicity to control all user traffic with a single command, flexibility to control exactly which users can run what apps.
Over 3,000 applications	Highly granular visibility and control.
21+ application categories	Simplify control over different types of traffic.
Enforce quality-of-service (QoS) tags	Prioritize one application over another
Block unwanted applications	Conserve bandwidth and stop unwanted activities.
Rate limits for applications or application categories	Permit non-essential traffic while preventing it from overwhelming mission critical applications.

Table 9

Remote Access Point (RAP) capabilities

With the same ArubaOS AP license, Aruba RAPs can be deployed in disparate locations such as small offices/home offices (SOHO) or temporary work sites. Each builds a hybrid IPSec/SSL VPN connection to a Mobility Controller, which takes on a dual-role as a VPN concentrator (VPNC) as well. (See Figure 3 and Table 10)

Virtual Intranet Access (VIA) VPN support

A VIA add-on license lets remote users securely connect to an Aruba network through a hybrid IPSec/SSL VPN client without the need for a dedicated VPNC in an enterprise DMZ. Users devices adhere to the same policies and service definitions used at headquarters or a branch. ArubaOS supports Windows, Mac, iOS, Android, and Linux, using split- or full-tunnel connections. (See Table 11)

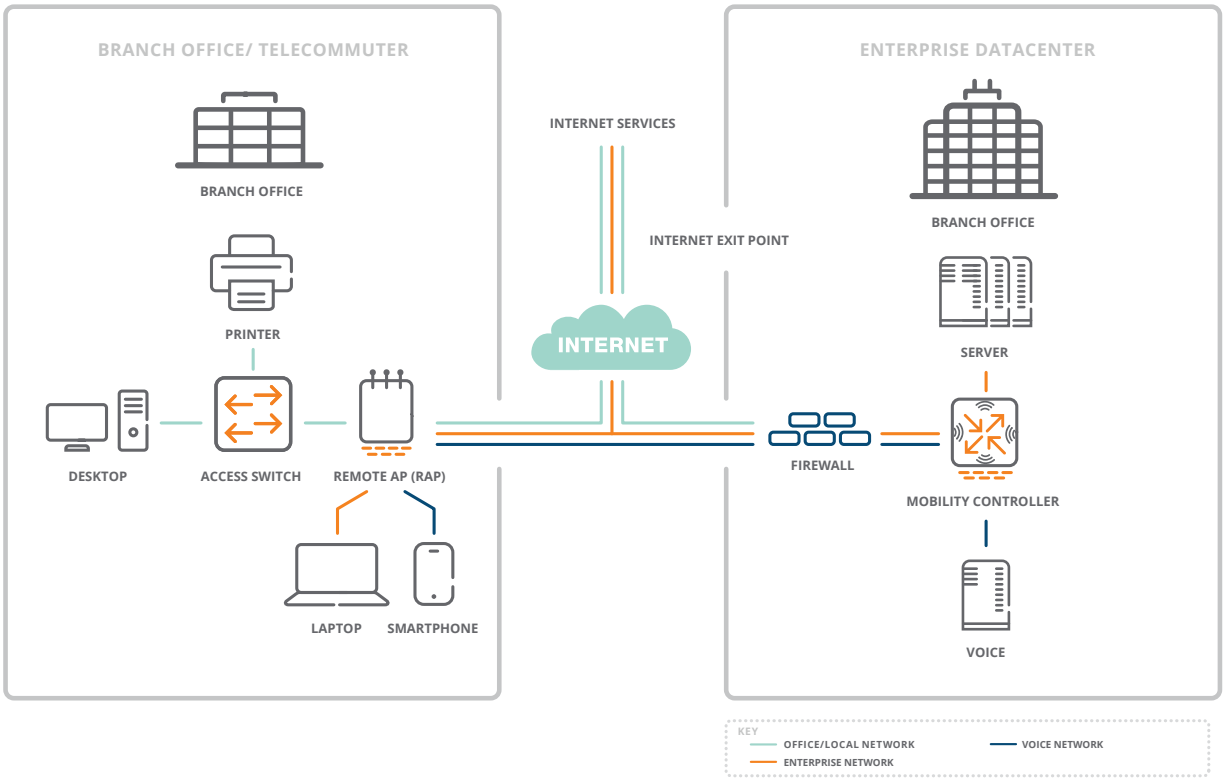


Figure 3: Aruba RAPs for secure mobile connectivity to micro-branch and small offices

Telecommuters with Remote Access Points	
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.
3G/4G LTE WAN connection	RAPs support USB wireless WAN adapters (EV-DO, HSDPA) 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.
Supported APs	RAP-3, RAP-100 series, RAP-155, AP-105, AP-220 series, AP-130 series, AP-110 series, AP-100 series, AP-90 series, AP-175 series
Minimum required link speed	64 kbps per SSID
Encryption protocol (RAP to Mobility Controller)	AES-CBC-256 (inside IPsec ESP)

Table 10

Secure VPN Connectivity for Remote Access	
Tested client support	• Aruba VIA client on Windows, Mac OS, Android, iOS, Linux • Cisco and 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

Table 11

Advanced Cryptography (ACR)

Fully FIPS 140-2 validated and Common Criteria-certified, the ACR add-on license provides Suite B cryptography which enables secure access to remote users who handle controlled unclassified, confidential and classified information.

Enhanced Wi-Fi authentication security

The addition of WPA3 support brings stronger encryption and authentication methods, and Enhanced Open provides per user encryption on open networks. New MPSK feature enables simpler passkey management for WPA2 devices – should the Wi-Fi password on one device type needs to be changed; no key changes are needed for other types of devices on the network. (See Table 1) Read the white paper.

Web classification (WebCC)

With an optional subscription, ArubaOS provides a cloud-based web content classification, policy and reputation service for URL filtering, IP reputation and geolocation filtering – which can be used to block and rate-limit connections based on Aruba's identity-based controls. (See Figure 4 and Table 12)

WIPS/WIDS and rogue AP protection

To protect against ad hoc networks, man-in-the-middle attacks, denial-of-service attacks and to distinguish between Wi-Fi and non-Wi-Fi sources, the ArubaOS RFProtect module provides integrated WIPS/WIDS/rogue AP containment and classification without requiring a separate system of RF sensors and security appliances. Aruba's rogue AP classification algorithms accurately differentiate between rogue APs connected to the network versus nearby interfering APs.

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.

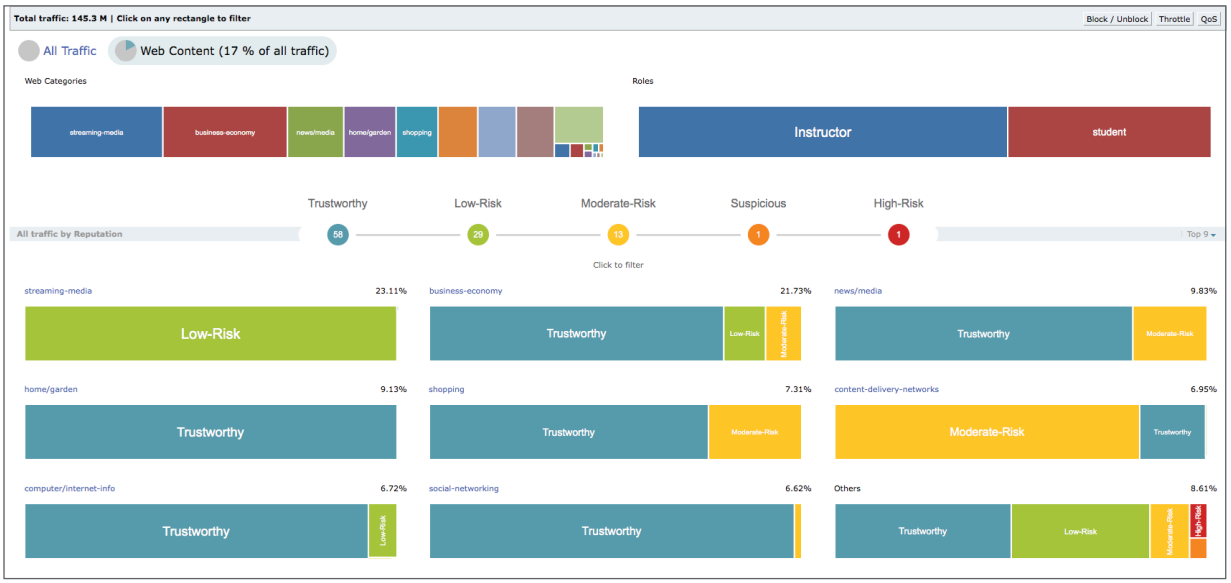


Figure 4: WebCC dashboard

WebCC features	
Categorize web traffic into 83 categories	Determine how network bandwidth is being used
Block websites by category	Enforce network acceptable use policies
QoS and bandwidth control by category	Reduce network usage of recreational applications
Block websites by reputation	Reduce the opportunity for malware to enter the network

Table 12

MICROSOFT FEATURES

Aruba's integration with Microsoft enables unique application intelligence that detects Office 365, Teams and Skype for Business traffic and then prioritizes them over less critical applications. For Skype for Business/Lync traffic, IT can also prioritize specific media such as video, voice, and messaging.

UNIFIED COMMUNICATIONS & COLLABORATION (UCC)

Integrated dashboards

With an integrated UCC dashboard, ArubaOS provides call quality metrics (latency, jitter, packet loss) for Microsoft Skype for Business/Lync, Alcatel Lucent New Office Environment (NOE), Microsoft Teams*, Apple Facetime, Cisco Jabber, Cisco Spark, Cisco Skinny Call Control Protocol (SCCP), Spectralink Voice Priority (SVP), SIP, H.323, and Vocera. This provides network managers with enhanced application visibility, as well as key Wi-Fi troubleshooting capabilities. Aruba's application fingerprinting technology also enables ArubaOS to follow encrypted signaling protocols and postpone ARM scanning and ClientMatch roaming to optimize user experience during active call sessions. (See Figure 5)

Wi-Fi Calling support

Wi-Fi Calling is used by carriers to offload cellular voice traffic on Wi-Fi networks to improve their reach inside buildings and areas of poor cellular coverage. ArubaOs treats Wi-Fi Calling as a UCC voice application and applies quality of service, blocks and throttles calls through an integrated UCC dashboard. Aruba also offers visibility on a per-user, per-device and a per-carrier basis.

WAN PERFORMANCE

Routing and metrics

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. (Figure 6)

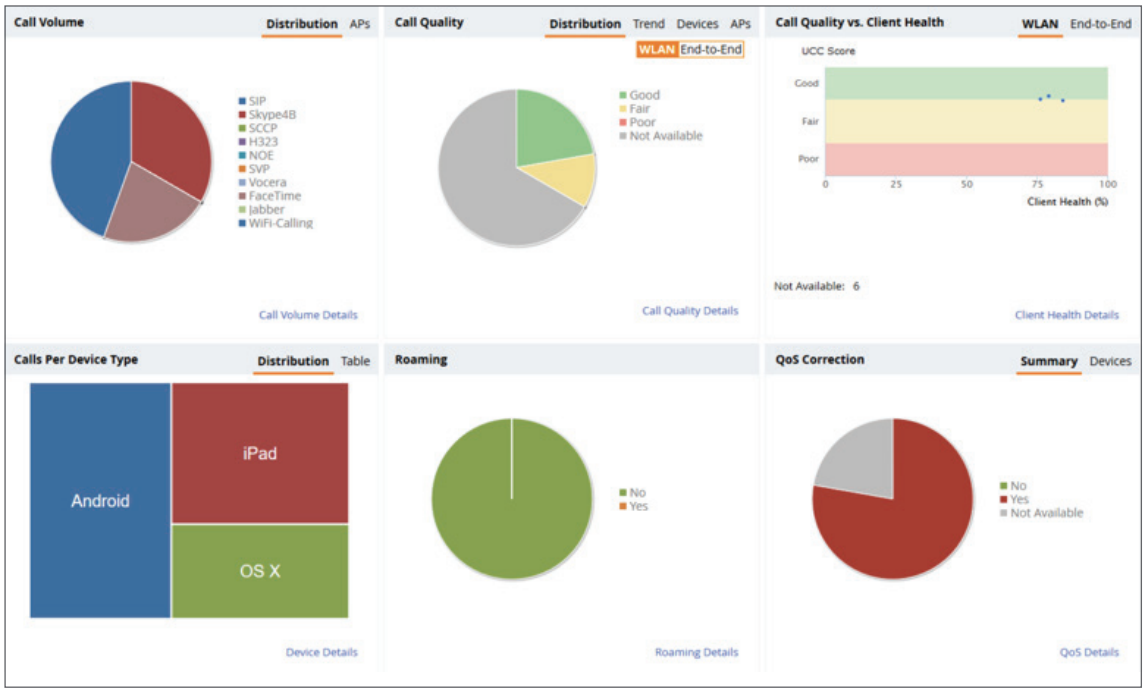


Figure 5: UCC dashboard

Figure 6: WAN dashboard

OPERATIONS

Integrated captive portal

For headless client devices or those without WPA, VPN or other security software, ArubaOS supports a web browser-based captive portal that provides secure web-based authentication. Captive portal authentication is encrypted using SSL, and can support both registered users with a login and password or guest users who supply only an email address. For advanced guest access needs, refer to Aruba ClearPass Guest.

MDNS and DLNA support (AirGroup)

Aruba improves Apple, Google, and third-party services like AirPlay, AirPrint, and Google Cast through AirGroup, a unique capability that optimizes IP multicast video traffic, prioritizes services, and adds policy controls.

Simple configuration options ensure that these client devices can see each other, while advanced options limi access to certain devices based on physical location, time of day, and user/role based details.

Point-to-point and mesh capabilities

ArubaOS supports a flexible, wire-free design for AP uplinks in the absence of fiber or cable runs. Most commonly deployed for point-to-point wireless backhaul, security camera use cases and for network access in on-premises locations, wireless mesh provides the same enterprise network services as standard wire-based design. Aruba uses an intelligent link management algorithm between each AP to automatically adjust and optimize traffic paths and links. Network managers can repurpose any Aruba indoor or outdoor AP, or utilize new 802.11ad technology for high-performance and extended range requirements. (See Figure 7 and Table 13)

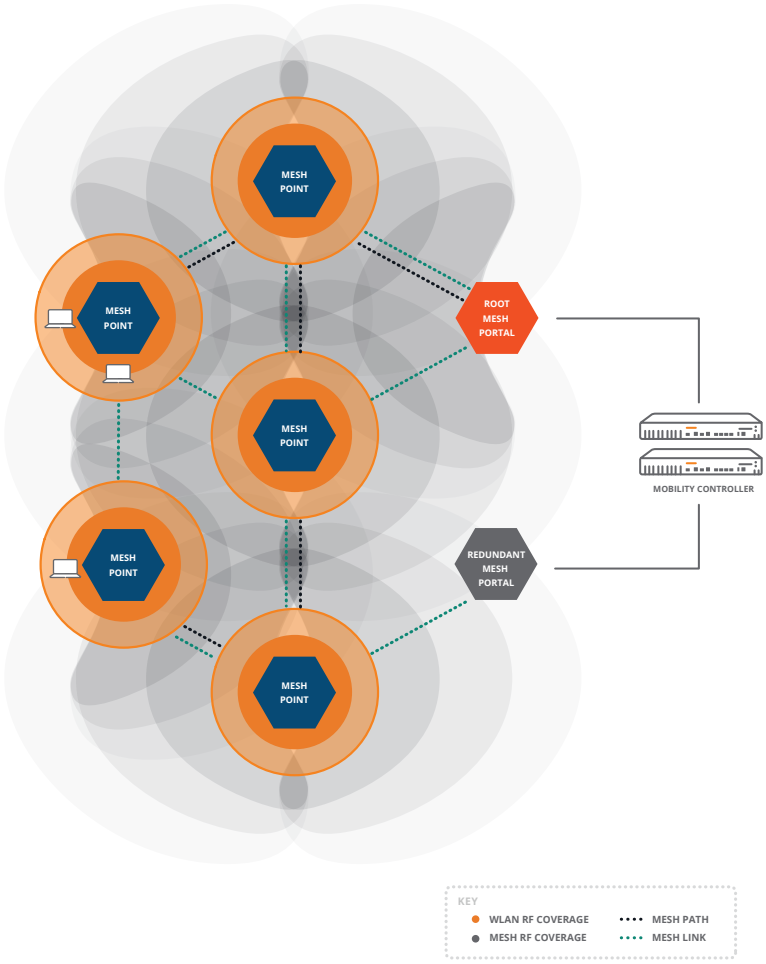


Figure 7: Secure Enterprise Mesh

Secure Enterprise Mesh	
Broad application support	Wi-Fi access, concurrent wireless intrusion protection, wireless backhaul, LAN bridging, and point-to-multipoint connectivity.
Unified network access	Integrates mesh networks with campus and branch office WLANs. Users roam seamlessly between campus and branch 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 overcomes a broken 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 AP is stolen.
Centralized management	All mesh nodes are configured and controlled centrally by Mobility Controllers. No local management is required.
Extensive graphical support tools	Full network visualization includes coverage heat maps, automatic link budget calculation, floor plans, and maps with network topology.
Standards-based design	Secure enterprise mesh based on design principles from IEEE 802.11s.

Table 13

IPv6 support

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). (See Table 14)

Multivendor network management

Aruba AirWave provides unified network management for Aruba controller managed APs and multivendor wireless, wired and WAN environments. AirWave can be used for planning and deployment to monitoring, analysis and troubleshooting. It also provides long-term trending and reporting, helpdesk integration tools and customizable alerts.

Network analytics and assurance

ArubaOS integration with Aruba NetInsight offers automated network optimization and performance enhancements. AI-powered machine learning algorithms gather data from ArubaOS, benchmarks the network against similar peer networks and recommends configuration changes as needed for RF, authentication and DHCP request performance.

Advanced policy management

ArubaOS integrates with Aruba ClearPass for policy management, AAA functions, advanced guest access and onboarding of devices across multivendor wired, wireless, and distributed remote networks. ClearPass addresses the security requirements for enterprises with increasing IoT, BYOD, and segmentation challenges. (See Table 1)

IoT and location-ready wireless support*

ArubaOS includes integration with Aruba Meridian, ALE, and third-party Wi-Fi, BLE, Zigbee and USB-based vendor solutions. Each Aruba AP serves as an IoT and location-ready gateway with no additional ArubaOS software required.

IPV6 Support	
IPV6 IPsec	Yes
Management over IPv6	GRE, SSH, Telnet, SCP, Web UI, FTP,TFTP, Syslog, SNMP
IPv6 DHCP server	Yes
Captive portal over IPv6	Yes
Support IPv6 VLAN interface address on Mobility Controller	Yes
Support AP-Mobility Controller communication over IPv6	Yes
USGv6 certified firewall	Yes

Table 14

ENHANCED MOBILITY CONDUCTOR CAPABILITIES

AI-powered RF management (AirMatch)

An RF management innovation, AirMatch automates network-wide RF channels, channel width and radio power assignment. By utilizing machine learning algorithms, AirMatch proactively learns and acclimates the network based on changing environmental conditions and system capacity. (See Table 15)

Hierarchical configuration and improved visibility

ArubaOS running on the Mobility Conductor, uses a centralized, multi-tiered architecture that consolidates all deployment models (e.g. all-conductor, single-conductor/multiple-local, and multiple-conductor/local) through a dedicated management console. Network configurations can be implemented and distributed from the Mobility Conductor through zero-touch provisioning (ZTP) to all Mobility Controllers. The Mobility Conductor also allows for licensing pools that can allocate licenses to individual controllers based on site requirements.

Hitless Failover and automated load balancing

Using Controller Clusters, user sessions and AP traffic are load balanced to optimize network utilization during peak periods and maximize availability during unplanned outages (Figure 1). 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 and multiple version support

With Mobility Conductor, ArubaOS can be upgraded while supporting active user sessions – eliminating the need for planned maintenance windows or downtime. Each Controller Cluster or individual service modules (AppRF, AirGroup, ARM, etc.) can be selectively upgraded without impacting the rest of the network.

Multi-tenancy Wi-Fi support (MultiZone)

Different controllers can be used with the same AP infrastructure to terminate different SSIDs on different Aruba controllers while maintaining complete segmentation and security for all networks, policies, management and visibility. 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. For more information, refer to the MultiZone technical brief.

Northbound APIs (NBAPI)

The Mobility Conductor includes a full set of NBAPIs that enable deep visibility into the network. NBAPIs provide RF health metrics, app utilization, device type and user data in an easy-to-integrate format. 3rd party applications can receive this information for improved visibility and monitoring.

AirMatch Benefits	
Even Channel assignment	Provides even distribution of radios across available channels, interference mitigation and maximized system capacity.
Dynamic Channel width adjustment	Dynamically adjusts between 20MHz, 40MHz and 80MHz to match the density of your environment.
Automatic transmit power adjustment	Examines the entire WLAN coverage and automatically adjusts the transmit power of APs to ensure the best coverage and user experience.

Table 15

CERTIFICATIONS

- Wi-Fi Alliance certified (802.11a/b/g/n/d/h/ac/ad, 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
- 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

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 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 802.11n 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 Bootstrap Protocol (BOOTP)
- RFC-1542 Clarifications and Extensions for the Bootstrap Protocol
- RFC 2131 Dynamic Host Configuration Protocol
- RFC 1591 DNS (client operation)
- 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 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 2660 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 and encryption

- IEEE 802.1X Port-Based Network Access Control
- RFC 1661 The Point-to-Point Protocol (PPP)
- RFC 2104 Keyed-Hashing for Message Authentication (HMAC)
- 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 3736 DHCP Services for IPv6
- 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 6106 IPv6 Router Advertisement Options for DNS Configuration
- IETF Draft RadSec – TLS encryption for RADIUS

SERVICE AND WARRANTY INFORMATION

- Hardware: 1 year parts/ labor, can be extended with support contract
- Software: 90 days, can be extended with support contract

For additional information on Aruba WLAN products, please refer to the following web pages:

Aruba Access Points

Aruba Gateways and Controllers

Aruba VPN Services

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 DEPLOYMENT

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_SK_120520 a00073441enw