DATA SHEET

ARUBAOS 6.5

The operating system designed with scalable performance

ArubaOS 6.5 is the operating system and application engine for all Aruba Mobility Controllers and controller-managed wireless LAN (WLAN) access devices. Designed for scalable performance, ArubaOS 6.5 consists of three core components.

First, a hardened, multicore, multithreaded supervisory kernel manages administration, authentication, logging and other system operation functions. This control plane is distinctly separate from the packet forwarding components to ensure continuous availability.

Second, an embedded real-time operating system powers dedicated packet-processing hardware. This highly parallel architecture includes support for high-performance deep packet inspection of every connection that traverses the controller, and implements all routing, switching and firewall functions.

Third, a programmable encryption/decryption engine built on dedicated hardware delivers client-to-core encryption for wireless user data traffic and software VPN clients.

ArubaOS 6.5 comes with an extensive set of integrated technologies and capabilities:

Aruba Clarity

Today, most mobile connectivity issues are quickly attributed to "bad Wi-Fi." Very often it may not be a wireless or RF related issue at all. However, tasked with providing the best user experience possible, IT organizations end up having to access multiple systems just to identify the problem.

With Clarity, IT organizations now have visibility into non-RF metrics (RADIUS, DHCP and DNS server), not only giving them end-to-end visibility into a wireless user experience, but also the ability to foresee connectivity issues before users are even impacted.

To find these non-RF client connectivity issues, the controller looks at all of the requests passing through and keeps track of DHCP, DNS and RADIUS response times and failure rates by linking those requests back to the servers that are responding.

In addition to looking at real traffic flowing through the network, Clarity also enables WLAN administrators to simulate traffic to identify service outages and performance issues before users experience the same. This proactive workflow can either be on-demand or scheduled across thousands of locations. Network and application level traffic can be simulated using client serving access points or air monitors to assess user experience.

ClientMatch technology

Patented ClientMatch technology eliminates sticky clients and boosts Wi-Fi client performance by continuously gathering session performance metrics from mobile devices and using this information to steer each one to the best WLAN AP and radio.

This technology also groups and steers MU-MIMO clients to the closest MU-MIMO capable access points, enabling simultaneous transmission to multiple devices and improving the overall WLAN capacity.

AppRF technology

AppRF technology, part of the optional ArubaOS Policy Enforcement Firewall (PEF) module, brings application awareness to WLANs. It uses deep packet inspection to identify enterprise, cloud and mobile apps.

It also enables IT to prioritize applications for each user and scales for BYOD transaction and device density. The PEF module also provides critical identity-based controls to enforce application security and prioritization.

WebCC Bundle

The WebCC Bundle is a separate subscription which includes URL filtering, IP reputation and geolocation which provides the visibility and control that's essential to identify how users spend their time online. This enables IT administrators to reduce or eliminate inappropriate or malicious web traffic from enterprise networks.

WebCC gives IT administrators critical insight into the risks of malware, phishing, and other security problems associated with Internet usage, and provides the vital tools to block dangerous content.

AirGroup technology

AirGroup makes it easy to share Apple TVs, printers, Google Chromecast, and other mDNS-advertised devices across subnets. Simple configuration options ensure that all devices can see each other while advanced options reduce the scope of sharing based on physical location, time of day, role and self-provisioned sharing islands.

Adaptive Radio Management (ARM) technology

ARM dynamically optimizes Aruba WLAN access points (APs). By ensuring radios stay clear of RF interference and dynamically adjust their transmission power, ARM creates a more reliable and higher-performing WLAN infrastructure in constantly-changing RF environments.

Integrated threat protection

To protect network resources from wireless threats, ArubaOS 6.5 integrates the industry's leading rogue AP containment and classification solution that can be deployed with or without dedicated RF sensors.

For the ultimate in RF security, the ArubaOS RFProtect module integrates wireless security into the network infrastructure without requiring a separate system of RF sensors and security appliances and enables government-grade wireless intrusion protection.

RFProtect also includes powerful Spectrum Analyzer capabilities, which provide a critical layer of visibility into non-802.11 sources of RF interference and their effects on WLAN channel quality. It eliminates wireless threats and interference, while optimizing network performance

Advanced cryptography

The ArubaOS Advanced Cryptography (ACR) module brings military-grade Suite B cryptography to Aruba Mobility Controllers, enabling user mobility and secure access to networks that handle sensitive, confidential and classified information.

Approved by the U.S. National Security Agency (NSA), Suite B improves performance, eliminates unwieldy workflows and strict handling requirements, allows interoperability, and supports commercially available mobile devices – all at a fraction of the cost of previous-generation cryptographic methods.

Virtual Intranet Access (VIA) client

VIA is a free hybrid IPsec/SSL VPN that automatically scans and selects the best secure connection to the corporate network. Unlike traditional VPN software, VIA offers a zero-touch end-user experience and automatically configures WLAN settings on client devices.

VIA is completely Wi-Fi-aware. From a non-corporate network – a home Wi-Fi, 3G or public Wi-Fi hotspot – VIA automatically launches a VPN-on-demand connection to a centralized Mobility Controller. Connectivity and authentication occur transparently with no complicated logins.

Wi-Fi Calling

As Wi-Fi calling becomes more prevalent, we need to prepare our internal Wi-Fi and re-evaluate Wi-Fi network design, handoffs, QoS, and RF coverage goals. ArubaOS 6.5 improves indoor Wi-Fi coverage and applies quality of service, blocks or throttles calls and gives visibility into client health- providing a carrier-grade voice experience for customers.

In addition to enhancing high quality of service Aruba also offers visibility into Wi-Fi calling on a per-user, per-device and a per-carrier basis.

ENABLING A UNIFIED ACCESS FRAMEWORK

Older access layer networks were not built for the mobility and security requirements of today's distributed enterprises. Traditionally, networks were built with a focus on Ethernet ports and physical locations, rather than the user or device connecting to the network.

Consequently, the addition of secure mobility to such networks becomes overly complex and costly, often requiring large-scale equipment upgrades.

Aruba allows any user, regardless of physical location, whether wired or wireless, to securely access the enterprise network with an always-on, consistent experience.

Uniform security and access policies are applied to users in headquarters, branch offices, home offices, and on the road. Users and devices join the network through simple lightweight access devices or software, which securely and automatically connect to Mobility Controller.

Powered by ArubaOS 6.5, Mobility Controllers manage Aruba access devices and access software. They also manage software images, configurations and user connection states, and enforce policies.

The entire infrastructure – wireless and wired – is controlled through a single pane of glass by Aruba AirWave, which lets IT manage the application and device experience of users across several generations of multivendor networks.

With visibility into everything that affects wireless and mobility service-level agreements (SLAs), AirWave lets you proactively plan for capacity, visualize client performance and troubleshoot application issues before you get a helpdesk ticket.

FLEXIBLE AND ADAPTABLE DESIGN

Network design with Aruba is not a one-size-fits-all approach. Some organizations need pervasive Wi-Fi, while some are purely wired. Branch offices have different requirements than corporate headquarters.

And within a corporate campus, some organizations value a centralized traffic forwarding model where all network traffic flows to the data center, while other organizations need a more distributed approach. The incredible flexibility of ArubaOS lets it adapt to the unique needs of any organization.

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

ENTERPRISE SECURITY FRAMEWORK

To secure the enterprise network, ArubaOS performs authentication, access control, and encryption for users and devices.

With Aruba's architecture, authentication is standard and can be implemented for wired and wireless networks. For wired, 802.1X is the standard for authentication. For wireless, 802.1X is one component of the WPA2 and 802.11i protocols widely recognized as state-of-the-art for Wi-Fi security.

ArubaOS uniquely supports AAA FastConnect, which allows the encrypted portions of 802.1X authentication exchanges to be terminated on the Mobility Controller, allowing it to federate between different identity stores, including RADIUS and LDAP. Supporting PEAP-MSCHAPv2, PEAP-GTC, and EAP-TLS, AAA FastConnect removes the requirement for external authentication servers to be 802.1X-capable.

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, and can support both registered users with a login and password or guest users who supply only an email address.

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.

APPLICATION-AWARE MOBILITY FIREWALL

The ArubaOS PEF license enhances user-centric security, application visibility, and control. It brings the power of a next-generation mobility firewall to the wireless edge, where most users traffic first touches the network. It uses DPI to classify and optimize traffic for over 1,500 apps and gives you full traffic visibility through a simple dashboard.

PEF simplifies and enhances access security by adding full identity-based security with integrated firewall controls applied on a per-user basis at the wireless edge. This allows ArubaOS to create a security perimeter around each user or device, tightly controlling how that user or device may access enterprise network resources.

The VLAN a user is assigned is no longer important – roles are applied to users based on their role. Roles can be derived in many different ways, based on RADIUS attributes, Active Directory membership, device type, and many other factors.

In addition to traditional Layer 4 access technology, PEF includes AppRF technology. AppRF brings application awareness and control to the WLAN. By providing visibility into the types of traffic running on the Wi-Fi network, AppRF allows administrators to understand what user traffic is consuming the vital air resource.

AppRF also provides unprecedented control over that traffic, allowing flexible and powerful controls that allow administrators to pick which traffic is permitted in the air, by which users, and at what priority. AppRF uses a powerful concept called Application Categories to enable control over entire types of traffic, such as streaming media or social media, with a single command.

If the PEF license is not activated, a user or device can be mapped to a particular VLAN based on the port or wireless SSID. Once the user has been mapped to a particular VLAN, external firewall systems or routers can be used to provide basic access controls.

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 1,500 applications	Highly granular visibility and control.
19 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.

WEBCC SUBSCRIPTION BUNDLE

Web content is another important part of the security puzzle. More and more applications are now nothing more than web sites. And more and more malicious web sites are appearing on the Internet every day.

Since the web has become an essential yet dangerous place, we want to be able to quickly determine the type of sites users are visiting and gauge the relative threat that these sites pose to the network and its users.

In order to do that in the most accurate and up-to-date way possible, ArubaOS offers an optional subscription for URL filtering, IP reputation, geolocation, which can be used to block and rate limit with appropriate policies.

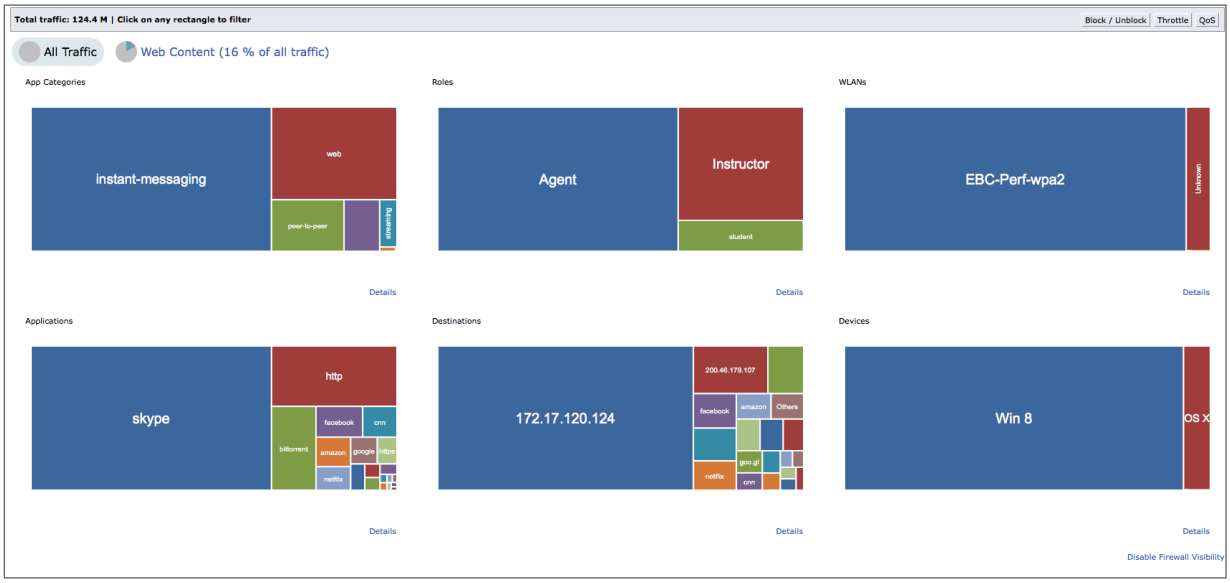
These URLs are then looked up in a locally-cached database that contains commonly used and recently accessed web sites. If the user's site is not on the list, the Mobility Controller makes a request for the category, classification and reputation of the web site from the service. This cloud service is continuously updated.

Each web site is classified according to the type of content it serves and the reputation of the web site. Content captures the spirit of the site, such as news, gambling, adult or social media. Web Reputation captures the likelihood that a user visiting the webs ite will be the victim of a malware attack or phishing scam.

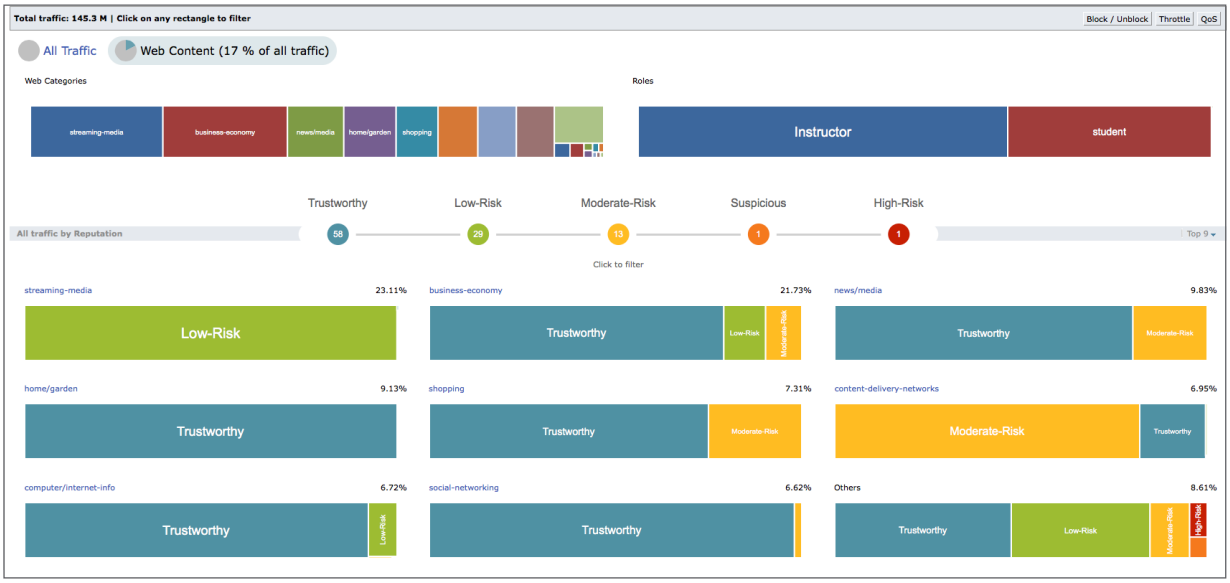
WebCC stats:

- 600+ million domains and 27+ billion URLs classified
- 83+ site categories, including high risk categories
- 45+ languages
- 12 million dangerous IPs correlated with URLs

Also the Geo-location filtering allows to associate source / destination IP addresses with location. PEF can be leveraged to apply policies to permit or drop inbound or outbound communications with certain countries.



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



AIRGROUP

Mobile devices, smart TVs, video game consoles, and set top boxes were all designed primarily to be used in small home networks.

AirGroup technology makes it incredibly easy for these devices to wirelessly print and share media that leverage UPnP®, DLNA®, AirPrint™ and AirPlay® technology. It also provides QoS and policy enforcement to control resource sharing based on group, user, role, time and location.

Typical use cases that are solved by AirGroup include:

- Enables users to discover network services across IP subnet boundaries in wireless and wired networks.
- Allows users to access conference room Apple TVs during presentations using group-based access privileges.
- Identifies AirPrint-enabled printers and enables user access based on location.
- Teachers can project to an Apple TV in a classroom using a laptop or iPad, while student access is prevented.
- Students get exclusive access to Apple TVs in their dorm rooms based on personal access privileges, while access by other residents is not allowed.

ARCHITECTED FOR SEAMLESS MOBILITY

Enterprise users increasingly require network access while moving from location to location, whether from a classroom to a library, a cubicle to a conference room, from headquarters to a branch office, or from the office to a user's home.

For Wi-Fi networks, ArubaOS provides seamless connectivity as users move throughout the network. With roaming handoff times of 2-3 milliseconds, delay-sensitive and persistent applications such as voice and video experience uninterrupted performance.

ArubaOS integrates proxy mobile IP and proxy DHCP functions letting users roam between subnets, ports, APs, and controllers without special client software. This ensures seamless performance even when users wander far afield of the AP to which they initially connected as they move throughout the network doing their jobs.

VLAN pooling is another powerful access edge feature that simplifies network design. Instead of pulling VLANs to the network edge, they are centralized in the Mobility Controller and tunneled to APs.

This has major advantages, including reducing network configuration complexity and spanning tree diameter. User membership of VLANs is load-balanced to maintain optimal network performance as large groups of users move about the network.

Aruba's unified access approach also extends the enterprise to remote locations, over private WANs or using the public Internet, giving users the same access experience regardless of location.

To connect users who are away from enterprise network infrastructure, Mobility Controllers operate as standard VPN concentrators, linking remote users through the same access and security framework as other enterprise users.

With Aruba, there is no need to build separate access networks for each work location – the company's unified access approach treats all locations the same.

Fast roaming	• 2-3 msec intra-controller • 10-15 msec inter-controller
Roaming across subnets and VLANs	Sessions do not drop as clients roam 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

ENTERPRISE-GRADE ADAPTIVE WLANS

Aruba's ARM technology takes the guesswork out of AP deployments. Once APs are brought up, they immediately begin monitoring their local environment for interference, noise, and signals being received from other Aruba APs. This includes detection of other APs or Wi-Fi networks and the channels they are using.

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 802.11ac has been deployed with mixed VHT20, VHT40 and VHT80 channel types.

Users expect high-performance Wi-Fi, even in crowded areas like lecture halls. Advanced ARM features take care of this by dynamically adapting the infrastructure to ensure optimal network performance in the toughest high-density heterogeneous Wi-Fi client environments.

ARM ensures high performance and multi-media QoS through techniques such as band steering, which moves dual-band clients out of the crowded 2.4-GHz band, and airtime performance protection, which prevents slower clients from bringing down performance of the entire network.

Finally, in areas with dense AP coverage, ARM ensures the optimal use of each channel through automatic channel load balancing and co-channel interference mitigation.

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

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

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

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

ArubaOS collects aggregate and raw wireless statistics on a per station, per channel and per user basis. Statistics can be recorded and analyzed through the AirWave management platform, and are also available via SNMP for easy integration with third-party management and analysis applications.

Live packet capture is available that can turn any Aruba AP or air monitor into a packet capture device, able to stream real-time 802.11 frames back to monitoring stations such as WireShark or WildPackets OmniPeek. With this detailed information, administrators can quickly troubleshoot user problems, determine top wireless talkers and diagnose congested APs.

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

Once classified as rogue, these APs can be automatically disabled through the wireless and wired network. Administrators are also notified of the presence of rogue devices, along with their physical location on a floor plan, so they can be promptly removed from the network.

Rogue AP classification and containment is available within base ArubaOS and does not require additional Mobility Controller licensing.

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

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

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

ArubaOS includes advanced location visualization and tracking of 802.11 devices. RF signature-based location triangulation allows administrators to physically locate any 802.11 user or device within one meter of accuracy.

With Aruba's real-time location tracking (RTLS), devices are simultaneously and continuously located and tracked. Device location can be displayed on building floor plans through the AirWave management platform or linked to outside systems through a simple API.

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.

HIGH AVAILABILITY

Today, modern Wi-Fi networks are more essential to businesses than traditional wired Ethernet networks. Therefore, ArubaOS has a robust set of high-availability capabilities designed to minimize downtime in the unlikely event of a Mobility Controller failure.

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.

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.

REMOTE NETWORKING FOR BRANCH OFFICES AND TELEWORKERS

Aruba remote networking solutions provide a simple, secure, and cost-effective way to extend the corporate network to branch offices, clinics, SOHOs, stores and telecommuters.

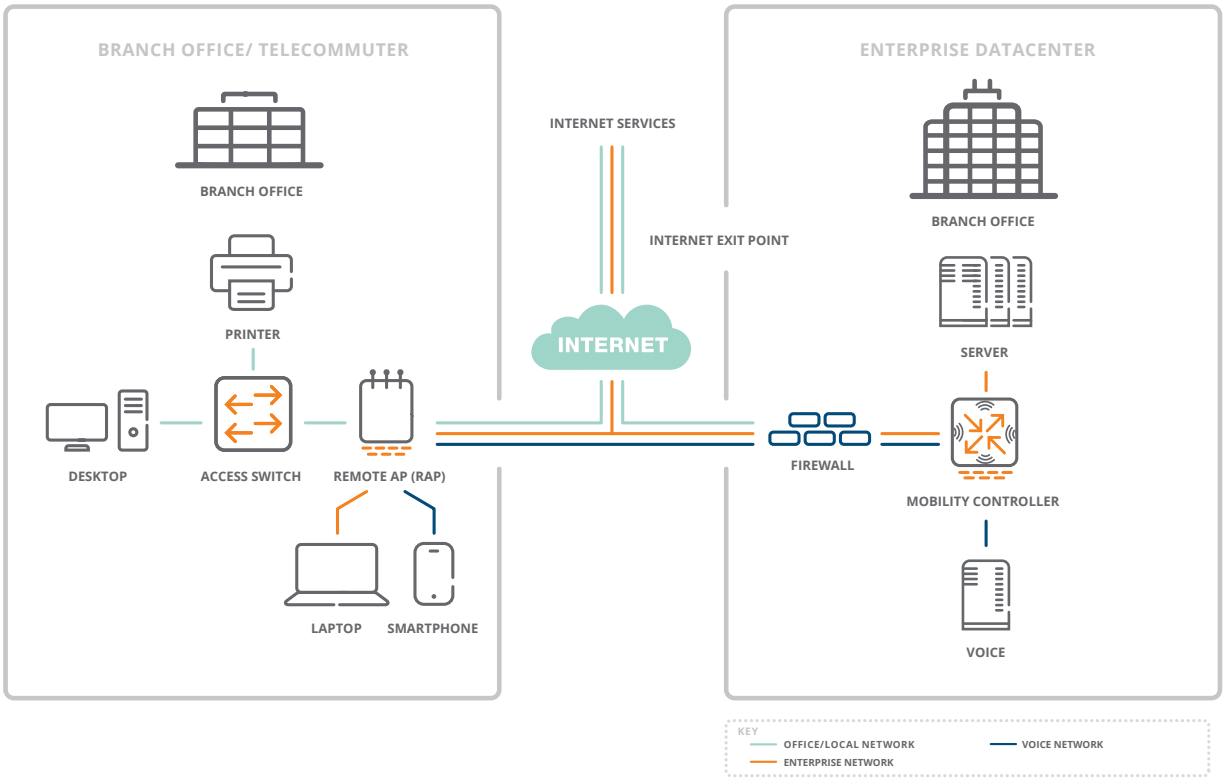
Traditional remote networking solutions replicate routing, switching, firewall, and other services at each remote location. Managing and controlling user access to network services, applications, and resources requires proliferating ports, subnets, and VLANs – effectively creating multiple networks at each site. This is costly and complex to deploy and maintain.

Whether supporting branch offices of one or one hundred users, Aruba delivers full-service networking without compromises. As the head-end component of the remote networking solution, data center-based Mobility Controllers handle all complex configuration, management, software updates, authentication, intrusion detection, and remote site termination tasks.

Branch and remote network services are virtualized in the data center controllers and then extended over any public or private IP network to the Mobility Controllers (MCs) for branch networks, and affordable Remote Access Points (RAPs) for remote users to provide secure connectivity and services.

MOBILITY CONTROLLERS AS BRANCH GATEWAYS	
Zero-touch provisioning	Administrators can deploy CSCs without any pre-configuration. IT can simply factory-ship each CSC directly from the manufacturer to a remote site with cloud-based Aruba Activate™
Wired and wireless	Users connect to CSCs via wired Ethernet, Wi-Fi, or both.
Dedicated WAN Dashboard	Increase your visibility of branch WAN details only on the 7000 series
Flexible authentication	802.1x, captive portal, MAC address authentication per-port and per-user
Centralized management and optional policy enforcement	No local configuration is performed on APs – Configuration and management are done by the Mobility Controller and/or AirWave Network Management, and optional ClearPass Policy Manager
WAN Optimization (Compression)	Compression is enabled on Site2Site tunnels, and enabled on all 7000 and 7200 series Mobility Controllers, except the 7205, to maximize data transfer
WAN health checks and bandwidth contracts	Analyze latency, jitter, throughput, and MOS on each uplink, and limit traffic for individual applications or categories
Multiple WAN uplinks	Designed for hybrid WAN or WAN redundancy, CSCs can support dual-Ethernet uplinks and 3G/4G LTE, or connect to an existing private circuit
Policy-based Routing	On each uplink interface, forward packets through an IPsec tunnel defined by the specified IPsec map, a device on a nexthop list or multiple lists, GRE tunnel, or tunnel group
Per port App Visibility	Application awareness with Deep Packet Inspection is provided by AppRFTM for over 2,000 individual applications and application categories

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)



Aruba RAPs provide secure mobile connectivity to branch and home offices.

SIMPLE, SECURE CONNECTIVITY FOR TRAVELING PROFESSIONALS

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

With Aruba, remote VPN users are treated like any other user. They leverage the same access policies and service definitions used at headquarters or a branch office RAP deployment. Mobility Controllers act as VPN concentrators, eliminating the need for a parallel access infrastructure.

ArubaOS is compatible with several popular VPN clients and the VPN clients built into major client operating systems. It also provides the optional VIA client, which can be installed on Android, iOS, Mac OS X and Windows devices.

By merging access networks together, policy and access configuration is unified, the user experience is improved, helpdesk calls are reduced, and IT expenses are lowered.

Tested client support	• Aruba VIA client on Windows • Cisco 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

SECURE ENTERPRISE MESH

The Aruba secure enterprise mesh solution provides a flexible, wire-free design allowing APs to be placed wherever they are needed – indoors and outdoors. The absence of fiber or cable runs significantly reduces network installation costs and requires fewer Ethernet ports.

The solution fully integrates with the Aruba unified access framework, enabling a single, enterprise-wide network wherever users roam. The secure enterprise mesh is based on programmable software and does not require specialized hardware; any Aruba indoor or ruggedized outdoor 802.11n AP can function as a mesh AP.

The secure enterprise mesh can support all enterprise wireless needs including Wi-Fi access, concurrent wireless intrusion protection, wireless backhaul, LAN bridging, and point-to-multipoint connectivity, all with a single common infrastructure.

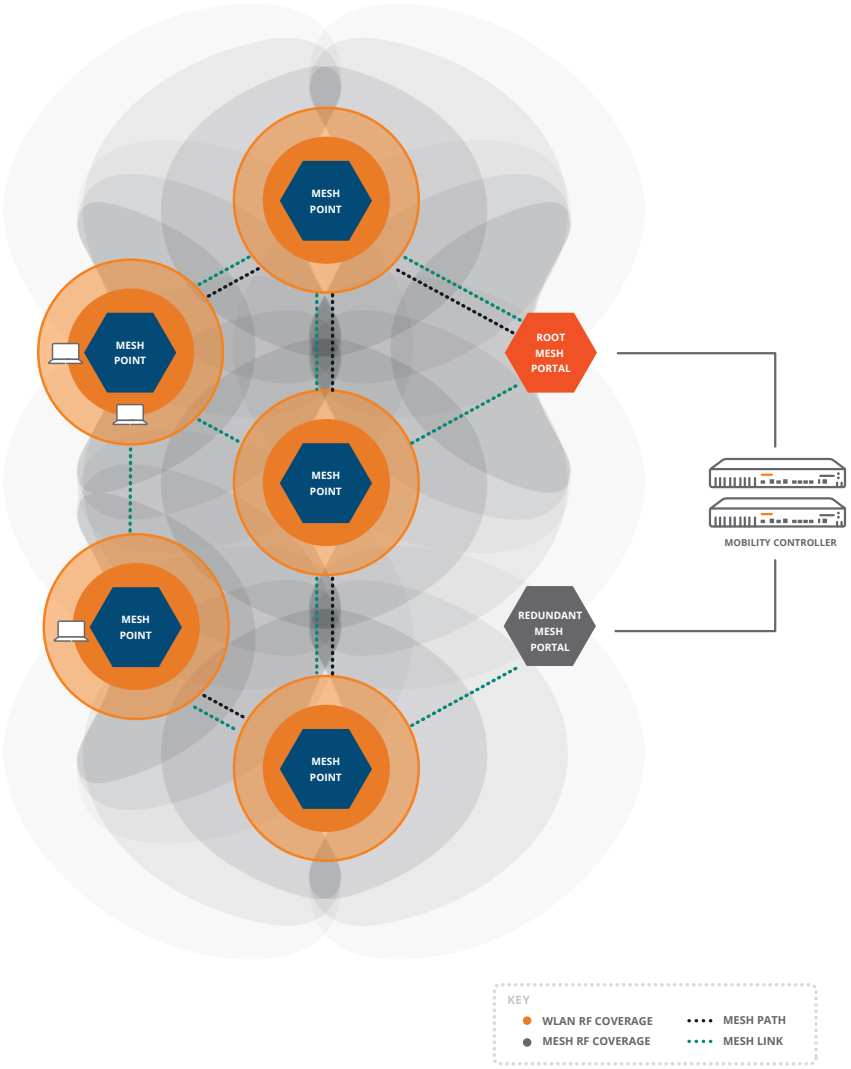
This is an excellent solution for connectivity applications, including inter-building connectivity, outdoor campus mobility, wire-free offices, and wire-line back-up; security applications, such as video and audio monitoring, alarms and duress signals, and industrial applications and sensor networks.

Through cooperative control technology, Aruba uses an intelligent link management algorithm to optimize traffic paths and links.

Mesh APs communicate with their neighbors and advertise a number of RF and link attributes – such as link cost, path cost, node cost, loading – that allow them to make intelligent selection of the best path to take for the application.

Mesh paths and links automatically adjust in the event of high-loads or interference. Further, application tags for voice and video traffic are shared to ensure latency sensitive traffic is prioritized over data.

The cooperative control technology also provides self-healing functionality for the mesh network in the event of a blocked path or AP failure.



Broad application support	Wi-Fi access, concurrent wireless intrusion protection, wireless backhaul, LAN bridging, and point-to-multipoint connectivity.
Unified 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.

MANAGEMENT, CONFIGURATION AND TROUBLESHOOTING

Mobility Controller configuration, management, and troubleshooting are provided through a browser-based GUI and a command line interface that will be familiar to any network administrator.

ArubaOS also integrates with AirWave, which eases management during all stages of the WLAN lifecycle – from planning and deploying to monitoring, analyzing and troubleshooting. AirWave also provides long-term trending and analysis, helpdesk integration tools, and customizable reporting.

All APs and Mobility 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.

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

Web-based configuration	Allows any administrator with a standard web browser to manage the system.
Command line	Console 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 master 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.

ARUBAOS SUPPORT FOR IPV6

With the depletion of available IPv4 addresses, organizations are now planning for or have already begun deployments of IPv6 within their networks.

While IPv4 and IPv6 both define how data is transmitted over networks, IPv6 adds a much larger address space than IPv4 and can support billions of unique IP addresses.

As organizations transition from IPv4 to IPv6, network equipment must support dual-stack interoperability of IPv6 within an IPv4 network or full deployments within a pure IPv6 environment.

ArubaOS facilitates the deployment of Mobility Controllers and APs in today's IPv6 and dual-stack environments. Nearly all functions with the exception of IPsec can be deployed in native IPv6 mode. Every aspect of management, monitoring, and firewalling are fully IPv6-aware.

ArubaOS also has a built-in IPv6 DHCP server.

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

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.

With the addition of the Aruba PEF module, voice-over-IP protocols – including Lync, session initiation protocol (SIP), Spectralink Voice Priority (SVP), Alcatel New Office Environment (NOE), Vocera and skinny call control protocol (SCCP) – are followed within the Aruba Mobility Controller. Aruba's application fingerprinting technology enables Mobility Controllers to follow encrypted signaling protocols.

Once these streams are identified, Aruba WLANs prioritize them for delivery on the wireless channel and trigger voice-related features.

These voice-related features can include commands like postpone ARM scanning for the duration of a call and prioritize roaming for clients that are engaged in an active call. This is critical to enabling the large-scale deployment of enterprise voice communications over Wi-Fi.

Additionally, ArubaOS now includes device fingerprinting technology, allowing network administrators to assign network policies on device types in addition to applications and users. Device fingerprinting delivers greater control over which devices are allowed to access the network and how these devices can be used.

ArubaOS can accurately identify and classify mobile devices such as the Apple iPad, iPhone, or iPod as well as devices running the Android or BlackBerry operating systems. This information can be shared with AirWave for enhanced network visibility for all network users, regardless of location or mobile device.

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

CERTIFICATIONS

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

STANDARDS SUPPORTED

General switching and routing

- RFC 1812 Requirements for IP Version 4 Routers
- RFC 1519 CIDR
- RFC 1256 IPv4 ICMP Router Discovery (IRDP)
- RFC 1122 Host Requirements
- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 894 IP over Ethernet
- RFC 1027 Proxy ARP
- RFC 2236 IGMPv2
- RFC 2328 OSPFv2

- RFC 2338 VRRP
- RFC 2460 Internet Protocol version 6 (IPv6)
- RFC 2516 Point-to-Point Protocol over Ethernet (PPPoE)
- RFC 3220 IP Mobility Support for IPv4 (partial support)
- RFC 4541 IGMP and MLD Snooping
- IEEE 802.1D-2004 – MAC Bridges
- IEEE 802.1Q – 1998 Virtual Bridged Local Area Networks
- IEEE 802.1w – Rapid Spanning Tree Protocol

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

a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com