

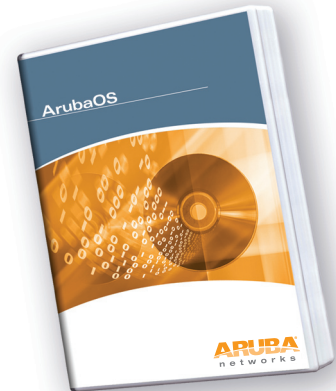


ARUBAOS MOBILITY - SOFTWARE

Die ArubaOS Software-Suite dient als Betriebssystem und Anwendungs-Engine für alle Aruba Mobility Controller sowie als Hauptkomponente für die Implementierung benutzerzentrierter Netzwerke. ArubaOS bietet standardmäßig für jeden Aruba Mobility Controller uneingeschränkte Kontrolle über das gesamte mobile Netzwerk und errichtet die einzigartigen adaptiven Drahtlosnetzwerke mit den identitätsorientierten Sicherheitsfunktionen und Application Continuity Services von Aruba.

Das Basispaket von ArubaOS umfasst Funktionen für die intelligente Authentifizierung und Verschlüsselung und bietet Schutz gegen nicht autorisierte drahtlose Access Points. Zudem beinhaltet es uneingeschränkte Mobilität durch Fast Roaming, adaptive Funkverwaltung, Analyse-Tools, zentrale Konfiguration, Standortverfolgung und vieles mehr.

Darüber hinaus sind optionale Zusatzmodule für erweiterte Funktionen verfügbar wie z. B. Wireless Intrusion Protection (WIP), identitätsorientierte Sicherheitsfunktionen mit benutzerzentrierter Gewährleistung von Richtlinien, mobile Network Access Control (NAC), sicherer Fernzugriff sowie verbesserte Technologien für die Netzwerkkonnektivität. Diese ArubaOS-Module umfassen Wireless Intrusion Protection, Policy Enforcement Firewall, VPN-Server, Remote Access Points, externe Dienstschnittstellen, Voice Services, Wireless Mesh und die erweiterte Layer 2-Verschlüsselung xSec.



SICHERE AUTHENTIFIZIERUNG, VERSCHLÜSSELUNG UND ZUGRIFFSSTEUERUNG

- 802.1x-Authentifizierung mit WPA, WPA2 und 802.11i
- AAA FastConnect™ für hardwarebasierte Beschleunigung und lokale Verarbeitung der 802.1x-Authentifizierung
- Programmierbare hardwarebasierte, zentralisierte Verschlüsselungs-Engine für geschützte Verbindungen zwischen Clients und Datenzentren
- Webbasiertes Captive Portal für browserbasierte SSL-Authentifizierung
- Automatische Erkennung, Klassifizierung und Eindämmung nicht autorisierter Access Points

UNEINGESCHRÄNKTE MOBILITÄT

- Roaming-Zeiten von 2–3 Millisekunden ermöglichen extrem schnelle Übergaben für verzögerungsempfindliche Anwendungen.
- Durch Proxy Mobile IP und Proxy DHCP können sich Benutzer frei zwischen Access Points und Mobility Controllern bewegen.

FUNKVERWALTUNG, FUNKPLANUNG UND FEHLERBEHEBUNG

- Adaptive Radio Management (ARM) für einfache Selbstkonfiguration aller Funkparameter mit dynamischer Interferenzvermeidung
- RF-Live für Echtzeitüberwachung und -anzeige der Funkabdeckung und -interferenzen
- Automatische Erstellung, Planung und Platzierung von Access Points und Funkbildschirmen entsprechend den jeweiligen Kapazitäts-, Abdeckungs- und Sicherheitsanforderungen
- Packet Capture-Tools für detaillierte Aufnahmen der gesamten drahtlosen Netzwerkumgebung

NETZWERKVERWALTUNG UND HOHE VERFÜGBARKEIT

- AZentrale Steuerung und Verwaltung aller Mobility Controller und Access Points über eine einzige Konsole
- Redundante Controller-Arrays mit VRRP
- Automatische Funkfehler toleranz zur Vermeidung von Funklöchern und zur Erstellung von Access Point-Backups

QOS, VOIP-UNTERSTÜTZUNG UND STANDORTVERFOLGUNG

- 802.11e-, WMM- und 802.1p-Unterstützung
- Automatisches Mapping von WMM-Prioritäten für 802.1p und IP-DSCP
- Lokalisierung jedes beliebigen 802.11-Geräts mit Echtzeitbildschirm

SICHERE AUTHENTIFIZIERUNG, VERSCHLÜSSELUNG UND ZUGRIFFSSTEUERUNG

ArubaOS bietet marktführende Lösungen zur Sicherung von Datenverkehr, Geräten und Benutzerdaten im mobilen Unternehmensnetzwerk. Diese unterstützen eine Vielzahl von Authentifizierungsmethoden einschließlich der Industriestandard-Protokolle WPA2 und 802.11i, die derzeit als aktuelle Sicherheitsstandards für Drahtlosnetzwerke anerkannt sind. ArubaOS verfügt über die neueste Layer 2-Verschlüsselungstechnologie. Dank des programmierbaren Hardware-Verschlüsselungsprozessors lässt sich der Aruba Mobility Controller zudem aufrüsten, um zukünftige Verschlüsselungsstandards zu unterstützen.

ArubaOS unterstützt als einzige Software AAA FastConnect™, wodurch die verschlüsselten Teile des 802.1x-Authentifizierungsaustausches bis zum Mobility Controller reichen, der mit Hilfe der Hardware-Verschlüsselungs-Engine von Aruba eine deutlich erhöhte Skalierbarkeit und Performance erzielt. Dank der Unterstützung von PEAP-MSCHAPv2, PEAP-GTC sowie EAP-TLS müssen externe Authentifizierungs-Server durch AAA FastConnect nicht mehr 802.1x-fähig sein. Zudem wird die Skalierbarkeit dieser Server durch die Verarbeitung mehrerer hundert Authentifizierungsanfragen pro Sekunde deutlich erhöht.

ARUBAOS MOBILITY SOFTWARE

Für Clients ohne WPA, VPN oder einer anderen Sicherheitssoftware unterstützt Aruba ein webbasiertes Captive Portal mit einer sicheren browserbasierten Authentifizierung. Die Captive Portal-Authentifizierung ist SSL-verschlüsselt (Secure Sockets Layer) und unterstützt sowohl registrierte Benutzer mit Benutzernamen und -kennwort als auch Gäste, die nur über eine E-Mail-Adresse verfügen. Dank des integrierten GuestConnect-Systems von Aruba bietet Captive Portal eine sichere Zugangslösung für Gäste, da das Frontdesk-Personal in der Lage ist, Authentifizierungsberechtigungen für Besucher auszustellen und zu verfolgen.

Zum Schutz gegen nicht autorisierte drahtlose Geräte kann das System mit Hilfe von Klassifikationsalgorithmen für unerwünschte Access Points genau zwischen bedrohlichen, unerwünschten Access Points im lokalen Netzwerk und benachbarten interferierenden Access Points unterscheiden. Sobald ein Access Point als nicht autorisiert eingestuft wurde, kann dieser automatisch sowohl über die drahtlosen als auch über die drahtgebundenen Netzwerke deaktiviert werden. Administratoren werden darüber hinaus auch über das Vorhandensein dieser Geräte informiert, wobei hier zur einfacheren Lösung des Problems auch deren exakte Position auf einem Grundriss angezeigt wird.

UNEINGESCHRÄNKTE MOBILITÄT

ArubaOS gewährt Benutzern im gesamten Netzwerk uneingeschränkte drahtlose Konnektivität. Durch Roaming-Zeiten von 2–3 Millisekunden werden verzögerungsempfindliche Sprach- und Video-Anwendungen mit hohem Durchsatz unterbrechungsfrei ausgeführt. ArubaOS vereint Proxy Mobile IP- und Proxy DHCP-Funktionen, so dass sich Benutzer ohne spezielle Client-Software frei zwischen Subnetzen, Access Points und Controllern bewegen können. Die Mobilitätsfunktionen von Aruba sind mit allen Access Points von Drittanbietern kompatibel. VLAN-Pooling reguliert das Nutzeraufkommen im VLAN per Lastverteilung, so dass auch bei einer großen Anzahl von Netzwerkbenutzern eine optimale Netzwerkperformance gewährleistet wird.

FUNKVERWALTUNG, FUNKPLANUNG UND FEHLERBEHEBUNG

Die Adaptive Radio Management-Funktion (ARM) von Aruba ermöglicht eine präzise geplante Aufstellung von Access Points.

Sobald ein Access Point aufgestellt wurde, beginnt dieser, die lokale Umgebung nach Interferenzen und Signalen von anderen Aruba-Access Points zu scannen. Die entsprechenden Informationen werden an den Mobility Controller gesendet, der die optimale Kanalzuweisung und die Leistungsstufen für die einzelnen Access Points im Netzwerk festlegt. Sobald das Netzwerk eingerichtet ist, werden mit Hilfe der RF-Live-Funktion von Aruba auf dem Farbbildschirm in Echtzeit Signalstärke, Funkabdeckung sowie Interferenzen der Funknetzumgebung angezeigt. Da WLAN-Abdeckung und Kapazitätsplanung zu den RF-Live-Funktionen gehören, kann auf häufige und kostenintensive manuelle Standortinspektionen verzichtet werden.

ArubaOS sammelt zusammengestellte und reine Statistiken zu Drahtlosnetzwerken pro Station, pro Kanal und pro Benutzer. Alle Statistiken können mit Hilfe der intuitiven Fehlerbehebungs-Tools von Aruba angezeigt werden und zudem über SNMP einfach in Verwaltungs- oder Analyseanwendungen von Drittanbietern integriert werden. Mit Live Packet Capture kann jeder Access Point oder Air Monitor von Aruba zu einem Packet Capture-Gerät aufgerüstet werden, das Echtzeit-Frames (802.11) an Überwachungsstationen wie z. B. Enterprise Analyzer, Ethereal oder WildPackets OmniPeek von Aruba übertragen kann. Administratoren können dank dieser detaillierten Daten Fehler schnell beheben und wichtige drahtlose Sender sowie überlastete Access Points rechtzeitig erkennen.

NETZWERKVERWALTUNG UND HOHE VERFÜGBARKEIT

Das Netzwerkverwaltungssystem von Aruba ermöglicht eine einfache Administration während jeder Phase des WLAN-Lebenszyklus – von der Planung über die Bereitstellung, Überwachung, Analyse bis hin zur Fehlerbehebung. Dabei verwendet das System eine grafische Benutzeroberfläche und eine vertraute Befehlszeilenschnittstelle (CLI).

Alle Access Points und Mobility Controller – selbst diejenigen, die sich in anderen Unternehmensniederlassungen befinden – können dabei zentral verwaltet werden. Softwareaktualisierungen und Richtlinien werden zentral konfiguriert und an alle Controller weitergeleitet. Aruba Mobility Controller können in 1:1- und 1:n-VRRP-basierten redundanten Konfigurationen mit Unterstützung redundanter Datenzentren eingerichtet werden.

QoS, VOIP-UNTERSTÜTZUNG UND STANDORTVERFOLGUNG

Die 802.11e- und WMM-Unterstützung gewährleistet QoS in Drahtlosnetzwerken für verzögerungsempfindliche Anwendungen mit Mapping-Funktion zwischen WMM-Tags und internen Hardware-Queues.

Aruba Mobility Controller unterstützen zudem das Mapping von 802.1p und IP-DiffServ-Tags an Hardware-Queues für QoS kabelgebundener Netzwerke. Die Layer 2-QoS-Funktionen lassen sich einfach mit Hilfe des zusätzlichen Policy Enforcement Firewall-Moduls auf Layer 3+-Workflow-Management and DiffServ aufrüsten. Darüber hinaus umfasst ArubaOS eine verbesserte Standortvisualisierung und -verfolgung von 802.11-Geräten. Über die signaturbasierte Standortbestimmung im Funknetz per Dreiecksmessung können Administratoren jeden 802.11-Benutzer oder jedes 802.11-Gerät mit einer Genauigkeit von unter einem Meter orten. Mit der Echtzeit-Standortverfolgung von Aruba können darüber hinaus mehrere Geräte gleichzeitig kontinuierlich geortet und verfolgt werden. Der Standort von Geräten kann auf Gebäudegrundrissen angezeigt werden, so dass sich Administratoren über die webbasierte grafische Benutzeroberfläche mit diesen verbinden können. Alternativ kann hierzu die zusätzliche externe Dienstschnittstelle verwendet werden, die über eine einfache Programmierschnittstelle (API) mit externen Systemen verbunden ist.

TECHNISCHE DATEN

SICHERE AUTHENTIFIZIERUNG, VERSCHLÜSSELUNG UND ZUGRIFFSSTEUERUNG

Authentifizierungstypen	<ul style="list-style-type: none"> • IEEE 802.1X (EAP, LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, EAP-POTP, EAP-GTC) • RFC 2548 Microsoft, herstellerspezifische RADIUS-Attribute • RFC 2716 PPP EAP-TLS • RFC 2865 RADIUS-Authentifizierung • RFC 3579 RADIUS-Unterstützung für EAP • RFC 3580 IEEE 802.1X RADIUS Richtlinien • RFC 3748 Erweiterbares Authentifizierungsprotokoll • MAC-Adressen-Authentifizierung • Webbasierte Captive Portal-Authentifizierung
Authentifizierungs-Server	<ul style="list-style-type: none"> • Interne Datenbank • LDAP/SSL Secure LDAP • RADIUS • TACACS+ • Authentifizierungs-Server von Drittanbietern Geprüfte Kompatibilität: Microsoft Active Directory, Microsoft IAS RADIUS-Server, Microsoft NPS RADIUS-Server, Cisco ACS-Server, Funk Steel Belted RADIUS-Server, RSA ACE-Server, Infoblox, Interlink RADIUS-Server, FreeRADIUS, A-10 Networks IDSentry
Verschlüsselungstypen	<ul style="list-style-type: none"> • WEP: 64 und 128 Bit • WPA-TKIP, WPA-PSK-TKIP, WPA-AES, WPA-PSK-AES • WPA2/802.11i: WPA2-AES, WPA2-PSK-AES, WPA2-TKIP, WPA2-PSK-TKIP, WPA2 (gemischter Modus) • Secure Sockets Layer (SSL) und TLS: RC4 (128 Bit) und RSA (1024 und 2048 Bit) • Programmierbare Hardware, erweiterbar für die neuesten Verschlüsselungsverfahren

ARUBAOS MOBILITY SOFTWARE

Erkennung nicht autorisierter Access Points	Ja
Klassifizierung nicht autorisierter Access Points	Ja
Eindämmung nicht autorisierter Access Points	Kabellose und kabelgebundene Netze

SEAMLESS MOBILITY

Fast roaming	2-3 ms, Intra-Switch 10-15 ms, Inter-Switch
Roaming zwischen Subnetzen und VLANs	Ja
Mobile IP-Unterstützung	Ja
Proxy Mobile IP	Ja
Proxy DHCP	Ja
VLAN Pooling	Ja

FUNKVERWALTUNG, FUNKPLANUNG UND FEHLERBEHEBUNG

Adaptive Radio Management (ARM)	Ja
Verschiedene ESSIDs pro Access Point	Ja
Automatische Kalibrierung von Access Points	Ja
Automatische Fehlerbehebung bei fehlgeschlagenen Access Points	Ja
Lastverteilung auf Basis der Benutzeranzahl	Ja
Lastverteilung auf Basis der Netzwerknutzung	Ja
Erkennung von Funklöchern und Interferenzen	Ja
Timerbasierte Zugriffskontrolle für Access Points	Ja
Funkplanungs- und Deployment-Tool	Ja
Wireless RMON/Package Capture	Ja
Plugins für Analyse-Tools von Drittanbietern	Ethereal, OmniPeek, Air Magnet
802.11h-Erweiterung (5 GHz) für Europa	Ja
Zusätzliche regulatorische Domänen (802.11d)	Ja

NETZWERKVERWALTUNG UND HOHE VERFÜGBARKEIT

Webbasierte Konfiguration	Ja
Befehlszeile	Console, telnet, SSH
Syslog	Ja
SNMP v2c	Ja
SNMP v3	Ja

Aruba private MIB	Ja
MIB-II	Ja
Zentrale Konfiguration der Mobility Controller	Ja
Zentralisierte Bildaktualisierung für Mobility Controller und alle Access Points	Ja
VRRP	Ja
Zentralisierte Bildaktualisierung für Mobility Controller und alle Access Points	Ja

QUALITY OF SERVICE, VOIP-UNTERSTÜTZUNG UND STANDORTVERFOLGUNG

802.1p-Unterstützung	Ja
802.11e-Unterstützung	Ja
T-SPEC/TCLAS	Ja
WMM	Ja
U-APSD (Unscheduled Automatic Power Save Delivery)	Ja
IGMP-Snooping für effiziente Multicast-Übertragung	Ja
Echtzeit-Standortverfolgung und -überwachung	Ja
Programmierschnittstelle (API) für Standortverfolgung zur externen Integration	Ja

ZERTIFIZIERUNGEN

Wi-Fi Alliance-Zertifizierung (802.11a/b/g/d/h, WPA™ Personal, WPA™ Enterprise, WPA2™ Personal, WPA2™ Enterprise, WMM™, WMM Power Save)
ICSA Wireless LAN v1.0
ICSA Firewall, Corporate v4.1 (mit optionalem Policy Enforcement Firewall-Modul)
FIPS 140-2-validiert (für den Betrieb im FIPS-Modus)
RSA-Zertifizierung
Spectralink VIEW-Zertifizierung

UNTERSTÜTZTE STANDARDS

GENERAL SWITCHING

RFC 1812-Anforderungen für IPv4-Router
 RFC 1519 CIDR
 RFC 1256 IPv4 ICMP Router Discovery (IRDP)
 1122 Host-Anforderungen
 RFC 768 UDP
 RFC 791 IP
 RFC 792 ICMP
 RFC 793 TCP
 RFC 826 ARP

ARUBAOS MOBILITY SOFTWARE

RFC 894 IP over Ethernet
RFC 1027 Proxy ARP
RFC 2338 VRRP
RFC 2516 Point-to-Point Protocol over Ethernet (PPPoE)
IEEE 802.1D - 1998 Spanning Tree Protocol (STP)
IEEE 802.1Q - 1998 Virtual Bridged Local Area Networks

WIRELESS

IEEE 802.11a/b/g 5GHz, 2.4GHz, 2.4GHz High-Rate
IEEE 802.11d Zusätzliche regulatorische Domänen
IEEE 802.11e Quality of Service
IEEE 802.11h Spectrum- und TX Power Control-Erweiterung für 5 GHz in Europa
IEEE 802.11i MAC-Sicherheitsverbesserungen

VLANS

IEEE 802.1Q VLAN Tagging
Portbasierte VLANs

QUALITY OF SERVICE UND RICHTLINIEN

IEEE 802.1D - 1998 (802.1p) Packet-Priorität
IEEE 802.11e - Quality of Service-Verbesserungen
RFC 2474 Differenzierte Dienste

NETZWERKVERWALTUNG UND DATENVERKEHRSANALYSE

RFC 2030 SNMP, Simple Network Time Protocol v4
RFC 854 Telnet-Client und -Server
RFC 783 TFTP Protocol (Revision 2)
RFC 951 1542 BootP
RFC 2131 Dynamic Host Configuration Protocol
RFC 1591 DNS (Client-Betrieb)
RFC 1155 Struktur der Mgmt-Informationen (SMIPv1)
RFC 1157 SNMPv1
RFC 1212 Konkrete MIB-Definitionen
RFC 1213 Verwaltungsinformationsbasis für Netzwerkverwaltung von TCP/IP-basierten Netzwerken - MIB-II
RFC 1215 Konventionen für Trap-Definitionen mit SNMP
RFC 1573 Schnittstellenentwicklung
RFC 2011 SNMPv2-Verwaltungsinformationsbasis für Internet-Protokoll mit SMIPv2
RFC 2012 SNMPv2-Verwaltungsinformationen
RFC 2013 SNMPv2-Verwaltungsinformationen
RFC 2578 Struktur der Verwaltungsinformationen (Version 2, SMIPv2)
RFC 2579 Textuelle Konventionen für SMIPv2
RFC 2863 Schnittstellengruppe (MIB)
RFC 3418 Management Information Base (MIB) für Simple Network Management Protocol (SNMP)
RFC 959 File Transfer Protocol (FTP)
RFC 2660 Secure HyperText Transfer Protocol (HTTPS)
RFC 1901-1908 SNMP v2c SMIPv2 und verbesserte MIB-II
RFC 2570-2575 SNMPv3, benutzerbasierte Sicherheit, Verschlüsselung und Authentifizierung
RFC 2576 Nebeneinander der Versionen 1, 2 und 3 von SNMP
RFC 2233 Schnittstellen-MIB
RFC 2251 Lightweight Directory Access Protocol (v3)
RFC 1492 Access Control Protocol, TACACS+
RFC 2865 Remote Access Dial In User Service (RADIUS)
RFC 2866 RADIUS-Accounting
RFC 2869 RADIUS-Erweiterungen
RFC 3576 Dynamic Authorization Extensions to Remote RADIUS
RFC 3579 RADIUS-Unterstützung für Extensible Authentication Protocol (EAP)
RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS)

RFC 2548 Microsoft RADIUS-Attribute
RFC 1350 TFTP-Protokoll (Revision 2)
Secure Shell-Server (SSHv2)
Konfigurationsprotokollierung
Mehrfachbilder, Mehrfachkonfigurationen
BSD System Logging Protocol (SYSLOG) mit mehreren Syslog-Servern

SICHERHEIT/VERSCHLÜSSELUNG

RFC 1661 Point-to-Point-Protokoll (PPP)
RFC 2406 IP Encapsulating Security Payload (ESP)
RFC 2661 Layer Two Tunneling-Protokoll (L2TP)
RFC 3193 Securing L2TP mit IPsec
RFC 2451 ESP CBC-Modus, Verschlüsselungsalgorithmen
RFC 2403 Verwendung von HMAC-MD5-96 mit ESP und AH
RFC 2401 Sicherheitsarchitektur für Internetprotokoll
RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2409 Internet Key Exchange (IKE)
RFC 2405 ESP DES-CBC Verschlüsselungsalgorithmus mit Explicit IV
RFC 2403 Verwendung von HMAC-SHA1-96 mit ESP und AH
RFC 3602 AES-CBC Verschlüsselungsalgorithmus mit IPsec
RFC 4017 Extensible Authentication Protocol (EAP), Methodenanforderungen für Drahtlosnetzwerke
RFC 3706 Datenverkehrsbasierte Methode zur Erkennung von Dead Internet Key Exchange (IKE) Peers
RFC 3947 Negotiation of NAT-Traversal in the IKE
RFC 3748 Extensible Authentication Protocol (EAP)
RFC 3079 Abgeleitete Schlüssel mit Microsoft Point-to-Point Encryption (MPPE)
RFC 4137 Zustandsautomaten für Extensible Authentication-Protokoll (EAP), Peer und Authentifikator
RFC 2716 PPP EAP TLS-Authentifizierungsprotokoll
RFC 2246 TLS-Protokoll (SSL)
RFC 2407 Internet IP-Sicherheitsdomäne zur Interpretation für ISAKMP
RFC 3948 UDP-Datenkapselung von IPSec-Paketen
Internet-Draft EAP-TTLS
Internet-Draft EAP-PEAP
Internet-Draft EAP-POTP
Internet-Draft XAuth für ISAKMP



[WWW.ARUBANETWORKS.COM](http://www.arubanetworks.com)

1322 Crossman Avenue, Sunnyvale, CA 94089 | Tel. +1 408.227.4500 | Fax. +1 408.227.4550