

## FEATURES

### Complete Multi-Layered Security

- Integrated wireless LAN intrusion protection (WIP) locks the air
- Controllable, automatic rogue AP and ad-hoc network neutralization
- L2 security with 802.1x, WPA, WPA2, dynamic WEP and xSec
- L3 security with IPsec, PPTP and L2TP VPNs
- Policy enforcement firewall for dynamic per-user security and control
- Role-based and SSID-based VLANs for segmenting users and traffic types
- Secure guest access with integrated Web-based authentication over SSL

### Centralized Mobility Control

- Centralized configuration eliminates the creation of VLANs everywhere
- Standards-based tunneling using IPsec or GRE between Aruba controllers and APs
- Programmable platform for future-proof upgrades and new applications

### Advanced RF Management

- Adaptive Radio resource Management (ARM) dynamically optimizes available RF resources
- Multi-band RF scanning
- Best-in-class QoS for voice-over-wireless and other mission-critical applications
- Load balancing automatically distributes clients across multiple APs
- Automatic interference avoidance, coverage hole detection and correction
- Location tracking for 802.11 devices down to one meter

### Seamless Enterprise Mobility

- Secure enterprise-wide mobility across different subnets, APs and controllers
- Fast roaming delivers uninterrupted performance for all users and applications including enhanced voice QoS
- Proxy Mobile IP eliminates client software requirement for transparent mobility
- Proxy DHCP enables application persistence as users roam across subnets

### Resiliency

- Modularity and redundancy among all system components provides fault tolerance
- Redundant controller arrays using VRRP
- Automatic RF fault tolerance avoids radio dead spots and provides AP back-up

### Secure Voice-over-Wireless

- Supports voice-aware RF scanning and multiple queues over the air
- Stateful flow classification for prioritization of VoIP and streaming media
- Bandwidth contracts to enforce usage limits
- Fast handoffs between APs for VoIP mobility

# Aruba

## Mobility Controller Systems



Aruba Networks mobility controller systems completely change how 802.11 networks are deployed, secured and managed. Aruba mobility controllers deliver the most advanced hardware-accelerated encryption available and are the only mobility controllers with an integrated ICASA-certified stateful firewall. The highest performing and most scalable on the market, the Aruba platform includes a family of modular and fixed configuration mobility controllers that scale from 4 to 512 APs. Automatic configuration and monitoring frees administrators from the costly and time-consuming process of managing individual APs. With centralized and programmable encryption capability, new mobile services and security standards are easily implemented on Aruba's mobility controller and propagated throughout the enterprise.

Aruba mobility controllers deliver superior performance through dedicated control plane processing, powerful packet processing with 10/100/1000 Mbps Ethernet switching, stateful identity-based LAN-speed firewalling, VPN client termination, wireless intrusion protection and advanced, adaptive RF management – all within a single network device. Because Aruba mobility controllers centralize and process native 802.11 traffic, enterprises have visibility and control of the RF environment like never before. All Aruba mobility controllers deploy and integrate seamlessly and non-disruptively into any existing L2/L3 wired network with no logical or physical reconfiguration required.

## TRANSPARENT AP-TO-CONTROLLER CONNECTIVITY

Aruba “thin” access points forward 802.11 traffic to Aruba mobility controllers across any IP network using standard IPsec or GRE (Generic Routing Encapsulation) tunnels. There’s no need to create new VLANs and IP subnets in every wiring closet for wireless APs and users. VLANs, if desired, only need to be created inside the centralized mobility controllers. APs can now be securely deployed and managed across an untrusted IP network such as the Internet.

## CENTRALIZED SECURITY PROTECTS THE AIR, THE DATA, THE NETWORK AND THE USER

Only Aruba’s mobility controller systems deliver multi-layered network security that protects the air, the data, the network and the users. A patented classification engine, coupled with sophisticated RF monitoring, lets administrators protect the air by automatically detecting unauthorized users, disabling rogue APs and ensuring users don’t associate with non-enterprise APs. Link layer encryption with support for WEP, TKIP (WPA), AES (WPA 2.0) and xSec protects user data.

802.1x authentication is used with standard authentication databases such as RADIUS, LDAP or Active Directory and combined with link layer encryption to ensure user privacy. Network layer security lets enterprises terminate VPN tunnels at LAN speeds inside the corporate intranet. An ICSA-certified policy enforcement firewall lets administrators create and enforce stateful policies that follow users as they roam.

## SECURE MOBILITY

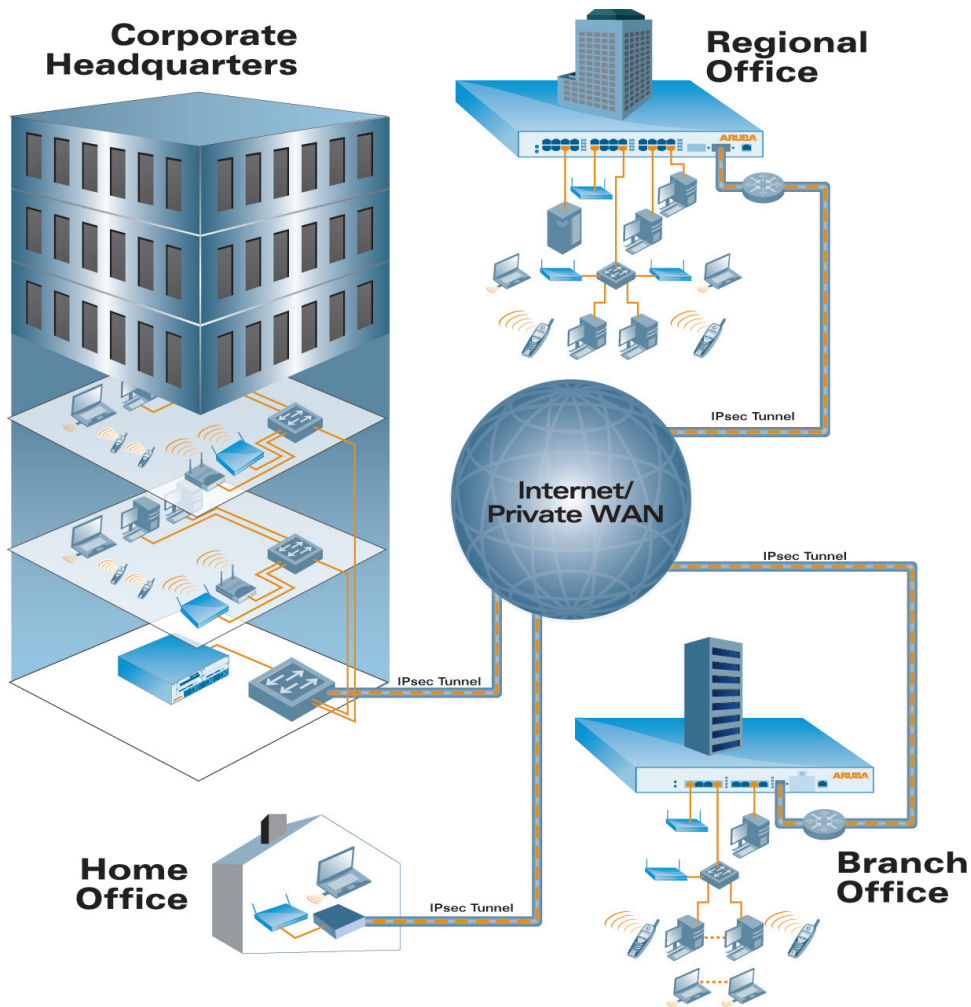
Aruba’s mobility controllers give users of laptops, PDAs and other mobile devices secure access throughout campus buildings and corporate subnets. L2 and L3 mobility between APs, subnets and mobility controllers eliminates lost sessions and the need for users to re-authenticate as they move. With an integrated policy enforcement firewall that can be applied on a per-user or per-group basis, administrators can establish unique access, service and security policies for different users or user groups. Policies can be based on any combination of parameters such as user, group, duration, time-of-day and location. These policies are centrally configured and propagated throughout the network so administrators can enforce desired levels of security and QoS for users as they move.

## AUTHENTICATION AND ACCESS CONTROL

Aruba mobility controllers support a variety of user authentication methods including the IEEE 802.1x framework that allows the use of PEAP, EAP-TLS, EAP-TTLS and LEAP. VPN authentication with L2TP/IPsec and PPTP is also supported. In addition, users can be authenticated against existing LDAP, RADIUS or Microsoft Active Directory servers, as well as a local database inside the Aruba mobility controller. Role-based access control allows specific user policies to be defined. Web-based authentication allows guest and clientless users to access the network secured with standard SSL.

| FEATURE   | BENEFIT  |
|---|--|
| <b>Multi-layered (L1, L2, L3 and L4-7) security</b>     | Simultaneously protects RF, data, network and users  |
| <b>Wireless Intrusion Protection</b>                    | Protects against malicious attacks and station and AP impersonations   |
| <b>Identity-based policy enforcement firewall</b>       | Allows role-based firewall policies to be created and enforced as each user roams  |
| <b>System resilience and redundancy</b>                 | High system availability. Auto-failover between controllers using VRRP. Auto-failover of APs.<br><br>Modularity and redundancy among all system components   |
| <b>Centralized encryption</b>                           | One simple upgrade at controller for entire system. Data encrypted across the network  |
| <b>Patented classification engine</b>                   | Automatically classifies and validates users and devices on network. Stations, APs and devices are classified as valid, rogue or interfering   |
| <b>Advanced RF monitoring</b>                           | Gives IT staff visibility and control of entire 802.11 environment from a single point   |
| <b>Integrated hardware-based encryption</b>             | Eliminates time-consuming upgrade. Delivers multigigabit encrypted throughput on a single system   |
| <b>Flow classification</b>                              | VoIP or other delay-sensitive traffic classified and prioritized over the air and wire   |
| <b>Interference avoidance</b>                           | Pinpoints interfering RF sources and adjusts APs dynamically   |
| <b>Backbone (indirect) connect</b>                      | Centralized deployment within backbone with no physical or logical reconfiguration. APs attached to existing wired IP network  |
| <b>Wireless RMON and remote packet capture/analysis</b> | No overlay networks required for remote wireless troubleshooting. On-demand access to wireless traffic statistics with centralized packet analysis   |
| <b>Bandwidth contracts</b>                              | Enforces per-user limits on bandwidth consumption  |
| <b>Seamless and secure mobility</b>                     | Eliminates lost sessions and need for roaming users to re-authenticate.<br><br>Allows secure and transparent user mobility across different subnets, APs and controllers, eliminates client software, keeps VPN tunnel state |
| <b>Role-based and SSID-based VLANs</b>                  | Automatically places users and traffic into correct VLAN using existing wired VLAN assignments. Segments different users and traffic types over single mobility infrastructure   |
| <b>RF planning with auto calibration</b>                | Eliminates need for expensive site surveys, eases deployment effort, provides optimal coverage on an ongoing basis   |
| <b>Automatic location tracking</b>                      | Any 802.11 device can be tracked and physically located within 1 meter of accuracy through sophisticated RF triangulation  |

## FLEXIBLE DEPLOYMENT OPTIONS



### PLUG AND PLAY DEPLOYMENT

Aruba mobility controllers can be centrally deployed and connected to access points across the installed IP infrastructure. Each controller stores the configuration of every Aruba AP. When a new Aruba AP is connected to the system, it is automatically discovered and configured by the controller. The Aruba mobility controller provides complete control of the power and channel settings of each AP. Aruba offers the only solution to deliver Ethernet, console and power over a single CAT 5 cable to any Aruba or third-party AP.

### ADVANCED WIRELESS CAPABILITIES

Aruba's advanced mobility features include bandwidth contracts to limit low priority users, classified and prioritized traffic flows to support delay-sensitive applications like VoIP, and automatic VLAN membership through roles derived from backend authentication systems that leverage 802.1x, captive portal or VPN authentication methods.

### NETWORK MANAGEMENT

Aruba's network management system (NMS) eases management during all stages of the WLAN lifecycle—from planning and deploying to monitoring, analyzing and troubleshooting.

With Aruba's NMS, administrators can centrally view, configure and manage all APs and mobility controllers, even those distributed in branch and regional offices.

Software upgrades and policies are configured centrally and propagated to all controllers. Administrators can secure and control the RF environment, capture wireless traffic and remotely troubleshoot problems anywhere on the wireless network.

The NMS includes an easy-to-use Web-based GUI, a familiar command line interface (CLI), and full support for SNMP (v3). Aruba's NMS easily integrates with third-party management systems such as HP OpenView or CA's Unicenter. A plug-in capability enables the integration of third party applications for advanced analysis and troubleshooting, location-based services and more.

### AUTOMATIC LOCATION TRACKING

Locating a mobile user, access point or other wireless devices has never been easier. Aruba's mobility system includes advanced location visualization and tracking of 802.11 devices. RF signature-based location triangulation allows administrators to physically locate any 802.11 user or device within one meter of accuracy. With Aruba's real-time location tracking capabilities, multiple devices can be continuously located and tracked simultaneously.

## MOBILITY CONTROLLER SYSTEMS

### THE ARUBA 5000 AND 6000



### THE ARUBA 2400

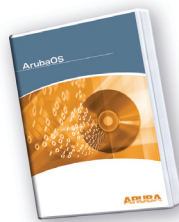


### THE ARUBA 800



## SOFTWARE

### ARUBAOS MOBILITY SOFTWARE



# ARUBA

1322 crossman avenue | sunnyvale california 94089  
tel 408 227 4500 | fax 408 227 4550  
www.arubanetworks.com

**The Aruba 5000 and 6000** are the only modular mobility controllers on the market. The four-slot Aruba mobility controllers integrate an ICSA-certified policy enforcement firewall and a hardware-accelerated encryption engine. The Aruba platforms support up to 8 Gbps of clear / 7.2 Gbps encrypted throughput, up to 72 10/100 Mbps ports, 8000 simultaneous users and from 4 to 512 APs. Hot swappable line cards house 24 10/100 Mbps serial and power over Ethernet (SPoE) ports and two GBIC ports.

**The Aruba 2400** is a stackable, 24-port mobility controller that supports up to 48 APs. Designed for regional headquarters or dense building deployments, the Aruba 2400 supports up to 512 simultaneous users and delivers up to 400 Mbps of encrypted throughput.

**The Aruba 800** is a fixed configuration mobility controller designed for small and branch office applications. The Aruba 800 provides eight 10/100 Mbps user ports and one copper or fiber gigabit uplink. Programmable hardware-based encryption supports 200 Mbps of full-duplex encrypted traffic.

**ArubaOS** provides the world's most robust and sophisticated suite of capabilities found in any enterprise mobility system. ArubaOS is the operating system and application engine for all Aruba mobility controllers.

Standard with every Aruba mobility controller, the base feature set of ArubaOS includes seamless mobility with fast roaming, secure authentication and encryption, sophisticated RF planning and RF analysis tools, centralized configuration and management, redundancy and much more.

Additional modules are available for:

- ArubaOS Wireless Intrusion Protection
- ArubaOS Policy Enforcement Firewall
- ArubaOS VPN Server
- ArubaOS Client Integrity
- ArubaOS Remote AP
- ArubaOS External Services Interface
- ArubaOS Advanced AAA
- ArubaOS xSec