

User-Centric Networks for Federal Government Applications

Aruba has pioneered a new approach to FIPS-140-2 compliant secure mobility. Aruba's user-centric networks integrate adaptive WLANs, identity-based security, and application continuity services into a cohesive, high-performance system for campuses, office buildings, remote offices, outdoor areas and telecommuters. The result is a centrally managed network that mobilizes applications across the LAN, WAN, and Internet, making users more productive without compromising security. Aruba's user-centric networks overlay on top of existing networks, preserving existing investments and minimizing disruptive infrastructure changes.

Unique Aruba Capabilities

BUILT-IN SECURITY FOR REGULATORY COMPLIANCE

Aruba's user-centric networks are secure mobility solutions that keep the government moving, and meet the following requirements:

- FIPS 140-2 Level 2 validated encryption
- 802.11i standards compliance
- DoD Directive 8100.2 compliant
- End-to-end security over an assured channel
- Common Criteria Certification
- 802.1x authentication (including Common Access Card)
- JITC certification
- Wireless Intrusion Detection and Prevention

IDENTITY-BASED SECURITY – CONTROL ACCESS BY SECURITY CLEARANCE LEVEL

Mobile applications require that the network securely follow users as they roam. Traditional access control methods, determined by the point of network entry, hamper mobility. Mobile access control takes into account the user's organizational role, security clearance, device type, location, time,

and even usage behavior. Employees, contractors and guests can be assigned unique levels of access and even different authentication methods (802.1x, VPN, and captive portal) and directory structures (RADIUS, LDAP, or Active Directory).

Aruba Multi-Service Mobility Controllers and access points are uniquely positioned to provide these capabilities. Aruba implements an ICSA-certified role-based stateful firewall that allows for unique roles to be created and applied for each user, their security clearance level and device. The firewall also provides blacklisting of clients that violate policy, terminating a session and denying further connectivity to the network. Aruba's user-centric networks overlay on top of existing networks and integrate with any directory structures in place.

CENTRAL MANAGEMENT AND TROUBLESHOOTING

Aruba's centralized network and policy management is designed to simplify deployment and operation. Configuration data are automatically and securely propagated throughout the network, across access points and controllers, both locally and remotely.

The Aruba Advantage:

- **Identity-based security** follows users as they move across the LAN, WAN and Internet
- **Central management** is easy to configure, monitor and troubleshoot
- **Application-awareness** is optimized for converged data, voice and video over wireless
- **Flexible and scalable network** enables overlays to avoid upgrades and network redesigns

A single interface is provided for IT to implement and protect the underlying policies that ensure the integrity, security, and operation of the entire network.

Aruba provides remote packet captures and RF views so IT managers can troubleshoot problems at other locations across town or across the world. Network managers can perform upgrades and maintenance centrally, from one location, and receive alerts about events as they happen.

APPLICATION AWARE

To support voice and video, a network must implement QoS over the air and over the wire, adjusting traffic patterns to optimize quality. The Aruba solution maintains a centralized context for both QoS and security, and can easily follow voice and video users as they move through the network. Voice traffic is prioritized using 802.1p and DSCP QoS tags. The system automatically recognizes the most common protocols

and applies priorities. Additional prioritization can be performed using Call Admission Control to dynamically move traffic above a threshold to neighboring APs, keeping voice and video quality exceptionally high.

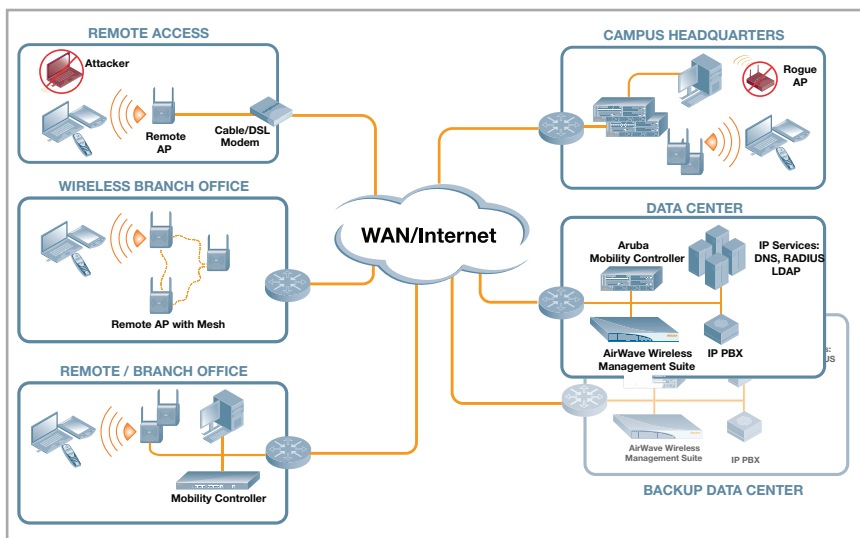
SCALABLE AND FUTURE PROOF

Aruba Networks has developed innovations to automate RF configuration, offload backend AAA servers and scale VLANs to accommodate variable usage patterns. Additionally, Aruba provides computationally powerful, massively scalable, purpose-built platforms with high throughput that leverage existing applications, IT infrastructure, and standard clients. Designed to accommodate the requirements of users today and in the years ahead, most Aruba products also feature an upgradeable modular software architecture that can be enhanced over time as new features become available.

The Aruba Networks Federal Solution

The Aruba solution consists of just a few key components – thin Access Points (APs), central Multi-Service Mobility Controllers and software application modules; and optional management analytics and threat prevention appliances. APs provide secure wireless connectivity, using existing LANs/WANs to tunnel all wireless traffic over a GRE or IPsec tunnel to a controller installed in the data center. The controller is the central point of configuration, management, application continuity services and security.

Data Center: One or more master Multi-Service Mobility Controllers are installed in the data center for global configuration and management. These controllers can also terminate APs used for wireless connectivity. A master controller can support up to 500 remote controllers and provide back-up in case of an outage. For larger deployments, multiple master controllers can share the management load.



Large and medium sized offices: All Aruba controllers run the same software and have the same functionality, but differ in AP capacity. Local controllers obtain their configuration from the master controller. Application-continuity and security policies are enforced at a per-user level by the local controllers. Different user roles are applied based on group policy defined in the authentication infrastructure, and guests can be tunneled outside of the network to terminate in the DMZ. Local controllers also offer Wireless Intrusion Protection and provide local authentication services and/or pass-through requests to the data center. To extend wireless coverage in areas that are hard or costly to wire, APs can backhaul over Wi-Fi using Aruba's award-winning secure enterprise mesh technology.

Remote users and small offices: Remote APs are a cost-effective solution to provide secure and centrally managed wireless connectivity to locations that need only one or two APs. Remote APs connect via public/private Internet connection or a LAN, automatically discover the master controller, and establish an IPsec tunnel to the data center. They deliver the same services, and enforce the policies, remotely as they do locally.

COMPLETE END-TO-END SECURITY
Aruba provides encryption with seamless transition between AES-CCM/802.11i and AES-CBC 256 bit for both wired and wireless devices without hardware upgrades. Combined with defense-in-depth security, this feature provides integrated multi-layered support that locks the air, the wire, the network and the user.

Aruba also provides EAP-offload capability in its FIPS-validated software. With EAP-offload, sensitive authentication and key management transactions are completed within the secure cryptographic boundary of the central Multi-Service Mobility Controller and do not need to be transmitted as clear text or using weak encryption algorithms between the controller and an external RADIUS server.

Alternately, Aruba can secure EAP-capable RADIUS servers by using RADIUS-over-IPsec functionality as recommended by RFC 3579. This offers the industry's first single-box FIPS solution for non-disruptive wireless overlay deployment.

Federal Security Certifications:

RELEVANT STANDARDS

- Wi-Fi Alliance 802.11n
- WFA 802.11a
- WFA 802.11 b/g
- WFA WME Certification for Quality of Service (QoS)
- AES-128 / AES-256 CCMP; AES-GCM (due 2011)
- 802.11i / WPA2
- 802.1x including CAC card support
- IPsec

INFORMATION ASSURANCE VALIDATIONS

- ICISA Certified Stateful Inter-User Firewall
- FIPS 140-2 Level 2 for ArubaOS v2.4.8.25
- FIPS 140-2 Level 2/Level 3 for ArubaOS v3.3.2.19
- FIPS 140-2 Level 2/Level 3 for ArubaOS v3.4.2.2 (pending)
- Common Criteria EAL-2+
- Common Criteria EAL-4 (pending)

DEPARTMENT OF DEFENSE

- DoD Directives 8100.2, 8500.1, 8420.1 Compliant
- UC-APL Listing
- DDR1494 JF12 Equipment Radio Frequency Allocation Guidance

CITS / USAF

- ATO for USAF CITS 2GWLAN
- I-TRM purchase list
- JITC ICTO

ARMY

- Listed on US Army Information Assurance Approved Products List (IAAPL)
- US Army Technology Integration Center (TIC) tested (passed)
- US Army Type Accreditation

JMIS TIMPO / NAVY

- IATO from JMIS and NAVNETWARCOM
- Navy HERO certification

MILITARY HEALTH SYSTEM (MHS)

- ATO for all MHS facilities



WWW.ARUBANETWORKS.COM | 1344 Crossman Avenue. Sunnyvale, CA 94089

1-866-55-ARUBA | Tel. +1 408.227.4500 | Fax. +1 408.227.4550 | info@arubanetworks.com