



Aruba's Unified Secure Mobility for Enterprises

What's your vision? To provide secure wireless access to your users throughout a building? A campus? The world? To provide a ubiquitous user-experience and security to your users everywhere they connect? To reduce telephony costs and boost user productivity with voice-over-wireless LAN and Fixed Mobile Convergence?

Aruba has pioneered a new approach to help you achieve your vision. Aruba's unified secure mobility platform integrates adaptive WLANs, identity-based security, and application continuity services into a cohesive, high-performance system for corporate campuses, office buildings, branch offices and telecommuters. The result—a centrally managed network that mobilizes business applications across the LAN, WAN and the Internet making users more productive without negatively impacting security. In contrast to other solutions, Aruba's user-centric network overlays on top of existing networks, preserving existing investments and preventing disruptive network changes.

Unique Aruba Capabilities

IDENTITY-BASED SECURITY

Mobile applications in the enterprise require that the network securely follow users as they roam. Traditional access control methods, determined by point of network entry, simply cannot support mobility. Mobile access control requires context of the user—including organizational role, device type, location, time, and even usage behavior—when establishing policy. Different groups of employees, contractors and guests will require unique levels of access and even different authentication methods (e.g., 802.1x, VPN, and captive portal). Finally, all of this has to be achieved without increasing network complexity and must seamlessly integrate with existing directory structures such as RADIUS, LDAP or Active Directory.

Aruba Networks Mobility Controllers and access points are uniquely positioned to provide these capabilities. Unlike other solutions that tie policies to specific SSIDs/VLANs to secure and segment a network, Aruba implements

an ICSA certified role-based stateful firewall allowing for unique roles to be created and applied for each user and device. The firewall also supports 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 integrates with any directory structures in place.

CENTRAL MANAGEMENT AND CONTROL

Deploying and managing a global enterprise network can be a daunting task if not addressed correctly. Aruba's centralized network and policy management is designed for ease of deployment and operation. With Aruba's centralized management, configuration data are automatically and securely propagated throughout the network, across access points and Controllers, both locally and remotely. A single interface is provided for IT to implement and protect the underlying

The Aruba Advantage:

- **Identity-based security:** Security follows users as they move across the LAN, WAN and Internet
- **Central management:** Easy to configure, monitor and troubleshoot with centralized control
- **Application-aware:** Optimized for converged data, voice and video support over wireless
- **Flexible and scalable network:** Overlay deployment model prevents upgrades and network redesigns
- **Future-proof:** Software upgradeable for new technologies such as 802.11n, NAC, mesh and eFMC

Enterprise Solution

policies that ensure the integrity, security, and operation of the entire network. The centralized control function also includes performance profiles that are used by Aruba access points to optimize their operation and reliably support mission-critical applications. The result is a massively scalable network that is simple enough to be used by technically unskilled users.

APPLICATION AWARE

Voice and video services over IP are becoming more prevalent in the enterprise with the introduction of Wi-Fi-enabled mobile phones and the increased popularity of multimedia communications. To support services such as voice, the network must be capable of implementing QoS over the air and over the wire, securing voice calls and adjusting traffic patterns to optimize voice quality. The Aruba solution is fully voice-aware, taking advantage of an application-based firewall to secure and prioritize voice. Because the architecture maintains centralized context for both QoS and security, it can easily follow voice 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 voice protocols (notably SIP, SVC, and SCCP) and applies strict priority to voice traffic. Additional call

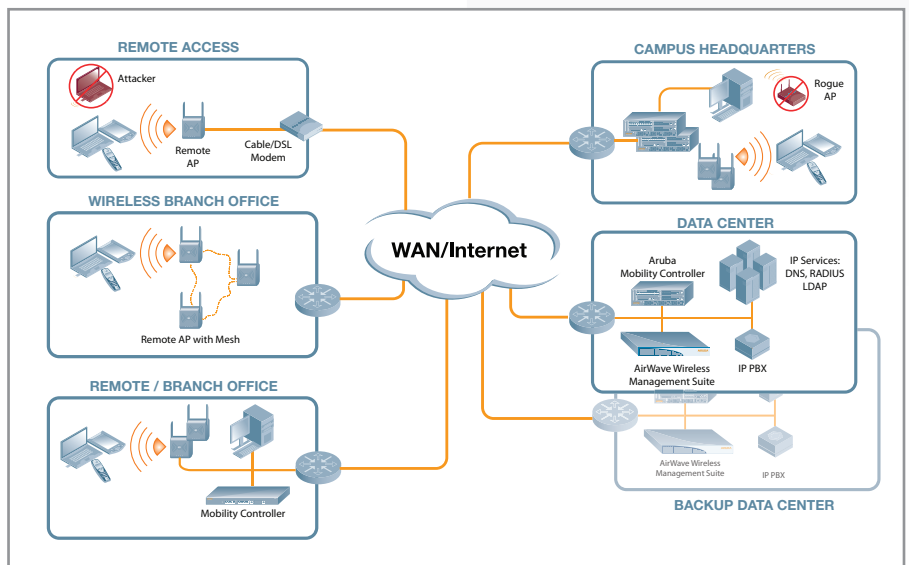
prioritization can be performed using Call Admission Control (CAC). CAC sets an upper limit on voice calls per AP, dynamically moving any calls above this threshold to neighboring APs and keeping voice quality exceptionally high.

SCALABLE AND FUTURE-PROOF

A WLAN system must support the existing requirements of an enterprise as well as accommodate for growth and future adoption of mobile devices and applications. The key challenges of scaling an enterprise wireless LAN relate to user and device density, instantaneous loads during peak hour usage, and the mobility of users between different areas across the LAN, WAN and Internet. Aruba Networks has developed innovations to automate RF configuration, off-load back-end 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 feature an upgradeable modular software architecture that can be enhanced over time as new features become available.

The Aruba Networks Enterprise Solution

The Aruba solution consists of a few key components – thin Access Points (APs), central Mobility Controllers and software modules for the Mobility Controller; and optional management analytics and threat prevention appliances. APs provide secure wireless connectivity to devices and connect over existing LAN/WAN systems to tunnel all wireless LAN traffic (over a GRE or IPsec tunnel) to a Mobility Controller installed in the data center. The Mobility Controller is the central point of configuration, management, application continuity services and security. With security modules for Mobility Controllers, Aruba offers the necessary security for regulatory compliance.



Following is an explanation of a wireless network in an enterprise environment with centralized IT services:

Data Center: One or more master Mobility Controllers are installed in the data center, which can be used as the central configuration and management point for the entire global network. These Controllers can also terminate APs used for wireless connectivity in the HQ and remote APs used by telecommuters, home workers or small ad-hoc offices. A master Controller can support up to 500 remote Controllers and can also back up a Controller in a remote location in the case of an outage. To scale for larger deployments, multiple master Controllers can share the load of managing local Controllers and APs in remote sites, and the Mobility Management System (MMS) can be used as the single interface of management and configuration.

Large and Medium Sized Offices: Depending on the number of APs required in each location, a different model of Aruba Controllers (called local Controllers) is installed. All Aruba Controller models run the same software and have the same functionality, but differ in AP capacity—from 4 to 512 APs. Each local Controller gets its configuration from the master Controller. Application-

continuity and security policies are enforced at a per-user level by the local Controller. 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 security and can provide local authentication services and/or pass-through requests to the data center. Each local Controller automatically calibrates the RF coverage to optimize application performance and fill any coverage holes. Further, to extend wireless coverage in areas that are hard or costly to wire, Aruba APs can backhaul over Wi-Fi using its 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 only need one or two APs. Remote APs can connect directly via Ethernet to a public/private Internet connection or to the LAN. Remote APs automatically discover the master controller, establish a VPN tunnel back to the data-center and extend secure wireless connectivity to the user. Application traffic can be tunneled back to the data center or bridged locally



WWW.ARUBANETWORKS.COM

1344 Crossman Avenue, Sunnyvale, CA 94089 | Tel. +1 408.227.4500 | Fax. +1 408.227.4550