



Aruba's User-centric Networks for Finance

What's your vision? To enforce a no-wireless policy for your users, while securely providing wireless internet access to guests? To boost user-productivity with secure wireless access for data and voice applications throughout a building? A campus? The world? To provide business continuity even in the case of disruptions such as caused by weather delays, unforeseen events and disasters?

Aruba has pioneered a new approach to help you achieve your vision. Aruba's User-centric Networks integrate adaptive WLANs, identity-based security, and application continuity services into a cohesive, high-performance system to address your needs for secure mobility—from blocking access through wireless intrusion protection services (IPS) to providing access to guests to enabling pervasive mobility and business continuity. Aruba's centrally managed network is designed to mobilize 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.

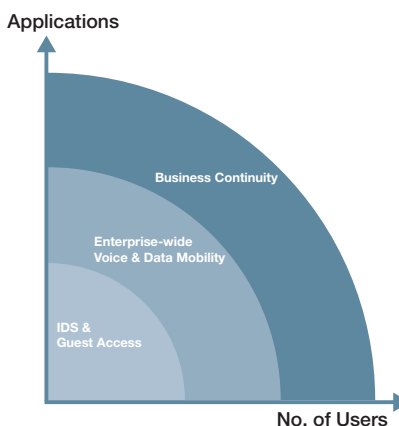
Unique Aruba Capabilities

ONE PLATFORM, MULTIPLE USES

Network managers agree that mobility requirements grow faster than planned. It pays to plan ahead and choose a system that will grow with you. With Aruba, you can start with blocking wireless access, deploy guest access, slowly migrate to pervasive enterprise-wide mobility and even provide business continuity via remote access for thousands of users, all on the same platform with common underlying software. Such depth of capability and application flexibility is enabled by the unique integration of wireless LAN, security and remote access capabilities on one, centrally managed platform.

IDENTITY-BASED SECURITY

Aruba's identity-based security is designed to securely allow employees, contractors and guests on the network simultaneously, while protecting network assets from unauthorized users and one user from another. Aruba's



approach combines user identity, device posture, type of traffic, time of day and other parameters to create role-based access policies, which are continuously enforced with an ICSA certified firewall and endpoint compliance technologies. Aruba's centralized architecture extends security and access rules to follow the user throughout the building, campus and even across the Internet.

The Aruba Advantage:

- **Single integrated platform:** Provides security for no-wireless policy, guest access, secure in-building wireless and remote access for business continuity
- **Identity-based security:** Enables secure guest and employee access, while meeting data confidentiality needs for regulatory compliance
- **Central management:** Single point of control for networks in main offices, branch offices and home offices make it easy to configure, monitor and troubleshoot
- **Application continuity:** Ensures reliable operation of converged data, voice and video support over wireless
- **Flexible and scalable network:** Overlay deployment model avoids upgrades and network redesigns

With identity-based security, financial institutions can securely provide both guest access and employee access while meeting data confidentiality requirements for regulatory compliance.

Guest Access: Guests and contractors need Internet access, but using VLAN segmentation is simply not a secure solution as it is open to impersonation attacks. Identity-based security that encapsulates and separates corporate traffic from guest traffic ensures that no secret information is ever compromised. The Aruba solution directly terminates all GRE encapsulated guest traffic to a DMZ router.

Data Confidentiality for Regulatory Compliance: With Aruba, data is protected at both Layer 2 and Layer 3. Moreover, all data is encrypted and stays encrypted from the client to the data center. At no point in this transmission is the information ever unencrypted or available in plain text. In a mixed use environment, where potential conflicts of interest may exist, Aruba's solution ensures full access control and encryption-based separation of information as mandated in SOX and GLBA compliance requirements.

Business Continuity: Business continuity planning is essential in today's information-driven enterprise as business interruptions due to inclement weather, pandemic scares and disasters become increasingly frequent. However, deploying business continuity can be very expensive and complex given the lack of enterprise-grade home office solutions. Neither consumer-grade products nor enterprise-grade branch office solutions fit the bill. On one hand, there are reliability and security concerns, and on the other, costly expert installation and management is required. Aruba's Remote AP solution bridges the gap with an innovative design that provides full office-like connectivity for voice and data at employee homes. With the Remote AP, Aruba has taken the innovation of thin access points and applied it to remote access. By moving the management to the HQ, Remote APs are user-installable and centrally managed, thereby eliminating the operational expense and reducing the capital expense.

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 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 CONTINUITY

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.

The Aruba Networks Finance Industry 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.

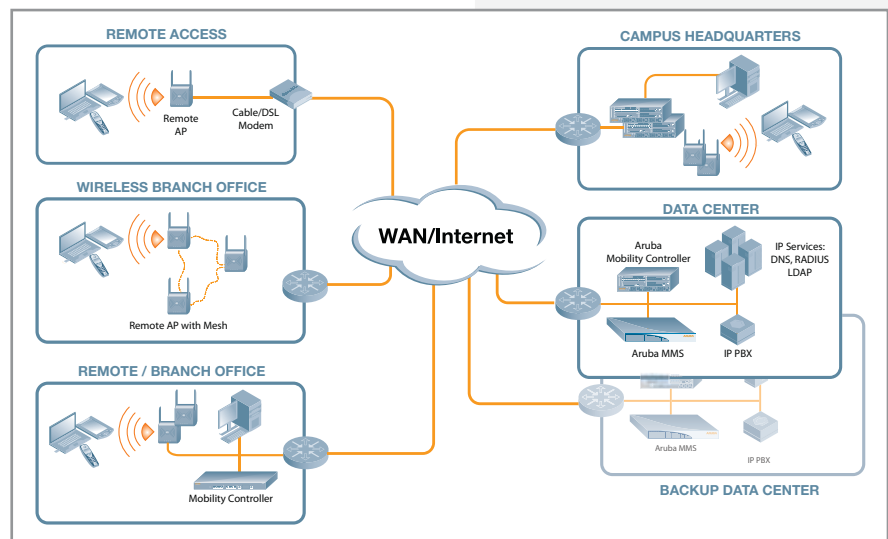
Following is an explanation of a wireless network in an enterprise environment with centralized IT services:

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 offer 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

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