Secure Mobility Solutions for Industrial Environments

Aruba’s unified mobility solutions provide a secure, robust means of connecting mobile workers to the plant network, reliably delivering business-critical applications no matter where users roam or the environment in which they work. Our adaptive wireless LANs, identity-based security, and application continuity services offer a safer, more reliable, and more transparent means of supporting your business processes – and enabling new ones. From shop-floor to board room, the cost, convenience, and security benefits of our unified mobility solutions are fundamentally changing how and where we work.

Wireless networks increase productivity by bringing the plant networks to workers instead of forcing them to go to fixed workstations. Minimizing the number of workstations frees up valuable floor space and allows for more flexible equipment layouts. By simultaneously supporting data, voice, and streaming video, wireless networks provide full access to existing applications and enable new ones such as all-wireless mesh-based telemetry, voice recognition, and streaming video surveillance. Wireless networks reduce the need for expensive network-related power and data cable plant and equipment, lowering CAPEX and potentially expensive maintenance headaches.

The wireless Follow-Me Factory moves in lock-step with users:

- Follow-Me Connectivity: 802.11a/b/g/n Wi-Fi networks ensure that users are always within reach of mission-critical information;
- Follow-Me Security: Identity-based security assigns access policies to users, enforcing those policies whenever and wherever a network is accessed;
- Follow-Me Applications: Remote access solutions and cellular network integration ensure uninterrupted access to applications as users move.

Unique Aruba Capabilities

PURPOSE-BUILT FOR HARSH ENVIRONMENTS

Aruba’s ruggedized industrial wireless access points set the standard for robustness and flexibility, while the rich feature set accommodates a wide range of installation scenarios:

- Rugged IP68, NEMA UL 50 enclosure and wide operating temperature range permit operation in physically and environmentally challenging applications;
• ATEX Zone 2 explosion rating, combined with fiber optic or wireless mesh operation, enables access points to be situated where standard commercial equipment cannot;
• Aruba’s Adaptive Radio Management technology continuously and automatically optimizes network performance in the face of noise and impairments;
• Over-the-air set-up, diagnostics, and downloading lowers life-cycle costs by minimizing the need to physically access equipment;
• Ethernet, fiber optic, and wireless mesh communication options offer unparalleled flexibility;
• Flexible power options - including solar panels, battery, high voltage AC, and Power-over-Ethernet – accommodate virtually any installation scenario;
• High-intensity front panel LEDs provide status at a glance, without a ladder climb.

ALL-WIRELESS WORKPLACE
Aruba’s high-performance 802.11n solutions enable a smooth transition away from wired networks to more scalable, easily modified, and highly secure all-wireless networks. Able to leverage existing network infrastructure, Aruba 802.11n solutions were designed specifically for today’s mobile manufacturing workforce. Our 802.11n networks can fundamentally change the dynamics of your organization, lowering CAPEX of wired network infrastructure and the OPEX required to support them.

For challenging installation environments, Aruba’s award-winning secure enterprise mesh technology allows access points to communicate without data cabling. Instead, packets hop wirelessly from access point to access point. Upon arrival, packets can be broadcast over Wi-Fi and/or delivered over Ethernet or fiber optic cable. Mesh is an ideal way to lower deployment costs and reach otherwise inaccessible locations.

Not yet ready for an all-wireless workplace? Aruba’s solutions interoperate with existing wired infrastructure, complementing existing edge and core data and security equipment with identity-based security not otherwise available in a wired network.

Remote access solutions further enhance productivity by granting traveling executives, satellite offices, and remote plants with secure access to the corporate network without the hassle of VPN-like clients. Easy to configure, simple to manage, remote access solutions bring your network to remote users wherever the work or roam.

REAL-TIME APPLICATIONS
Wireless networks need to be continuously optimized in real-time to reliably support mobile voice, bar code scanning, inventory management, and data terminal applications in the presence of noise and interference. Using standards-based mechanisms such as 802.1p and DSCP QoS tags, Aruba’s networks monitor the type and traffic patterns of applications in use and automatically adjust parameters to ensure reliable application delivery. The result? High-speed data, toll-quality voice, and interruption-free streaming video.

UNCOMPROMISED SECURITY
Mobile manufacturing devices, unlike commercial laptop PCs, are often embedded computers with rudimentary security like WEP. Aruba’s identity-based security securely connects these devices to the network and provides per-user firewall and intrusion detection to protect against malicious attacks. By overcoming the limited security of legacy devices.

LOW TOTAL COST OF OWNERSHIP
Aruba’s centralized management is a field-proven means of reducing IT support costs by tightly controlling policies and processes of even the largest network. Capabilities include painting an in-depth view of the RF footprint in each remote location, device-level diagnostics and remote packet captures for advanced troubleshooting. Aruba controllers and access points in remote locations automatically discover the data center master controller, download their configuration, and commence operation. Centralized management makes wireless LAN installation in remote locations a “zero-touch” project, saving travel time and expense.
System Description

The heart of an Aruba unified mobility solution is the Multi-Service Mobility Controller. Computationally powerful, massively scalable, and 802.11n-ready, this family of products runs the ArubaOS, manages software applications, coordinates security policies, and continuously optimizes the performance of the wireless LAN. Designed to support business-critical data, toll-quality voice, and streaming video applications, Multi-Service Mobility Controllers can simultaneously use centralized, distributed, split-tunnel, and/or secure mesh forwarding architectures to accommodate virtually any installation scenario or redundancy requirements.

Wireless intrusion detection/protection, endpoint compliance, locationing/RFID, cellular-to-Wi-Fi enterprise fixed mobile convergence, and a wide variety of additional applications run on, or in conjunction with, the Multi-Service Mobility Controllers. All under the direction of Aruba’s network management application.

Wireless 802.11a/b/g/n access points provide connectivity with bar code reader, laptop, hand-held, phone, and related mobile clients, linking them with Multi-Service Mobility Controllers over secure mesh, LAN, or WAN tunnels. Aruba offers a wide range of access points, from diminutively packaged devices that can be carried by traveling executives to explosion-resistant ruggedized units for harsh environments.

Aruba access points can be repurposed over the network, allowing one common SKU to serve many applications. Configured as a remote access point, the device provides secure network access to roaming users – on the road, at remote sites, at contractor facilities. Users gain access to the same network resources they would have at work, with the same level of security, but without the headaches of a managed client. Configured for secure mesh operation the access points communicate wirelessly, and ideal way to signal over short or long distances without cable drops. Ideal for overcoming challenging installation scenarios, mesh is an invaluable tool where all-wireless signaling is a must.