Enabling Mobility in Medicine via an Application-Aware Wireless LAN

Anywhere, anytime wireless network access to health records, for voice communications and for medical devices has proven to improve quality of care and reduce costs. The mission-critical and sometimes life-critical nature of medical processes requires the enabling wireless network to be designed with the highest levels of reliability and security. Thus far, meeting such stringent requirements have dictated the need for a dedicated “application-specific” wireless network infrastructure for each service, raising both the total installation expense and the ongoing operating expense burden. Aruba Networks drastically reduces network complexities and costs with its “application-aware” wireless LAN that reliably delivers data, voice and medical device traffic over one common network.

Only Aruba offers a high-speed 802.11n wireless LAN for hospital-wide mobility with:
- Adaptive Radio Management (ARM) to ensure consistent application performance using unique over-the-air Quality of Service (QoS) and interference mitigation algorithms
- Role-based security to protect users, devices and health records in an environment with a diverse community of network users and a wide-array of network traffic type.
- Centralized management console to handle multiple vendors and generations of wireless LANs.

Aruba’s application-aware wireless LAN has been used by thousands of hospitals and clinics to enable:
- **EMR access at the Point-of-Care:** Wi-Fi enabled laptops, tablets, PCs, PDAs, and computers-on-wheels (CoWs) have been certified with Aruba’s high-speed 802.11n wireless LAN to securely access electronic medical records. Aruba’s integrated role-based firewall prevents unauthorized access to health records, a capability necessary for regulatory compliance.
- **Voice over WLAN:** Boost nurse productivity by recovering the hundreds of hours per year spent locating assets and traveling to answer phone calls. Aruba’s application-aware 802.11n wireless LAN allows access to health records while simultaneously providing disruption-free access to Wi-Fi voice handsets (including Polycom, Avaya, Vocera, and Cisco).
- **Guest Internet Access:** Securely enable internet connectivity for hospital vendors, visitors, and patients using Aruba’s GuestConnect™ capabilities which feature the industry’s only integrated role-based firewall.
- **Telemetry and Portable Patient Monitors:** Improve the quality of care and reduce facilities costs with the use of portable patient monitors and telemetry devices. Aruba’s unique Over-the-Air QoS mitigates congestion to ensure error-free operation of patient monitors and telemetry equipment on the same wireless network as voice and data devices.
- **Asset Tracking:** Reduce the costs associated with the loss of RFID-tagged shared medical equipment, such as wheel chairs and infusion pumps, by using Aruba’s built-in real-time location tracking capability.

**What Makes Aruba Different:**
- **Unmatched reliability:** Only Aruba has “application-aware” wireless coverage management to ensure uninterrupted application performance in the wake of interference and congestion.
- **Military-grade security:** Only Aruba has an integrated role-based firewall and wireless intrusion detection system that ensures patient records are protected and meets regulatory compliance requirements.
- **Highest capacity 802.11n wireless LAN:** Aruba’s controllers scale to 80Gbps (vs. 8Gbps max from other vendors) to enable uncompromising high-speed 802.11n access.
- **Easily extend hospital-like connectivity:** Only Aruba can replicate hospital LAN and WLAN across the entire healthcare enterprise using the plug-n-play Remote Access Point technology, eliminating the need of dedicated routers and VPN clients.
- **Cost-effective:** one platform for high performance 802.11n, network security, and remote access, eliminating the need to acquire, install, and manage multiple disparate systems.
- **Telemedicine:** Reduce facilities costs and securely extend data, voice and medical device access to outside of the hospital using Aruba’s “zero-touch,” client-free remote access points deployed in doctors’ offices, ambulatory facilities and patient residences.

**The Aruba Solution:**

Aruba’s application-aware 802.11n wireless LANs are designed to provide reliable, hospital-wide wireless access to a wide variety of users (including clinicians, administrators, patients, and visitors) and applications (including clinical information, voice communications, and connectivity for portable medical devices).

The architectural scheme of the Aruba solution typically includes centrally-managed 802.11a/b/g/n Access Points (APs), Multi-Service Mobility Controllers and a centralized management console. APs provide secure wireless connectivity to client devices and tunnel all wireless LAN traffic over a GRE or IPsec tunnel to one or more mobility controllers located in the distribution or core of the network.

Typically one or more master Multi-Service Mobility Controllers are installed in the data center, and are used as the central configuration and management point for all Aruba wireless LAN and remote access points. Large sites typically use a master controller which can support up to 500 remote controllers and can back-up a controller in a remote location in the event of an outage. Multiple master controllers can share the load of managing local controllers and remote sites, providing an elegant and cost effective system for supporting a healthcare enterprise’s business continuity and disaster recovery needs. The AirWave platform is a single management console for installations with multiple master controllers as well as for legacy non-Aruba wireless LANs.

For ambulatory facilities, physicians’ offices, and large clinics that are geographically separated from the main healthcare facility, a local mobility controller is required for application-continuity and security policies. The local controller automatically obtains its configuration from a master controller. User roles are applied based on group policies that are defined in the authentication infrastructure, and guests can be tunneled outside of the network to terminate in the DMZ. Each local controller automatically calibrates RF coverage to optimize application performance and fill any coverage holes. To extend wireless coverage into areas that are too costly to wire, Aruba APs can backhaul over Wi-Fi using a wireless mesh.

For physician-offices, patient homes, and satellite clinics, Aruba’s Remote Access Points (RAPs) cost-effectively and securely extend hospital-like connectivity. RAPs connect to the data center through any internet connection using either a local ISP or a 3G wireless modem, and then are automatically discovered and brought on-line without any user intervention.