U.S. DEPARTMENT OF DEFENSE MILITARY HEALTH SYSTEM PRESCRIBES ARUBA FOR WIRELESS CONNECTIVITY

The U.S. Department of Defense Military Health System (MHS) is responsible for providing health care to active duty and retired U.S. military personnel and their dependents. MHS serves approximately 9.5 million beneficiaries and employs more than 137,000 personnel in 65 hospitals, 412 clinics, and 414 dental clinics at facilities across the nation and around the world, as well as in contingency and combat-theater operations worldwide.

TECHNOLOGICAL INNOVATIONS DRIVE THE NEED FOR WIRELESS

Like all healthcare enterprises, MHS recently faced the need to fulfill growing demand for state-of-the-art health care amid requirements to reduce ever-increasing costs. Fortunately, technological advances in the health care field have produced many solutions that address the competing goals of improving care and reducing costs.

Applications such as electronic medical records systems, real time asset tracking and patient monitoring systems all work to improve processes and free healthcare providers from paperwork, allowing them to spend more time with patients.

MHS' specific technology initiatives include the Armed Forces Health Longitudinal Technology Application (ALTHA), replacing the military's paper-based medical records system with an electronic medical records (EMR) system, and the Defense Medical Logistics Standard Support (DMLSS) program which streamlines the management of medical supplies.

To support these new applications, MHS needed a network that enabled fast, secure and reliable transmission of medical data, untethered its mobile workforce, and could be easily incorporated into existing systems.

MHS also required a single network architecture that supported mobile personnel, medical devices and patient care applications in a reliable and cost effective manner and could interoperate with the differing networks already deployed throughout all MHS facilities.

REQUIREMENTS:

- Fast, secure and reliable transmission of data through a variety of devices including laptops, handheld clients and medical equipment

- Wireless connectivity that could be easily incorporated into existing systems

- Adherence to federal security requirements including FIPS, DoD Directive 8100.2 and Common Criteria

- A single network architecture that supported mobile personnel, medical devices and patient care applications

- Installation in a wide variety of buildings, some with older infrastructure, allowing mobility throughout the facility

SOLUTION:

- Aruba 6000 Mobility Controller
  - Policy Enforcement Firewall (PEF) software enforces per-user and per-application security policies
  - Wireless Intrusion Protection software defends the network against wireless threats to network security
  - Adaptive Radio Management (ARM) automatically configures every AP to idealize the RF/WLAN based on their neighbors and the environment
- AP-70 and AP-65 APs

Additionally, MHS needed a solution that provided secure transmission of data through a variety of devices including laptops, handhelds and medical equipment. Since staff and equipment were always on the move, MHS required a network that would allow for mobility throughout their installations.

MHS faced some significant challenges. Many healthcare technology solutions require dedicated and often proprietary networks for each type of medical system or application, inflating both capital and operating budgets.

Most commercial wireless network solutions did not meet stringent government and DoD-specific security requirements such as FIPS and DoD Directive 8100.2. These early wireless solutions were often slow and unreliable, suffering from an inability to effectively propagate RF signals throughout all of the MHS installations, some of which were 50+ year-old buildings.

SECURELY PROTECTING SENSITIVE DATA

To address these needs and challenges, MHS selected Aruba Networks as one of two approved vendors for their health care mobility networks, and Aruba's partnership with MHS has been phenomenal. As of April 2010, Aruba wireless LANs have been installed in 47 hospitals and 10 clinics, representing over 80% of all MHS secure WLAN deployments.

The Aruba solution provides secure FIPS-compliant WLAN systems that include centrally managed 802.11 a/b/g/n access points (APs) and Mobility Controllers.

Unlike other solutions, Aruba WLAN systems are completely self-contained and do not require ancillary security appliances or cryptology overlays. All functions, such as wireless intrusion detection, encryption/decryption and firewalling are provided by the Aruba Mobility Controller.

The result is a significant reduction in costs by eliminating the need for additional hardware, and less hardware also means Aruba WLANs are easier to manage because all functions are within one device.

In addition, having all user data managed for security and quality-of-service (QoS) functions by one device lowers latency and increases overall performance. Further, because all security features are centrally located in the Mobility Controller, the APs transparently pass the encrypted data between users and the Controller, and therefore do not pose a security risk as they do not contain sensitive key material, eliminating the need for secure enclosures and regular inspections of the APs.

IMPROVING PERFORMANCE AND REDUCING COSTS

Aruba's Adaptive Radio Management (ARM) addressed the RF issues posed by the older MHS facilities by using automatic, infrastructure- based controls to maximize client performance and enhance the stability and predictability of the entire WLAN.

BENEFITS:

- The Aruba FIPS certified multi-service controller has an integrated role-based firewall and wireless intrusion protection system to safeguard medical and patient data

- End-to-end security where both user authentication, traffic validations and encryption extends from the client – including laptops, handheld devices and other wireless devices – to the Mobility Controller

- The Aruba solution has the ability to handle real time applications such as voice and video without requiring the addition of client proprietary software

- The Aruba solution is easy to install and can also be deployed as an overlay, plugging APs into any port on the network

- All management is performed within the centralized Mobility Controllers, which reduces costs by eliminating the need for AP security and management

- Aruba's Adaptive Radio Management (ARM) automatically maximizes coverage and identifies interference, eliminating the need for site surveys and ensuring all mission critical applications get sufficient resources

Using ARM, the Aruba system detects challenging RF environments and accommodates them automatically through changes to the channel and power settings. This eliminated the need for expensive site surveys or manual performance tuning and allowed MHS to get their network up and running more quickly. ARM gave MHS a high-performing network without all the costs and management oversight traditionally associated with wireless networks.

FACILITATING THE ADOPTION OF NEW TECHNOLOGIES AND APPLICATIONS

Another unique feature of the Aruba solution is the ability to handle real-time applications such as voice and video. Aruba's ARM software, housed in the controller, allows mixed 802.11a/b/g/n client types to interoperate at the highest performance levels, allocates RF airtime fairly and avoids or mitigates co-channel interference, all without requiring the addition of client proprietary software.

ARM allows sharing and optimizing of bandwidth so there is no need to set up separate classes of service for data, voice or video. The Aruba controller is the only MHS approved solution that is able to specifically identify a voice call and optimize the network accordingly.

The versatile Aruba solution allows MHS staff to speed adoption of mandated initiatives such as AHLTA and has also sparked new use cases from various MHS installations.

Some facilities are using Aruba's system to wirelessly keep track of medical equipment such as wheelchairs and defibrillators, enabling staff to view a screen on their client device that indicates where a piece of equipment is, whether it is in use and how long it has been idle.

Other sites are investigating using the Aruba network to wirelessly monitor IV pump monitors and similar equipment. And because the Aruba solution can easily handle real time applications, one hospital is using Aruba's WLAN with the Vocera Nurse Call System giving caregivers instant access to patient bedside notifications and respond more quickly to patient needs.

Aruba is the MHS' overwhelming choice for its healthcare mobility solutions. The Aruba WLAN system meets or exceeds all DoD security requirements such as FIPS, Common Criteria and DoD Directive 8100.2, and is compatible with virtually all existing wire line and wireless networks within MHS facilities making deployment quick, easy and cost effective.

The centralized management function simplifies security and improves RF management and system performance. Most importantly, the Aruba solution has allowed MHS to develop and deploy numerous technological advances that help MHS achieve its goal of offering state-of-the-art, cost effective patient care across the nation and around the world.