

Sharp HealthCare Switches to Aruba for Centralized Management and Protection of Open Wired Connections

Sharp HealthCare, an integrated regional health care delivery system with 11,000 employees, provides a full spectrum of health care facilities and services to a population of more than three million San Diego county residents. To enhance the quality of treatment, Sharp initially deployed a distributed wireless system. Sharp is now making a system-wide move to centralize its wireless infrastructure to lower operations costs, tighten security and automate management and troubleshooting.

Installation of Sharp HealthCare's wireless environment was originally driven by three factors:

- 1) The deployment of the Electronic Medical Record (EMR) System on mobile carts used to access patient admission data, health history and lab results
- 2) Innovative new mobile applications such Wi-Fi equipped intravenous (IV) pumps that safeguard medication applications to patients remotely and
- 3) Capitalizing on the efficiency of hand-held units preferred by hospital workers as they moved throughout the hospital treating patients.



A critical consideration in the decision to establish a wireless LAN (WLAN), however, was the need for multi-layered security that addressed protecting the air, the data, the network and the user - simultaneously. The federal government had issued new standards for patient confidentiality under the Health Insurance Portability and Accountability Act (HIPAA). During the transfer of wireless data, there needed to be absolute certainty that patient records were not put into jeopardy.

Covering seven hospitals and forty clinics spread over fifty square miles, Sharp's legacy wireless environment was built using conventional access points attached to the existing wired network. For link layer security, Sharp initially used Wireless Equivalency Protocol (WEP), but then moved to the Lightweight Extensible Authentication Protocol (LEAP). With the move came headaches as changes to hundreds of APs had to be manually administered. Now, unsure of LEAP's viability, Sharp is adopting a 802.1X model using PEAP. But this time, the move is as simple as flipping on a switch - literally.

While LEAP worked initially, eventually problems arose, as troubleshooting became an issue. Migrating from the old APs to new APs came as a result of this evolution. Even with this change in place, the IT staff had to physically sit in the hospital units (for example, surgical intensive care) to troubleshoot applications running on the wireless networks - a major issue for hospital staff dedicated to saving lives in critical care situations.

Consequently, Sharp is undertaking a system-wide migration to a centralized wireless architecture from Aruba Networks to streamline the deployment and ongoing management of its entire wireless environment. Sharp estimates that the move to centralized wireless will reduce operational costs currently associated with its existing distributed WLAN by up to 80 percent.

SHARP®

Company Overview

Headquartered in San Diego, CA, Sharp HealthCare provides health care facilities and services to a population of more than three million San Diego county residents.

Requirements

- Seamless integration with existing Cisco wireless network
- RF monitoring
- Centralized management
- Secure authentication and access controls

Solution

- Aruba 5000 modular Mobility Controller
- Dual-band, dual-purpose 802.11a+b/g Aruba 52 access points

Benefits

- 80% less time spent on maintenance
- Ease of scalability and integration
- Centralized security and control for entire WLAN
- Visibility of traffic on network

Initially, the Aruba Networks Access Points (APs) were utilized as RF monitors to identify and disable rogue APs on each hospital network. Now, from its data center, Sharp can handle all hospitals wireless network deployments as a single system. In addition, Sharp is using the Aruba WLAN system to secure open wired ports in conference rooms, lobbies and other open areas. To protect against viruses and potential misuse of the network, guests connected to open wired ports are challenged to authenticate before receiving network access via a captive portal on the Aruba system. Authenticated users are then provided access to certain resources based on their access policies while non-authenticated users are limited to Internet-only access. With Aruba's integrated user-aware firewall, a single SSID supports unique user groups, each with different authentication requirements as well as access controls. To simplify management, configuration and administration, multiple VLANs can be mapped to a single SSID.

Sharp currently has 200 third-party "fat" access points installed across its health care system to support hundreds of wireless users and devices. As it moves to a centralized wireless architecture, Sharp is doubling the number of APs, adding dedicated RF monitors and introducing 802.11a services in key areas such as emergency rooms and intensive care units.

Sharp has deployed the Aruba 5000 modular Mobility Controller in its data center and dual-purpose Aruba AP 52 access points scattered throughout its hospitals - creating a seamless WLAN overlay that leverages Sharp's existing L2/L3 IP network as transport. Dedicated gigabit links connect each hospital to Sharp's data center. Sharp plans to deploy Aruba 2400 Mobility Controllers in each hospital for resilience, direct power and serial-over-Ethernet connectivity and 802.1X support for wired users.

The Aruba mobility controller contains a patented classification engine coupled with sophisticated RF monitoring that lets administrators protect the air by automatically detecting unauthorized users, destroying rogue APs and ensuring users don't associate with interfering APs. With the portable nature of the hospital staff, Aruba's secure mobility gives users of 802.11 mobile devices secure access while moving within and between campus buildings and subnets. An integrated firewall applied on a per-user basis allows administrators to establish unique access and security policies for different users/user groups. Policies are centrally configured and propagated throughout the network so administrators can enforce desired security levels.

"Distributed architectures are neither efficient nor economical. In the past, we were forced to manage and troubleshoot our wireless network manually. When wireless problems occurred at a hospital, we literally had to drive to the location, troubleshoot the problem in the hospital, capture wireless traffic, then come back to perform analysis," said Gary Jenkins, Senior Network Engineer. "With the Aruba system, I can now do in minutes what took me at least two hours to do before - without the traveling or hospital disruption."

An additional benefit to integrating the Aruba devices in conjunction with existing devices was the ease offered in the plug-and-play APs. To add capacity Sharp merely has onsite hospital staff plug an Aruba AP into the Ethernet network. Once connected the AP automatically registers to with the switch, uploads its configuration, channel plans and power setting and is controlled by the Aruba controller. IT staff isn't required to drive to each hospital for on-site installation and configuration. Any changes or tuning required, is then performed by Sharp IT staff within its data center operations.

Moving forward, Sharp is migrating to an 802.1X security model for both its wireless and wired network and plans to leverage Aruba's RF location and triangulation capabilities to track users and devices in real time.

"Before Aruba we were RF blind, now we can see. Now, from my desk, I can easily capture traffic at any hospital and import it into my traffic analysis application to troubleshoot problems or optimize the wireless network."

Gary Jenkins
Senior Network Engineer
Sharp HealthCare