CASE STUDY

Healthcare

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 healthcare facilities and services to San Diego County's more than three million 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 initiatives:

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

A critical consideration in the wireless LAN (WLAN) decision, however, was the need for multi-layered security to protect the air, the data, the network and the user - simultaneously. This was in response to the Federal government's new standards for patient confidentiality under the Health Insurance Portability and Accountability Act (HIPAA). During the transfer of wireless data, patient records had to be absolutely secure.

Covering seven hospitals and forty clinics spread over fifty square miles, Sharp's legacy wireless environment was built using thick 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 made manually. 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 a switch – literally.

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

Consequently, Sharp is undertaking a system-wide migration to a centralized wireless architecture from Aruba Networks to streamline the deployment

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

and ongoing management of its entire wireless environment. Sharp estimates that the move to centralized wireless will reduce operational costs associated with its distributed WLAN by up to 80 percent.

Initially, the Aruba Access Points (APs) were used as RF monitors to identify and disable rogue APs. Now, from its data center, Sharp can handle all hospitals wireless networks 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 network misuse, guests connected to open wired ports must authenticate before receiving network access via a captive portal on the Aruba system. Authenticated users are 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 multiple user groups, each with different authentication requirements and access controls. To simplify management, configuration and administration, multiple VLANs can be mapped to a single SSID.

Sharp currently has 200 third-party "thick" access points 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 controller's patented classification engine works with sophisticated RF monitoring to protect the air by automatically detecting unauthorized users, blocking rogue APs and ensuring users don't associate with interfering APs. With the mobile nature of the hospital staff, Aruba provides 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 automatically propagated throughout the network.

"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 previously took me at least two hours to do – without the traveling or hospital disruption."

An additional benefit of 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 controller and downloads its configuration, channel plans and power setting. IT staff isn't required to drive to each hospital for on-site installation and configuration. Any changes or tuning required is performed by Sharp IT staff from 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.

CASE STUDY

Healthcare

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.

"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

ARUBA networks

WWW.ARUBANETWORKS.COM

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