



CASE STUDY Healthcare

Aruba Has the Right Medicine for the University of Utah Health Sciences Center

The University of Utah Health Sciences Center (UUHSC) is a multidisciplinary medical facility serving Salt Lake City and its suburbs. Named one of “America’s Best Hospitals” by U.S. News & World Report, the 400-bed teaching hospital was the first Level 1 trauma center in the Salt Lake Valley. It also maintains some 20 off-site specialty hospitals and clinics. Just as the community relies on the hospital for a full complement of medical services, UUHSC relies on Aruba Networks for its secure, scalable 802.11 wireless LAN (WLAN)—the mobility infrastructure that lets UUHSC keep pace with a staff that’s always on the move.

RUNNING VOICE AND DATA OVER A MEDICAL MOBILITY INFRASTRUCTURE

UUHSC’s mobility infrastructure supports both voice and data applications. The hospital’s Voice over Wi-Fi (VoFi) implementation enables doctors, nurses, and clinicians to communicate anytime, anywhere. Voice is literally a lifesaver in UUHSC’s Emergency Department, where every second counts. What’s more, the ability to get answers in real time streamlines and simplifies processes in other departments.



UUHSC also runs a mix of data applications over the same infrastructure without worrying about dropped sessions or degraded voice quality. Applications include e-mail, file and print services, and Internet access. In addition, laptop-based Computers-on-Wheels (CoWs) are used for EMR (electronic medical records) and a real-time charting application for rehabilitation patients. Both are deployed in a Citrix

thin-client environment to ensure that the loss of computing platforms does not compromise patient data. There’s also secure guest access for patients and visitors, segmented from UUHSC’s production environment using Aruba’s stateful firewall.

Mobility is a key contributor to UUHSC’s top-ranked patient care, as well as its ability to keep day-to-day operations time- and cost-efficient. Yet patients and personnel would not enjoy these benefits if Bo Mendenhall, director of wireless security, hadn’t convinced the administration to cast its legacy WLAN.

THE LIMITATIONS OF A LEGACY WLAN

UUHSC’s original WLAN was built with “thick” APs—chiefly Cisco 340/350s and Foundry IronPoint 200s. Centralized management was nonexistent; changes and upgrades had to be made manually, at each of the more than 200 APs. In addition, some of the APs were deployed in the ceiling ducts, making them difficult to access, and work done in the operating rooms or intensive care units compromised the sterile environment.

The lack of centralized management meant that Mendenhall and senior 802.11 wireless engineer Andrew Goble had no way of anticipating or identifying problems such as overburdened APs, or finding and shutting down rogue APs.



Requirements:

- Secure, scalable 802.11 mobility infrastructure
- Support for VoIP
- Support for mobile data applications, including EMR, Internet access, file transfers, and e-mail
- Centralized management
- Airtight security
- No dropped calls or sessions

Solution:

- 500 Aruba AP-65, AP-70, and AP-61 thin APs deployed across 35 buildings
- Aruba 6000 chassis running ArubaOS, equipped with Aruba PEF (Policy Enforcement Firewall) and WIP (Wireless Intrusion Protection) modules

Benefits:

- Mobile voice enhances patient care; increases efficiency hospital-wide
- Centrally managed mobility provides unified view of AP operation, load, attached devices; speeds troubleshooting
- Thin APs streamline and simplify deployment
- Advanced security detects and shuts down rogue APs, blacklists rogue users
- Identity-based policies simplify management while increasing security
- Sophisticated Quality of Service capabilities and very fast roaming ensure excellent VoFi performance

CASE STUDY

Healthcare

Mendenhall knew this legacy infrastructure couldn't support demanding mobile applications such as VoFi. And it had another major weakness: security. "When the Wi-Fi infrastructure was originally deployed, it offered no encryption," says Mendenhall. "We were wide open." Ultimately, UUHSC implemented WEP (Wired Equivalent Privacy) before it became clear that this scheme was easy to hack.

Faced with these shortcomings, the hospital administration gave Mendenhall the green light to build a mobility infrastructure that was secure, manageable, and able to support demanding applications like VoFi.



EASING DEPLOYMENT, MANAGEMENT, AND SECURITY

Mendenhall shortlisted five vendors: Aruba, Airepspace, Cisco, Extreme, and Trapeze. He called in a third-party to help make a final decision. The nod went to Aruba. What Mendenhall liked most about his new mobility partner was ease of deployment, centralized management, and security. He also cites Aruba's "constant commitment to innovation" as a deciding factor.

Mendenhall and Goble ultimately deployed approximately 500 Aruba APs in 35 buildings. Once the Ethernet drop is in place and Power-over-Ethernet is available, setting up an AP at an off-site clinic takes just a few minutes. It's merely a matter of "plugging it in and waiting for it to find and attach itself to the network," comments Mendenhall.

To ensure easy access, the Aruba APs are all mounted to the ceiling grid or below the ceiling line. "This ensures we're not lifting ceiling tiles or dragging ladders through ICU if we need to get to an AP," explains Mendenhall.

UUHSC deployed an Aruba 6000 mobility controller running ArubaOS, the modular and flexible operating system that forms the core of the Aruba Mobile Edge Architecture. The 6000 is equipped with Aruba's Policy Enforcement Firewall and Wireless Intrusion Protocol modules.

The result: Mendenhall can see and manage every AP from a central console. Aruba's PEF module enables identity-based policies that follow personnel on the move. Employees can all be placed on a single SSID/VLAN (Service Set Identifier/Virtual LAN), while still retaining individual access privileges.

The WIP module enhances security by shutting down rogue APs and blacklisting users who've attached to them. Mendenhall also employs about 80 thin APs as dedicated Air Monitors (AMs) to keep close watch on UUHSC's airlinks. The AMs can spot a rogue AP in seconds; they also assist with RF management and troubleshooting, increasing network stability.

PROTECTING VOICE CALL QUALITY

With a stable, secure 802.11 mobility infrastructure in place, Mendenhall turned his attention to VoFi. UUHSC relies on Vocera's hands-free voice badges to enable voice communication. Aruba's application awareness makes it possible to support call admission control for Vocera badges. Voice-aware scanning enables Aruba to detect the presence of a Vocera badge and postpone AP radio-scanning activities to ensure optimal Quality of Service (QoS).

Approximately 150 Vocera badges are currently deployed, including about 60 in the Emergency Department. To further ensure that calls aren't dropped, Mendenhall uses a dense AP deployment throughout UUHSC. Dense coverage also helps guarantee plenty of bandwidth for both voice and data.

Mendenhall realizes that mobility is an unstoppable trend. "Ultimately, everything is going to be wireless." He adds, "There's no limit to what we can do with the Aruba system."

Organization Overview:

The University of Utah Health Sciences Center (UUHSC), which was founded in 1955, is committed to superlative patient care, rigorous research, and advanced academic studies. The hospital maintains a Level 1 trauma center, as well as 20 clinics that provide general and specialized medical services to greater Salt Lake City. UUHSC has been honored as one of "America's Best Hospitals" by U.S. News and World Report more than a dozen times.

"Aruba gives me everything I need: security, centralized management, and ease of deployment and maintenance. There's no limit to what we can do with the Aruba system."

Bo Mendenhall

*Director of Wireless Security
University of Utah Health Sciences Center*



WWW.ARUBANETWORKS.COM

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