# Restoring a Hospital's Wireless LAN Back to Health

***Our thanks to Fluke Networks for allowing us to reprint the following article.***

**At a Glance**

**Industry:** Medical

**Challenge:** Wireless LANS provide a myriad of benefits in a hospital environment; however, deployment can be tricky due to unique challenges, such as building architecture, device interference, and security issues. And, when the wireless network in a hospital suddenly stops working, the consequences can be disastrous.

**Solution:** Fluke Networks' AnalyzeAir™ Wi-Fi Spectrum Analyzer

**Results:** Fluke Networks' AnalyzeAir allowed the user to quickly determine why the new patient monitoring system had suddenly failed. It immediately identified the type and exact location of the troublesome devices that were wreaking havoc on the wireless network.

**Overview**

When he left for home that night, the network engineer was no longer thinking about the wireless LAN (WLAN) deployment in the Critical Care Unit (CCU). That project had been completed almost two months ago and the patient monitoring systems were working perfectly. A few hours later, his phone started ringing off the hook and shortly after that, he was back at the CCU trying to figure out why the monitoring systems had suddenly stopped communicating on the WLAN.

**Wireless LANs – Just What the Doctor Ordered**

Wireless LANs are especially well-suited to hospitals. Patients and the staff are constantly moving, which is much easier to manage with a network that can follow them around. WiFi phones can be used for fast communications among staff. There are typically many guests in the hospital who desire wireless Internet access. Wireless LANs can even be used to track high-value portable assets, such as defibrillator carts and portable ultrasound machines. Studies show that hospitals cannot locate 15-20% of such devices they own.

Unfortunately, hospitals are also challenging environments for wireless LAN deployment. Most hospitals are multistory structures which introduce a third dimension into coverage planning as wireless network signals can easily pass through ceilings and floors. Signals can get lost in management spaces between floors dedicated to support systems such as backup power, oxygen, and telemetry. Interference with other wireless devices for patient telemetry must be avoided. Radiology and Nuclear Medicine departments have specialized shielding that can completely block wireless signals. And given the requirements for patient privacy (such as that driven by HIPPA), wireless networks in hospitals are required to be highly secured – especially as there may be hundreds of guests in the facility at a time.

Wireless LANs can be used to provide the patient monitoring, but are engineered to not interfere with telemetry patient monitoring services. Nor should they, in most cases, interfere with non-wireless, non-mission-critical medical equipment, such as heart monitors, defibrillators, or other digital devices. As with all hospital equipment, the biomedical department should perform an analysis and review for safety and compatibility purposes.

The most effective way to ensure a successful deployment under these conditions is to perform a site survey, using an expert consultant or with a tool such as Fluke Networks InterpretAir™ WLAN Site Survey Software. A site survey enables more accurate prediction of infrastructure needs prior to purchasing a WLAN infrastructure, resulting in more accurate time and cost estimates for the network deployment. It is also a process to help verify the WLAN is performing as designed after installation.

Using a full-featured wireless site survey software can save an enormous amount of time, money, and frustration when compared to paper-based site survey techniques.

**A Good Start**

By following good design principles, and performing a site survey, the medical center was able to get the CCU WLAN up and running successfully and began using it for patient monitoring. There was no impact on other wireless devices in the hospital, and the project was progressing smoothly.

But one evening, the patient monitoring system suddenly stopped responding – almost entirely. Since it had been working for several months with no complaint, the network engineer immediately suspected that something was interfering with the new WLAN.

**Solving the Problem**

The very next day, the Network Engineer hired a Radio Frequency (RF) Engineering Consultant to investigate the problem. Given the short notice and urgent nature, the four-hour study, complete with a spectrum analysis of the affected area, totaled nearly $5,000. The study confirmed that there was external interference on channels 6 and 11. Of course, the Network Engineer already suspected as much. The Consultant recommended the hospital restrict its access points to channel 1 in the affected areas.

Although that would allow them to manage the problem, being limited to a single channel also limited the number of access points they could deploy and would result in overloading and poor performance. Rather than settling for the sub-par solution, the network engineer arranged an overnight purchase of a tool designed specifically for locating wireless interference problems.

**Fluke Networks' AnalyzeAir™ Wi-Fi Spectrum Analyzer**

AnalyzeAir provides clear visibility of the RF spectrum used by 802.11 a/b/g/n WLANs. Unlike a conventional spectrum analyzer, AnalyzeAir is designed for use by networking professionals. It provides an easy-to-understand, fast-start solution, allowing users to quickly identify the source of RF problems that prevent WLAN connectivity and impact performance.

AnalyzeAir software interprets the RF energy in the spectrum or channel and lists the devices that are transmitting – associating real devices with the energy pulses. It automatically identifies Bluetooth® devices, cordless phones, microwave ovens, analog video cameras, and RF jammers. Then the "Device Finder" feature makes it easy to pinpoint the physical location of these troublesome or unauthorized devices.

**Fast Start, Fast Answers**

Within 30 minutes of installing and launching AnalyzeAir, the network engineer had identified the problem: a tiny analog video camera, which used the same bandwidth as the wireless network. This sort of camera has a powerful transmitter which allows it to be used far from the base station – but also wreaks havoc on an 802.11 network. After further checking, three more cameras were found. Where had these "unauthorized" cameras come from?

A little calling around led them to find a surprising culprit – the hospital's security department, who had installed the cameras in an attempt to reduce the high rate of theft in various areas. The security staff had no idea that these devices were so damaging to the wireless network and immediately agreed to replace them with 802.11-compliant devices that could use the existing wireless network without significantly impacting it.

**Wireless – Be Prepared**

Hospitals benefit more than most from wireless technologies, but must also work harder than most to deploy them. In order to do so, the IT staff should be equipped with the right tools for both pre- and post-deployment problem solving. This includes not only tools for site surveys and locating interference, but also portable troubleshooting tools and tools for monitoring the wired side of the network.


FLUKE networks

1547 N. Trooper Road • P. O. Box 1117 • Worcester, PA 19490-1117 USA
Corporate Phone: 610-825-4990 • Sales: 800-832-4866 or 610-941-2400
Fax: 800-854-8665 or 610-828-5623 • Web: www.techni-tool.com