

How Wireless LANs Can Enhance the Clinical Environment

Chris Riha

The last several years have seen a significant increase in the deployment of wireless local area networks (WLAN) in health care institutions. That trend is expected to continue. In one report, the California-based research firm Frost & Sullivan put the 2001 U.S. hospital market for WLANs at \$193 million—with 10% annual growth forecast through 2005.¹

Health care facilities deployed some of the first wireless networks, such as cardiac monitoring telemetry systems, more than 30 years ago. With increased demand for electronic medical records, hospital settings continue to seem ideally suited for wireless devices. Doctors and staff that appear to be in constant motion must be connected to knowledge bases for treatment and diagnosis of patients.

Wireless applications offer the following advantages over hardwired networks:

- ♦ **Mobility:** Physicians and staff are free to roam from patient to patient in an efficient manner while maintaining connectivity to a central network.
- ♦ **Ease of Installation:** With less cabling required, installation times are generally less than when having to install cable at each connection point.
- ♦ **Scalability:** It is a simpler task to expand or reconfigure a wireless network than a conventional hardwired network.

Background

In the 1960s the first application of wireless networks was an application of technology developed by NASA for monitoring physiological parameters of astronauts in flight. This technology evolved into commercial medical telemetry systems—low power, proprietary operating

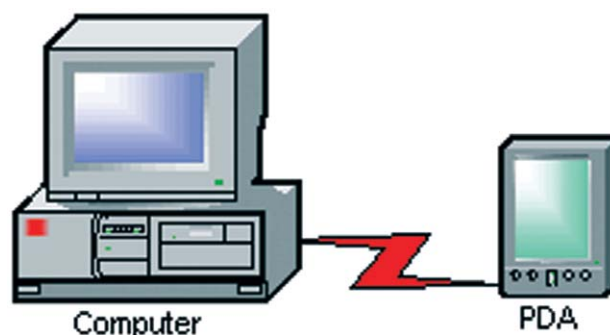


Diagram 1. An infrared connection from a desktop device to a PDA.

systems transmitting in the 450-470 MHz range. Ethernet was developed in the mid-1970s by Xerox. Xerox was soon joined by DEC and Intel in developing standards published in 1980 in the Ethernet Blue Book. The initial manufacturers standards were known as the “DIX” standards. The acronym is comprised of the letters of the original corporations behind the research and development of a 10 megabits per second (Mbps) wired network.

Pressure for a more generic and open standard resulted in the Institute of Electrical and Electronic Engineers (IEEE) developing the first open Ethernet standard in 1983 called the IEEE 802.3, named after the working group responsible for its development.

In the early 1990s, the first wireless non-medical telemetry proprietary networks developed and operated in the 900 MHz range were low speed (1-2 Mbps) with little commercial acceptance. In the mid-1990s wireless manufacturers began offering products operating in the unlicensed 2.4 gigahertz (GHz) spectrum, which enabled transmission rates more comparable to hard-wired Ethernet networks.

In 1997, the IEEE published the 802.11 standard, which supported infrared and two types of radio frequency (RF) transmission protocols, in the 2.4 GHz fre-

Chris Riha, CCE, is currently the PACS manager for the Information Services Department of the Carilion Health System in Virginia. Riha has previously been a member of DICOM Working Group 15.

Current Issues

How Wireless LANs Can Enhance the Clinical Environment

quency band: Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). Today, several 802.11 standards exist: 802.11b, which supports transmission speeds up to 11 Mbps; and the newer 802.11g, which supports speeds up to 54 Mbps.

The Wireless Ethernet Compatibility Alliance (WECA) has established further standards called the WiFi standard for manufacturers to ensure interoperability. Products that meet this standard will have the WiFi label and offer a greater chance for a plug-and-play connection between different manufacturers.

While international manufacturing standards may be in place, governments in many countries regulate RF transmission power from wireless network devices as demonstrated by the following examples:

- ♦ 1 watt for the United States
- ♦ 10mW per 1 MHz in Europe
- ♦ 10mW for Japan.

Additionally there are different frequencies approved for use in Japan, the United States, and Europe. Thus, interoperability and coverage areas for products differ in

Asia, Europe, and the U.S., although the 802.11 standard does require frequencies in the 2.4 GHz range to be used for the RF carrier.

WLAN Transmission Techniques

The vast majority of commercial wireless networks today employ the RF spectrum rather than infrared due to the increased coverage available with a RF signal, and the security options offered with FHSS and DSSS technologies. The two types of RF transmission protocols described below were developed by the military for securely transmitting data on a RF carrier frequency:

- ♦ **Frequency-Hopping Spread Spectrum (FHSS):** FHSS uses a narrow band RF carrier that changes carrier frequencies in a pattern known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise with no intelligible information.
- ♦ **Direct-Sequence Spread Spectrum (DSSS):** DSSS generates a chipping code, which encodes each data

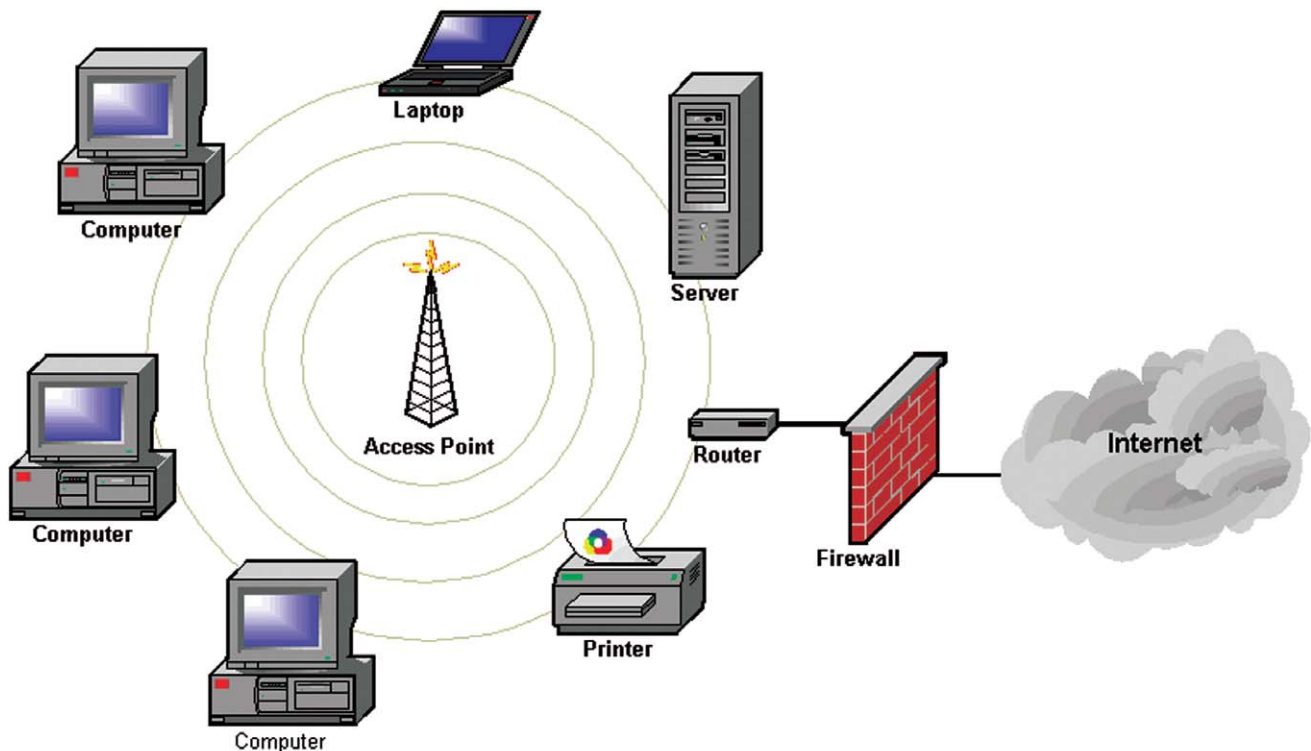


Diagram 2. Multiple users connect to a common server.

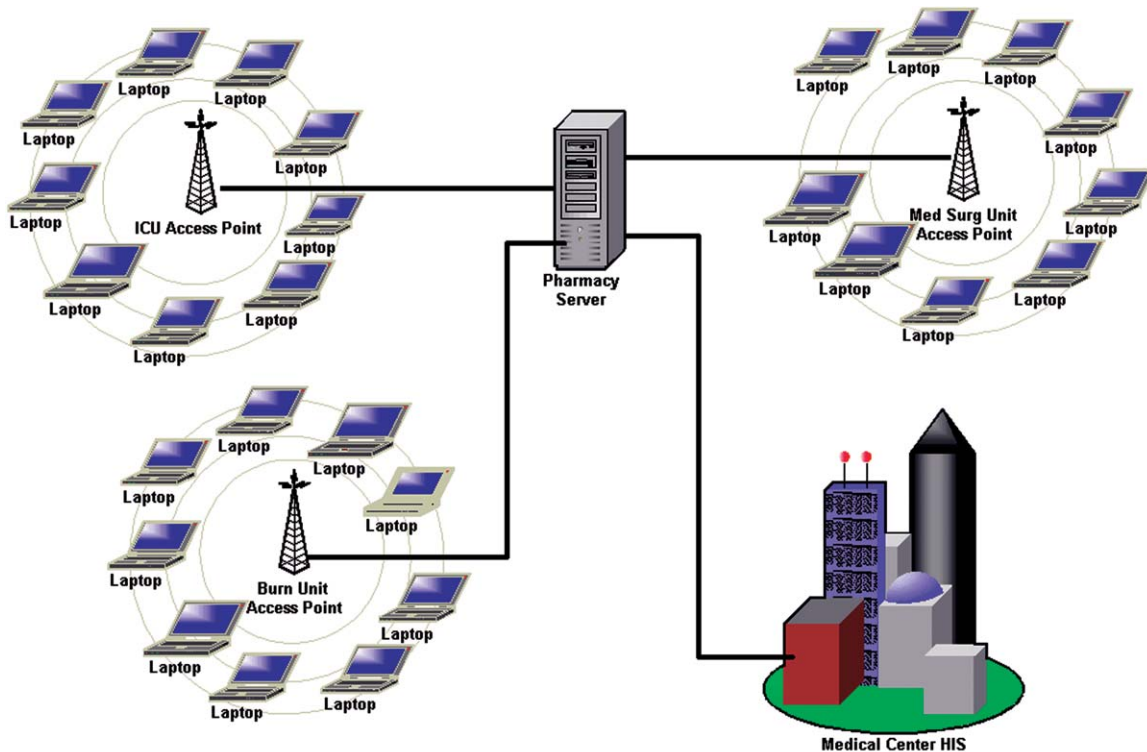


Diagram 3. A wireless network integrated into a health care facility's wired backbone.

bit. This produces a low-power, wide-band noise in the frequency domain (thus rejected by narrow-band receivers). The greater the number of chips in the chipping code, the less likely that original data will be lost. This is the most commonly used among spread spectrum technology. To an unintended receiver, DSSS appears as low-power, wide-band noise and is rejected (ignored) by most narrow band receivers.

- ♦ **Infrared:** Infrared transmissions are most commonly short distance line-of-site transmissions and are predominately a peer-to-peer type of network. Examples of these would be a PDA to another PDA or a portable device to a printer. Diffuse or reflective infrared systems are also available to expand the range of this technology but are rarely used in commercial applications.

Network Topologies

The simplest wireless technology is the peer-to-peer network, as depicted in Diagram 1 (see page 45), with an infrared connection from a desktop device to a PDA.

A simple WLAN may consist of several wireless

devices networked together via an RF access point, which effectively doubles the range that networked devices can connect. The configuration shown in Diagram 2 can support a number of networked devices with a single access point and is commonly utilized in a smaller physical area such as a freestanding clinic. This topology allows multiple users to connect to a common server, which could contain a database or application. Users would also have a single-secure access to the Internet via the router.

A more complicated WLAN is shown in Diagram 3, which depicts a wireless network integrated into a health care facility's wired backbone. Diagram 3 is intended to show how a patient medication administration application could be used on portable devices by clinical staff in multiple locations.

Note that the connection from the access points to the pharmacy server is via the hospital backbone, as is the connection from the server to the hospital information system (HIS). This type of configuration would allow clinicians to easily move from patient to patient while maintaining the connection to a database detailing medications for each patient.

Key Considerations

Several factors must be considered when planning or installing WLANs in health care applications. The two predominant factors are security and reliability.

Security is an important issue and patient identifiable health information is protected by law in many countries. In the U.S., it is protected under the Health Insurance Portability and Accountability Act (HIPAA). Once data is transmitted via a RF carrier, it is much easier to intercept than physically tapping into a hardwired network. Therefore encryption techniques are mandatory. Both FHSS and DSSS protocols were designed to ensure secure transmissions of data. However, these technologies do not encrypt the data; instead they code the transmissions. There are encryption techniques that can be employed to add another level of security, which is required by HIPAA. Information on wireless encryption tools is available from the National Institute of Science and Technology (NIST).³

Reliability is another key issue due to the potential for RF interference as the 2.4 GHz spectrum is unprotected. RF interference may come from a wide variety of sources: aircraft avionics and radar, weather radar, military communications, other WiFi devices, and microwave transmissions (either from ovens or microwave transmitting towers). A complete RF survey should be incorporated into any project planning process to reduce the chance of conflicting signals. Additionally, when additional RF nodes are added to an existing WLAN, caution should be exercised to ensure that new devices do not interfere with existing traffic.

Summary

WLANs deployments in health care institutions offer clinicians opportunities to increase productivity and improve patient care with additional point-of-care access to information systems. However, they are not a panacea. Any data that needs guaranteed reliability and protection for outside interference, such as real-time cardiac monitoring, should be on networks operating in the Wireless Medical Telemetry Service (WMTS) range.

“WLANs offer many advantages over conventional wired LANs but they also offer many challenges in addressing security and reliability issues.”

—Chris Riha

The WMTS range, (608-614 MHz, 1395-1400 MHz, and 1429-1432 MHz), was established in 1999 by the FCC as a protected frequency range (in the U.S.) making these products less likely to have interference problems than devices operating in the 802.11 range.

Security challenges must also be addressed as each access point is synonymous with installing a RJ45 network jack in the parking lot of a facility and inviting the general public to connect to a network. Also, increased mobility of electronic devices means battery power; thus consideration will need

to be given to charging, maintaining, and disposal of batteries.

WLANs offer many advantages over conventional wired LANs but they also offer many challenges in addressing security and reliability issues. WLANs are not designed to replace conventional hard-wired network infrastructure; they are designed to augment the connectivity of LANs. Even with the 802.11g standard, which supports connectivity up to 54Mbps, large medical image files would not have enough bandwidth on this type of wireless network. Wireless networks can enhance the health care technology infrastructure but proper selection of technology and focus on the security and reliability during the planning and installation is a definite requirement.

Acknowledgment

The author would like to thank Brian Brindle for sharing some of his experiences in managing wireless networks in a health care environment. ♦

References

1. **Health Data Management.** 2002. Study: Wireless LANs. Available at: www.healthdatamanagement.com/html/PortalStory.cfm?type=trend&DID=8607. Accessed August 5, 2004.
2. **Department of Health and Human Services—Office for Civil Rights.** HIPAA: 2002. Washington, DC Department of Health and Human Services. Background information available at: www.hhs.gov/news/press/2002pres/hipaa.html. Accessed August 5, 2004.
3. **National Institute of Standards and Technology.** NIST Wireless Security Guidance SP 800-48. Dec. 4, 2002. Available at: http://csrc.nist.gov/wireless/S05_NIST-tk2.pdf. Accessed August 3, 2004.