ST. LUKE'S HEALTH CARE SYSTEM

Hospitals have been some of the earliest adopters of wireless local area networks (WLANs). The clinician user population is typically mobile and spread out across a number of buildings, with a need to enter and access data in real time. St. Luke's Episcopal Health System in Houston, Texas (www.stlukestexas.com) is a good example of a hospital that has made effective use wireless technologies to streamline clinical work processes. Their wireless network is distributed throughout several hospital buildings and is used in many different applications. The majority of the St. Luke's staff uses wireless devices to access data in real-time, 24 hours a day. Examples include the following:

- **Diagnosing patients and charting their progress:** Doctors and nurses use wireless laptops and tablet PCs to track and chart patient care data.
- **Prescriptions:** Medications are dispensed from a cart that is wheeled from room to room. Clinician uses a wireless scanner to scan the patient's ID bracelet. If a prescription order has been changed or cancelled, the clinician will know immediately because the mobile device displays current patient data.

- **Critical care units:** These areas use the WLAN because running hard wires would mean moving ceiling panels. The dust and microbes that such work stirs up would pose a threat to patients.

- **Case management:** The case managers in the Utilization Management Department use the WLAN to document patient reviews, insurance calls/authorization information, and denial information. The wireless session enables real time access to information that ensures the correct level of care for a patient and/or timely discharge.

- **Blood management:** Blood management is a complex process that involves monitoring both patients and blood products during all stages of a treatment process. To ensure that blood products and patients are matched correctly, St. Luke's uses a wireless bar code scanning process that involves scanning both patient and blood product bar codes during the infusion process. This enables clinicians to confirm patient and blood product identification before proceeding with treatment.

- **Nutrition and diet:** Dietary service representatives collect patient menus at each nursing unit and enter them as they go. This allows more menus to be submitted before the cutoff time, giving more patients more choice. The dietitian can also see current patient information, such as supplement or tube feeding data, and view what the patient actually received for a certain meal.

- **Mobile x-ray and neurologic units:** St. Luke's has implemented the wireless network infrastructure necessary to enable doctors and clinicians to use mobile x-ray and neurologic scanning units. This makes it possible to take x-rays or to perform neurological studies in patient rooms. This minimizes the need to schedule patients for neurology or radiology lab visits. The mobile units also enable equipment to be brought to the bedside of patients that cannot be easily moved. The wireless neurology and x-ray units have also helped to reduce the time between diagnosis and the beginning patient care.

Original WLAN

St. Luke's first WLAN was deployed in January 1998 and made the hospital an early pioneer in wireless health care applications. St. Luke's first wireless LAN was implemented in a single building using access points (APs) made by Proxim (www.proxim.com).

A principal goal of this initial installation was to improve efficiency. However, sometimes the WLAN had the opposite effect. The main problem was dropped connections. As a user moved about the building, there was a tendency for the WLAN to drop the connection rather than performing the desired handoff to another access point. As a result, a user had to reestablish the connection, log into the application again, and reenter whatever data might have been lost.

There were physical problems as well. The walls in part of the building were constructed around chicken wire, which interfered with radio waves. Some patients' rooms were located in pockets with weak radio signals. For these rooms, a nurse or doctor would sometimes lose a connection and have to step out into the hallway to reconnect. Microwave ovens in the kitchenettes on each floor were also a source of interference.

Finally, as more users were added to the system, the Proxim APs, with a capacity of 1.2 Mbps, became increasingly inadequate, causing ongoing performance issues.

Enhanced LAN

To overcome the problems with their original WLAN and reap the potential benefits listed earlier in this case study, St. Luke's made two changes [CONR03, NETM03]. First, the hospital phased out the Proxim APs and replaced them with Cisco Aironet (www.cisco.com) APs. The Cisco APs, using IEEE 802.11b, operated at 11 Mbps. Also, the Cisco APs used direct

sequence spread spectrum (DSSS), which is more reliable than the frequency-hopping technique used in the Proxim APs.
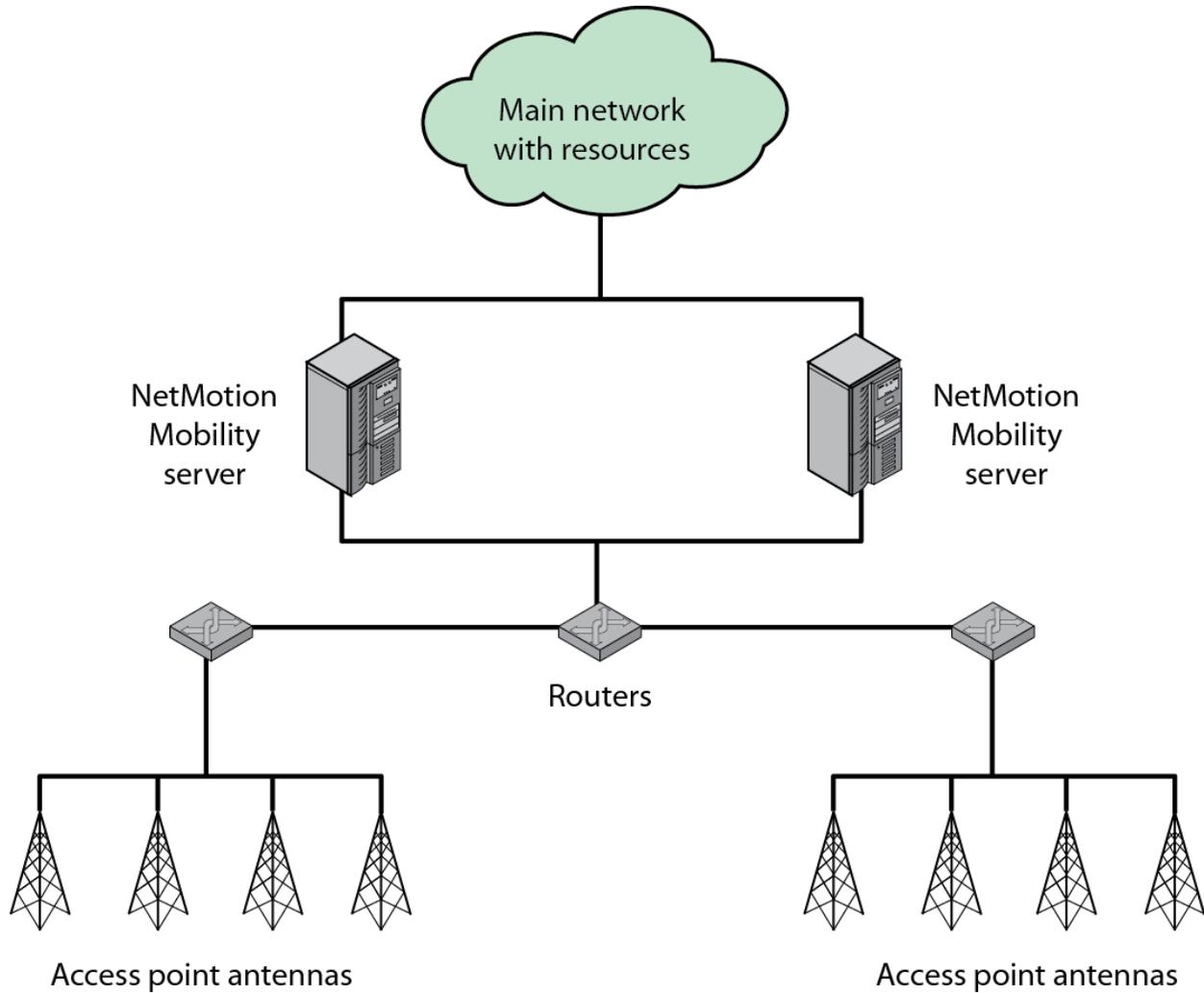

Figure C9.1   St. Luke's Wireless LAN

The second measure taken by St Luke's was to acquire a software solution from NetMotion Wireless (netmotionwireless.com) called Mobility. The basic layout of the Mobility solution is shown in Figure C9.1. Mobility software is installed in each wireless client device (typically a laptop, handheld, or tablet PC) and in two NetMotion servers whose task is to maintain connections. The two servers provide a backup capability in case

one server fails. The Mobility software maintains the state of an application even if a wireless device moves out of range, experiences interference, or switches to standby mode. When a user comes back into range or switches into active mode, the user's application resumes where it left off.

In essence, Mobility works as follows: Upon connecting, each Mobility client is assigned a virtual IP address by the Mobility server on the wired network. The Mobility server manages network traffic on behalf of the client, intercepting packets destined for the client's virtual address and forwarding them to the client's current POP (point of presence) address. While the POP address may change when the device moves to a different subnet, from one coverage area to another, or even from one network to another, the virtual address remains constant while any connections are active. Thus, the Mobility server is a proxy device inserted between a client device and an application server.

Enhancing WLAN Security

In 2007, St. Luke's upgraded to Mobility XE mobile VPN solution [NETM07]. This migration was undertaken to enhance security and compliance with HIPPA data transmission and privacy requirements. Mobility XE server software was deployed in the IT department's data center and client software was installed on laptops, handheld devices, and tablet PCs.

With Mobility XE running on both clients and servers, all transmitted data passed between them is encrypted using AES (Advanced Encryption Standard) 128-bit encryption. Mobility XE also serves as an additional firewall; devices that are not recognized by the Mobility XE server are not allowed to access the network. This arrangement helped St. Luke's achieve its IT goal of having encryption for all wireless data communications.

Mobility XE also enables the IT department to centrally manage all wireless devices used by clinicians. This allows them to monitor the

applications currently being used by any device or user, the amount of data being transmitted, and even the remaining battery life of the wireless device. If a Mobility XE device is stolen or lost, it can be immediately quarantined by network managers.

IT executives at St. Luke's view wireless networking as key lever in their quest to increase clinician productivity and improved patient care. Mobile EKG units have been deployed bringing the total of wireless devices in use to nearly a 1,000.

Discussion Questions

1. Visit the NetMotion Web site (www.netmotionwireless.com) and access and read other Mobility XE success stories. Discuss the patterns that can be observed in the benefits that Mobility XE users have realized via its deployment and use.

2. Do some Internet research on the security implications of HIPPA requirements for hospital networks. Discuss the major types of security mechanisms that must be in place to ensure hospital compliance with HIPPA requirements.

3. Do some Internet research on the use of VLANs in hospitals. Summarize the benefits of using VLANs in hospitals and identify examples of how St. Luke's could further enhance its wireless network by implementing VLANs.

Sources

[CONR03] Conery-Murray, A. "Hospital Cures Wireless LAN of Dropped Connections." *Network Magazine*, January 2003.

[NETM03] Netmotion Wireless, Inc. "NetMotion Mobility: Curing the Wireless LAN at St. Luke's Episcopal Hospital. *Case Study*, 2003. Netmotionwireless.com/resources/case_studies.aspx.

[NETM07] Netmotion Wireless, Inc. "St. Luke's Episcopal Health System: A Case Study in Healthcare Productivity." 2007. Retrieved online at: http://www.netmotionwireless.com/st-lukes-case-study.aspx