The Wireless Challenge
Achieving a Robust And Reliable Network

Phil Raymond

There is little argument that wireless connectivity in a hospital has many benefits in terms of clinical workflows, remote patient surveillance, mobility for clinicians and their patients, and even achieving meaningful use with data connectivity between clinical systems. There is also ample data showing that hospitals have chosen 802.11 wireless technology as the de facto standard for whole hospital data connectivity.

So are wireless medical devices, applications, and systems the perfect match for 802.11 wireless networks? Before answering, consider what we are trying to accomplish and how best to get there.

Why Do I Need a Robust and Reliable Network?

Today's hospital clinical systems are now depending on the wireless network as an enabling technology, so the answer to this question may be as simple as, "Why wouldn't I?" But it is important to explore the ways in which the wireless network is used in your hospital. Each hospital will have different systems, different types of devices, different numbers of devices, and even different policies, for example, those relating to BYOD or "bring your own device." And, of course, all this adds up to a radio frequency (RF) environment that is unique to that facility. From accurate departmental billing to using location technologies to provide patient family Internet access, there are many ways the wireless network is used, and each use may have different clinical implications or none at all.

A first step is to understand how your nurses and doctors are using their devices as part of their clinical workflows and daily operation. Do they rely on wireless network access to deliver safe and effective patient care? For example, if a doctor wants to pull up a radiology image while in a patient's room, is there a need for a robust and reliable wireless network? If a nurse is making a wireless "voice over Internet protocol" (VoIP) call at 2 a.m. to request assistance "stat," do you need a robust and reliable network?

If the answer to these questions is "yes," then why is a robust and reliable network required? Obtaining an understanding of what types of devices are used and how they are used is important for more than just determining whether you need a robust and reliable network. It is also vital to designing and maintaining a robust and reliable network.

What Is a Robust and Reliable Network, and How Do I Get There?

How do you put the cart before the horse? Design a wireless network(s) and then figure
out what number and types of devices and applications that the network must support. Understanding both the networking performance characteristics and clinical requirements of the devices prior to the design and deployment of the wireless network is crucial to creating a robust and reliable wireless ecosystem.

There are many ways to define a robust and reliable network, some of which are technical and others that are marketing focused (so-called “marketectures”). This paper focuses on a few of the technical attributes of a robust and reliable wireless network, and some design best practices to meet the connectivity needs of your hospital. Note that a network with a marketing branding of “medical grade” can be, but isn’t necessarily, robust and reliable. It needs to meet the requirements of the given hospital and the medical devices therein to be considered robust and reliable.

**Coverage and Capacity**

It is one thing to cover an area with wireless access; it is another to make sure there is enough capacity in that wireless access to support all the devices. Consider how cellular coverage sometimes isn’t every place you want it to be and that during emergencies, the cellular networks are typically oversubscribed so calls cannot be completed. Providing coverage and capacity can be done in several ways. One way is to make use of available spectrum. If cellular coverage is sufficient in the hospital, then you may carry your voice calls over that network using regular cellular phones. You may also take advantage of the wireless medical telemetry system (WMTS) band for specific medical devices. You will most likely have an 802.11 network operating in unlicensed spectrum that is enabling data connectivity. You could even try and use the 802.11 network for converged services, such as voice, video, and data. It is the choice of each hospital as to how to effectively use the spectrum and available technologies, but there are options—all of which carry varying degrees of risk, technical competencies, and management. Within 802.11, channel reuse allows support of large numbers of 802.11 devices across the hospital.

The bottom line is that you need coverage wherever devices are used, but you also need to account for the capacity needs, or bandwidth, to allow all of these devices to coexist peacefully in terms of networking performance. These decisions are made in the planning phase and always include risk management.

**Mobility**

When a device is mobile, it will roam across the wireless network and in the case of a wireless local area network (WLAN), it will perform handovers between APs. The efficiency of this handover is crucial to maintaining a robust connection to the network. Clearly, it is critical that this handover occur very quickly, especially when the device requires a persistent connection to the network as in a VoIP call or a cardiac monitoring telemetry device. For example, 802.11 is a “break before make” technology, where the device must disassociate from an AP before it can connect to another AP. The time delta between the “break” and the “make” must be very short—in the order of milliseconds generally—because during this time the...
device is not connected to the network. Good implementation of strong security, such as WPA2-Enterprise by both clients and the network, achieves this. Be sure that your network and devices support fast roaming.

**Quality of Service**

Measuring quality of service (QoS) in networking terms is usually done with metrics such as packet latency (aka delay), packet loss, and jitter (time variation between packet-to-packet arrival times). When measuring the performance of a network, you may send a sequence of packets across the network with time stamps and receive them at the other end to determine the time it took to traverse the network. Network-monitoring tools use these metrics to evaluate the health of the network and are important to use in a network that needs to be robust and reliable.

Wireless QoS may be defined by additional metrics such as signal strengths, interference, signal-to-noise ratios (SNR), and packet error rate (PER). When you install a wireless network, there should be an RF site survey to measure signal strengths, co-channel interference, and SNR over the field of desired coverage. You generally want to design a WLAN RF environment to meet the needs of your most demanding application. That might be a VoIP application, video streaming, or patient surveillance. You also want to overprovision your network because the demand on the network will vary over the course of the day. It not only allows for high-usage scenarios, such as an emergency situation during which many users suddenly access the network, but also allows for scalability as more devices are connected to your network. A robust network supports the QoS requirements of the most demanding devices while also providing network access to every device.

In the end, the goal is a positive and satisfying quality of experience (QoE) for users of the network, whether they are nurses, other hospital staff, or a patient's family members. Properly designing and verifying the performance of the wireless network using the metrics of QoS will help to achieve that goal.

**Now That I Am There, How Do I Stay There?**

Once your WLAN is operational and devices are successfully connecting and achieving their networking performance needs, implementing an effective maintenance program and change control process is important to staying robust and reliable.

**RF Spectrum Management**

RF propagation in a hospital environment is a time-varying principle that can work for you one day and against you the next. Maintaining the RF environment takes diligence. One tool that is applicable is the periodic use of an RF site survey. As mentioned, it is very important to perform an RF site survey during the design and deployment phase, but follow-up site surveys should be performed as part of the maintenance of the WLAN. They can be quarterly or every six months, but should be a key aspect of a quality maintenance program. Such surveys should also be done when there are changes to the WLAN, such as adding in access points, extending coverage into new areas of the hospital, or physical changes to the hospital.

**Network Monitoring**

Many tools exist to monitor not only the performance of the network, but also the end devices. Network monitoring provides information for troubleshooting and management. It also can provide notification of degradation in performance of the network before the end devices experience poor connectivity. In the case of 802.11 WLANs, there are usually tools built into the controllers that measure bandwidth usage, number of clients, central processing unit (CPU) burden, PERs, and myriad other performance metrics. These tools should be used as part of the daily evaluation of the networking performance. This evaluation also can show the usage of the network to alert to higher capacity needs as the number of wireless devices increases.
devices increases. One approach is to trend the worst-performing devices so you can be aware of when a piece of network gear starts to have issues. If the worst-loaded AP has typically 30 clients and a typical peak bandwidth of 15 Mbps, then increases over time to 40 clients and 20 Mbps, and finally 50 clients and 21 Mbps, there is a good chance this AP is oversubscribed. Watching to see if PERs trend up or SNRs trend down allows an information technology (IT) department to respond in time—rather than react to a network brownout.

Change-Control Process
IT engineers are familiar with the concept of applying a change-control process to the management of the network. Adding medical devices and their associated clinical functionality adds another dimension. Taking down a network for a software upgrade without coordinating with the clinicians and healthcare technology management staff can lead to disasters. Checking with medical device vendors to see if their devices are validated for the updated infrastructure can help decrease testing and may lead to choosing a specific version of the network software that has been validated. Having a database of medical devices on the network and contact information for those devices allows an efficient way to do this.

Additional considerations for testing devices on either a lab setup or part of the actual network—but not on live patients—should also be part of the change-control process. Adding new devices to the network usually requires configuration changes on the infrastructure, so testing and managing the go-live process not only should ensure that the new devices can connect and perform as needed, but that existing devices are not negatively impacted.

References

