Wireless Technology Infrastructure: A Business Strategy

David Hoglund

For this installment of IT World, I am happy to introduce David Hoglund from Integra Systems, Inc. It is no secret that along with the growth of computer networks in healthcare, wireless networks are growing, too, and they present unique challenges to both information technology and medical technology professionals. David has a great perspective on the design, installation, maintenance, and service of wireless networks. The issues go beyond just the technology, though. Here David presents additional areas you must consider when installing or working with wireless rather than wired networks. Perhaps the most important of these is to define a business strategy, which will drive the entire planning process, from financial to facilities. Read on!

—Jeff Kabachinski, IT World columnist

Check Points

Defining a business strategy for wireless technology can't be done in a vacuum. Many different departments within your facility can and should play a role, including:

- ✓ Clinical engineering
- ✓ Nursing
- ✓ Finance
- ✓ Facilities
- ✓ Risk management

As all flavors of wireless technology have exploded onto the healthcare scene, the need to give thoughtful consideration to designing the correct overall wireless business and technology strategy has become evident. This strategy should include all current wireless technologies as well as future possibilities, all areas of patient care, and all departmental models. Careful attention should be given to defining measurable metrics for the deployment's success. The development of this business strategy will ensure that the intended technology investments will provide a measurable return on investment based on improvements in productivity, workflow, and the potential reduction of risk.

Defining the Business Strategy

The importance of wireless technology planning has reached a level never before seen in the traditional departmental planning process in healthcare. It demands a solid business strategy. Even though traditional wireless technologies such as telemetry (VHF/UHF and now wireless medical telemetry service, or WMTS) have been common in the biomedical community, the information technology (IT) department has by default been the "go to" area for wireless planning, deployment, and even support. This adoption of integrated 802.11a/b/g radio cards has been primarily to drive improvements in safety, clinical efficiency, and work-flow. For example, the initiation of the bar code medication administration (BMCA) and computers on wheels (COWs) for the electronic medical records (EMR), has required "wireless" to be integrated into multiple manufacturers' infusion pumps and is now a standard offering in every laptop computer. (See sidebar for more on 802.11.)

In the face of rapid change, quality of service and security within these medical devices need to be addressed. To further complicate things, new medical devices are regularly added to the converged data and voice network. This demands a strategy that ensures quality of service and appropriate security methodologies. Now rapidly approaching is the need for voice communication technologies such as Voice over Internet Protocol (VoIP), cellular, and Evolution-Data Optimized (EVDO), which have added another dimension to wireless or mobile technologies, including whether or how to adopt 802.11n (Multiple Input Multiple Output, or MIMO).

Should these wide-area radio frequency (RF) sub-band models be converged into an 802.11a/b/g strategy? What can you do to plan for voice capacity? Only when all the applications and technologies are looked at from a holistic perspective can proper business planning happen. This will help avoid some of the traditional "wild wild west" wireless and technology deployments and the lack of business process accountability that have hampered integration in the past.

Develop a strategic business plan that involves all departmental areas and takes into account all business and clinical requirements. The plan should focus on both the current and the perceived application areas and what will or may occur as business requirements change. One option is to use modeling and test tools from www.ixiacom.com (Chariot for WLAN testing) to help determine the ultimate capacity success of these technology deployments across all departmental areas.

With the acceleration of these technologies, though, comes the risk of improper planning, the allocations of proper fiscal technology investments, and the value of improvements of the care process. These, too, will demand a solid business strategy.

Technology Requirements

The WIFI Market

The wireless technology landscape has accelerated rapidly since the advent and approval of WIFI (802.11b) in 1999. In the healthcare arena, one immediate need was for WIFI for computers on wheels, which was a significant step toward EMR adoption. This early-stage deployment, however, was often limited to a single clinical area and was not widespread throughout the healthcare enterprise.

Legacy Access Point Approach

The legacy access point can be defined by the early 802.11b or WIFI access hub point that was part of a controller-based architecture.

The initial legacy access point generation provided a quick plug-and-play approach from the IT department. Predictive site surveys varied widely among institutions, if they were conducted at all. Healthcare IT departments were generally staffed to deal with software and hardware deployments, but not radio frequency (RF) spectrum management or spectrum analyzers. Third-party organizations varied in terms of actual wireless competency and therefore were not always an ideal solution either.

The market has accelerated to the controller-based design to handle the more sophisticated security and quality-of-service issues dictated by the release of 802.11i and 802.11e. These controller-based environments identified continuous inspection of packet-by-packet data that could provide quality of service for latency-sensitive applications. The transition has been gradual, but today a handful of patient monitoring companies are focusing on migrating WMTS to a 802.11a/b/g environment and providing a shared application environment for wireless.

As VoIP use grows, these second-generation intelligent wireless designs have helped pave the way for more intelligent RF and network management. In 2006, third-generation designs have evolved to handle the capacity issues required by the convergence of data, voice, and video on a wireless network. These wireless array designs seem like a logical move from a controller-based design. As in any wireless or RF design, physics does place limitations on the capabilities of the applications and the convergence of designs needs to be examined carefully.

Then, of course, there was the move from VHF/UHF to the WMTS band and the realization that WMTS may not be the perfect answer for the growing market for telemetry and ambulatory monitoring. Why not use 802.11a/b/g and provide a highly RF-managed environment? Should you have to install a dedicated antenna

What is 802.11?

IEEE 802.11 is a set of standards for wireless local area network (WLAN) computer communication, developed by the IEEE LAN/MAN Standards Committee (IEEE 802) in the 5 GHz and 2.4 GHz public spectrum bands. Although the terms *802.11* and *WIFI* are often used interchangeably, the WIFI Alliance uses the term *WIFI* to define a slightly different set of overlapping standards. In some cases, market demand has led the WIFI Alliance to begin certifying products before amendments to the 802.11 standard are complete.

Beginning in 1999, amendments have been passed to the standard, and in 2003, task group TGma was authorized to roll up many of the amendments to the 1999 version of 802.11. REVma or 802.11ma, as it was called, created a single document that merged eight amendments (802.11a,b,d,e,g,h,i,j) with the base standard. Upon approval in 2007, 802.11REVma was renamed to the current standard IEEE 802.11-2007.This is the single most modern 802.11 document available that contains cumulative changes from multiple sub-letter task groups.

design for "telemetry"? There is a common lack of understanding of what it means for WMTS to be "protected" by the Federal Communications Commission (FCC). Many in the healthcare community have come to believe that WMTS implementations or systems were designed to prevent interference, that interference of any kind will not be tolerated by the FCC, and that the FCC will in fact take action if there is interference. The reality today is that this interference can arise from many instances, including initial poor filtering on WMTS systems or lack of standard practices of implementations. There simply are no commercially available tools to monitor this spectrum space on a real-time basis.

Finally, cellular voice and data need to work reliably inside a building. Will the WIFI design be able to provide adequate VoIP? Will you need a distributed antenna design? Should this be passive, active, or use ROF (RF over fiber)? Will new combined handsets that provide VoIP and EVDO/CDMA be the answer? In the United States and overseas, there are many different economic and business case models that provide the right quality of service for mission-critical environments.

The acceleration of technology in both indoor and outdoor spaces has been rampant. Transferring high bandwidth across long distances can be costly, with a monthly fee as well as initial set-up costs. For example, supporting a picture archiving and communication system (PACS) may require costly T-1 lines if fiber optics are not available. An example is imaging centers connected to integrated delivery networks (IDN). Today there are wireless capabilities to transmit huge bandwidth up to 600MB/second over many miles. As part of the overall wireless strategic business plan, this capability can help lower the total cost of ownership for infrastructure deployment.

Metropolitan networks are extending the WIFI reach outside of buildings via mesh networking (a network implemented over a wireless network system such as a wireless LAN). Beyond simple data use, this can enhance security through remote video monitoring of garages and entrances.

Prioritization Requirements

Once the business model has been assessed by all representative parties, it is important to prioritize the business requirements. VoIP, for example, will need to include cellular requirements and have an understanding of how the various technologies could converge in a potential multimodal model. Will your current 802.11a/b/g deployment be able to handle the bandwidth capacity of voice, or will you need a managed wireless design for cellular traffic?

Most facilities have enjoyed the benefits of a legacy 802.11b environment and are looking forward to adopting 802.11a/b/g or even 802.11n (MIMO). These generations of infrastructure have moved from the first tier to the second- and then third-tier design. Are your plans ensuring a migration pathway that will take into account your data, voice, video, and location tracking requirements and converge the outdoor with the indoor environment?

Consider how location tracking systems might play out in your healthcare system, now and over the next couple of years. The benefit of tracking infusion pumps is fairly obvious, but what about locating thousand of other assets? If WIFI-based location tracking systems are being considered, how will this affect the capacity of the designed system? Should you look at alternative technologies such as Zigbee (a suite of high-level communication protocols that use small, low-power digital radios) or ultrawideband for location tracking requirements?

Management of Services

As you look at the business strategy from a holistic perspective, do the same for the physical environment. Static site surveys cannot take into account the ongoing building renovation environment of healthcare. Consider using a "predictive tool" (www.airmagnet.com, www.ibwave.com, and www.cognio.com are a few options) for RF planning purposes. This will ensure that the initial design model takes into account all the respective types of materials, walls, etc. It will serve as a template for site engineering design. These predictive tools are available for both the indoor and outdoor environment. Additional new tools are available that provide for an ongoing, round-the-clock spectrum analysis of WIFI, but could be looked at for all spectrum ranges as well as RFID.

The foundation of any wireless network is the radio link. Common workplace items such as cordless telephones, microwaves, and even fluorescent lights can overcrowd the wireless spectrum and reduce zones of coverage and quality of service. Because RF waves are invisible, the optimization of access points can be a guessing game of what may be causing interference or where access points should be placed for maximum strength, efficiency, and coverage. One solution is to utilize RF spectrum analysis and predictive tools (see above), which

until recently have been cost prohibitive in most environments. These management system tools allow the proactive management of the settings of the access point and create an enterprise approach to the management of your environment. One reason that WMTS may be a short-lived solution is that this proprietary design cannot take advantage of predictive modeling or ongoing real-time spectrum management, or be incorporated into network management plans such as simple network management protocol (SNMP).

A wireless network management system should enable administrative and help-desk personnel to manage and troubleshoot an extended wireless network. Keep in mind that the network will serve a diverse user population equipped with a wide range of mobile computing devices connected from many locations through access points that could number into the thousands.

To the extent that your wireless strategy will grow from one facility to multiple facilities, there should be a way to manage holistically, irrespective of multiple vendor legacy or controller environments, or even the manufacturer. Again, all of this points to the need to develop a business plan to support all of these requirements and needs and to look away from the proprietary technologies of the past.

Conclusion

Today's healthcare environment and rapidly changing wireless technology landscape demand a strategic business plan. Planning can no longer be silo-based, looking at the needs of only one department. When departmental and business needs are carefully looked at, the investments in the intended technology will pay off in the desired improvements of productivity, workflow, and reduction of risk, and will ultimately provide the best return on investment. The use of commonly accepted enterprise planning tools, spectrum management, and network management will allow the creation of multi-faceted wireless infrastructure to occur. ■

David H. Hoglund has been in the medical device space as well as the wireless design environment for more than 20 years. Integra Systems, Inc., was started by Hoglund in 1997 as a wireless incubator and engineering consultancy. Some of Hoglund's accomplishments in the wireless and medical device space include the initial design and concepts for OneNet, a shared wireless and wired patient monitoring infrastructure for Draeger Medical, Inc.