FAQs

For the Wireless Challenge in Healthcare

Developed by
The AAMI Wireless Strategy Task Force
About AAMI

AAMI is a diverse alliance of nearly 7,000 members from all around the world united by one critical mission—supporting the healthcare community in the development, management, and use of safe and effective medical technology.

AAMI serves as a convener of diverse groups of committed professionals with one common goal—improving patient outcomes. AAMI also produces expert and objective information on medical technology and related processes and issues. AAMI is not an advocacy organization and prides itself on the objectivity of its work.

About AAMI’s Wireless Strategy Task Force

AAMI’s Wireless Strategy Task Force (WSTF)—which is composed of manufacturers, regulators, users of technology, and other interested parties—is developing educational resources and tools and sharing best practices to address wireless challenges in healthcare. For more information about the WSTF, visit www.aami.org/hottopics/wireless.
Introduction

AAMI’s Wireless Strategy Task Force (WSTF) developed this document to provide answers to frequently asked questions (FAQs) regarding wireless issues in the healthcare environment. A special thanks to Steve Baker, PhD, senior principal engineer at Welch Allyn, for leading the project and writing much of the content; as well as to Rick Hampton, wireless communications manager at Partners HealthCare Systems, Scott Coleman, network technologies manager at Welch Allyn, and Paul Sherman, a consultant retired from the U.S. Department of Veterans Affairs, who developed responses to many of the questions.

This document is intended to help healthcare technology, information technology, and facilities management professionals understand the state of wireless technologies, their use in healthcare, and how they can best be managed. The answers are provided by members of the WSTF and have been reviewed by a team of healthcare technology management professionals out in the field. We give firm answers to purely informational questions. However, for guidance questions, there is no one right or wrong answer. The goal is to provide information and pointers for the reader to make an informed decision. AAMI will publish excerpts from this FAQ and other FAQ documents in future editions of *Biomedical Instrumentation & Technology (BI&T)*.

Table of Contents

General Questions ........................................ 3
Radio/Network Choices, Options, and Coexistence .......... 6
Prepurchase/Preinstallation ................................ 8
Regulatory Questions and Guidance Documents .............. 10
Maintenance and Management of the Wireless Network ... 12
Security .................................................. 16
Reliability and QoS ...................................... 19
Architecture and Network Design ........................... 22
802.11 .................................................. 27
WMTS .................................................. 32
General Questions

1. **Wireless support has been added to my responsibilities, and I don’t know anything about it. Where can I go to learn?**

   The first thing you need to do is a lot of reading and to educate yourself on wireless technologies. Understanding what wireless is, what it does, how devices communicate on wireless, coverage area, and security risks. Hire or get a good team, if possible. Read *Wireless Networks for Dummies* to start, followed by the *CWNA Certified Wireless Networks Administration Official Study Guide*, and then take the training class. At the same time, make sure you document and/or get trained on your wireless architecture via a readable network drawing. A network diagram really is worth 1,000 words or more! Doing this will help you understand how controllers and access points are connected physically and their current locations. Sign up and take wireless training courses. If you don’t have the budget, many wireless vendors have good online seminars, training, white papers, configuration guides, and documentation that can help you get started. “Learning Wireless LAN Technologies,” available from wlanpros.com, has some good methods for learning.

2. **Where do I go if I need more help?**

   Here are a few sources to consider:
   
   - Organizations such as AAMI.org, IEEE.org
   - This FAQ
   - Wireless certifications such as CWNA, CWNP
   - Terminology research—go to google.com or wikipedia.com and search for key words/phrases such as 802.11, wireless networks, wireless access points
   - Hire a consultant
   - Wireless vendor sites
   - Wireless tools—spectrum analyzers, sniffers, heat map surveys
   - AirMagnet

“You see, wire telegraph is a kind of a very, very long cat. You pull his tail in New York and his head is meowing in Los Angeles. Do you understand this? And radio operates exactly the same way: you send signals here, they receive them there. The only difference is that there is no cat.”

—Albert Einstein, when asked to describe radio
3. Are personal wireless devices (e.g., phones, iPads, etc.) in a hospital really a problem?

Personal wireless devices can present various problems if the institution does not have a strategic plan allowing for their use. While most people still think of the risks of personal wireless devices only in terms of electromagnetic interference (EMI)—interference causing a medical device to malfunction—today’s smartphone is far more problematic in other ways. Smartphones used by staff can be used to connect to the hospital network and store sensitive information, leading to a data breach if compromised or stolen. Smartphones now contain sensitive cameras and microphones, creating the potential to violate patients’ rights if used incorrectly by visitors or staff. Smartphones also can be used to decode barcodes, so any sensitive information encoded on patient wristbands can now be decoded by anyone. Healthcare delivery organizations (HDOs) can no longer afford to focus only on one risk associated with a particular type of device, but must assess all risks and create a mitigation plan for each one.

4. What are the biggest mistakes that healthcare delivery organizations (HDOs) make in managing wireless issues?

Please see page 32 of AAMI’s Going Wireless publication. At a high level, these mistakes may be summarized as, “The biggest mistake a healthcare delivery organization can make with wireless is failing to create a strategic plan on how to use and implement wireless technologies.” Each wireless technology, whether WMTS telemetry, cellular telephones, Wi-Fi networks, or proprietary technologies for RFID, requires a significant investment in infrastructure and presents multiple risks, including security breaches, patient safety issues, and adverse impacts to other wireless applications. Failure to create foundational strategy increases the probability that the risks become adverse events.

5. Is there a glossary of terms that would help me understand all of the acronyms people throw around?

Yes. You will find a glossary of terms on pages 30–31 of AAMI’s Going Wireless publication. Page 32 has a list of additional reading materials that will also help.

6. I’m a biomed. Why should I care about wireless when it’s not in my job description?

Whether it’s specifically written into your job description or not, a certain mastery of wireless is essential to doing your job well. If you are touching medical devices, you are touching wireless. Also, if you want job security, then developing the skills to address and help solve wireless issues will make you a more indispensable part of the team. Consider it as adding job security, because wireless is here to stay.
7. Why are there so many contradictions in best practices, and what is the best place to go for standards related to best practices for wireless devices?

Best practices for wireless devices are specific to each vendor. Each vendor may have slightly different interpretations of standards or different names for the same technology that need to be implemented for maintenance and support. Please visit the website for the specific vendor you are researching. You can search for data sheets, release notes, and white papers.

For clarification on the technology standards vendors use as a source, a great place to start is IEEE.org, IETF.org, or AAMI.org, and search for specific standards.

8. What attributes should my team have to support a wireless network for wireless devices?

The list depends on your network and needs. A starting list to consider is:

- A very well-trained group of wireless/network engineers
- A keen interest in quality of support, device, and architecture integration (the cheapest is not the best)
- A willingness to adapt, learn, and keep up with technology
- A serious interest in security
- The discipline to plan and test
- Proper tools to monitor, maintain, and troubleshoot infrastructure and devices
- Constant communication with various organizations within your business concerning the challenges and requirements of a wireless network that should include: published policies, change control, security, guest access, devices supported, and general access (to name a few)
- Patience
9. What is WMTS and how is it different from Wi-Fi? How do they differ from MBAN and MedRadio?

WMTS (Wireless Medical Telemetry Service) is a set of radio frequencies dedicated to wireless patient monitoring. The telemetry monitors send patient signals to a manned central station. This allows patients to walk about a ward. Equipment used in WMTS is sold only to healthcare providers. Wi-Fi is a brand name associated with wireless networking (wireless local area network, or WLAN). Most consumers use Wi-Fi to mean WLAN. WLAN is low-cost wireless networking that operates in a group of frequencies called ISM (Industrial, Scientific, and Medicine). These are available for use by anyone who chooses to buy equipment. These bands are shared with other technologies, including Bluetooth and amateur radio.

MedRadio is a group of radio frequencies set aside to allow short-range wireless communication between an implant or patient-worn therapy device and a control unit.

Medical Body Area Network (MBAN) and Medical Implant Communication Service (MICS) are part of MedRadio.

MBAN is intended to replace the wires connecting a patient to his or her bedside. It’s designed primarily for in-room use; if a patient leaves the vicinity of the MBAN receiver (or “hub”), then they will likely not be monitored, similar to the case with a Bluetooth/Bluetooth low-energy sensor. Regardless of the radio used, carrying a small hub with no wires may provide improvement in patient comfort and compliance to prescribed monitoring. See “MBANs Could Advance Patient Care, But Interoperability Is a Concern” at www.mddionline.com for more information.

10. What is all this wireless stuff, and why should I care?

Connectivity is a hidden cost of electronic health records (EHRs). If you don’t have connectivity, you have to manually type in everything, which is inefficient and creates additional risks of human data entry error.

More and more, meaningful use and other metrics related to the use of the EHR will require the use of connected devices (e.g., for closed-loop medication safety). If nothing else, the drive for greater value and efficiency in healthcare will demand high reliability wireless, because otherwise we are using humans to pile up sandbags and plug holes in dikes rather than building a new dam or levee.
11. Is there an issue with Bluetooth and Wi-Fi co-existence?

First, keep in mind that the vast majority of Bluetooth devices operate only in the 2.4 GHz band, although the protocol can be used in other spectrums. Wi-Fi also operates in both the 2.4 GHz and 5.8 GHz spectrums. In the early days of Bluetooth, the protocol was unable to detect and avoid other nearby wireless devices using different protocol, such as Wi-Fi, and there were problems. Later versions of Bluetooth were enabled with mechanisms to detect other wireless devices and actively avoid them, so problems are much less pronounced than just a few years ago. That being said, Wi-Fi and Bluetooth still rely upon sharing the spectrum in both the time and frequency domain. Healthcare delivery organizations that fail to create a strategic plan for using wireless in their facilities run a greater risk of overusing shared spectrum and creating problems between these two ubiquitous technologies.

12. Does it work to have two Wi-Fi networks in the same physical space? What are the key considerations?

It is not possible to discuss all of the factors that go into the proper design of a reliable Wi-Fi network in this document. That said, if the groups responsible for installing and maintaining the wireless infrastructures know at a deep level how the technologies work, it is possible to install two Wi-Fi networks in the same physical space. The easiest way to accomplish this is to create separate networks using different channels in the 5.8 GHz 802.11a band. With careful design and monitoring of the system, two overlapping systems can be installed using the 2.4 GHz band, but such shared spectrum requires serious constraints on the use of systems installed this way.

13. Is telemetry for patient monitoring considered wireless?

Put bluntly, any communications system that doesn’t use wires to communicate is wireless. These systems may use different frequencies and operate under different regulatory rules, but they are all wireless, and the facility using them must perform a complete risk assessment in order to install and use them safely.
Prepurchase/Preinstallation

14. **What should I look for in a medical device and the company that supplies it in terms of wireless capabilities, expertise, and support?**

First and foremost, the medical device should meet the clinical requirements for the job to be performed. The manufacturer should have a solid and demonstrable understanding of the wireless technologies they have chosen for their device. The manufacturer also should be able to provide documentation adequate to ensure that it meets the security requirements of your facility, as well as adequate instructions to ensure that the device can be supported in a manner that ensures its safety and efficacy when installed on the chosen wireless infrastructure.

15. **What wireless specifications should I be writing into my RFPs for medical devices?**

Generally speaking, you should include specifications that reflect the wireless security and operational policies of your facility. You also should include requirements for the vendors of both the medical equipment and information technology (IT) equipment to provide information necessary to ensure the proper functioning of the medical equipment and continued support. For more detailed information, you should consult the IEC 80001-1 risk management standard and its technical reports covering wireless network design considerations and responsibility agreements.

16. **How much should I budget to buy and maintain my wireless infrastructure?**

It depends on the size of the installation and the radio frequency (RF) coverage level required to support your networked devices. You should budget as much as it will take to install, operate, and monitor wireless systems in a manner that will ensure their proper and reliable operation. Scrimping on any of these tasks will guarantee a poorly performing system that adversely affects the applications running on it and exposes the facility to risks of data breaches and patient harm.

17. **How can I convince my C-suite that these issues are worth the investment of the right resources?**

One option would be to proceed by addressing risk management: security, consistency, and timeliness of data. All of these have an impact on clinical outcomes which are at the heart of the quality and affordability agendas. Another point to consider is the potential impact to brand—positive and negative. It is important to note that these are not limited to wireless, but apply to any networked and/or integrated system. Articulate the quality components (table stakes) and the affordability components (differentiators). That is, understand how your particular initiative (strategy and tactical plan) address both of these critical agendas, as virtually every health system has these in some form at the forefront of every conversation.
A healthcare technology management leader at a large health system shared some of their experiences:

“We removed the veil of technical secrecy from the requests and communicated very clearly the value of the investment from the standpoint of clinical efficiency and improved patient outcomes. Including very specific data on how proposed wireless and wired infrastructure upgrades would improve clinician access to the system, reduce downtime, and speed up transactions made it very obvious to the C-Suite that the resources needed to be approved.

“It was common several years ago for IT infrastructure requests to be among the first items cut when there was a need to cut the capital budget. The turning point was the integration of mobile and fixed computing devices into the clinical workflow. When we were preparing to implement our EHR at our first sites, it became readily apparent that our existing infrastructure would negatively impact clinical workflow and ultimately patient outcomes.

“Wireless VoIP (Voice over Internet Protocol) phones transitioned from being ‘nice to have’ to a critical part of the clinical workflow. Communicating how the investment in better phones and enhanced wireless infrastructure would better support clinical workflow and patient outcomes helped the C-suite understand the importance of the investment.

“Quantifying costs using indirect measures such as communicating return on investment (ROI) in dollars may be difficult. Executives realize that every clinician waiting an extra 30 seconds for a refresh from the EHR server multiple times per day adds up to wasted dollars. Similarly, the count of lost connections that have to be restarted due to inadequate wireless infrastructure adds up to wasted dollars and clinician frustration. Frustrated clinicians leads to turnover, and the costs of clinician turnover have been well documented. Similarly, the cost of EHR downtime (estimated by a large hospital chain at more than $10k per hour) may be used to justify upgrading the system to reduce downtime.”

18. How do I choose a wireless infrastructure?

You should first understand that all wireless infrastructures have unique advantages and disadvantages. All must be installed and optimized to the particular environment where they will be used and they must be monitored to ensure proper functioning. Given this knowledge, it is more important to first select the medical equipment which will meet clinical needs and then install the wireless networking infrastructure necessary to ensure the safety, efficacy, and security of the medical equipment. The medical device manufacturers should be consulted in order to understand the unique networking requirements of their equipment.
19. Where does a vendor’s responsibility end and my responsibility begin for managing the wireless infrastructure, network, and wireless devices?

In general, the vendor’s (whether medical or IT) responsibility ends when they sell you the equipment and provide you with the instructions for installing the equipment to meet specifications. Unlike years ago, when the healthcare facility would purchase the networking equipment from the medical device manufacturer as a complete and pretested package, when the medical facility decides to connect the medical equipment over the facility’s IT network, the facility assumes all responsibility to ensure that the IT network meets all of the requirements for supporting the medical equipment. It is, after all, the facility’s IT network—installed, maintained, and operated by the facility—not the medical device or IT vendor’s network.

20. What is 80001? How is it different from 14971?

Both IEC 80001-1 and ISO 14971 are international consensus standards which outline how to identify, assess, and manage risks associated with medical devices. While ISO 14971 focuses on manufacturers and the manufacturing processes, IEC 80001-1 focuses on healthcare delivery organizations that connect medical devices to their facility’s IT network. While there is considerable overlap in some aspects, only those concepts directly applicable to healthcare facilities are included in IEC 80001-1.

21. What is risk management in the context of wireless networks and how do you perform it? What are the essential elements of it?

Risk management in the context of wireless is much the same as risk management of connecting a medical device to any network, wired or wireless, and is described in the standard IEC 80001-1: Application of risk management for IT Networks incorporating medical devices—Part 1: Roles, responsibilities, and activities. This involves retaining the three key properties of the networked medical device—patient safety, device efficacy, and system security. The essential elements include network change management, identification of lifecycle support issues, and system monitoring.
22. How can 80001 help me with allocating these responsibilities between my organization and the vendor(s)? How expensive is it to comply with 80001?

IEC 80001-1 defines the roles and responsibilities of the entities and personnel needed for the health delivery organization to establish a risk management program. The associated technical reports provide detailed examples for implementation. While it is not possible to give definitive values for the costs of compliance with 80001-1, most of the elements required by 80001-1 already are known by healthcare delivery organizations, if they aren’t already being used.

23. Do we have legal liability if we don’t make these issues a priority?

Healthcare delivery organizations, as well as industry, are responsible for mitigating risks that are “known” or that can reasonably be anticipated. A thoughtful risk management program is an excellent way to mitigate risk and to show later, if challenged, that the organization took risk management seriously and analyzed all known and reasonably anticipated risks. A well-known risk issue that needs careful management with wireless medical devices is reliability. Another is security. If a healthcare delivery organization does not make these issues a priority, it will definitely be much more difficult to defend and answer the question, “Why didn’t you make this a priority when you knew or should have known there was a significant risk?”

24. What do the FDA’s recent guidance documents on cybersecurity, mobile devices, and use of wireless technologies mean for my organization, and why should I care?

The guidance documents recently published by the FDA can be used by healthcare delivery organizations (HDOs) to understand the variables that medical device manufacturers must consider when designing their products. This, in turn, allows the HDO to examine what must be done to ensure that the medical device operates safely and reliably in the intended environment. They also inform the HDO when altering the medical device or network equipment might cause the HDO itself to become a medical device manufacturer regulated by the FDA.

25. Is there anything in the meaningful use requirements from the Office of the National Coordinator that will make wireless a higher priority for healthcare delivery organizations?

The requirements for e-prescribing in Meaningful Use Stage 2 make certain assumptions about wireless capability as an underpinning to the requirements. “Closed loop” medication safety requires bedside barcoding and other automated functions that need high reliability wireless capability.
26. **What tools do I need to check my wireless infrastructure?**

The tools needed to monitor a wireless infrastructure depend upon the type of infrastructure being monitored. Depending on the parameter of interest, spectrum analyzers, protocol analyzers, and network analyzers may be used. In instances of proprietary networks, there may not be appropriate equipment available to the end user. Specific recommendations for test and monitoring equipment can be provided by the manufacturers of both the networking equipment and medical devices.

27. **We are experiencing a high rate of interference. What does that mean and how can I troubleshoot it?**

Interference occurs when a first transmission and at least a second transmission occur at the same time, in the same frequency band, and are received by the same receiver. It is analogous to having two people talking to you at the same time. At the point the interference makes it impossible to understand the transmission, the term “harmful interference” might be applied. A high rate of interference indicates that receivers have harmful interference at a high enough rate that data communications are delayed or fail.

RF emissions may be characterized as intentional and unintentional. Intentional transmissions are due to devices such as radios that purposely transmit data. Unintentional interference is due to emissions that occur as a consequence of device operation, such as sparks on motor bushings, faulty/failing fluorescent light ballasts, high-speed switching of data and address lines in a computer, and the like.

For tracking, use the tools indicated in Question 26 and make regular measurements of the peak noise and noise floor in the RF bands for which the healthcare delivery organization has medical/IT equipment. For troubleshooting, add some good detective work to determine where the source is located and if it is intentional or unintentional. For devices in the 2.4 and 5 GHz ISM bands, the interference is typically intentional; that is, due to other devices trying to transmit and communicate. For WMTS devices in the 608–614 MHz band, the interference might be from adjacent-channel TV stations (intentional) or emissions from faulty/poorly designed electrical equipment and motors.

Once located, remove the interference source if possible. If it must be in place, try to relocate it (having an interference source adjacent to a receiver such as an access point (AP) is a good way to ensure that no data is received). If the source can’t be moved, the other option is to ensure that the intended signal, as detected by the receiver, is stronger than the interference signal. This can be accomplished by adding more receivers so that receivers are closer to transmitters. One might attempt to solve the issue by increasing the transmission power of an AP, but the AP transmitting at high power does not solve the problem of an AP unable to receive data from a lower-power client. See also Question 57.
Other possible causes of interference include poor channel planning where neighboring APs are on the same channel (always a problem with 2.4 GHz Wi-Fi where only three non-overlapping channels are available) and oversubscribing APs where there is insufficient bandwidth to support all of the clients. For more information on the former, see also Questions 54 and 69. A solution for the latter issue is increasing AP density with lower power for each AP. This works better when clients subscribe to the 802.11d power constraint element.

28. How do you know if you are running out of spectrum, have enough spectrum, etc.? My hospital is running out of spectrum. What should I do?

Network capacity issues are typically the result of inadequate planning by the healthcare delivery organization to understand how they use wireless technology and ensure a proper design and installation of infrastructure. Acute changes in capacity can be caused by sudden increases in the number of wireless clients, physical changes to the building, and “bugs” in software/firmware upgrades.

The best way to solve these problems is to plan for network growth in the first place, following the guidance from IEC/ANSI/AAMI 80001-1:2010 and the Wireless Technical Report. Use the tools mentioned in Question 26 to determine if there truly is a bandwidth issue. It may be that data isn't arriving as intended because of interference.

Assuming more bandwidth is required, one possible solution is to take advantage of the large number of channels available in the 5 GHz band. It is possible to reuse channels analogous to the solutions used by cellular providers: install more APs with lower transmission powers. Ensure that all areas are covered by strong (at least -65 dBm for 802.11a/g) so that devices can transmit at the highest data rates.

29. Should healthcare technology management (HTM) manage the health of the wireless network, or should IT?

The short answers are: both, and it depends. IT should manage the vast majority of wireless networking, since it is primarily used for nonmedical, administrative, and public communication. If any of the network is used medically, such as for patient monitoring, radiologic image transfer, infusion pump management, etc., then both HTM and IT must jointly manage the wireless network. IT will have access and networking expertise, but rarely has patient safety and risk management expertise. HTM provides that vital patient safety priority. For example, in the IT world, voice and video have the highest priority for network resources. In the hospital, direct patient support must have the highest priority. Wireless networks used for patient care should be built and operated to IEC 60601-1-2 standards, which IT is unaware of. Consider also a stand-alone WLAN for patient care.
30. When should I update the software on my wireless network? Vendors seem to release multiple updates each year.

Update the network when the risk/reward ratio of updating is lower than the risk/reward ratio of not updating. As some are fond of saying, “Tried and true is better than new.” In an easy example, if the WLAN vendor implements a patch to support 802.11ac and you have no 802.11ac devices, the reward for updating is zero, so the risk/reward ratio is infinite.

Typically, a patch adds more than just one feature, includes bug fixes, and includes new bugs. Because of this, national network providers such as Sprint, Nextel, Comcast, Verizon, and AT&T usually have very stringent and exhaustive tests to qualify new network equipment. Once qualified, they stick with the same versions for a long time because of the time and cost of qualification.

A more difficult scenario to consider is when there is a security patch. Considering only IT security, one would install the patch as soon as possible to quickly remove the risk of a security vulnerability. The hazard and probability of occurrence of the security vulnerability being exploited needs to be weighed against the probability and occurrence of potential issues that might include:

- Infusion pumps may not be able to update formularies.
- Patient monitors may not be able to deliver alarms.
- Picture archiving and communication systems (PACS) may not be able to upload images.
- Mobile EHR interfaces may not to be able to access patient records.
- Voice over WLAN system may not operate correctly.

The only real way to know if this works is to test against those devices whose failure causes an unacceptable hazard. Most medical device companies are loathe to OK working with a new WLAN operating system without testing on their own, which rarely, if ever, is available when the patch is released.

31. How do I determine the performance of medical or other devices in my wireless environment?

There are several aspects to this:

a. Most wireless vendor equipment has built-in monitoring systems to some degree or another. Learn and train and take advantage of those systems.

b. Learn SNMP (Simple Network Management Protocol), set up a server to capture SNMP monitoring information from devices and infrastructure in your network, review and purchase software that will help organize that data, set alarms, and send notifications when bad things happen.

c. Monitor data and trends using software to get a good picture of what is going on in your network with all of the different types of devices you are required to support.
d. Medical and other devices may also have built-in tools to help you measure and track their performance. Learn and understand what those are and integrate that information into your monitoring systems, if possible. If not, ensure that you have a good support agreement with device vendors to help with troubleshooting.

e. Tools like iPerf, Wireshark, HP Openview, Fluke Truview, Fluke Visual Performance Manager, and many others may be options to pursue if you need additional help or data. Thoroughly research those tools and try demos if available to determine if they meet your needs.

32. **What are the best wireless network management tools?**

Please see Question 26 for a list of the different tool types.

33. **What is a site survey (aka wireless survey) and how often should I do one?**

A site survey is typically a manual mapping of the RF coverage. At a high level, one imports a facility floor map into site survey software and walks around the building while the software records the signal strength of each AP. Postprocessing provides heat maps or other ways to visualize the RF coverage. Different tools add other features, such as overlays for RF utilization and methods to indicate redundant coverage (as opposed to just the strongest coverage in that area).

A site survey should be updated any time there is substantial change to the network of the physical environment. Since automatic RF coverage algorithms may change the AP transmission power and channels, a site survey may be used to objectively evaluate the effect of the algorithm, particularly when it is first enabled. Periodic evaluations should be run, and the time between these evaluations depends on the output of a risk analysis. As a guide, an annual site survey is prudent and may also include looking at the noise floor using either the site survey tool or a spectrum analyzer.

Some WLAN vendors’ tools and third-party applications build RF coverage maps using information each AP collects about how strong it hears other APs. If one compares this data to a manual site survey and there is a strong correlation, it may make sense to use these tools.

34. **Is a wireless sniffer such as Wireshark the only way to tell why packets get lost in the air?**

If you are in a troubleshooting mode, wireless devices are losing packets in the air, and your device isn’t reporting or keeping logs that describe the issue, then using a sniffer to capture the communication exchanges in the air between the device and the access point is the best way to get a true picture of what is happening in your wireless network. A wireless sniffer trace can provide information such as latency, channel, data rate, packet retries, packet acknowledgements, packet sizes, beacons, basic service set identification (BSSID), and many other details. Wireless traces can be combined with wired traces to get a full end-to-end picture of how data is traversing the network. For ease of analysis, ensure that network time protocol (NTP) is synced on the sniffer capturing devices. If you are unfamiliar with Wireshark, wireshark.org has instructions, training, examples, discussion forums, and free downloads.
35. **What’s the difference between encryption and authentication?**

Encryption is the process of converting data into a form that is not readable/understandable by an unauthorized person or device. Authentication is the process of ensuring that the other person/device is actually the person/device it claims to be. In 802.11, encryption and authentication are sometimes confused because the authentication is used as a seed for the encryption algorithm and because WPA/WPA2 specify both authentication and encryption.

36. **How does cybersecurity affect the choice of a wireless network?**

There are three concepts to consider: how vulnerable is the wireless network infrastructure, does the wireless network provide strong authentication and encryptions, and what tools are there to protect against hackers? Consumer-class devices rarely are subjected to the rigorous testing that enterprise-class products are. Products based on mature software are more likely to have been tested for vulnerabilities thoroughly than new software. Within the realm of established enterprise class solution, vulnerability differences haven’t been shown to be a deciding factor. Enterprise-class 802.11 solutions provide EAP authentication and the advanced encryption standard (AES). Enterprise-class wireless network providers have IDS/IPS products and there are also third-party solutions.

37. **Do I really need to deal with all of this security hype?**

Yes. A healthcare delivery organization may be considered negligent, given the well-documented security risks and existence of off-the-shelf solutions. At a minimum, a risk analysis should be run to understand the vulnerabilities and threats, and insecure solutions (802.11 open and WEP) should be avoided/removed. It is reasonable to have a lower security stance in a small clinic compared to a large hospital chain. Given that EHR/EMR solutions essentially require wireless connectivity, implementation of meaningful use creates a very large attack surface for hackers because personal medical data and personally identifiable information (PII) will be available in many databases crossing multiple interfaces between the clinician, data centers, hospital, insurance companies, and the patient and family.

38. **Why is the FDA starting a cybersecurity lab and what are they doing?**

Security researches have exposed vulnerabilities in multiple medical devices, including infusion pumps and implantable defibrillators. *Regulatory Focus* reports that the National Institute of Standards and Technology and the U.S. Department of Homeland Security both called for the FDA to be given the authority to assess the security of medical devices before they are allowed to market and to form a postmarketing database to track software vulnerabilities.
In a notice posted in July 2013 on the Federal Business Opportunities website, the FDA said it was “developing a cybersecurity laboratory in which a fuzz testing capability is to be integrated.” Few details about the lab have been released since then, but we can reasonably assume it is part of a process to improve the security stance of medical devices. Brian Fitzgerald of the FDA indicated that the first three devices to be tested are an external defibrillator, an infusion pump, and a patient monitor. The FDA has published an alert and a draft guidance document pertaining to cybersecurity.

39. **What is fuzz testing and why is the FDA using it?**

Fuzz testing is a type of negative testing often used by hackers to discover vulnerabilities in software. Most software testing is positive testing: “If the input is X, then the software should do THIS.” Contrast negative testing: “If the input is Y, then the software should NOT do THIS.” For example, if an infusion pump receives an input of negative one (-1) it should NOT accept this as a valid flow rate. The FDA is likely responding to reports from the U.S. Department of Homeland Security titled, “Attack Surface: Healthcare and Public Health Sector,” as well as increased issues coming to light. An article in *The Washington Post* quotes William H. Maisel of the FDA as saying, “Over the last year, we’ve seen an uptick that has increased our concern. The type and breadth of incidents has increased.” The thought is that, through testing of medical devices using the same tools that hackers use and removing vulnerabilities, medical device reliability and security will be reduced.

40. **How do I deal with legacy medical devices with obsolete security features?**

The best solution from a networking point of view may be to immediately replace all of the unsecure devices, but if this were an option, we wouldn't have the question! Unfortunately, enough healthcare delivery organizations are still purchasing medical devices with obsolete security features and radios that the market continues to support them. Create a plan for phasing out these devices and protecting the network from the security holes of the legacy devices. Such a plan would have steps similar to those outlined below and might choose to follow the guidance in ANSI/AAMI/IEC TIR80001-2-2:2012, *Application of risk management for IT-networks incorporating medical devices—Part 2-1: Step-by-step risk management of medical IT networks*, and ANSI/AAMI/IEC TIR80001-2-3:2012, *Application of risk management for IT-networks, incorporating medical devices—Part 2-3: Guidance for wireless networks*.

a. Do not purchase any device for your network that does not support WPA2, preferably WPA2-AES (see Question 62). Put WPA2-Enterprise in any requests for quotation (RFQs) that are sent out.

b. Evaluate the risk to patients and the network. A small clinic or doctor’s office may not have the same risk as a large hospital chain. Bear in mind that any device connected to an 802.11 network using open WEP (wired equivalent privacy) means that segment of the network is wide open for a hacker to infiltrate.
c. Assuming the risk analysis indicates that mitigations are required, consider these two options. Put the insecure devices on their own network segment with that segment firewalled from all other devices including the server (if any) that the devices connect to. Disable all ports through the firewall except those required for the device to function.

41. Are there any security risks if I broadcast my service set identifier (SSID)?

No. Hiding the SSID provides a false sense of security, but this is about as reliable as the safety gained by hiding one’s head in the sand. Even if the SSID is hidden, it is transmitted in the clear by every device that is connected to that SSID and also by the AP itself in probe response frames. Moreover, many clients send out probe requests with the SSID visible even when outside of the facility, meaning the SSID is being transmitted for people to “hear” wherever the PC/tablet/smartphone is located. Hiding an SSID may make it more difficult for a newbie to get onto your network, but it presents no challenge to a hacker. For real security, use WPA2. Microsoft TechNet has an excellent article with a section explaining why nonbroadcast networks are not a security feature.

There are several issues related to hiding the SSID. It makes it more difficult for the intended users to connect the first time and, for PCs at least, causes the connection to take longer (see the Microsoft TechNet explanation). On PCs and mobile devices, the connection process requires more steps. For DFS channels, where clients are not allowed to transmit until they hear another device transmitting, hiding the SSID can make it difficult or impossible for valid clients to connect as they wait to hear their SSID in a broadcast packet. Again, using WPA2 (particularly the enterprise class with certificate-based authentication) will ensure that only the proper clients are allowed to connect to the WLAN.

There are also reasons to hide the SSID. When many SSIDs are broadcast, guests may have trouble finding the right SSID for a connection. Some IT managers have found that hiding all of the other SSIDs reduces the calls from people seeking guest access. Before hiding an SSID, be sure that there are no devices that will experience network connection problems when the SSID is hidden.
Reliability and QoS

42. What is wireless Quality of Service (QoS)?
   Quality of Service refers to providing preferential treatment to high-priority data. 802.11 provides four access categories (QoS levels): voice, video, best effort, and background (listed in descending order of priority). Devices with voice settings have the best opportunity to connect to the network and so, statistically, should have the lowest jitter, dropped packet rate, and latency. The article “Medical-Grade, Mission-Critical Wireless Networks” referenced on page 32 of AAMI’s Going Wireless publication provides a good discussion of QoS. See section 5.5 of ANSI/AAMI/IEC 80001-2-3:2011 for information on QoS mechanisms.

43. What parameters define wireless QoS?
   Typically throughput, latency, jitter, and dropped packet rate are the parameters considered, although a particular medical device might specify other parameters.

44. What QoS level is required for a wireless network with medical devices?
   Determining the QoS required for your organization might include these steps:
   
   a. Obtain the specifications for each type of wireless device supported on the WLAN. As long as someone is putting the list together, consider keeping it up to date as a tool for the future as new devices are brought online and old devices are removed.
   
   b. Determine the maximum allowed jitter, latency, and packet loss rate (plus any other parameters a device manufacturer may include). The network should be able to meet those performance requirements under worst-case loading.
   
   c. See section 5.4 of ANSI/AAMI/IEC TIR80001-2-3:2012 for more information on network performance requirements.

45. What tools do I need to determine if my organization’s wireless infrastructure meets the minimum QoS requirements?
   First, review Questions 34–36 to ensure that you have a good understanding of what QoS requirements you need to support. Major wireless manufacturers have tools and debugging capabilities built into their products that monitor, measure, and report QoS parameters. Some additional tools for more granularity in troubleshooting and measuring performance include iPerf, Wireshark, and multiheaded AirPcap adapters for simultaneous channel packet captures. Networking companies such as Cisco, Fluke Networks, HP, and Siemens provide performance and troubleshooting software and hardware.
46. How reliable is reliable enough for my WLAN?

This is similar to Question 44, determining the QoS requirements for a wireless network, and the answer depends on what devices are supported by the network and the risks associated with connection failures and/or the entire network failing. If a device required 99% packet reliability, then the network itself must have an uptime much better than 99%. A way to gain an understanding is to begin with the device list from the QoS survey to understand what the devices’ network requirements are, and the clinical use cases to understand the hazards that will occur if the WLAN fails. A WLAN that supports life-critical applications requires a higher reliability than one that does not.

47. Are there medical devices on the wireless network which can interrupt patient care if they fail? What are the risks and risk mitigation strategies?

Any device that requires network connectivity to fulfill its intended use and on which clinicians depend for patient care should be considered as part of an overall risk management strategy. Notice the term is “network connectivity.” This is because the hazard is the same whether the network connection is wired or wireless. A wired-connection patient monitor that is depended on to deliver clinical alarms to a central station cannot fulfill its intended use if its Ethernet connection fails. Differences in the risk analysis of wired vs. wireless include the probability of occurrence, the ways in which the hazards may occur, and the mitigations.


An example of risk analysis for a wireless patient monitor is given below. In some cases, statistical analysis may be used. When this is not available, input for experts is often used.

a. Hazard: Patient monitor unable to transmit clinically important data such as alarm status.

b. Possible harm: Delay in treatment, may lead to morbidity/mortality.
c. Probability of occurrence:

- Primary flow (network operating as designed): Assume that the medical-IT network is designed and tested to support 99.9% successful packet transmission. Assuming 10,000 alarm packets are transmitted each day (average of 50 per patient multiplied by 200 patients being monitored), then 10 packets would be missed. If patient monitors automatically retransmit alarm packets within a few seconds, then typically the second transmission would mitigate the loss of the first packet. Assuming packet losses are independent of each other, one alarm in 1,000,000 would be missed after the first retransmission and one alarm in 1,000,000,000 would be missed after the second retransmission. The probability of occurrence of a missed alarm in this situation is so low that the risk (probability multiplied by harm) is acceptably low and no mitigation is required.

- In the case of primary AP failure: If there is no backup RF coverage, then all alarms for the patient area covered by the failed AP will not be transmitted to the central station. AP MTBF is 200,000 hours, so the Annual Failure Rate is $1 - \exp\left(\frac{24\times365}{200000}\right)$ or 3.13%. One expects 3.13% of APs to fail annually. Repair time is typically one to six hours, and an AP covers about 10 patients. This lack of coverage is determined to be unacceptable.

- Mitigation: Install APs for redundant RF coverage so that if one fails, the backup AP provides coverage. Probability of two neighboring APs failing in the same year is 0.1% and failing on the same day is much lower.

d. RF Interference blocks transmissions:

- Mitigation: Site survey to ensure that system noise floor is low enough to support required bandwidth. Periodic (every six months) review of the noise level and upon major changes. Monitor the RF performance of APs and proactively respond to increases in noise floor (e.g., removing noise source, installing additional APs, etc.).

e. Other reasons for loss of data packets include overloaded network, interference from patient devices brought into the hospital, failure of IT switch, router, or wireless controller, AP Ethernet cable unplugged, configuration changes to network incompatible with patient monitor, firmware upgrade to network incompatible with patient monitor.

f. Other hazards include poorly protected data detected by a hacker, patient monitor’s wireless interface is vulnerable to attack, patient moves into an area outside the AP’s coverage, patient roams from one AP to another, AP is on a Dynamic Frequency Selection (DFS) channel (see also Question 66), a radar event is detected causing the AP to change channels.
Architecture and Network Design

48. Is there a gateway which separates the wireless portion of the network?

A gateway is a type of network node that separates and allows you to gain access from one type of network or media to another. Any wireless system that separates wired from wireless is a gateway. The type of wireless infrastructure and the configuration you have chosen to deploy will determine what that gateway can and can't do in terms of features and functionality. For example, in controller/access point (AP)-type wireless networks, the AP acts as the wireless to wired gateway and, depending on the vendor, will tunnel the device traffic through the wire back to the controller or route the traffic directly to the destination. If the traffic is tunneled through the network back to the controller, the controller then acts as the gateway, allowing an administrator to implement rules that the traffic must follow in order to reach its destination.

49. Are there diagrams/graphical representation documents which show a wireless network’s layout/architecture?

Yes, many vendors provide best practices and working examples of layouts and/or architecture you might be interested in reviewing prior to purchasing or deploying, based on your wireless requirements and needs. There also are programs that will help you document a wireless network, such as Airmagnet site survey.

50. What kind of antenna system should I put in?

Many hospitals and device manufacturers believe the best practice is to use the antennas that the AP manufacturer designed and tested to work with the system. As of this writing, Cisco’s distributed antenna system (DAS) positioning statement includes:

a. Cisco does not certify, endorse, or provide RF support for Wi-Fi deployments over ANY DAS.
b. Some 802.11 features may not work as designed over a DAS.
c. Some DAS vendors have implementations for supporting 802.11n MIMO. Customers should carefully evaluate and validate that these systems meet their requirements and perform to expectations. Reduced MIMO support will affect overall performance of the WLAN.
d. Cisco Wi-Fi customers may choose to deploy Wi-Fi over a DAS solution, but these customers should fully understand the caveats and design, deployment, and support implications.

For customers who choose to use a DAS, see Question 51.
51. What’s the difference between the antenna that comes with my AP and a distributed antenna system (DAS)?

The antenna that comes with the AP has been fully tested by the WLAN manufacturer and qualified by the FCC. The FCC allows other antennas to be used as long as the gain is less than or equal to the gain of those in the FCC equipment authorization.

Early instances of DAS included leaky coax (aka vampire taps) and were marketed to include 802.11 support. This solution allowed a larger coverage area than was supported by the AP’s original antenna. It also allowed all of the noise from the covered area to aggregate at the AP, which could result in a much higher system noise figure than the AP with its original antenna. (See the Managing Interference case study on page 61 of “Wireless Systems and Alarm Management,” published in the fall 2011 issue of AAMI’s Horizons.)

More recent solutions include active antennas and some attempts to support MIMO at the same level as did the original equipment. Current solutions, while marketed as DAS, are not much different than how a WLAN manufacturer would install a system independent of the DAS. The “distributed antenna system” includes multiple, discrete APs throughout the enterprise with each AP hard-wired to an antenna (either using the original antennas or multiple, discrete antennas specific to the DAS vendor). From the RF perspective, these current solutions are not using a DAS. In some cases, the DAS is used for the data backhaul (but this is still not a DAS implementation for the 802.11 AP) and in other cases, the APs are connected to Ethernet as would be done when there is no DAS.

A DAS may make sense for your healthcare delivery organization, but as Cisco recommends, “Customer should carefully evaluate and validate that these systems meet their requirements and perform to expectations.”

52. What is bandwidth? Why is it important? What sort of bandwidth should I expect to be used?

Bandwidth often is confused with throughput. Bandwidth is the amount of data that theoretically can be transferred between two points across an end-to-end link in a given amount of time, expressed as bits per second (bps). Kilobits per second (Kbps) equals 1,000 bps. Megabits per second (Mbps) equals 1,000,000 bps. Gigabits per second (Gbps) equals 1,000,000,000 bps. Throughput is a measure of how much successful data can be sent per unit of time across a network, channel, or interface; the actual throughput of a link is less than the stated bandwidth due various factors. Understanding bandwidth and throughput allows network architects to correctly identify the type of infrastructure needed to support all of the devices communicating on the network at any given time. Lists of network bandwidth requirements for media traffic can be found at technet.microsoft.com/en-us/library/jj688118.aspx.

More details on throughput can be found at en.wikipedia.org/wiki/Throughput. For comparison, the bandwidth of a continuous patient monitor may be in the 10–20 kb range with a few packets per second, a VoIP transmission might be 64 Kbps with 50 packets per second, and streaming video may have data rates of up to 6–12 Mbps for high definition quality video.
53. My CIO believes that we should have a single network for everything, including critical care medical devices. What are the pros and cons of this approach? Is there data to support a separate network for critical medical devices?

Please also see Question 10. Hospitals have successfully used both a single WLAN solution and overlaid WLAN solutions. The implementations range from IT runs everything to the IT and biomedical networks are completely separate (even from different manufacturers). In all cases, IT and the HTM teams need to communicate to ensure that the systems are configured to coexist. Some of the tradeoffs are discussed below.

In the case of everything running on the IT infrastructure, one network doesn't need to “worry” about the configuration of another network and there is only one network to maintain. On the other hand, there is more on the network and, if it fails, everything fails. The IT team must consider the needs of additional stakeholders who need to be informed well in advance to prepare for down time. For example, routine upgrades that take the WLAN down for 10 minutes may result in clinicians being blind to patient alarms and nurse call requests. Some hospitals assign critical medical devices to a separate virtual local area network (VLAN) to reduce the traffic load seen by those medical devices. The IT network may need additional RF coverage to reach corners of bathrooms and patient rooms that weren't considered in an IT-only installation. HTM can benefit from the knowledge IT has for configuring the system for VLANs, authentication servers, virtual private networks, and the like.

In the case of running completely separate 802.11 solutions, there are two networks to maintain, but often the biomedical team can leave their network untouched for long periods of time. This may be good for stability, but may be weak from a security perspective. This topology is often used with some of the 802.11a channels to biomedical devices and the others to IT devices (in fact, this solution is what some of the DAS vendors provide—see Questions 12 and 50), and this helps ensure that oversubscription by clients on an AP doesn't cause problems for the medical device traffic. This topology may restrict some of the opportunities for hackers and/or malware to move from the IT network to the clinical network, but these clinical networks often have neither antivirus nor intrusion detection systems.

54. How do I ensure that my wireless network is and stays reliable?

One concept is to remove single-fault failures: install APs to provide redundant coverage, alternate AP Ethernet returns to different switches, install redundant controllers. Other guidelines include:

a. Stay vigilant by monitoring and understanding that wireless is a fluid technology and can change by the second—what may have worked yesterday may take additional fine-tuning today or tomorrow. Keep up to date with current technology, patches, and software/hardware upgrades, but review and test these prior to deployment to ensure that they do not cause other issues in your network.
b. Keep a current list of all types of devices running on your network and understand device requirements and best practices.

c. Apply network monitoring and setup alarms and triggers for fault events, and check these every day.

d. Complete a wireless survey/heat map, design for primary and secondary wireless coverage, and review twice a year or as needed depending on your environment.

e. Implement security, both wireless and wired, and lock down easily accessed Ethernet ports. Minimize USB drive sharing between devices due to potential malicious software.

f. Work with device vendors to understand product requirements, best practices, performance, and expectations, and to provide feedback to them on performance and requirements for product improvement.

55. Should I fix the power on my APs? What about fixing the power to 100 mW as this results in better coverage maps in a site survey?

Communication is a two-way process that works best if both sides are able to hear the other. Consider an analogous case where two people are trying to talk, but can’t hear one another. One person increases his transmission power by using an amplified megaphone. The second person can now hear the first person speaking, but not vice versa. A typical system may have an AP capable of transmitting at powers up to 20 dBm (100 mW) and a typical client device transmits at 14 ±2 dBm (16 to 40 mW). If the AP is configured at 100 mW, then the client may indicate acceptable coverage, but the AP’s received signal is only 16% of what the client detects. For many areas of so-called AP coverage, the AP cannot successfully decode the received data, and communication failures occur.

Ideally, client devices should support the 802.11d power constraint element so that if the client can transmit at a higher power than the AP is using (as might be the case in a very dense deployment), then the client automatically adjusts its transmission power down to match the AP.

Some hospitals and medical device manufacturers recommend bracketing the AP’s power to ±3 dB of the typical client transmission power of 14 dBm (25 mW). This keeps the automatic algorithms in check as far as the range of power settings. For dense deployments, the AP power settings might be bracketed ±3 dB around a lower transmission power, perhaps 10 dBm.
56. **Should I fix the channels on my APs?**

This depends on whether your infrastructure provider’s automatic algorithm works to your satisfaction. Early versions of these algorithms had some “features” that some hospitals found objectionable, and they found that hand-tuning the channel assignment and power levels worked best. Unfortunately, for a large installation, this becomes difficult to maintain.

Many 802.11 infrastructure providers allow setting groups of APs to use subsets of channels. For example, a hospital that chooses to run clinical data on one set of APs and IT data on another set of APs might assign some channels for clinical use and some for IT use.

57. **What is the best method for setting up APs to provide a quality signal and performance?**

It is important to understand the requirements to which you are designing. Do you need RFID tracking? Are there latency-sensitive medical devices that use wireless? What kind of signal and data rates do you need to support? Is there a lot of interference in all or parts of your environment?

Once you understand the requirements and the areas that will be supporting wireless communications, using a wireless survey system like AirMagnet, you can make a record of the coverage area you have currently and adjust to fit your needs by either adding APs or moving current AP locations. It is important that you set the APs to no greater than 25mW and your production devices’ lowest supported data rate during this review so that you can get a more realistic picture of coverage area issues such as gaps between APs.

58. **Why is it a good idea for wireless devices to support active directory?**

Active Directory is a (Microsoft database) means of providing central authentication and authorization services for systems that support it. Active Directory also allows administrators to assign policies, apply updates, deploy software, and track device access. Along with wireless authentication and encryption, Active Directory is another layer of security in authorizing devices and/or the end user of that device to a network.
802.11

59. What is 802.11, and what do all of the letters mean?

The IEEE 802.11-1997 is a wireless networking standard published by the IEEE in 1999. Many amendments and additions have been made. Amendments are indicated by a letter or pair of letters, e.g., 802.11b, 802.11g. Once the alphabet was exhausted, a second letter is used, e.g., 802.11ac. Occasionally, the existing amendments are rolled up into a new version of the general standard, e.g., 802.11-2007 and 802.11-2012. See the IEEE 802.11 web page at standards.IEEE.org/about/get/802/802.11.html and Wikipedia web page at en.wikipedia.org/wiki/IEEE_802.11 for more information. The Wikipedia IEEE 802.11 web page includes a full list of the 802.11 amendments.

Some of the more common amendments are:

- 802.11-1997. The original 802.11 specification covering DSSS, FHSS, and infrared (IR) physical layers at 1 and 2 Mbps data rates. Of these, only DSSS still has any support in manufactured products. DSSS uses 24-MHz wide channels and FHSS uses 1-MHz wide channels.

- 802.11-2007. New release that includes amendments a, b, d, e, g, h, i, and j.

- 802.11-2012. New release that includes amendments k, n, p, r, s, u, v, w, y, and z.

- 802.11a. Introduced OFDM with data rates from 6 to 54 Mbps in the 5 GHz band using 20-MHz wide channels.

- 802.11b. Introduced complementary code keying (CCK) to provide 5.5 and 11 Mbps data rates in addition to 1 and 2 Mbps DSSS. Operates in 22-MHz wide channels.

- 802.11e. Quality of Service enhancements that provide for prioritized traffic flow.

- 802.11g. Added OFDM support with data rates from 6 to 54 Mbps in the 2.4 GHz band using 20-MHz wide channels. Achieves backwards compatibility with 802.11b (which in turn is backwards compatible with legacy 802.11 1 and 2 Mbps DSSS) through transmission of management frames using legacy modulation and channels.

- 802.11 h, Spectrum management. Introduced rules for European compatibility, specifically dynamic frequency selection (802.11 masters detect protected RF signatures on some channels and dynamically move to different channels) and transmit power control to ensure that devices don't exceed the regulatory maximum for the current country and channel.

- 802.11i, Security enhancements. Introduced the Advanced Encryption Standard (AES), aka WPA2, to remediate the security flaws in WEP. Also introduced an interim solution, Temporal Key Integrity Protocol (TKIP), aka WPA, as a stopgap solution to improve security on legacy devices, as implementing AES required new hardware. Provided for both pre-shared key (PSK) and certificate-based authentication using the Extensible Authentication Protocol (EAP).
802.11k. Defines and exposes radio and network information to facilitate the management and maintenance of a mobile wireless LAN. Provides information for the client to discover the best available access point.

802.11n. Allows higher throughput up to 600 Mbps, achieved by multiple radios to simultaneously transmit (or receive) on multiple inputs and multiple outputs (MIMO), wider bandwidth (up to 40-MHz wide channels) and improved efficiencies in the MAC layer such as frame aggregation (send more than one frame per transmission) and shorter guard intervals.

802.11r. Sets standards for fast base station subsystem (BSS) transitions (fast roaming from one AP to another), specifically while using EAP authentication. 802.11i allowed these features, but this led to multiple vendors having different methods.

802.11ac. Provides higher speed improvements to 802.11n for the 5 GHz band, primarily through 80- and 160-MHz wide channels and additional, simultaneous transmission (or reception).

60. What are the advantages of 802.11n over 802.11a and 802.11g? Are there any disadvantages?

As with many other discussions of specific Wi-Fi protocol, a detailed discussion of 802.11a/g/n is beyond the scope of this document. Generally, 802.11n is considered to have greater range and data throughput than 802.11g or 802.11a. Part of this increase in data throughput is achieved by using two Wi-Fi channels simultaneously. This also has the disadvantage of reducing the number of usable Wi-Fi channels in an enterprise environment by one-half. In the 2.4 GHz 802.11b/g bands, where there are only three orthogonal (nonoverlapping) channels, 802.11n allows only one channel, which is considered insufficient for enterprise infrastructures. As a result, 802.11n operation in the 2.4 GHz band is not recommended for enterprise networks. In the 5.8 GHz 802.11a band, where there are 20 channels, the use of 802.11n results in 10 orthogonal channels, enough to allow two completely separate wireless networks to operate independently of one another.

61. What parts of 802.11 have been deprecated/are no longer supported? How will this impact my organization and wireless medical devices?

Officially deprecated:

- WEP (en.wikipedia.org/wiki/Wired_Equivalent_Privacy)
- TKIP aka WPA (see also Question 52) (en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol)

Effectively deprecated by lack of adoption:

- IR Phy
- FHSS Phy
- 802.11e HCF Controlled Channel Access (HCCA)
62. **What is the difference between WPA2-PSK and WPA2 Enterprise?**

WPA2-PSK is a method of encrypting data and authenticating wireless clients to the network and vice versa, using a pre-shared encryption key (PSK). The PSK is used with all devices connected to the same network. While the use of a PSK is generally considered adequate for consumer use in the home environment, it is generally not considered sufficiently secure for enterprise environments. To overcome the deficiencies of PSKs, a Remote Authentication Dial In User Service (RADIUS) server is used to provide unique encryption keys for each user via centralized authentication, authorization, and accounting (AAA) management.

63. **Why is 802.11a/n better than 802.11b/g? Isn’t 802.11b/g newer?**

There are several aspects to this question including available bandwidth, spectral efficiency, and propagation distance. This question might be better phrased, “Why should I use the 5 GHz versions of 802.11 vs. the 2.4 GHz versions?”

Bandwidth is to data transport as blood is to oxygen transport. The 2.4 GHz band has a 79-MHz wide band that only supports three channels, making it impossible to have even single coverage without nearest-neighbor APs being on the same channel. This leads to RF interference, and attempts to provide redundant RF are challenging. In contrast, the 5 GHz band supports 25 channels in 555 MHz of bandwidth (USA) and the FCC is working to add another 195 MHz of bandwidth. See also Question 54.

Both 802.11a and 802.11g use identical modulation methods with high spectral efficiency (spectral efficiency is the ratio of data rate to bandwidth). In contrast, 802.11b uses complementary code keying for 5.5 and 11 Mbps, and the original 802.11 physical layer that supports 1 and 2 Mbps uses direct sequence spread spectrum. Consider the maximum data rate of 802.11a/g at 54 Mbps in (approximately) the same channel width as 802.11 and 802.11b use. Devices transmitting at 54 Mbps require less air time, so more data and/or more devices may be supported.

However, 802.11a is in the 5 GHz band and 802.11g is in the 2.4 GHz band. Generally, lower frequencies travel through obstacles such as walls with less attenuation than higher frequencies, and we see that RF plans designed for 802.11a typically have more APs than those designed for 802.11g only.

64. **Should I turn off lower 802.11a/g data rates to get better performance?**

A common reason for disabling the lowest data rates on a Wi-Fi network is to prevent devices with poor connections or lower capability (e.g., 802.11b only) from adversely affecting the throughput of other devices that have connections capable of supporting higher data rates. This technique can cause problems if the network does not have sufficient coverage or a large proportion of the wireless devices are capable only of 802.11b. This FAQ can’t address the specific circumstances of any one hospital, but can give some guidance on the questions that need to be answered.
One needs to understand the benefits and costs of turning off lower data rates and consider the effects on all system components. The obvious is this: turning off low data rates forces all devices to run at higher data rates. Higher data rates result in a lower duty cycle and therefore allow an AP to provide a higher data throughput. So far, everything sounds good. However, higher data rates require a higher signal strength and a higher signal-to-noise ratio at the receiver in order to decode the message. What this means is that the range at which the AP provides coverage is decreased so each AP covers less area. The decreased coverage area by each AP often leaves holes in the coverage when the original installation didn't include requirements for full coverage at high data rates, so a cost-benefit analysis may be prudent. For medical devices and systems that support them, the cost-benefit analysis is usually viewed as a risk analysis.

Considering the elimination of low data rates from a risk-analysis perspective as presented in ANSI/AAMI/IEC 80001-1, we must consider how much improvement is generated compared to the increased risk to safety, effectiveness, and data & system security. Security is independent of data rate and may be ignored here.

- **Improvement:**

  As mentioned above, when the AP only transmits at high data rates, higher throughput is supported. However, since most clients automatically use the highest data rate that can reliably be used to transmit data, it may be that clients are using those higher data rates except when lower rates are needed to maintain a network connection. If this is the case, changing the network configuration adds risk (less coverage) and little benefit.

- **Patient safety concepts to consider:**

  Does the reduced coverage require the installation of new APs?

  - Many installations use redundant AP coverage to mitigate risks associated with the failure of a single AP. Does decreasing each AP's coverage result in the elimination of redundant coverage?

  - Whether single or redundant coverage exists, does the change result in any areas that previously supported WLAN connectivity to lose the ability to support a reliable connection?

  - **Tests to consider to demonstrate that effectiveness is not diminished:**

    If low data rates are disabled, test to ensure that all client devices continue to operate without issue in all areas that are expected to have WLAN coverage. If some devices use redundant coverage to mitigate risk of AP failure, test to ensure that redundant coverage exists everywhere at the lower data rates.
65. Should I turn off lower 802.11b data rates to get better performance on my 802.11b/g network?

Many companies and hospitals have embraced the strategy of obsoleting 802.11b support to improve network efficiency. (Since 802.11b and 802.11g use different modulation schemes, the network has to transmit management frames using 802.11b modulation to ensure that old clients can “hear” the management traffic. The lowest 802.11g data rate is 6 Mbps, so keeping the 5.5 Mbps 802.11b rate isn’t a big hit, but keeping the 1 Mbps data rate means that management frames essentially take six times as long to transmit as they would on a pure 802.11g or 802.11g/n WLAN.)

It is important to have a plan that includes an inventory of devices to ensure 802.11b is supported as long as 802.11b devices exist. Often, a first step is to disable the 1 and 2 Mbps data rates and leave 5.5 and 11 Mbps data rates. Only the oldest (earlier than ca. 2000) devices support just 1 and 2 Mbps, and these support the original 802.11 (not 802.11b) standard. 802.11b introduced 5.5 and 11 Mbps. 802.11g devices (starting ca. 2003) are backwards compatible to run on 802.11b networks and add data rates 6, 9, 12, 18, 24, 26, 48, and 54 Mbps.

66. What are the pros and cons of using DFS channels in 802.11a/n?

Background: DFS channels allow 802.11a/n devices to share spectrum with other users, such as military radar, on the condition that if the other users are detected, the channel is quickly vacated.

Pros: Adds a significant amount of bandwidth. For the USA, there are nine non-DFS channels: 36, 40, 44, 48, 149, 153, 157, 161, and 165. There are 15 DFS channels: 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, and 140.

Cons: If an AP on a DFS channel determines that it must vacate the channel, then clients might lose connection for a period of time. This connection loss is mitigated when there is redundant RF coverage that allows the client to have a backup AP in the case of a DFS event. If the AP moves to another DFS channel, then it must remain off-line for 60 seconds while it scans for RF activity. If the AP moves to a non-DFS channel, it may immediately begin broadcasting beacons and responding to probe requests from client devices.

Depending on the RF coverage and the network requirements of the client devices it supports, the added bandwidth of the DFS channels may improve the network performance without unacceptable risk, but for every hospital, the inputs and outputs to the risk analysis will be different. Consult IEC 80001-1:2010 and the associated technical reports for more guidance on managing IT-networks that support medical devices.
67. **What is the “channel 37 issue,” and why should I care?**

As part of the Middle Class Tax Relief and Job Creation Act of 2012, Congress requires that the FCC repurpose and auction spectrum for commercial use (Section 6403 of the Act). TV channel 37, the 608–614 MHz band used for medical telemetry (part of WMTS), is included in that law. The Act accommodates relocating channel 37 incumbents, but only if relocation costs do not exceed $300 million. If implemented without any changes, healthcare will lose the use of channel 37 for medical telemetry, severely limiting its use and causing much hardship to currently deployed users (we estimated the cost to redeploy/replace at $2.0 billion). AAMI and ASHE formed the WMTS Coalition to address this issue. The coalition lobbied with the FCC and wireless vendors to keep channel 37 allocated to WMTS. The FCC and most wireless vendors support leaving channel 37 alone. While there are a few wireless companies still pushing for reallocation, it appears that channel 37 will remain dedicated to medical telemetry. See thetracejournal.com/u/Philips/8cCahi0OyJNwcqzn/754619/Feature-Story.htm for a discussion of the channel 37 issue, including an interview with John Collins, engineering and compliance director for ASHE.

68. **Our monitoring vendor uses a 1.4 GHz WMTS-band wireless system while our 802.11b/g/n WLAN runs on 2.402 to 2.483 GHz. What are the implications for these different spectrums?**

For a general discussion of WMTS vs. a Wi-Fi wireless LAN for patient telemetry, see Question 70. The 608–614 MHz band provides 6 MHz of bandwidth, and 1.4 GHz bands provide 8–10 MHz of bandwidth. If dedicated channels are used for each telemetry transmitter, and assuming 25 kHz per telemetry channel, there is sufficient bandwidth to support about 120 patients. Some WMTS solutions use an architecture modeled after 802.11 where each AP runs on a different channel and the APs bridge from WMTS to Ethernet. In this case, the vendor’s specifications determine the number of patients that can be supported. The 2.4 GHz ISM band in which 802.11b/g/n supports three non-overlapping, 20-MHz wide channels supports data rates of up to 54 Mbps (for b/g). With three non-overlapping channels, it is difficult to have an AP layout where nearest-neighbor APs are always on different channels as is preferred to minimize interference. This issue aside, due to frequency reuse, more telemetry channels can be supported in the 2.4 GHz band than can be supported in the 1.4 GHz WMTS band. Many medical device manufacturers recommend using the 5 GHz band with 555 MHz of bandwidth in the USA (with an FCC notice of proposed rulemaking (NPRM) proposing an additional 195 MHz). For other countries, please search for a list of WLAN channels on Wikipedia.

Note that 802.11n can use either 20-MHz or 40-MHz wide channels. In the former case, three non-overlapping channels are supported, with data rates up to about 300 Mbps. In the latter case, one non-overlapping channel is supported, providing about twice the bandwidth of the narrower, 20-MHz wide channel. The single 40-MHz channel overlaps the 802.11b/g channels. Running 802.11n in the 2.4 GHz band is generally considered a consumer-class solution and not recommended for enterprise deployments.
69. **How does the ASHE WMTS registration work? Why should I bother registering our channels?**

WMTS registration works by enabling a WMTS-based telemetry user to “claim their place” in the WMTS frequency bands. Detailed information can be found on the ASHE WMTS web page at www.ashe.org/resources/WMTS/. A hospital goes to the WMTS website at www.wmtssearch.com to register its site as a user. Then, when telemetry is about to be deployed, the telemetry vendor provides a list of telemetry transmitters and their frequency to the hospital, and the hospital registers those transmitters on the website. To limit the risk of interference/overlap with other nearby hospitals, the vendor often checks the database to see what frequencies are available and “tunes” the telemetry transmitters to those open frequencies.

Registration is important for a few reasons. First, while the risk of interference from a neighboring hospital is minimal, it does exist. In the case of any interference or dispute, the hospital that registers their transmitter first has priority. It doesn’t matter who deployed first, only who registers first. Recently, registration became important for a completely unforeseen issue. With Congress pushing the FCC to auction off TV channels, including channel 37 (dedicated to WMTS), the numbers of registered users enabled the WMTS coalition to make excellent and successful arguments to leave channel 37 alone. Plus, if a user must leave channel 37, any money available will go to registered telemetry users; others will get nothing. Another reason to register is to ensure notification of adjacent-channel TV station operation (TV channels 36 and 38). The registration system notifies WMTS users of potential adjacent-channel TV operations so that hospitals can manage their systems effectively. Finally, registration is an FCC requirement—it’s the law.

70. **What are the advantages and disadvantages of WMTS and Wi-Fi for medical telemetry?**

Before comparing the WMTS and Wi-Fi (WLAN) telemetry, it is important to note that clinical and support capabilities are far more important than the differences in technologies. Simply, buy based on your needs, not the technology used. Neither offers enough advantages over the other to override the clinical features.

- **WMTS advantages:** Dedicated frequencies; protected use; not shared with other, nonmedical users. Also has the capability for adopting new technologies and limited two-way communication. IT has no involvement in the system, reducing the risk of network upgrades disrupting monitoring.

- **WMTS disadvantages:** Slight risk of interference from other hospitals; in some cities, TV channels 36 and/or 38 will crowd channel 37 telemetry. Registration is required, but not well enforced (estimates are that at least 1,000 hospitals have failed to register), so one can’t be sure who else is using the WMTS frequencies. While new technologies and two-way communication are allowed, vendors have generally chosen not to implement them, limiting the maximum use of the frequencies and error correction. Dedicated frequencies require a dedicated antenna system.
• WLAN telemetry advantages: Using WLAN technology minimizes interference risks, plus the technology’s two-way communication enables error correction and minimizes lost information. It also runs on a commonly used infrastructure, reducing installation costs.

• WLAN telemetry disadvantages: This depends upon the hospital’s WLAN installation—experience shows that the WLAN infrastructure varies widely, from excellent to nearly useless. Life cycle support will depend upon IT’s capabilities and priorities. In WLAN standards, voice and video are the highest priority traffic; medical doesn’t exist. Successful deployment requires a WLAN built and maintained to IEC 60601-1-2 standards.

Your Feedback

Do you have other questions that the Wireless Strategy Task Force (WSTF) could answer? Do you have comments on questions and answers already posted? If so, submit your comments at www.aami.org/hottopics/wireless/FAQs/feedback.html.
AAMI Guidance For Healthcare Providers Managing Medical IT-Networks

Order Code: 8000101 or 8000101-PDF
List $130 / AAMI member $78

TIR80001-2-1:2012, Part 2-1: Step by step risk management of medical IT-networks; Practical applications and examples
Order Code: 800010201 or 800010201-PDF
List $150 / AAMI member $90

TIR80001-2-2:2012, Part 2-2: Guidance for the communication of medical device security needs, risks and controls
Order Code: 800010202 or 800010202-PDF
List $150 / AAMI member $90

Order Code: 800010203 or 800010203-PDF
List $140 / AAMI member $84

TIR80001-2-4:2012, Part 2-4: General implementation guidance for healthcare delivery organizations
Order Code: 800010204 or 800010204-PDF
List $110 / AAMI member $66

Order your Copy Today!
Call +1-877-249-8226
Visit http://my.aami.org/store

SOURCE CODE: PB
Wireless
Move Your Healthcare Technology Career Forward

Education
News
Medical Device Standards

Career Growth
Networking
Leadership

Join AAMI and receive:
• Subscriptions to AAMI publications;
• Opportunities to serve on AAMI committees;
• Access to listserves and members-only content on aami.org;
• Discounts on AAMI products and educational offerings;
• Free posting of your resume and 50% discount on online job postings;
• Networking events;
• and much more.

Attention Students and New Professionals!
Receive discounted membership dues! Reference the Individual Membership Application for more information.

Joining is Easy!
Become a Member
www.aami.org/membership