Dispelling Wireless Technology Myths and Developing a Roadmap for Success

Shawn Jackman

Wireless technology is amazing, magical, and simple. Wait, simple? Look around you right now. I bet someone’s chin is lit up using a wireless device at this very moment. If you are bold enough, go ask them if they could comfortably go back to the pre-wireless days. They’d look at you like you’re crazy.

What if you told them that their network connection would be faster and more reliable if they wired their mobile device to the wall? How many takers do you think you’d get? Probably not many. Wiring a mobile device sounds like an oxymoron.

For the vast majority of consumers, a “good enough” network connection is a worthwhile sacrifice in order to gain untethered mobility. Now, what if we said your child or parents will be hooked up to a wireless device to monitor their critical health condition? If you are cringing or uncomfortable right now, you’ve likely experienced when wireless doesn’t quite work perfectly.

I’ll double down on my earlier bet and say that you have Wi-Fi in your home. I’ll triple down that you own a cellular device. Typically, we set up a wireless access point and forget about it for a few years. Wireless is pretty darn amazing, magical, and simple—when it works right and when your requirements also are simple. When it doesn’t, we can add the word “frustrating” to the mix.

The Tricky Parts

With all of the amazing progress we’ve made in wireless technologies, why isn’t it better? Progress, it turns out, can be measured by several means. Different wireless technologies use different techniques. Cellular, for example, uses licensed spectrum that prevents other systems from interfering (though this may change). Wi-Fi, Bluetooth, and many other wireless technologies with which we are familiar use unlicensed frequencies that share common radio spectrum across many technologies. As if transmitting reliably over a radio frequency (RF) spectrum wasn’t difficult enough, we also must use methods to properly secure those same transmissions, adding a level of complexity not commonly used with lower-level wired network protocols.

To gain an appreciation for what makes wireless tick, we need to first explore the unseen.

Physical Layer

Let’s start with RF, the most fundamental building block of wireless communication. Wireless wasn’t taught when I went to college for computer science in the early 1990s. I think my electrical engineering colleagues had a class or two that incorporated wireless at some level. To my knowledge, none of them are information technology (IT) or clinical technology (CT or “biomed”) professionals deploying wireless networks.

About the Author

Shawn Jackman is co-chair of the AAMI Wireless Strategy Task Force and founder and CEO of Clinical Mobility, Inc., in the San Francisco Bay Area. Email: shawn@clinical.mobi
With wired networks, you run a physical cable and usually perform a test using a special tool to ensure it was installed and terminated properly. Effectively, this is a one-time event and you cross it off your list of concerns. RF, on the other hand, is the physical medium upon which wireless operates. Even cellular companies that purchase dedicated licensed spectrum will tell you, RF is not a reliable “test-once-and-forget” component of a network design. We must always suspect the physical medium as a concern when designing, deploying, operating, and troubleshooting wireless networks.

Clean RF Spectrum. When we communicate using speech as humans, we are doing so over a shared audio spectrum. RF is no different in that it requires its own spectrum to communicate. Many of the wireless technologies we use today operate over unlicensed or otherwise shared radio frequencies. Using a shared radio spectrum doesn’t mean that everyone plays by fair rules. Some technologies can completely dominate and render the spectrum unusable to other wireless technologies. For example, certain types of wireless video systems use a type of wireless technology that continuously transmits a signal without any interruptions. While this certainly works to transmit video, the RF spectrum used by this type of system becomes unusable to any other nearby system occupying that same RF bandwidth. This is equivalent to someone yelling right next to you—except they never have to take a breath to pause and they never stop.

You have to always assume your physical layer as suspect when troubleshooting problems in a wireless network, especially when using unlicensed frequencies. In contrast, how often do you think about that when troubleshooting a wired connection?

Radio Performance. As animals, our ability to hear or create sound is not equal. Variance exists in frequency range, volume, and sensitivity. Wireless radio technology shares this variance. We all have experienced other human beings who cannot hear very well. This usually requires you to raise your voice. However, many wireless devices are unable to talk any louder because their volume often is fixed or they have upward limits that cannot overcome a deficiency in receiving power. The radios used in either side of the wireless link greatly influence overall network performance and user experience.

Balanced Power. If a person is standing on a faraway hill with a megaphone, can that same person also hear a normal person’s voice with the same intensity? A megaphone only amplifies the transmission and not the reception. The effective range of a wireless link is largely dictated by the weakest link in bidirectional communication. Pretend you are at a rock concert and you try asking the band a question from way off in the stadium. The band cannot hear you without the aid of voice amplification. Amplification is expensive and consumes lots of precious battery power—two critical design
Antennas. Antennas vary considerably in type and quality. How and where antennas are positioned greatly affects performance and deployment considerations. Even though human ears vary in shape, our collective ability to hear remains relatively consistent. Antennas can vary widely by quality, frequency, number of elements, direction, and pattern (shape), in addition to overall performance. Have you ever cupped your ear when you had a hard time hearing someone? This minimizes (rejects) interfering sound coming from the opposite direction of what you are trying to hear and reflects more sound into your ear canal, effectively amplifying the volume of what you are listening to (and anything else coming from that same direction). Antennas can serve a 360° pattern and as little as a few degrees, depending on the type.

RF Channel/Bands. Ever hear a dog whistle? It produces a high-frequency sound outside of a normal human’s ability to hear or reproduce. Wireless devices are designed specifically to support certain frequencies and even entire bands. But as regulations have changed over the years, devices manufactured and certified under previous regulations are not forward compatible. If your wireless carrier adds 5G towers, you can assume your current cell phone will not be able to take advantage of it. That is also true for old medical devices that incorporated wireless a decade ago.

Areas of OSI (Open Systems Interconnection) Layer 2
We’ve covered some of the most important lower-level details, so now let’s move up to the next logical layer used in wireless communications.

Roaming Behavior. Roaming is a mobile device’s ability to transition between infrastructure radios similar to roaming between towers with a mobile phone. Some wireless technologies have elegant methods for this transition, whereas with others, it was an afterthought. Wi-Fi, for example, is one of those technologies that has loosely defined roaming mechanisms, and the decision is left completely up to the

Antennas can vary widely by quality, frequency, number of elements, direction, and pattern (shape), in addition to overall performance.
client device in nearly all cases. Depending on the manufacturer’s chipset and software types (or versions), a wide range of behavior can be witnessed. Be careful upgrading software, as severe bugs or behavior changes often can be seen in roaming behavior.

**Data Rates.** My grandmother can talk very slowly. While she communicates the same information in words, she takes a lot more time to do so. Older wireless technologies (commonly used in healthcare) that use the same radio spectrum have this same problem. Performance degrades when devices have to wait until the RF channel is free. Older technologies using shared spectrum simply need to be replaced—there is no other way around it.

**Protocol Support.** How a wireless technology uses the wireless spectrum is based on a protocol. Even proprietary wireless technologies operate by a common protocol. Devices supporting only older protocols will not be able to take advantage of many newer capabilities. These capabilities can include everything from transfer speeds, security capabilities, and power-saving modes. In fact, some protocols can have a considerable performance and reliability impact on other devices. For example, Wi-Fi has evolved and matured greatly since its original introduction. Although older Wi-Fi technologies are still made compatible with newer ones, it is done so at an extreme performance cost. Running older Wi-Fi technology such as 802.11b wreaks havoc on everything else communicating on the same RF channel, penalizing every other device and overall network performance.

**Security: Authentication and Encryption.** Limiting security to a single line item is hardly fair, as it is a deep and wide topic. Mobile devices (should) incorporate many levels of security, with all of them being important. In healthcare, most would argue that we must incorporate many levels of security. Authentication and encryption—two of the most commonly discussed components—including how a device is allowed to join a network (through some type of an authentication method) and protecting the content of our transmission from third parties (through an encryption method). Proprietary wireless technologies commonly have limited authentication options, but even massively adopted open wireless standards such as Wi-Fi have limited enterprise authentication mechanisms. Consumer authentication (including WPA/WPA2 Personal) is not scalable for enterprise use and must be avoided for healthcare organizations. Encryption is a method of protecting wireless transmissions against tampering and other foul play—and ensuring privacy—one a communication link is authenticated and formed. Depending on the wireless technology, encryption may be too outdated, weak, or simply nonexistent for healthcare use cases.

The AAMI Wireless Strategy Task Force (WSTF) recommends the IEEE 802.1X/Extensible Authentication Protocol (EAP) or methods that use certificates exclusively on both the client and server as minimum authentication methods. The best EAP protocols use certificates to form an encrypted tunnel to transport device credentials for authentication. IEEE 802.1X and EAP protocols are an open framework used by many wireless or wired systems. The minimum encryption level recommended by the AAMI WSTF varies by wireless technology, but the task force generally agrees on those that leverage the AES protocol. For Wi-Fi, this would be a variant called AES-CCMP and is the method standardized with WPA2.

**Feature Parity.** Configuring specific wireless channels, data rates, protocol features, and other factors must be harmonized across a wireless network deployment. For example, the features used in a wireless infrastructure design must also be in parity with the features used on the devices leveraging the infrastructure. This includes enabling or disabling specific infrastructure or mobile device features such as wireless frequency bands/channels, power-saving modes, security mechanisms, and many more. Hundreds of feature toggles are present in most infrastructure products.

I can keep going on with the complexities of wireless, but hopefully you get the point. A lot is going on under this shroud of magic and simplicity! Healthcare is one of the most aggressive adopters of wireless technologies. Therefore, you must consider many factors when designing and implementing a wireless system, rather than just the infrastructure. At a minimum, the system in this instance means the entire end-to-end ecosystem of infrastructure, security, and end-user devices.
Developing Higher Reliability and Safety
It can get really ugly when one or more of the core elements to a wireless connection is compromised. As a result of the high level of frustration with wireless, in 2015, the Food and Drug Administration (FDA) and Federal Communications Commission (FCC) jointly hosted a Wireless Test Beds Workshop at FCC headquarters. A wide range of industry experts was invited to help solve the problem of achieving wireless reliability. Wireless “test beds” were the theme and proposed solution to many wireless problems for medical and nonmedical uses.1

Many of the members of the AAMI WSTF attended and presented at the event. Making wireless safer, more reliable, and secure is core to the mission of WSTF—so we took up the challenge to further define, design, and develop a strategy and direction for wireless test beds. However, we kept getting mired in the details. Common questions kept recurring where we had no clear-cut answers:

What exactly is wireless? Does that include or exclude Wi-Fi, cellular, or WMTS (Wireless Medical Telemetry Service)? What standard(s) provide the best guidance? Is a test bed a place or a concept? What should we put in it? What should be tested, exactly? Passionate debates ensued.

Eventually, the WSTF took a step back and considered why there was a call to action over a test bed. A test bed is a potential solution to a problem, but what is the problem exactly? The debates ceased once we asked ourselves that question. We unanimously agreed that the problem really stems from a lack of reliability and safe use of wireless for critical applications such as medical. So it’s not really about test beds at all. We’re not saying that a wireless test bed isn’t useful. In fact, we all agree that it is. But a test bed represents only one approach to solving the systemic problems surrounding medical uses of wireless.
Roadmap for Success
If a wireless test bed isn’t the be-all-end-all answer, then what is? Some organizations seem to have figured out the formula more so than others. Therefore, the AAMI WSTF thought sharing this knowledge in the form of a roadmap for success would provide an initial step toward our goal of improving the state of wireless in healthcare.

- First and foremost, treat your wireless systems as exactly that—a system. At a minimum, consider infrastructure, security, and end-user devices in all decisions.

- Set minimum design and security standards and evaluate for conformance. This isn’t a one-time exercise. Each device software upgrade needs to be evaluated to confirm sustained conformance to policy.

- Do not even consider using devices that lack enterprise-grade authentication and encryption. Wi-Fi devices that only use WPA/WPA2 Personal authentication do not scale and can expose healthcare delivery organizations to security vulnerabilities.

- Understand your devices and applications that operate on your hospital networks. You may have heard of device or application profiling. Profiling allows you to implement authorization rules. These protect an organization’s key assets by implementing per-device or application security rules that enable their key function.

- Devices should encrypt their transmissions wirelessly. In addition, HIPAA (the Health Insurance Portability and Accountability Act) requires patient data also to be encrypted at rest. This includes data on devices and network storage locations.

- Implement a wireless intrusion detection system. If your organization accepts credit card transactions electronically, Payment Card Industry (PCI) compliance requires it. Depending on your organization’s PCI tier, you also may be required to maintain a 24/7 active response mechanism for detected events.

- Dedicate staff to manage your wireless infrastructure and systems. Chances are that you have several types of wireless systems operating in your environment that support clinical care. Don’t assume an IT person with network knowledge or a CT professional understands the intricacies of RF. Give them the proper training to be successful.

- Develop a device and application intake process. This may sound like an organizational hurdle to implement new devices or applications, but a service-oriented and customer-friendly device/application intake process gives your organization a proactive leg up to prevent serious problems before they occur. This allows your organization to design a proper strategy for

Improving Wireless in Healthcare: Highlights

- Ensure you have a professionally designed, healthy RF infrastructure with mechanisms to monitor for interference and performance degradation. This is sometimes referred to as “site surveys.” When it comes to RF, a well-designed radio infrastructure is the most critical success factor to properly implementing a wireless network. Hire a qualified professional or organization and hold them accountable. Routine signal validations should also be performed. Don’t count on predictive RF surveys to work right. Use scientific methods to determine infrastructure radio placements and eliminate as much guesswork as absolutely possible. Most of the time, predictive RF surveys are a waste of time and money.

- Embrace a “systems approach” in all decisions.

- Set minimum design and security standards and evaluate for conformance.
deploying, maintaining, and securing devices and applications in advance of deployment. One of the key benefits of this intake process is documentation, which helps when it comes to preventive maintenance, security breaches, support issues, knowledge transfer, and recalls.

- When issuing requests for proposals (RFPs), ask device vendors if they support security capabilities consistent with your organizational policy. Ask how they comply to the FDA guidance.²

- Build a certificate infrastructure (i.e., PKI [public key infrastructure] or CA [certificate authority]) and ask device vendors if they support certificates (especially in the RFP process) for use in authentication and encryption. Build a validation process into your device intake process to validate and test that this capability works as advertised. Note that building and operating your own PKI doesn’t guarantee security—it’s quite complicated and you can expose huge security holes if you aren’t careful. If possible, hire a qualified professional to build a properly designed PKI for your organization. Many organizations have wasted time and money due to the complications and inherent risks of the PKI not working as intended.

- Perform due diligence. Ask your information security teams to be extra diligent pre-deployment with devices that handle sensitive data, large device deployments, operating systems, and applications. This may include penetration testing, negative testing, and fuzz testing. In addition to security, minimally perform RF and 802.11 protocol testing. Does the tested device support all of the channels or modes your organization uses? How does the device roam and perform power savings? Many performance issues reside in those two areas alone.

- Stop deploying Wi-Fi devices that only use 2.4 GHz. Period. Hospitals are increasingly utilizing the unlicensed 5-GHz spectrum and are perhaps even moving away from the clinical use of 2.4 GHz.

- Eliminate extreme legacy Wi-Fi devices that are limited to IEEE 802.11b. These devices severely degrade network performance and are unlikely to pass even a moderate security validation.

**Guidance for Manufacturers**

- Implement an IEEE 802.1X supplicant for wireless and wired devices capable of secure EAP protocols (e.g., EAP-PEAP, EAP-TLS, EAP-TTLS). When using usernames and passwords for authentication, ensure that credentials are stored in an encrypted fashion. Also when using the tunneled EAP types for username/passwords, ensure your implementation supports mutual authentication of the RADIUS (Remote Authentication Dial-In User Service) server before establishing the tunnel and submitting them for authentication.

- Follow the FDA guidance, *Radio-Frequency Wireless Technology in Medical Devices*.³

- Develop and maintain a wireless test lab with wireless network equipment and infrastructure devices commonly found in customer deployments. This includes configuring the equipment in an enterprise manner inclusive of security components. Make this lab easily accessible to developers. Assign a lab owner and key point of contact. Your customers assume that you have a sufficient test bed environment in your organization, and this is part of the cost of doing business. Publish a list of testing variations to customers to gain increased customer confidence.

Know the devices on your hospital network. Use only enterprise-grade authentication/encryption.

Devices should encrypt transmissions wirelessly. Follow HIPAA regulations for patient data.
Approaches to Wireless Technology in Healthcare

- Develop a master test plan that incorporates everything you believe can go wrong or a customer environment may incorporate. Evolve this test plan as new experiences arise or test cases become outdated.

- It’s beneficial to incorporate X.509 certificates for authentication and encryption. Applications can use those certificates to encrypt all application data that is in transit over the network.

- Never implement a Wi-Fi device that only operates at 2.4 GHz for use inside a hospital.

- Implement elegant roaming mechanisms such as IEEE 802.11r or leverage available vendor-proprietary methods.

- Maintain radio component supplies sufficient to last five or preferably 10 years, but for part replacements only. Adopt newer wireless technologies for new products.

- Develop metrics for minimum and target acceptance criteria. These metrics may be used for acceptance testing in customer deployments and provide meaningful baseline data compared with your organization’s testing efforts.

- Limit or eliminate traditional Bluetooth modes of operation. Bluetooth Low Energy (BLE) is only one mode of operation, and often traditional Bluetooth is still used for data transmission once devices are paired through BLE advertisements. Some hospitals strictly forbid the use of traditional Bluetooth modes of communication.

- Implement a convenient way of distributing authentication credentials, configuration, and upgrades onto all devices. This capability is needed for more than just during deployments; it also is needed for day-to-day operations and maintenance. This may include integration into a mobile device management platform or similarly featured system.

- Leverage quality of service (QoS) methods that aren’t one-sided and offered as a take-it-or-leave it method to your customers. Proprietary protocols, specific marking, and transmitting traffic on the highest-priority queues may be in violation of the customer’s QoS policy. For example, at least one smartphone manufacturer marks and prioritizes YouTube traffic in the highest QoS class, which cannot be overridden without advanced management tools. Instead, give customers the ability to make their own prioritization decisions based on use case and other business factors.

- Incorporate IEC 80001 into development and quality assurance processes.

- Develop a rigorous security testing process to heavily evaluate for security vulnerabilities. This includes penetration testing, negative testing, and fuzz testing.

- Publish known security vulnerabilities to customers and provide the status on remediation. Incorporate a scoring method, such as the Common Vulnerability Scoring System or equivalent.4

- Work with and publish information to your user or customer base for risk management related to the design, use, and maintenance of wireless systems. Include clear information on risks, including training programs and continuing education.

- Don’t assume that wireless and security are easy—they’re not. Ensure your organization maintains the right level of experience or hire people who can provide it. Incorporate a failure mode and effects analysis.5

Ensure a healthy radio-frequency infrastructure that can monitor interference and performance.

Dedicate staff to managing wireless systems.
Guidance for Healthcare Delivery Organizations

- Whenever possible, ensure your network is designed for sufficient wireless coverage when single radio outages occur. High-acuity areas are especially important. Keep infrastructure radio device spares on hand to quickly and fully recover from these events.

- Ensure high availability throughout the entire network path. Think about switches and how they are powered. Walk through each network hop in a network flow. What happens when each part fails? If you aren’t sure—or haven’t actually tested it—then you do not have high availability. Test high-availability mechanisms on regularly recurring intervals. This will sharpen your planning and develop fast recovery times for when they matter.

- Ensure QoS mechanisms are implemented and tested end-to-end within your network. One single network hop can strip QoS tag information or perhaps ignore the QoS tags altogether.

- Create and track metrics for network availability that target overall availability in addition to specific wireless and network technology segments. It helps to develop a bonus incentive for staff to attain high levels of availability.

- Develop emergency response processes and teams, then rehearse those processes. Assign staff to specific roles, each with certain responsibilities, and maintain the list as employees change roles.

- For devices that are critical to clinical workflows, ensure your device vendors maintain a strong relationship with their radio manufacturers or possess a deep level of control over their function. For example, that may include the ability to develop and/or correct key MAC (Media Access Control) layer capabilities that affect performance and security.

- To reduce risk in the event of a Wi-Fi access point failure, be careful eliminating IEEE 802.11a/g data rates too aggressively. For IEEE 802.11a/g, leaving 6 or 9 Mbps as a supported rate, but not mandatory, reduces overhead and allows devices to use the rates when needed. Eliminating all IEEE 802.11b rates (1, 2, 5.5, and 11 Mbps) is highly recommended if your network design supports it, as these are direct sequence spread spectrum (non–orthogonal frequency division multiplexing) data rates that invoke other performance degradations when they are in use. At a minimum, disabling 1 and 2 Mbps rates provides huge advantages.

- Back up all network configurations and track all changes, ideally through automated means.

- Create or assign positions of authority to enforce policy and provide risk management. Provide training and clear expectations for management and other personnel. A single break in the chain can create significant liability and risk.

For devices that are critical to clinical workflows, ensure your device vendors maintain a strong relationship with their radio manufacturers.
Still Think Wireless Is Simple?
Wireless deployed in a medical environment is incomparable to wireless used in an average home. The medical network faces a larger coverage area, supports more diverse devices, has much higher device quantities, and has higher security requirements. The more regulated the industry, the more demanding the applications. As diversity increases, so does the overall complexity.

We hope this checklist helps to set your organization on the right path. More pieces will emerge when executing each of these steps. That’s a good thing. Your organization will improve from the process and you’ll be well on your way to providing excellent wireless reliability and safety.

References
How Does Your Department Stack Up?

Compare apples to apples with AAMI Benchmarking.

Now there’s a way to compare your budget, personnel, and policies against those of your peers—so you can improve your programs.

Healthcare Technology Management
Learn methods for smart cost containment, and make the case for buying new equipment and hiring new staff.

Sterile Processing
Compare sterilization practices, prepare for accreditation surveys, and more.

For more information, visit www.aami.org/benchmarking or call 877-249-8226.