5-7-2011

Design of a Pragmatic Test Lab for Evaluating and Testing Wireless Medical Devices for Deployment on an Integrated IT Wireless Network

Allie Paquette
alliepaq@gmail.com

Design of a Pragmatic Test Lab for Evaluating and Testing Wireless Medical Devices for Deployment on an Integrated IT Wireless Network

Allie T. Paquette

B.S. Boston University, 2009

A Thesis

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Master of Science

at the

University of Connecticut

2011

APPROVAL PAGE

Master of Science Thesis

Design of a Pragmatic Test Lab for Evaluating and Testing Wireless Medical Devices for Deployment on an Integrated IT Wireless Network

Presented by

Allie T. Paquette, B.S.

Major Advisor: _____

Dr. John Enderle

Associate Advisor: _____

Dr. Wei Sun

Associate Advisor: _____

Mr. Frank Painter

Associate Advisor: _____

Mr. Jeffrey Bronke

University of Connecticut

2011

Acknowledgement

I would first like to thank the American College of Clinical Engineering (ACCE) for providing the topic for my research focus and their sponsorship of this project. Specifically, I would like to thank Mr. Jim Welch, Ms. Jennifer Jackson, and Mr. Frank Painter for their guidance and mentorship throughout the project. I would also like to thank Mr. Rick Hampton and Mr. Michael Fraai for sharing their time and knowledge with me. In addition, I would like to thank Masimo Inc. for providing their Patient SafetyNet System for testing during this project.

I would like to recognize Baystate Health for sponsoring my two year internship and my supervisor Jeff Bronke who supported my work on this project by allowing me to create a test lab and supplying me with the necessary tools to do so. Specifically, I would like to thank Mr. Lenny Vigneault and Mr. Sheetal Patel for their technical assistance. I would not have had access to the wireless network tools I needed and ultimately would not have been able to complete this project without the knowledge and assistance of Mr. Vigneault, thank you!

Table of Contents

Abstract

In today's healthcare environment, networking of medical devices is becoming more and more prevalent. Also, there is an increasing need for mobile technology to meet clinical needs. Wireless communication is the key component to allow medical devices to be able to move with the patient, while continuing to record and communicate patient data. A traditional example is telemetry monitoring, but other examples of wireless utilization include sending ECG test results to the EMR or remotely updating the drug library on numerous IV pumps. Each wireless application has varying demands on the connectivity infrastructure in factors such as availability, reliability, and data payload capability. Furthermore, these wireless medical device applications may share radio frequency (RF) spectrum resources with a host of other non-medical device applications such as wireless phones, barcode scanners, Bluetooth headsets, laptop computers accessing the Web, and remote control units.

While medical devices are commonly isolated on their own network, the recent trend involves utilizing the hospital's information technology (IT) network to deploy networked medical devices, particularly wireless medical devices. In order to address the increased risks which result from the incorporation of wireless medical devices onto a hospital's wireless network, thorough evaluation and testing of these devices has become an essential component of the implementation process. Despite the importance of testing new devices before implementation, strategies for performing the necessary tests are essentially non-existent in the clinical engineering field. By developing standard practices for developing a test environment and then demonstrating how the test lab can be utilized for performing risk assessment and verification testing, the groundwork will be laid for clinical engineering departments to more efficiently and safely manage wireless medical device implementations.

1.0 Introduction and Background

Based on the growth of wireless technology in medical devices, a research study and design experiment was carried out to explore the topic. A test lab with a segregated wireless network infrastructure was designed in the hospital's clinical engineering department in order to perform functional tests on wireless medical devices. A wireless medical device was provided and both a wi-fi analyzer and spectrum analyzer were utilized to perform a case study of medical device testing. A thorough background on radio frequency and wireless technology is presented, followed by the methods and results of the design project.

1.1.0 RF Basics

The foundation of wireless communications is in radio frequency (RF) technology. It is important to have a basic understanding of RF characteristics and behaviors, components, spectrum, signal propagation, and antenna concepts to understand wireless technology and be prepared to support wireless medical devices.

1.1.1 Characteristics and Behaviors

Radio frequency is at the low frequency end of the electromagnetic spectrum. RF signals are electromagnetic signals that radiate from an antenna with a particular wavelength, frequency, amplitude, and phase[1]. The relevance of these characteristics is that signals with higher frequency and shorter wavelength will have smaller range and coverage than a signal with lower frequency and longer wavelength.

RF signals are propagated in waves; however, environmental factors affect wave propagation. The RF signals can be absorbed, reflected, scattered, refracted, diffracted, and/or attenuated. Some examples of attenuation include free space path loss where

signal strength is lost due to the natural broadening of waves as they travel, as well as multipath which is an occurrence of two or more paths of a signal arriving at a receiving antenna at the same time[1].

1.1.2 Components

A basic RF system that makes up a wireless network consists of a transmitter, one or more antennas, and receivers. The transmitter initiates the RF communication by converting the data to an AC current signal and determines the frequency and the amplitude of the transmission. The antenna then gathers the signal from the transmitter and redirects it based on the antenna properties. Finally, the receiver receives and translates the signal and passes it to a computer for processing[1]. The three types of RF antennas include omnidirectional, semidirectional, and highly directional. Omni-directional antennas radiate RF coverage in all directions, while semi-directional antennas radiate RF as a beam in a general direction, and highly directional antennas radiate the RF in a particular area of focus[1]. Antenna coverage can be represented by azimuth (top-down view) and elevation (side view) charts, or antenna radiation envelopes. The choice of antenna for a given application will vary based on deployment location as determined in the site survey.

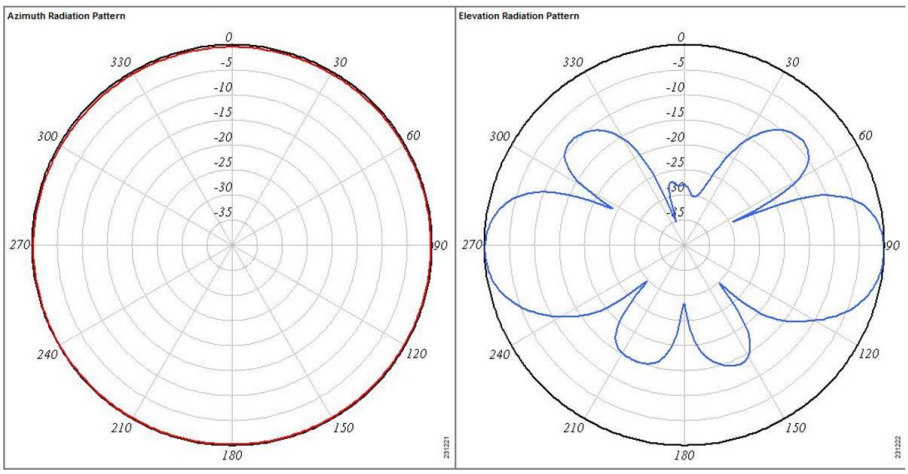

Figure 1. Azimuth and Elevation charts for a Cisco omni-directional antenna[2]

1.1.3 Radio Frequency Spectrum

The radio frequency spectrum spans an extremely wide range of frequencies, but the bands of interest for wireless networks in hospitals range from about 150MHz-6000MHz with different portions of this spectrum allocated by international and federal governments (i.e. International Telecommunication Union) for different uses (see figure 2). Of interest are the WMTS, Wireless Medical Telemetry System band and the ISM, Industrial, Scientific, and Medical band. There are two newer WMTS bands covering frequency ranges 608-614MHz, 1.395-1.400GHz, and 1.429-1.432GHz; the majority of new telemetry installations will fall within these frequencies. Two ISM bands will be explored in this project, 2.4GHz (802.11 b/g) and 5.0GHz (802.11 a/n). The ISM band of greatest challenge is the unlicensed 2.400-2.484GHz frequency under which fall the majority of current 802.11b/g/n wireless radio cards. This frequency band is populated by many device types such as wireless medical devices, cordless phones, Bluetooth, wireless video cameras, and baby monitors, and hence is very crowded. In addition to the bands shown in Figure 2 there are three Unlicensed National Information

Infrastructure (UNII) bands; one of these is 5.0GHz and this is where 802.11a/n radios communicate[1]. The IEEE 802.11a/b/g/n standards will be discussed in section 1.2.1.

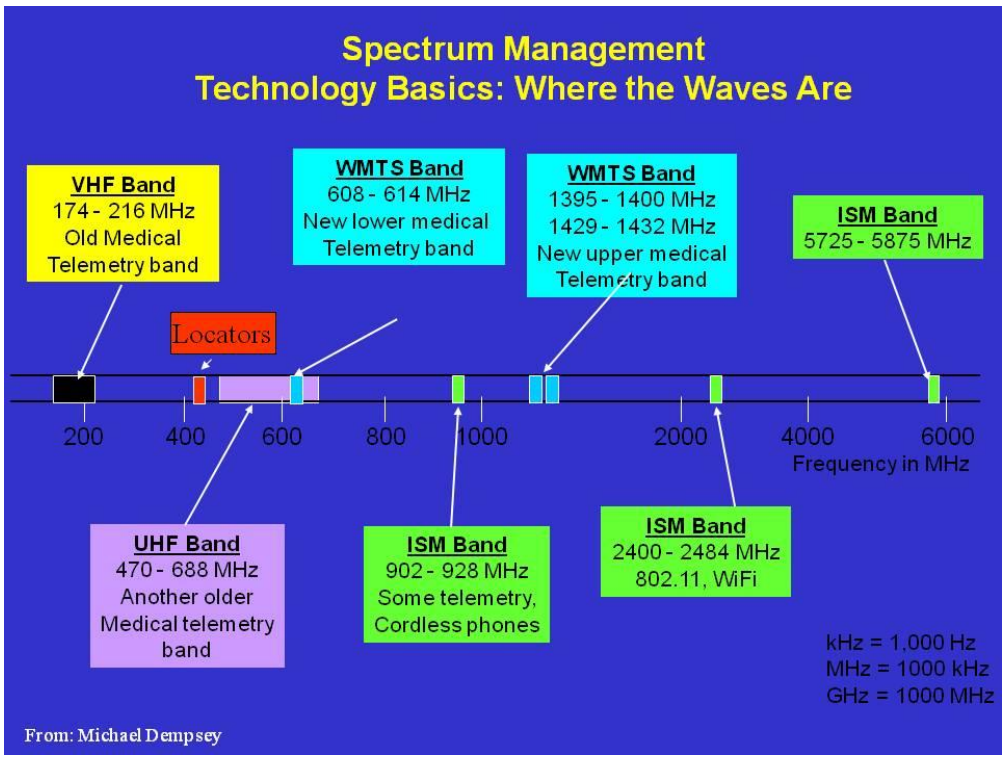

Figure 2. A sample of the radio frequency spectrum allocation of frequencies into particular bands is shown. Some bands are licensed and some are unlicensed, and each band is dedicated for a group of technologies[3].

1.1.4 Radio Frequency Transmission

Spread spectrum is a method of transmission for RF communication. Spread spectrum technology divides a narrow band transmission over a wider range of frequency space at a lower power, making it less subject to environmental and intentional interference. One form of spread spectrum transmission is frequency hopping spread spectrum (FHSS), which was used in legacy 802.11 radios and transmits with data rates of 1 and 2Mbps. FHSS works by using 1 MHz channels of frequency for a short period of time and then switching to a different channel based on a

random sequence for channel switching that is negotiated across the RF link. This hopping continues throughout the data transmission[1]. Another method is direct sequence spread spectrum (DSSS), which only utilizes the frequencies of a single 22 MHz channel to transmit data. DSSS is also transmitted with 1 and 2Mbps for legacy 802.11 radios, but for 802.11b, High-Rate DSSS (HR-DSSS) provides 5.5 and 11Mbps speeds[1]. Another popular communication technology is orthogonal frequency division multiplexing (OFDM). OFDM transmits across 52 separate, spaced frequencies allowing for higher data rates. This technology is used for 5.0GHz frequency transmissions. Also, there is extended rate physical OFDM (ERP-OFDM) which is essentially the same as OFDM except that it is referring to 802.11g, 2.4GHz frequency transmission[1].

Another important concept to consider when studying wireless communication in different frequency spectrums is the grouping of frequency bands into channels. Channels describe sections of frequencies within a given band and are defined by the center value of the range of frequencies in the channel. For example, the 2.4GHz ISM band is broken down into 14 channels and there are 23 channels in the 5.0GHz band[1]. Channel selection has implications for network design that will be discussed later.

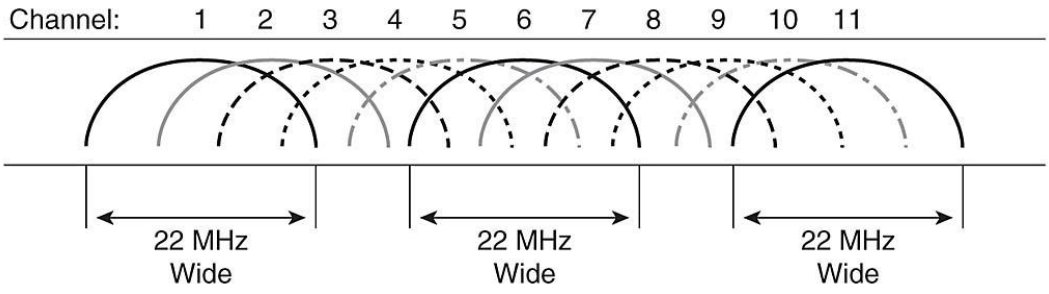

Figure 3. The breakdown of channels and their overlapping properties are shown[4]. Channels 1, 6, and 11 in bold will be discussed in the site survey process.

1.2.0 Wireless Standards

Wireless standards are developed and maintained by a number of organizations including the Federal Communications Commission (FCC), Institute of Electrical and Electronics Engineers (IEEE), International Organization for Standardization (ISO), and the Wi-Fi Alliance. IEEE has developed and maintains the 802.11 standard for wireless local area networks (WLAN), while the Wi-Fi alliance determines interoperability and certification of wireless devices for compliance with the standards[1]. Generally speaking, a WLAN is a connection between two or more devices via wireless distribution. Also, it often involves connection to the Internet through access points.

1.2.1 IEEE 802.11 Standard

The IEEE 802.11 standard on wireless local area networks was first written in 1997, with revisions and additions coming in 1999, 2003, 2007, and even continuing today. The IEEE 802.11-2007 standard is the latest official version. To manage this living document, there are different task groups that are formed to focus on different topics related to WLANs and to write draft amendments to the standard on that particular topic. Many of the amendments were written between 1999 and 2007 and were hence added to the 2007 revision of the standard. Each of the task group amendments are identified by a letter. Some important characteristics of each amendment are the frequency range, the data rates, compatibility, and techniques.

One of the earliest task groups was 802.11b, and this amendment was added in 1999. 802.11b uses HR-DSSS technology to communicate in the 2.4GHz ISM band. This standard consists of 11 channels (only three of which are non-overlapping: 1, 6, 11) and is capable of data rates of 1, 2, 5.5, and 11Mbps. In order to achieve these rates, a technique called complementary code keying (CCK) is utilized. Devices that fall under the 802.11b standard are backwards compatible with legacy 802.11 devices[1].

At almost the same time, the 802.11a amendment was developed. The focus of this amendment was on the Unlicensed National Information Infrastructure (UNII) frequency band, which had been newly allocated at the time of this amendment, 1999. The UNII band originally comprised three 100MHz bands in the 5.0GHz range. Data rates of 6, 12, 24, and 54Mbps are supported with this amendment, and when OFDM is utilized, additional data rates of 9, 18, 36, and 48Mbps are also supported. 802.11a provides a total of 12 channels and is advantageous in that the frequency band is currently much less crowded than the 2.4GHz band. Subsequently, additional 255MHz of additional spectrum was added to the existing UNII bands thereby extending the 802.11a standard to utilize up to 23 non-overlapping channels. FCC Rule 15 requires that UNII 2 and UNII 2 extended bands support dynamic frequency selection (DFS) to detect military or weather radars and automatically adjust channels in order to avoid interference. A disadvantage is that 802.11a radios are not compatible with 802.11b, 802.11g, or legacy 802.11 radios[1], however the new 802.11n radios are compatible with 802.11a.

In 2003, another amendment came out from task group g and the 802.11g amendment chose the 2.4GHz frequency band. The goal of this amendment was to achieve greater bandwidth by modifications to the PHY layer while remaining compatible with the 802.11 MAC sub layer characteristics[1]. PHY refers to the physical layer and MAC (medium access control) to a portion of the data link layer of the OSI 7-layer network model. The physical layer is the foundation of the networking model and defines the connection between a device and the transmission medium. The MAC sub layer determines how a device on the network gains access to data and how it gets permission to transmit[5]. The two techniques utilized in 802.11g are ERP-OFDM and ERP-DSSS/CCK. The Extended Rate Physical OFDM (ERP-OFDM) adds the higher

data rates: 6, 9, 12, 18, 24, 36, 48, and 54Mbps, while the ERP-DSS/CCK is used to maintain the backwards compatibility by utilizing data rates of 1, 2, 5.5, and 11Mbps[1].

802.11a, b, and g were three of the important amendments added to the 802.11 standard in the 2007 revision. Other amendments of note that were added in 2007 are 802.11i for robust security networks, 802.11e for quality of service (QoS) requirements for time-sensitive applications, and 802.11r for secure fast roaming, to name a few. Yet another amendment was ratified in 2009, 802.11n. The primary goal of 802.11n was to increase the throughput in both the 2.4GHz and 5.0GHz frequency bands. This is achieved through a technique called High Throughput (HT) that enhances the PHY and MAC sub-layers to reach throughputs of 100Mbps or greater[1]. HT radios use multiple-input, multiple-output (MIMO) technology along with OFDM to achieve these rates. MIMO uses multiple receiving and transmitting antennas and can receive multiple signals that would have previously been considered interference from multipath. There are also additional amendments that are still in their draft form that will be shaping the future of wireless technology.

Depending on the environment in which wireless devices operate, access point configuration is important to handle the different types of radios that may exist. The best option is an 802.11a/b/g/n access point which offers multiple configurations. One option is b-only mode which limits the functionality to DSSS, HR-DSSS, and ERP-DSSS/CCK. Because it is configured as a b access point, the data rates will be limited to 1, 2, 5.5, and 11Mbps and throughput will be that of an 802.11b network[1]. The next mode is g-only mode, and this mode only allows for 802.11g clients. These radios utilize ERP-OFDM technology, while disabling ERP-DSSS/CCK, HR-DSSS, and DSSS eliminating communication with any 802.11b clients. As such, data rates up to 54Mbps can be achieved. The b/g mode which supports ERP-DSSS/CCK and ERP-OFDM and hence

802.11 legacy DSSS, 802.11b, 802.11g clients can all communicate with the access points. The consequence of this compatibility is that whenever a legacy or b radio communicates, all of the g radios must enable protection which causes degradation of throughput. So although it is theoretically capable of data rates up to 54Mbps, an access point in b/g mode will likely have a maximum throughput of only 8Mbps[1]. Finally, the 802.11 a/n access point configuration contains a separate PHY layer radio that can negotiate wireless connectivity to 802.11 a/n clients. Thus in a single access point all the possible PHY layers are supported in a single physical structure.

1.2.2 802.11 Medium Access

Access to the wireless medium, which is air rather than cable or fiber, introduces complexities and therefore requires a set of rules so that access can be controlled, efficient, and secure. The two forms of access are Carrier Sense Multiple Access with Collision Detection (CSMA/CD) and CSMA with Collision Avoidance (CSMA/CA). While CSMA/CD is primarily used for Ethernet networks, CSMA/CA is the technique used for wireless networks. Before transmitting, a CSMA/CA radio, like collision detection (CD) stations, must first determine that no other stations are transmitting. If there is no traffic, a CSMA/CD device would then transmit immediately and monitor the traffic to determine if there is a collision, stopping if necessary. Because wireless communication is only unidirectional, there is no potential for collisions to be detected; therefore, CSMA/CA stations wait an additional period of time before transmitting after identifying a traffic free network in order to avoid collisions. This additional wait time is referred to as the back-off value. Because this technique is not perfect, there are additional functions, such as Distributed Coordination Function (DCF), that performs checks and balances to further work to avoid collisions[1].

Also related to medium access is the IEEE 802.11e quality of service (QoS) amendment. This has become a strong focus of the Wi-Fi Alliance and they have created a certification referred to as Wi-Fi multimedia (WMM). The purpose of QoS and WMM is to prioritize traffic and optimize the way the shared resources of the network are allocated to different applications[6]. Without QoS, all applications running on different devices have an equal opportunity to transmit data. A common application that is aided by QoS is voice over Wi-Fi (VoWiFi) phones. While most applications can handle retransmissions up to 10% without much consequence, the number of retransmissions must be less than 2% in order to clearly understand voice communications or any other time sensitive clients[6]. WMM defines four access categories: voice, video, best-effort, and background data, but allows a network administrator to determine which applications are assigned to which priority. The process of assigning packets to priority queues is shown in figure 4. Also, note that there is an internal collision avoidance mechanism in this prioritization system. QoS prioritization is essential for the deployment of medical devices on a hospital wireless network.

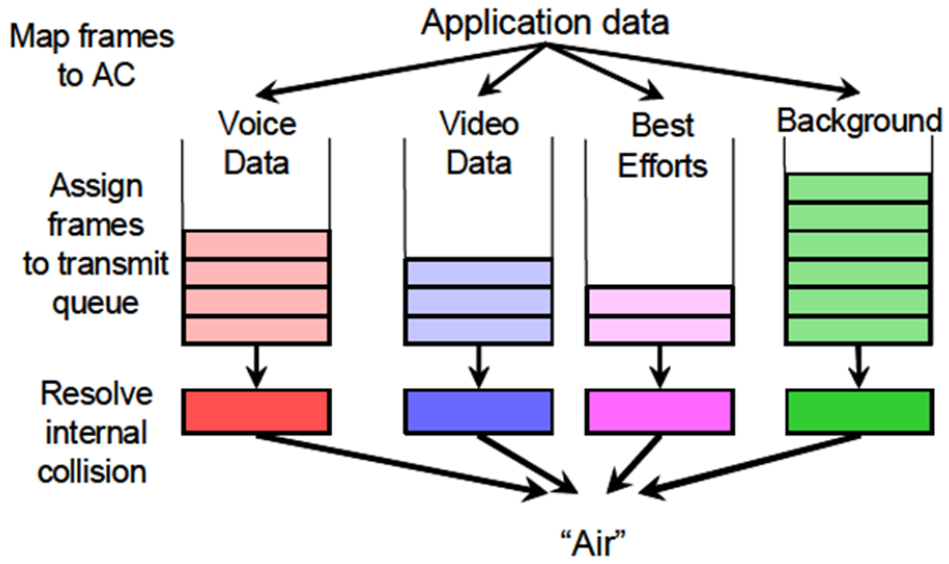

Figure 4. WMM QoS queues for application prioritization of network bandwidth[6].

1.3.0 Wireless LAN Network Design Considerations

The crucial decisions regarding the design of a wireless network are highly dependent on both the environment of deployment and the scope of the wireless project. A preliminary planning meeting with members from an institution, and possibly the networking vendor and site surveyor, will address the questions that will determine the characteristics of the network to be designed. Following this meeting, some decisions will be made based on the scope of the project, and the rest of the characteristics of the network will be identified in the site survey.

1.3.1 Network Design Planning and Site Survey Interview

The purpose of the site survey interview is to identify the scope of a project and the capacity needs of the wireless network. A site survey interview should be performed by the site surveyor with the clients. The questions that are answered within the site survey will lead to the defining characteristics of the network. Some of the important questions that must be considered include what applications will be used on the wireless local area network (WLAN), which users will be accessing the WLAN, and what types of devices will be connecting to the WLAN. Although it depends on the type of applications and the specific wireless network type, the average quoted number of data users per 802.11b/g access points is 12 to 15[1]. There are other issues with capacity and coverage to discuss and consider in the pre-site survey interview such as if there are any high usage areas, such as a nursing station, or peak on and off times. It is also crucial to identify whether there are any existing transmitters in the environment and therefore if the network must be backwards compatible. Another important clarification to make in the interview is the difference between a mobile network and having an actual mobility network, and which is required. The difference is that a mobile network implies the ability to access the network from different locations (i.e. desk, conference room) while a

network with mobility requires that a device will maintain a wireless connection while actively moving such as with a VoWiFi phone[1].

Most of these points should be taken into consideration whether creating a completely new wireless network or adding to an existing network, but when adding to a network, additional factors must be included in the planning phase. Any known sources of interference, dead zones, current types of equipment such as access point vendors and radio types (a/b/g/n) should all be considered. Also, the wireless network will be connected to some type of wired network infrastructure, so for a solid design roaming, antenna structure, Power over Ethernet (PoE), segmentation into VLANs, and user management should all be planned for accordingly[1]. Proper documentation from the site survey interview process is essential for identifying deliverables and ensuring that the wireless network implementation project is a success.

1.3.2 Considerations for the Healthcare Environment

While the issues described above apply to any wireless network environment, there are some specific questions that should be discussed that pertain to wireless networks in the hospital environment. The assumption is that the current implementation being described is a network for wireless medical devices. The major decision that has to be made before the network can be designed is whether or not these devices will be added to a shared wireless network that is used for transmitting data in the hospital. The alternative is an isolated network exclusively for medical devices with separate AP infrastructure. While there are healthcare organizations that choose to segregate a network for medical devices to avoid the risks of operating medical devices on the hospitals IT network, there are both financial and networking consequences that result making this an impractical option.

If the decision is to add the wireless medical devices to the hospital's existing wireless network, it is likely that this network will already exist, which reduces the number of decisions that have to be made. If creating a new or ideal network, the first decision that needs to be made is what type of wireless network you would like to deploy. The best decision would be to select a high throughput 802.11n wireless network with backwards compatibility. The backwards compatibility will likely be necessary because of the variety of medical devices that will potentially be added and the likelihood that they will not all contain the most up-to-date radio cards. In addition to the high throughput capabilities of 802.11n, another benefit is that 802.11n can operate in both the 2.4GHz and 5.0GHz frequency bands. One potential option for segregating medical devices and IS-type wireless data devices on the network would be to utilize 802.11n with IS-type data devices in the 2.4GHz range and medical devices in the 5.0GHz range. An 802.11b/g based network would be functional but would not provide the best potential for capacity and throughput on the network. An 802.11a infrastructure would have the benefit of operating in the less crowded 5.0GHz frequency band, but because of its lack of compatibility with 802.11b/g devices as well as its insufficient security mechanisms (which will be discussed further) it would probably be a limiting choice.

It is important to make sure that wireless networks are designed with 802.11e quality of service (QoS) capabilities as described in section 1.2.2 above. Whether or not all devices on the network have this functionality, QoS should be required on the network so that, when possible, device transmissions can be prioritized. QoS could be used to prioritize a life critical medical device's traffic over a non-life critical medical device if it was a medical device only network, or it could be used to prioritize medical device traffic over data traffic if a shared network is utilized. In conjunction with the QoS prioritization is the option or decision to segregate traffic on a wireless network with virtual local area networks (VLANs). Not only can VLANs be prioritized with 802.11e,

but they can be used to segregate data traffic from medical device traffic, or to segregate public wireless traffic from medical device traffic which is essential for security[7]. Another important characteristic to insist on in a wireless network implementation is that the network is capable of the highest level of security possible, enterprise WPA2 to date. This will be discussed further in the section on wireless security. Also, any type of automated network adaptation (APs distributing loads, channel changing, etc.) should be cautiously considered in healthcare environments due to the potential risks of life-critical patient data traffic.

Yet another consideration for a wireless network is redundancy. Assuming an institution's wired network is already designed for redundancy in the case of power failure, it is important to power the wireless network's access points via Power over Ethernet (PoE) so that they will effectively be backed up by the wired network's redundancy in the case of power failure. In addition to power redundancy, there should be AP overlap redundancy to try to minimize signal transmission drop out in the case that a single access point fails.

1.3.3 Physical Site Survey

The overall goal of the site survey is to determine access point placement and configuration based on coverage analysis and spectrum analysis[1]. A spectrum analyzer is an essential tool for a wireless administrator, not only for site survey and installation, but for troubleshooting as well. The range of frequencies that exist or need to be analyzed will determine the complexity of the spectrum analyzer required. It is a valuable exercise to walk through an environment with a spectrum analyzer to identify areas of interference as early on as possible so that it can try to be eliminated or worked around. In a hospital environment, this is particularly important to ensure that biomedical equipment does not interfere with the RF spectrum for wireless communication and vice

versa. Another important characteristic of the environment to capture with the spectrum analyzer is the noise level, which dictates the signal level needed for clear data transmission. It is recommended that the signal to noise ratio (SNR) be at least 18dBm for data networks and 25dBm for voice or other time-sensitive applications[1].

Coverage analysis is the second essential component of a site survey and this can be done either manually or with the assistance of a computer application. While the applications can be helpful, it is recommended to always complete a physical site survey. The goal of the coverage analysis is to measure the received signal strength at different distances and angles from an access point, thereby determining the coverage area of an access point. Various tools can be used to measure received signal strength, and it is a general rule of thumb to use -65dBm as the cell boundary level[1]; however, some medical device service level agreements (SLAs) may dictate otherwise. It is important to overlap the coverage areas of each AP to avoid dead zones but not overlap too much because that can cause roaming problems. Also, it is very beneficial to use the same type of access points (APs) and equipment in the site survey that are planned to be deployed in the environment for the most accurate results. The power settings of the access points should almost always be adjusted to lower levels than the default; while lower power will shorten the coverage area, it will prevent interference with other APs that would result if the power level was too high[1]. Also, by limiting the coverage area inadvertent access attempts, such as from someone outside the hospital will likely be avoided.

There is an important set of tools required to actually determine the boundaries of each access point, identify the locations of the APs, and classify the settings of each APs. There are two basic types of access points to choose from, lightweight and autonomous. While lightweight access points are more expensive than autonomous

APs, they allow for centralized control with a WLAN controller and therefore minimize support and maintenance costs[8]. As previously mentioned, a spectrum analyzer is required along with a signal strength measurement device or application. Blueprints of the space are essential, as well as at least one access point (preferably two), a WLAN controller (since most APs are lightweight), 802.11 client cards to represent the devices, and different antenna types to determine which is best at various locations throughout the environment.

Yet another aspect of the WLAN design can often be determined in the site survey process. This component is frequency channel selection. Each frequency band is segmented into channels that are non-overlapping. For 802.11b and 802.11g, there are 25MHz between the center frequencies of channels to ensure that they are not overlapping, and for the 2.4GHz frequency band, channels 1, 6, and 11 are the ideal non-overlapping channels. When defining the access point channels, they should be spread so access points of the same channel are not next to each other to avoid co-channel interference. Figure 5 below gives a simplified depiction of this concept.

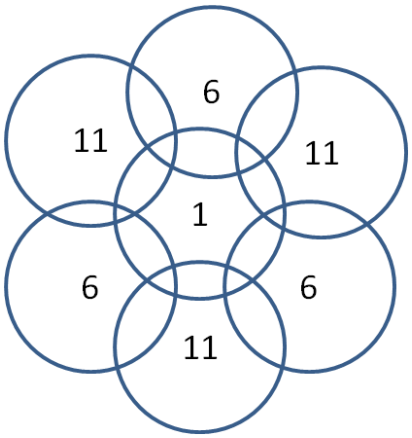

Figure 5. Access point coverage areas are shown with assigned frequency channels to avoid co-channel interference. This type of consideration should be made not only for each floor, but for each floor in reference to those above and below it.

1.4.0 Security

The security of any network is important, but the security of a hospital's wireless network containing mission critical patient data and potentially life critical patient monitoring information is of the utmost importance. In addition to the obvious criticality of the security of this information, there is the Health Insurance Portability and Accountability Act (HIPAA), which requires the protection of all patient information. There are security measures inherent within network characteristics, as well as additional security precautions that can be implemented on a network to ensure the protection of patient data.

1.4.1 Wireless Network Security Features

Depending on the wireless network type that is selected, the inherent security features may or may not provide acceptable levels of security. For example the first encryption mechanism used in legacy 802.11 wireless networks was called wired equivalent protection (WEP) and included confidentiality, access control, and data integrity. WEP encryption uses an RC4 cipher and static keys making it vulnerable in many ways[1]. This security mechanism is most definitely insufficient. Wi-Fi protected access (WPA) certification was the next to evolve which utilized TKIP encryption with RC4 cipher and dynamic keys. The significant improvement came when the 802.11i amendment became part of the 2007 standard, defining a robust security network (RSN) that incorporated authentication and authorization using an extensible authentication protocol (EAP), yielding WPA2 enterprise security. WPA2 uses CCMP encryption, AES cipher, and dynamic key generation[1]. Enterprise WPA2 is currently the best inherent security mechanism of a wireless network, and all wireless implementation should have this WPA2 security enabled. Also, note that there are different extensible authentication

protocols (EAP) that are used, some of which are vendor specific, like Cisco's Lightweight EAP (LEAP) and others that are based on standards such as Protected EAP (PEAP). EAPs are particularly important for wireless medical devices that do not have user interfaces to enter authentication information such as usernames and passwords; the bidirectional certificate based mechanisms are able to provide the proper authentication[9].

1.4.2 Wireless Network Vulnerabilities

It is the inherent nature of wireless networks, data being transmitted through open air, which make it so vulnerable to security threats. Two types of risk that exist are rogue access points, which can manifest from a variety of situations, and malicious attack. Rogue APs can appear from a nearby network, can be added accidently or intentionally within a network, or can even be introduced by visitors' electronic devices such as cell phones and video games. In regards to cell phones, some of today's "smart phones" have a "hotspot" feature that allows them to act like an access point and hence create a problem for the security of the hospital's network. Rogue access points must be monitored and hopefully eliminated as they can provide a gateway to a hospital's entire network for any intentional or accidental user. Malicious attacks are equally concerning. In general, wireless networks allow for anonymous hacking opportunities, and even with encryption and authentication, data in layers 1 and 2 is not protected. This provides an opportunity for denial of service (DoS) and "man-in-the-middle" attacks[10], as well as eavesdropping, peer-to-peer attacks, MAC spoofing, and wireless hijacking[1].

An additional security concern is that wireless medical devices often communicate with off-the-shelf software applications running on computers. There are inherent vulnerabilities in these programs through which worms and viruses could

potentially affect the medical device. There was a document issued by the FDA in 2005 that addresses this issue and attempts to give guidance on the topic[11]. Software vulnerabilities also present a related issue where software security patches that tend to be pushed out can have unforeseen consequences on medical devices.

1.4.3 Additional Protection Mechanisms

In addition to the inherent encryption and authentication protocols, wireless networks can be protected by intrusion detection systems (IDS) which monitor the activity on a wireless network and/or intrusion prevention systems (IPS) that attempt to mitigate the risks that may be presenting on the network. A wireless IDS (WIDS) usually consists of a server, management consoles, and sensors. The server is either a hardware or software based solution that serves as a central management point; management consoles are software based and connect back to the server. The sensors, which can either be hardware or software based, are placed in locations where they can observe wireless communications[1]. One basic security practice would be to use a wired network intrusion prevention system (IPS) at the point where the wireless network connects to the wired network. This could provide protection of a hospital's non-medical device data from wireless medical device traffic that may be more susceptible to security threats.

1.5.0 Risk Management

1.5.1 FDA

It is safe to say that risks should be mitigated for all networks, but again, the importance and criticality of mitigating risk on a hospital IT network with crucial patient information is even greater. A wireless network that is going to support life-critical

applications, for example physiological alarms, must be extremely reliable and should meet FDA verification and validation standards. It follows that the FDA, which regulates and approves medical devices, would be concerned with the network that a medical device is communicating over. The wireless network is not actually classified as a medical device, but when used with a medical device, it becomes a part of the medical device "system" and is therefore subject to FDA Good Manufacturing Practices. The FDA recommends that hospitals and both device and IT manufacturers should address wireless functional performance, wireless coexistence, wireless QoS, integrity of data transmitted wirelessly, security of data, and electromagnetic compliance[11]. It is well described by Baker and Hoglund: "A life-critical network is an enterprise-class network that has been verified to show that it operates as it was designed and validated for its intended uses, including the transmission of life-critical patient data[9]."

1.5.2 ANSI/AAMI/IEC 80001-1

Of recent importance in regards to risk is the recently approved ANSI/AAMI/IEC 80001-1, the application of risk management to IT networks incorporating medical devices. As a part of this project, there is a particular technical report draft offering guidance for wireless medical devices, 80001-2-x[12]. This document identifies eleven categories of risk that exist for systems that communicate wirelessly, some of which have already been discussed in this paper. The risks include the following: device level service level agreements (SLA), clinical use case and workflow, physical deployment location, spectrum allocation, spectrum management, network security, QoS, capacity management, verification testing, network and application management, and change control. In regards to change control, it is recommended that changes to the physical environment, hardware, software/firmware, and quantity of devices/application are taken

into account[12]. This list is very extensive and consideration of all of the potential risks presented is a considerable task.

Additional suggestions are also given on including wireless medical devices onto IT networks. One suggestion that has already been implied in this paper is segregating life-critical network traffic from general purpose IT traffic. The wireless technical report recommends categorizing medical devices by their performance characteristics, and designing the network to meet the most stringent needs. The document also describes the important performance characteristics that should be considered. These include: transceiver performance specification (e.g. receiver sensitivity, transmit power, minimum signal strength, minimum/maximum data rate, etc.), network delay (allowed latency per application), network jitter (the acceptable change in latency over time), packet loss (tolerance to lost packets), and bandwidth (how many packets and bytes per second are transmitted and/or received by the device)[12]. It is expected that an updated draft of this technical guidance document will be available in the near future.

1.6.0 Troubleshooting

Troubleshooting in the wireless environment can be particularly challenging due to the open air structure and radio frequency interference. In the case of wireless medical devices, troubleshooting is of the utmost importance.

1.6.1 Sources of Interference

1.6.1.1 Classifications of RF Interference

There are various types of RF interference that can cause either denial of service (DoS), corruption of frames, or excessive retransmissions and hence reduced throughput. One type of interference is narrowband interference in

which an RF signal interrupts a small, limited frequency and doesn't cause a complete denial of service but will result in disruption at that particular frequency. Wideband interference, on the other hand, has the potential to block an entire frequency band and therefore cause full DoS. There is also all-band interference that results from frequency hopping spread spectrum (FHSS) communication and causes corruption of frames. In order to eliminate these specific types of RF interference, the source must first be identified[1]. Other sources of interference include multipath which causes intersymbol interference, adjacent channel interference that results from poor channel design, and mismatched power settings of the client and access points causing them not to hear each other. When troubleshooting with a spectrum analyzer, a problem that might be discovered is retransmission of layer 2 packets. The discovery of these retransmissions would be an indication that one of the above listed issues is causing the problem with the wireless network.

1.6.1.2 Structural RF Limitations

Another factor that can cause wireless network issues is structural components of buildings, which can limit or prevent the transmission of RF signals[13]. This is of particular concern in the hospital environment where there tend to be varying construction materials, the most concerning of which is the lead shielded walls that surround some imaging rooms.

1.6.1.3 RF Interference with Medical Devices

An additional concern for the hospital environment is whether or not the RF transmitter in wireless devices will interfere with any medical devices. It is almost ironic that there has historically been concern about generic wireless

devices coexisting in an environment that also contained medical devices, and now the wireless devices under evaluation are medical devices themselves. Nevertheless, it is important that proper and sufficient testing be done to ensure that RF transmission from any wireless devices, even wireless medical devices, does not interfere with the proper function of other medical devices[14].

1.6.2 Spectrum Analyzer

A spectrum analyzer is a tool that can detect any radiofrequency signal in a particular frequency range that is being scanned. Spectrum analysis is likely the most essential troubleshooting tool for wireless environments. The type of spectrum analyzer can vary from a software solution with a network card and a laptop, to a physical spectrum analyzer tool, to sniffing radio cards placed throughout a wireless environment. The standalone spectrum analyzer or one built into a laptop can either be limited to a single frequency range or adjustable to fluctuate between different ranges, depending on its capabilities. Also, some spectrum analyzers can even classify the signal, such as identifying a Bluetooth device or microwave as the source of interference[1].

The other option for spectrum analysis can be described as sniffing radio cards and is referred to as a distributed spectrum analysis system (DSAS). Technically, this is analogous to a layer 1 wireless intrusion detection system (WIDS). These systems use a centralized server or WLAN controller to monitor the spectrum analyzer sensors that are placed throughout a given facility[1].

In addition to a spectrum analyzer, a protocol analyzers and Wi-Fi packet analyzers can also be used in wireless troubleshooting. A protocol analyzer is a tool that is used to decode packets being transmitted on a network[15].

1.6.3 Common Wireless Troubleshooting Scenarios

Although wireless troubleshooting can be complex and extensive, there are a few scenarios that are worth addressing specifically. One common problem is mismatched power settings between an access point and a client. The way to test for this particular problem requires the use of a protocol analyzer. If this problem exists, monitoring with the protocol analyzer will reveal that frames are not corrupted when you "listen" to the traffic near the client station, but are corrupted when "listening" near the access point[1].

Another wireless problem, referred to as hidden node, occurs when a client is able to communicate with the access point, but cannot be heard by all of the other clients in that basic service set (BSS). One of the principles of communication is that a client is supposed to listen to ensure that other clients are not transmitting so that it can have a clear channel for transmission. The hidden node results in a false perception of a clear channel and hence collisions result causing decreased throughput. A complaint of decreased throughput would be a clue to the network troubleshooter that there may be a hidden node. This could be verified and indentified through the use of a protocol analyzer. One would use the protocol analyzer to look for a particular MAC address with a higher level of retransmissions than the rest of the MAC addresses.

Likely, one of the most common issues that will occur in wireless is problems with roaming. Roaming however, is very difficult to troubleshoot. This is because when a client roams from one AP to the next, it is likely switching channels (assuming a proper channel reuse pattern was implemented in the design of a network). Therefore, a protocol analyzer would be needed for each channel in order to clearly identify the roaming problem[1]. Another challenge with roaming is that the roaming algorithms of clients are proprietary. The best way to prevent roaming issues is with a well designed wireless network infrastructure.

Finally, a troubleshooting scenario specific to the medical environment, is telemetry troubleshooting. For telemetry problems, there are three checks that most likely will be required but will be dependent on the telemetry vendor. The first utilizes is a simulator. Using a simulator on a telemetry box can verify that all of the leads are working or potentially identify a damaged lead. If nothing is identified with the simulator, there is software that can be used to identify if there are any internal errors in the particular telemetry box. Also, a spectrum analyzer can be used to determine if there is a gain problem with the device or any interference in the environment that might be interrupting the communication of the telemetry box[16].

1.7.0 Existing Wireless Medical Devices

There are many medical device types and other related hospital systems that are currently using wireless communication. Whether these devices/systems are deployed on hospital's enterprise wireless network or on a separate network exclusively for medical devices varies across different hospitals. Regardless, more and more devices are including the capability to transmit data wirelessly[14].

1.7.1 General Wireless Medical Devices

One example of a wireless medical device is SpO2 monitors that continuously monitor the patient and send the data wirelessly to a centralized monitoring station. Infusion pumps also have wireless capabilities, but the purpose is different; it is not for continuous monitoring of the infusion information, but rather for updating the drug library on smart pumps. Also, the "smart pumps" can receive the physicians' orders with electronic order entry and send the infusion information to the electronic medical record (EMR). ECG carts and ventilators are two additional medical devices that are entering into the wireless arena, and the list is growing rapidly.

In addition to medical devices, there are systems related to the delivery of medical care that utilize wireless. One of these is voice over Wi-Fi, VoWiFi, which is often used as a vital form of communication between clinicians on patient floors. Another is real time location systems (RTLS) that can be used to track assets. This has benefits for clinicians in need of high-volume equipment such as infusion pumps, as well as for the clinical engineering department who needs to locate equipment for routine maintenance. Yet another is what is commonly referred to as an alarm management system, allowing for wireless transmission of alarms to personal communication devices carried by clinicians such as cell phones or pagers.

1.7.2 WMTS Telemetry

One of the first wireless medical technologies in the hospital was telemetry, which is wireless monitoring of a patient's heart rhythm, or ECG. The telemetry system wirelessly transmits the patient data it is collecting to a central station for real time monitoring. However, unlike 802.11 wireless transmissions, telemetry algorithms do not traditionally involve two-way communication to provide confirmation that a packet is received; at most forward error correction (FEC) is used, which sends redundant data.

In 2000, the FCC allocated frequency bands exclusively for medical telemetry and termed it the Wireless Medical Telemetry System (WMTS) band. It was determined that the American Society for Healthcare Engineering (ASHE) would coordinate the WMTS band at that all transmitters must be registered[17]. While there are benefits to using the WMTS band for telemetry including custom architecture for simplified support and segregation from other wireless devices in the hospital, it is not totally isolated from interference, it falls within a smaller frequency band than ISM, and it results in increased infrastructure costs for an organization to have two separate networks[18].

	WMTS	ISM	UNII 1, 2, 2 ext , 3
Frequency	608-614 MHz, 1395-1400 MHz, 1427-1432 MHz	2400-2483 MHz	5150-5250MHz, 5250-2350MHz, 5470-5725MHz, and 5725-5825MHz
Total Bandwidth	16MHz	83 MHz	555 MHz
Protection	Licensed; Interference protection	Unlicensed; No interference protection	Unlicensed
Registration	Registration required	No registration	No registration
Frequency Coordination	Coordinated	Not coordinated	Dynamic Frequency Selection (DFS)
802.11	No	b/g/n	a/n

Table 1. Comparison of WMTS, ISM, and UNII frequency bands[19].

Therefore, a debate over telemetry exists as to whether or not the protected WMTS spectrum allows for sufficient successful transmission of life-critical patient data, and whether ISM 802.11 communication may yield better results. Despite the fact that the WMTS frequency spectrum is legally a "protected spectrum," it is impossible to completely protect from nearby RF emitters of from adjacent channel interference. Also, due to the limited bandwidth available in the WMTS band there is greater need for channel reuse and therefore greater challenges with providing telemetry coverage across multiple floors. The increased bandwidth of the ISM and UNII bands may allow for more successful transmission of telemetry data over 802.11b/g (ISM) or 802.11a/n (UNII).

1.7.3 802.11 Wireless Medical Device Systems

There are a few manufacturers that are currently leading the way in utilizing 802.11 wireless IT networks in the healthcare environment to deploy various patient monitoring systems: Masimo, Welch Allyn, and Draeger. It is very likely that other manufacturers and other device types will also have different wireless capabilities in the near future.

The Masimo Patient SafetyNet™ is a system for continuous monitoring of pulse oximetry. The system is targeted to general care floors where nurses are not constantly at the patient bedside and patients are not being continuously monitored by other vital signs monitoring equipment. Masimo's pulse oximetry devices are utilized and communicate either wired or wirelessly with RadNet™, a remote monitoring and notification system. The system, which requires a server, includes a computer based viewing station and the capability for alarms to be sent to nurses via a communication system (cell phones, pagers)[20].

Welch Allyn's FlexNet provides wireless vital signs monitoring using 5.0GHz, 802.11a IT networks. The system supports WPA2 Security and 802.11e quality of service with the patient monitoring data being given the highest priority[21]. Draeger also offers a non-WMTS telemetry solution with their Infinity M300. This system utilizes 802.11b/g technology to perform continuous monitoring, but should be implemented on a separate VLAN. While the Welch Allyn system has partnered with Aruba networks, Draeger's system is compatible with Cisco[22].

1.8.0 Alternative Wireless Technologies

In addition to 802.11 WLAN wireless medical devices, there are other technologies that are used and/or are being considered to enable wireless communication.

1.8.1 Distributed Antenna System (DAS)

A distributed antenna system (DAS) is a network of antennas connected by cabling and distributed spatially throughout a building to provide wireless coverage[15]. In a DAS deployment, the access points are centrally located and multiple antennas are connected to a single access point, both of which result in degradation of the network

properties[14]. Although DAS provides the benefit of combining and distributing Wi-Fi, cellular, paging and public safety communications, its high cost, required cooperation of cellular providers, and lack of standards make it a less than favorable solution for wireless coverage[23].

1.8.2 Bluetooth

Bluetooth is a technology that is widely used in communication, for example in wireless headsets or as the connection between a keyboard and a computer. Bluetooth communication takes place in the 2.4GHz ISM band and utilizes frequency hopping spread spectrum (FHSS) technology. Bluetooth is gaining attention in the healthcare industry for its use in personal area networks (PAN). It is believed that Bluetooth would be a good solution for non-life critical and often in-home patient monitoring such as measurement of blood pressure and blood glucose levels to name a few. The described advantages of utilizing Bluetooth for PANs is its large point of presence, the use of FHSS for spatial and interference robustness, PIN code mechanism for connection security, encryption capability for data security, and low-power fast-connection[24]. However, the existence of Bluetooth devices in a healthcare organization utilizing 802.11 WLAN has potential to cause interference.

2.0 Methods

2.1.0 Wireless Medical Device Implementation Process

With the changing trend in clinical workflow, there is an increasing need for wireless medical devices in the hospital. The shift in the field suggests that more and more medical devices will begin to utilize the IT network infrastructure in the hospital, particularly in regards to the wireless network. Due to the increased risk of operating

medical devices on the IT wireless network without isolation, there are multiple steps that are required to safely and effectively implement these types of devices. The entire process should include four steps: identification of RF spectrum usage in the deployment environment (presumably the hospital), classification and mitigation of risks through the ANSI/AAMI/IEC 80001 standard, development of a test environment within the hospital, and validation of the device performance by testing in the test environment. While focus has been placed on the RF spectrum management and recently on the risk assessment and mitigation via ANSI/AAMI/IEC 80001-1, there is substantial progress needed surrounding the development of a test lab and performance of testing within the hospital environment.

2.2.0 Creating a Test Lab

2.2.1 Selecting the Environment

In order to create a test lab, a location first must be selected. In order to select a location, the requirements for that space must be identified. In theory, an ideal wireless test environment would be shielded from all sources radio frequency (RF) interference. To achieve this goal, physical space and a substantial budget would be required. A standalone wireless network infrastructure would have to be developed in this shielded space to enable the connection and testing of any wireless medical devices. This type of test environment is impractical for clinical engineering use both due to resource constraints and the inadequacy for realistic simulation of the true deployment environment.

A more realistic and beneficial location to create the test lab would be a Clinical Engineering shop or a storage area in the basement of the hospital. The value of this

type of location would be that the physical space is relatively distant from clinical floors; thereby limiting the interference from the current patient care equipment as well as limiting the potential risk the device to be tested may pose to the clinical floor. It would also be advantageous to be in the hospital in order to utilize a segregated portion of the network infrastructure that is already in place. Also, although a test lab in this environment would not be totally isolated from sources of RF interference, it would allow for more practical test conditions as these sources of interference will exist on the clinical floors where the device will be deployed. In the current test lab design, the clinical engineering shop was selected to serve as the test lab.

2.2.2 Resources and Equipment

In order to connect and test wireless medical devices, a wireless network infrastructure is required. Depending on the system being tested, this will likely require both a wired and wireless network connection. For the wireless portion, access points (APs) will be required; however, these could be current hospital APs or could be added exclusively for the test lab. To run the WMDUT on existing APs would mean that the testing would be on the hospital's IT network. If different APs were installed, they could either be isolated with their own service set identifier (SSID) or by utilizing a different portion of the RF spectrum than the production APs. In the current design, two 5.0GHz, 802.11a access points were added. The 5.0GHz frequency was selected in order to segregate the testing traffic from the 2.4GHz 802.11b/g wireless coverage that existed in the physical space. A wireless local area network (WLAN) controller is helpful for managing the access points and therefore was put into place in the test network. There was also a wired side of the test network that linked to the backbone of the hospital's IT network infrastructure (see figure 6 below). The cost of each AP is about $450 and the cost of the wireless controller is about $6000, so the equipment for this test lab would

cost about $6900. However, this cost can be avoided if old network equipment can be obtained from the IT department as was the case in this experiment.

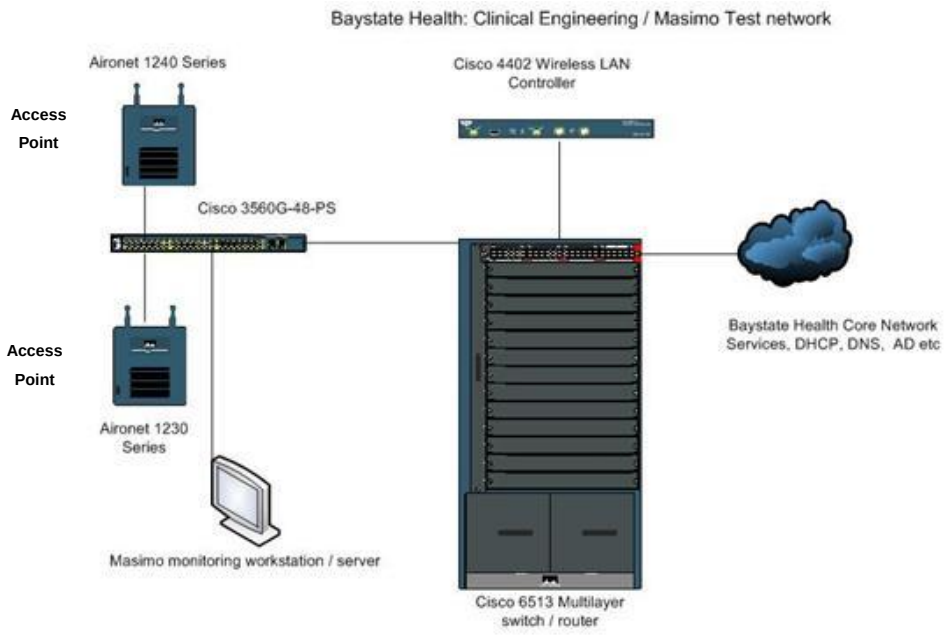

Figure 6. Network infrastructure of "CETest," the test lab network

In addition to the infrastructure, testing tools are essential for the functionality of the test lab. In order to analyze the RF characteristics of the test lab environment, as well as the wireless communication of a WMDUT on the network, a spectrum analyzer and a Wi-Fi analyzer are highly recommended. The level of complexity and cost of these tools can vary, but the benefits from even the simple systems are substantial. The spectrum analyzer measures all radio frequency signals within range of the antenna. Not all spectrum analyzers are able to scan all frequencies, so be sure to select one that covers at least the 2.4GHz and 5.0GHz spectrums. The Wi-Fi analyzer tool has multiple capabilities such as allowing for real time monitoring of wireless data traffic between devices and access points on a wireless network. AirMagnet Spectrum XT and Wi-Fi Analyzer Pro were utilized for testing in this study. These are both software application

with USB adapter antennas that were able to be used on a standard laptop computer. The total cost for the two applications, the two USB antennas, and 1-year warranty was $7600. It is assumed that the required laptop will already be available to the CE department.

Finally, in order to perform testing, a device of interest must be selected. In a practical situation, a device being considered by the hospital for purchase would be selected to be tested as a part of the pre-purchase evaluation. For this design project the wireless medical device under test (WMDUT), a system from Masimo Inc. was provided for experimental purposes, Masimo Patient SafetyNet and the Rad-87. This system consisted of a pulse oximetry device which continuously transmits data wirelessly to a central monitoring station. Assuming that the test device will be provided for testing free of charge, the total cost for the functional test lab is $14,500; however this is a one-time cost that will yield a test lab that can be used repeatedly.

2.3.0 Testing in the Test Lab

2.3.1 Spectrum Analysis

Initial work in the test lab was performed before the WMDUT was even connected. The purpose was to use the spectrum analyzer to measure the radio frequency signal of the access points and to identify any potential RF interference sources in the test space. The test network was a 5.0GHz 802.11a network, so spectrum analysis of the 5.0GHz channels was performed. Spectrum analysis of the 2.4GHz frequency range was also performed because many common wireless devices in the hospital utilize that frequency.

2.3.2 Connecting the WMDUT to the Test Network

The process of configuring and successfully connecting the desired WMDUT to the test network is in itself a test of the device's ability to work on a hospital's network. In order to achieve a successful connection, the device must be configured to comply with the hospital's security, authentication, and encryption standards. The desired connectivity standards for the hospital IT network where testing was performed were WPA2 enterprise security, AES encryption, and lightweight extensible authentication protocols (LEAP). The WMDUT was capable of meeting the requested security and encryption requirements, but was not capable of LEAP. A different protocol, protected EAP (PEAP) was able to work with the device and acceptable for the hospital's network with minor configuration changes. In addition to these configurations, the device was programmed to receive an IP address from the test network. Connection was ultimately achieved when data was transmitted from the device to the central monitoring station through the APs of the test network. A simulator was used in the pulse oximeter to generate data that could be viewed on the central monitor when the device was successfully connected (see Figure 7).

Figure 7. Masimo's pulse oximeter, the WMDUT, sending data wirelessly to the central station.

2.3.3 WMDUT Functionality Testing

2.3.3.1 Roaming

Upon successful connection of the device to the system through the "CETest" network access points, one of the first tests was to study how the device performed as it moved throughout the test space. Of interest were the boundaries of the coverage area and how and when the device changed its connection from one access point the other. The device and the computer with the Wi-Fi analyzer were placed on a cart and moved throughout the test lab (see Figure 8 below). With the Wi-Fi analyzer, the AP to which the device is connected could be monitored in real time.

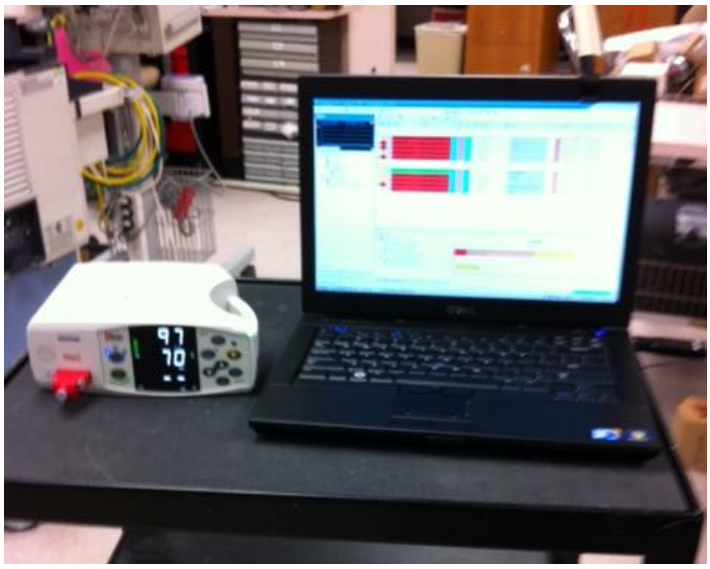

Figure 8. Mobile cart with WMDUT and test computer, used to test roaming and connectivity

Beyond monitoring which AP the device was connected to, additional tests were performed to evaluate roaming behavior. For example, the number of transmission control protocol (TCP) retries on the network was monitored as the

device moved from the range of one AP to the range of the other. Also, the delay time for the transfer of data between the device and the central station was measured when the device was located at the far edge of the coverage area, where the AP signal strength was reduced.

2.3.3.2 Effect of Bandwidth Utilization

In the test lab, the only device connected to the test network was the WMDUT. The behavior of the device with no competition for the network medium represents optimum performance conditions, but is very unrealistic compared to the conditions of a multiple device deployment on a production network that is heavily utilized. In order to try to simulate bandwidth usage with limited devices and resources, two computers were connected to the test network and large file transfers were made between the two computers over the test network medium. The network drive was mapped by IP address from one computer to the other, and a folder was then copied to the computer with the mapped connection. The folder being transferred was approximately 2.5GB and the speed of the network was 6Mbps. The file size was large enough so that the transfer would take enough time to perform testing, and the speed was limited by the AP configuration as per the hospital policy and. Under these conditions, the Wi-Fi analyzer was used to measure the number of retries for packets being sent to the APs and to monitor roaming behavior of the WMDUT.

In addition, the effect of bandwidth utilization was studied by measuring the delay time of information being sent from the device to the central station. Because the pulse oximetry simulator probe only generated constant values, it was difficult to detect if there was any delay in the transmittance of the data. The simulator probe was removed from the device and the time until the signal no

longer appeared on the central station was measured. The goal was to use the time to estimate the delay and compare it under normal conditions and during bandwidth utilization.

A second method used to simulate network utilization was to create additional SSIDs on the network with the wireless controller. Both test access points were assigned to the same channel, and 16 SSIDs were created on each AP. The additional SSIDs greatly increased the number of management frames being sent over the network, thereby driving up utilization. Network utilization, the ratio of current network traffic to the maximum traffic the network can handle, was driven up to 50-60% using this method. The average utilization of a hospital IT network should be about 10%, but heavy bursts of traffic can yield periodic higher utilization. Under these utilization conditions, a voice over IP (VoIP) phone on the 5.0GHz network in the test lab was unable to make outgoing calls.

2.3.3.3 Additional Tests

Another condition that was tested was co-channel interference. This condition was created by setting both access points to the same channel within the frequency band, and placing them close to each other in physical proximity. Roaming and delay tests were performed in an attempt to identify any consequences of this type of interference. Also in the co-channel interference scenario, the power settings on the APs were reduced and the impact on the device's connection speed was measured.

In addition to the spectrum analysis that was performed before connection of the WMDUT, spectrum analysis was used when the device was connected. The connected device was placed in proximity of other, non-wireless

medical devices. Spectrum analysis was used to determine whether or not there was any interference from the surrounding devices.

3.0 Results

3.1.0 Radio Frequency Spectrum Analysis

Spectrum analysis of the 5.0GHz spectrum was performed at the primary test bench in the test lab before any devices were connected. Results shown in Figure 9 below indicate no major sources of interference, which would be identified by irregular peaks in the power graph. The two APs of CETest at channels 149 and 161 can clearly be seen. Also, there is an additional access points that appears with less signal strength, and likely is located on another floor in the hospital. Both spectrum density and real-time FFT data are shown in the figure.

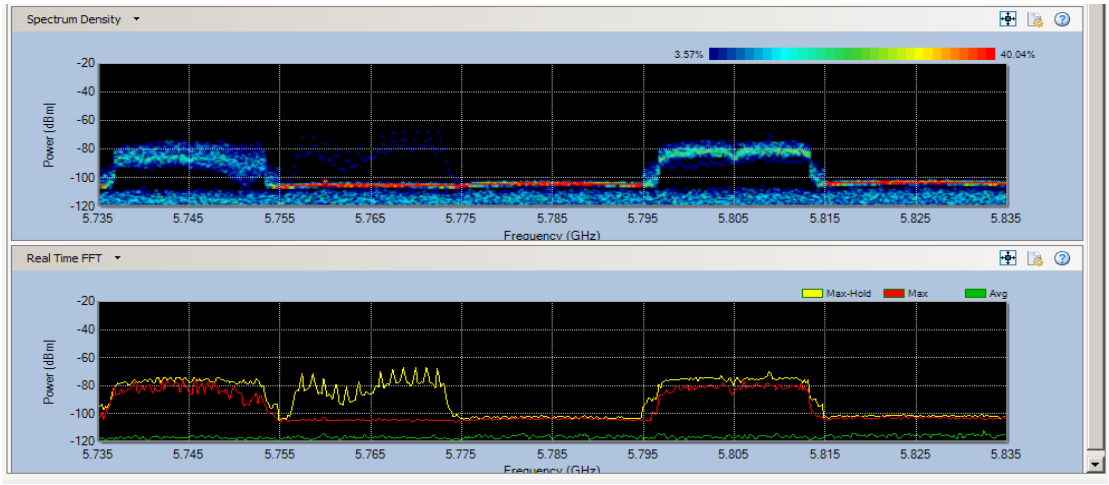

Figure 9. 5.0GHz spectrum analysis of test lab before WMDUT connection.

In order to study the RF interference of surrounding medical devices, a suction pump, a syringe pump, and a sequential compression device were run in close physical proximity to the WMDUT. Spectrum analysis was performed to determine if there was

any effect of these devices on the RF environment and hence on the WMDUT. Figures 10 and 11 show spectrum analysis data of the 5.0GHz range and the 2.4GHz range, respectively, with the medical devices running nearby. The RF interference generated by these devices is seen in the 2.4GHz range, and therefore there was no impact on the WMDUT which was deployed in the 5.0GHz frequency range. However, these results support the general understanding that there is potential for interference in the commonly used 2.4GHz range from the use of many motorized, RF emitting medical devices in the vicinity.

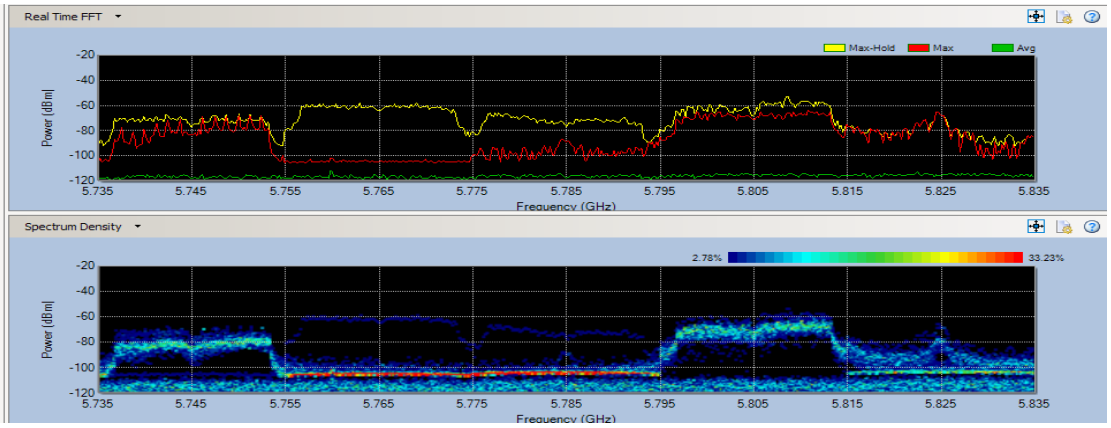

Figure 10. 5.0GHz spectrum data with WMDUT connected and medical devices running in the vicinity.

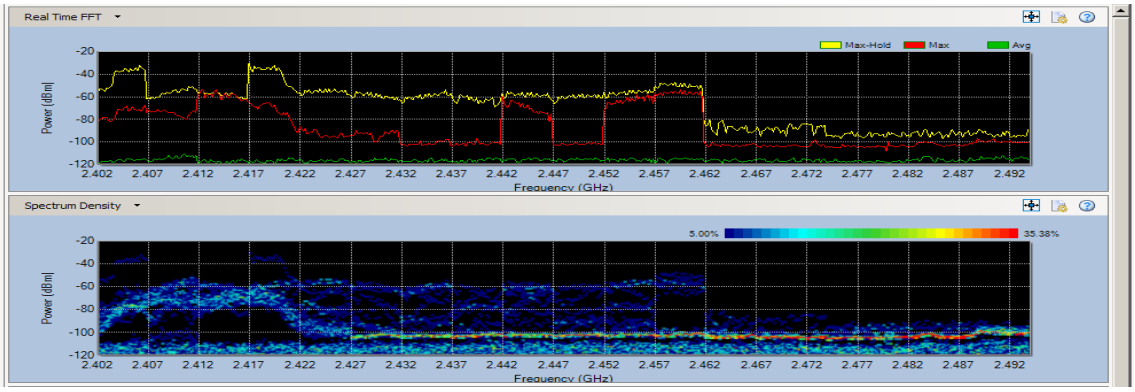

Figure 11. 2.4GHz spectrum analysis showing some interference from nearby medical devices.

Although it would not impact this particular testing scenario which utilized the 5.0GHz spectrum, the spectrum analyzer was used to show the interference from Bluetooth and microwave ovens in the 2.4GHz spectrum, the frequency range on which the majority of wireless devices (medical and non-medical) communicate. Figure 12 and figure 13 show the real time FFT, spectrum density, and spectrogram data captured with the spectrum analyzer during the use of a microwave and a Bluetooth phone respectively. The yellow, orange and red on the spectrogram represent the interference.

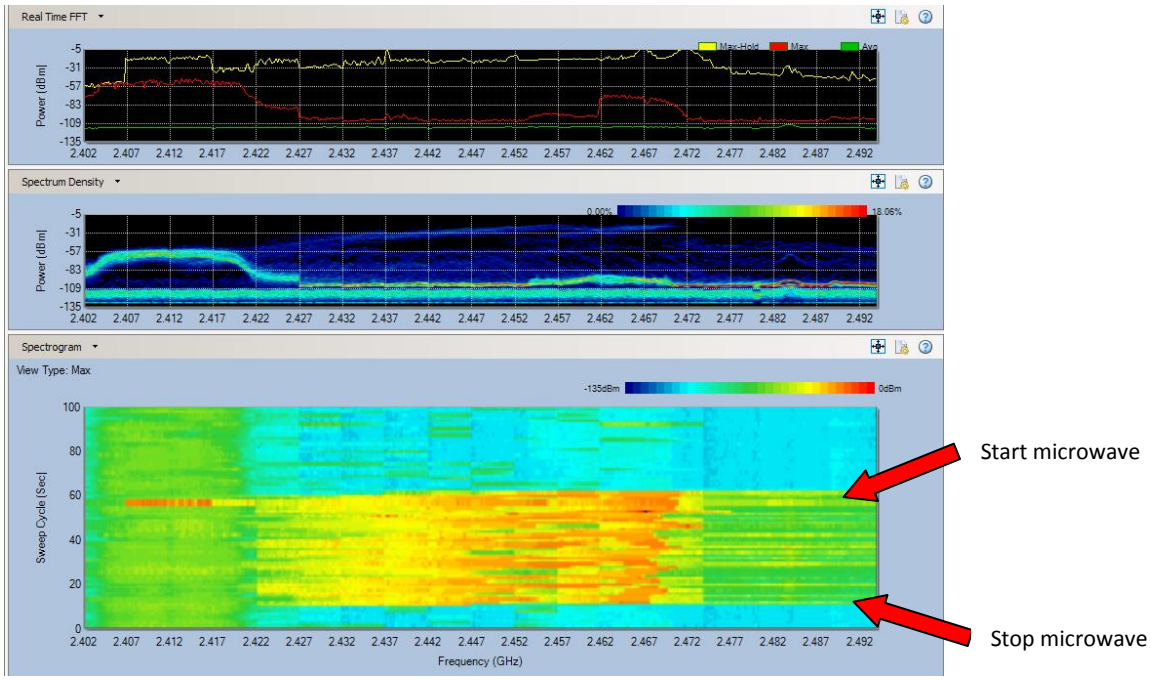

Figure 12. Spectrum analysis graphical data is shown for microwave oven interference in the 2.4GHz spectrum.

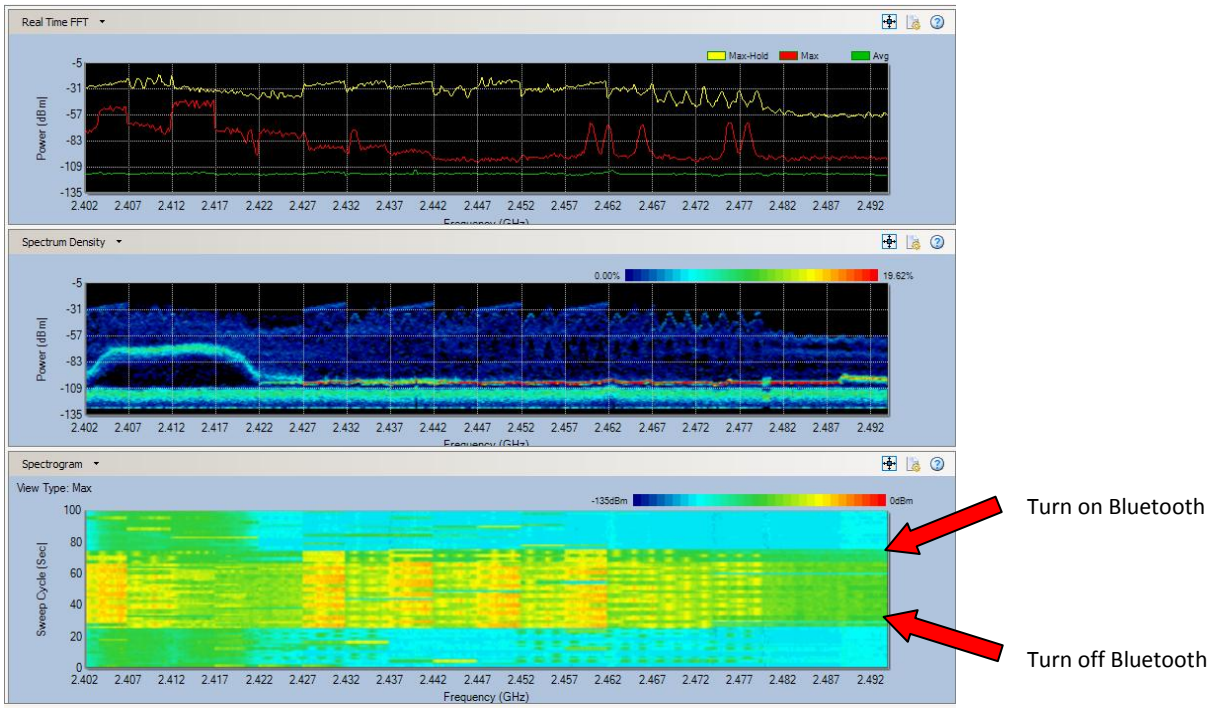

Figure 13. Spectrum analysis data showing interference from Bluetooth capable phones in the 2.4GHz range.

3.2.0 Roaming Behavior Analysis

Analysis of roaming behavior is difficult to capture quantitatively. Roaming algorithms are proprietary and vary greatly from device to device. In the analysis of roaming, it was expected that the device would be able to transfer from one AP to the next without losing connection with the wireless test network, but that the device wouldn't roam too quickly when it was unnecessary. The dashboard of the Wi-Fi Analyzer shown in Figure 14 below was used to identify which access point the WMDUT was connected to at any given time and when it switched. Testing showed that the device would remain connected to the initial connection AP even as it moved within range of the second AP, and would only switch over when the signal strength of the initial AP was significantly reduced.

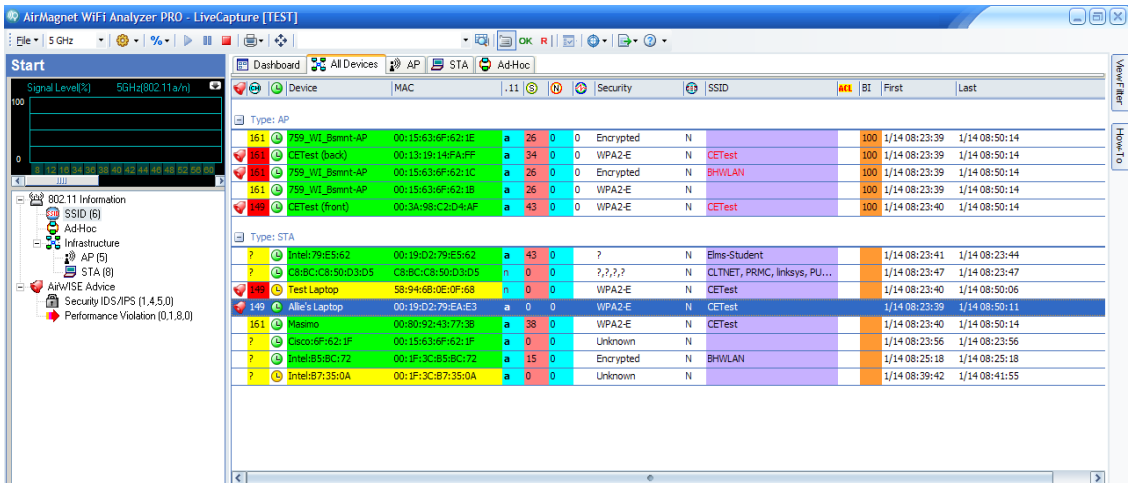

Figure 14. Dashboard view within Air Magnet Wi-Fi Analyzer showing access points, stations, and connection information.

A quantitative change that resulted was the increase in receiving and transmitting retry percentage during roaming. The *Infrastructure* feature of Wi-Fi Analyzer allowed real time measurement of this parameter. Figure 15 shows the data collected while moving the device that was originally stationary in proximity of the first AP and slowly walking from the center of that range to the opposite end of the test lab, where the connection eventually changed to the second AP, thereby successfully roaming. An increase and then decrease in retries was seen during this transition as indicated by the arrows in Figure 15 below. Note that the numerical values shown were real-time, so they are 0 because by the end of data collection, the device is connected to the new AP so the retries have ceased.

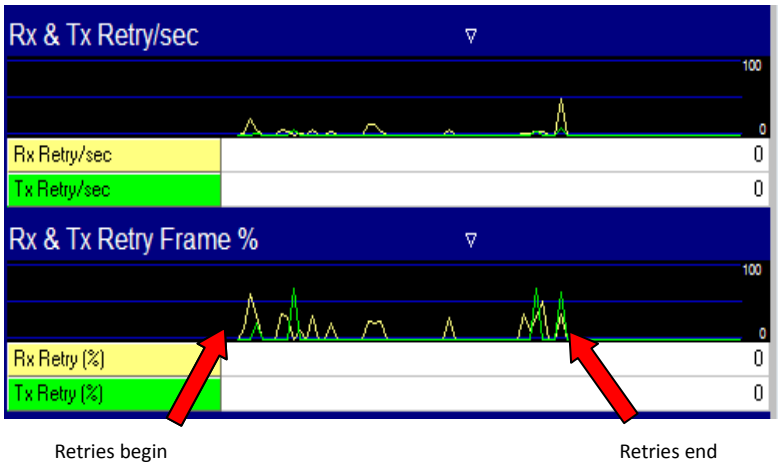

Figure 15. Increased transmit and receive retries during roaming.

Another test of roaming was simulated by connecting the WMDUT as well as two computers to the same access point. A large file transfer was carried out between the two computers and the Wi-Fi traffic was monitored. During this test, the device was located in the test lab around the cusp of coverage between the two access points. With the increased utilization from the file transfer, there was an increased number of retries for the network traffic, but the device did not lose connection from the network, nor did it roam to the other access point.

3.3.0 Bandwidth Utilization and Delay

Bandwidth utilization was increased by two methods in the test lab: file transfers over the test network and increased management frame traffic from the addition of SSIDs. The Wi-Fi Analyzer was utilized to capture the signal strength, retry frames, and control, management, and frames with CRC (cyclic redundancy check) errors for the AP channel (161) under normal conditions and during a large file transfer. The data for normal conditions is shown in Figure 16 and during the file transfer in Figure 17. Note that the y-axis scales change for retry frames from 150 to 5,000 and for management

frames from 100 to 3,000. This data shows increases in each of the three parameters collected during the file transfer; however the device remained connected during this increase. Also, the use of additional SSIDs to significantly increase management frames being transmitted over the network drove the utilization even higher; still the WMDUT remained connected to the network.

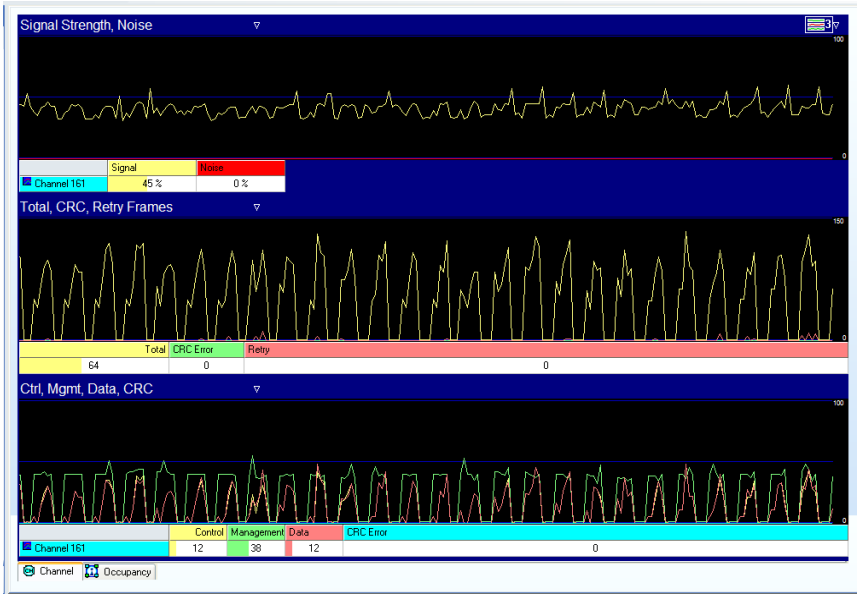

Figure 16. AP channel data during normal conditions.

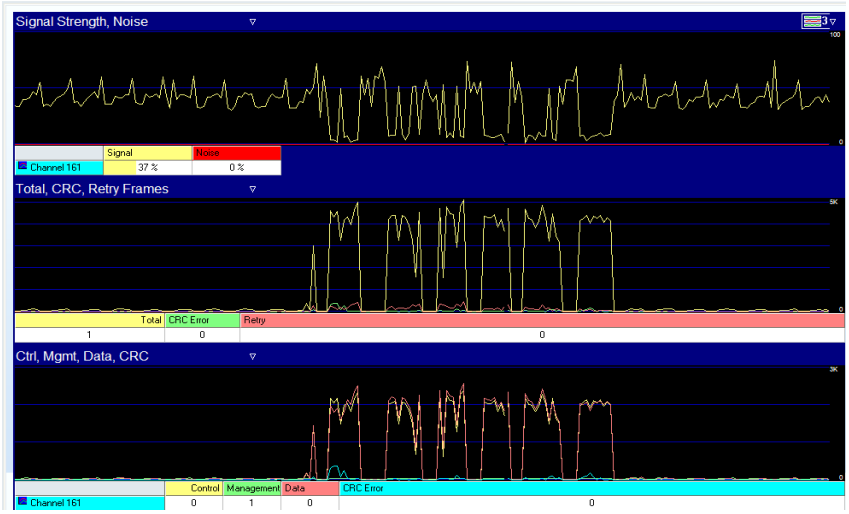

Figure 17. AP channel data during network utilization from a large file transfer.

The delay of the transmittal of data from the WMDUT to the central station was difficult to measure. With the current design and tools, a very simple approach was taken; the time it took the central station to receive the data from the WMDUT following insertion of the simulator probe was measured. This data is somewhat imprecise due to experimental error, but the same measurement procedure was performed for both test conditions with the same experimenter. Statistical analysis was performed with SPSS statistical software to determine if there was any significant difference in delay time under normal network conditions as compared to network conditions during a file transfer. Specifically, a Wilcoxon test was used and the results indicated a significant difference, $z = -2.49$, $p = .013$. The mean delay time, measured in seconds, for normal conditions was 1.3725±0.30549 and during the file transfer was 1.5675±0.36961 (see appendix C).

3.4.0 Other Results

After placing the two test APs in close physical proximity and using the wireless controller to set them to the same channel, the device was turned on to confirm the ability to connect and check for any performance issues. In this simplified, simulated scenario, there were no noticeable effects of co-channel interference on the WMDUT.

The wireless controller was then used to set one of the access points to channel 100, which is a channel in the UNII 2 extended band. The device was able to successfully connect to the AP at channel 100 as shown by the Wi-Fi analyzer, thereby confirming the device's ability to function in that frequency band.

Finally, the power settings of the access points were modified to be much lower. This was done to demonstrate that low power communication results in lower data rates for packet transmission across the test network. The data rates could also be monitored

with the AirMagnet Wi-Fi analyzer and, with the reduced power on the APs, dropped down to the lowest data rate of 6 Mbps.

4.0 Discussion

The current exercise included development of a wireless test lab and performance of meaningful tests on wireless medical devices, while exploring the challenges and successes of the process. The first and most important lesson is to understand and appreciate the necessity of testing wireless medical devices before they are deployed in for clinical use. Both the effects of the IT network on the device's performance and the effect of the device on the network and patient care environment are of concern. Basic testing in a test lab can address these concerns and allow for other components of the wireless device behavior to be explored. Due to potential overcrowding of a hospital's wireless network, the reason for a device to utilize wireless technology should be closely scrutinized before a decision is made. However there are cases where the benefits of wireless technology and mobility will provide value to clinical practice and workflow.

In order to effectively and safely deploy wireless medical device systems, thorough risk assessment is required. In order to do a complete risk assessment, testing and verification of the potential risks is required; this is another reason for utilization of the test lab. Depending on the resources, tools, and skill sets of individuals within the clinical engineering department, the extent of testing can vary and certainly be more extensive than tests that were performed in this exercise.

The design of the test lab is the first consideration in the process, and the selection of the location in essential. There are three general options that could be considered: a completely isolated environment, a somewhat isolated environment with simulated conditions, or a clinical environment with the hospital IT network. While pros

and cons can be identified for each of these choices, the somewhat isolated environment with simulated conditions is the most practical solution. The completely isolated environment would require high cost to achieve RF isolation and the installation of a wireless network infrastructure from scratch. It would most likely not be located in the hospital, which would make it inconvenient for clinical engineers and therefore would not truly resemble the network conditions of the hospital IT network in the clinical environment. On the other hand, to deploy the device directly in the clinical environment would be too risky. It would defeat the purpose of the testing which is to determine any possible issues the device might have and to prevent any negative effects it could have on the hospital IT network or any other medical devices. With these considerations, the simulated test lab appears to be the most logical solution. It is reasonable to find a space in the hospital that is not in close physical proximity to a clinical area, which reduces the risk of electromagnetic interference. Also, the network traffic can be isolated by utilizing a different frequency or by creating unique SSIDs for the test network.

The selection of the network infrastructure and frequency to be used for testing is also worthy of discussion. In the current study, 5.0GHz frequency range was used in order to isolate the test network traffic from the hospital IT network traffic because there was previously only 2.4GHz coverage in the test space. It was also selected because the tentative plan for the hospital would be to deploy wireless medical devices on the existing 5.0GHz network rather than on the overcrowded 2.4GHz network. However, the 5.0GHz test network posed some limitations, the first of which is that not all wireless medical devices are 802.11a capable (5.0GHz communication). Therefore, the 5.0GHz test environment is only recommended if the hospital intends to deploy the device on a 5.0GHz 802.11a network infrastructure. Due to the commonality of 2.4GHz networks in hospitals, a 2.4GHz test network would likely yield more practical and beneficial test

scenarios. SSIDs and virtual local area networks (VLANs) are required to segregate test traffic if the test network is on the same frequency is the production network; this will prevent testing from being able to negatively impact other devices on the hospital IT network. Also, the 2.4GHz spectrum is where the most other non-medical wireless devices communicate, and as such would allow for a better representation of the type of network traffic and potential interference that would exist in the production environment.

The tests that can be performed in the lab vary based on the type of wireless medical device, the tools available, and the skill sets of the individual working within the clinical engineering department. The availability of multiple of units of the same device type would allow for better evaluation of the device system. Also, the availability of multiple wireless medical device types that could be configured to run in the test lab at the same time would allow for the analysis of the devices' influence on each other. The level of the clinical engineering department's information technology (IT) skills and/or collaboration with the IT department will greatly expand or limit the network configuration and testing possibilities. The collaboration and assistance from the IT department, particularly the wireless network architect, was essential to the success of the trial and the types of network conditions that were able to be simulated.

In order to make wireless medical device testing a standard part of pre-purchase evaluation and risk management, there needs to be support from clinical engineering and hospital management. The case should be made to design a test lab as a standard practice of all clinical engineering departments and to have it available for wireless testing during pre-purchase evaluation. The test lab can also be utilized for troubleshooting and training purposes. In addition to these benefits, the new ANSI/AAMI/IEC 80001-1 standard for risk management can be used as justification for this request. Hospitals will not be successful in implementing pre-purchase wireless testing unless manufacturers of wireless medical devices recognize the need for and

benefit of in-house wireless testing by hospitals looking to purchase their devices. Configuration will likely be required to get any system to meet the specifications of a given wireless network and successfully connect, and therefore cooperation and assistance from the manufacturers to provide the devices and help with configuration is an essential part of the process.

5.0 Conclusion

There is currently a great shift in medical technology and clinical workflow practices that is producing a greater need for wireless technology in the hospital. The radio frequency spectrum, however, is not an unlimited medium, and therefore there are challenges and risks associated with this increase in utilization. The increasing presence of wireless medical devices in the hospital creates new challenges. First, there is the technical challenge of connecting the device and enabling it to function properly in an RF environment that is already overcrowded. Secondly, there are risks associated with using the wireless medium to transmit critical patient data. The network must be secure and reliable, and there must be back-up methods for communicating the information if the wireless network connection is lost. For both of these reasons, a test lab for clinical engineers would be an extremely valuable tool. With the expectation that the use of wireless medical devices will continue to expand, a large amount of focus is going to be placed on wireless technologies and testing in the coming years.

The technical and design component of this project was to develop a wireless test lab within practical constraints and resources, and demonstrate the utilization of the test lab to perform wireless testing on actual wireless medical devices. The motivation behind the testing is to determine if the device can connect to the hospital's network and if it could safely and effectively meet the needs of the hospital while performing to its specifications. However, the ultimate goal of this work was not just to design a one-time

use test lab, but to demonstrate proof-of-concept to the clinical engineering community. This case study has proven that for relatively low cost (under $15,000) and with minimal resource requirements, a test lab can be developed to become a vital component of the clinical engineering department's tool set.

6.0 Appendices

A. Publication

A presentation on related topics has been accepted and will be presented at the 2011 AAMI Conference and Expo on June 27th. Also, an introductory report based on this material has been submitted to AAMI BI&T for publication.

B. Equipment

Access points: (2) Cisco Aeronet 1240

WLAN controller: Cisco WLC 4402-12

AirMagnet WiFi Analyzer Pro - http://www.airmagnet.com/products/wifi_analyzer/

AirMagnet Spectrum XT - http://www.airmagnet.com/products/spectrum_xt/

Computer (for running AirMagnet products): Dell Latitude E6410

WMDUT:

- Masimo Patient Safety Net - http://www.masimo.com/generalFloor/system.htm
- Masimo Rad-87 - http://www.masimo.com/rainbow/Rad87.htm

C. Statistical Analysis

SPSS Statistics 17.0 was used to perform statistical analysis.

Results from the Wilcoxon test comparing connection delay for normal network conditions and for a file transfer are as follows:

Descriptive Statistics

	N	Mean	Std. Deviation	Minimum	Maximum
Normal	40	1.3725	.30549	.70	2.10
FileTx	40	1.5675	.36961	.90	2.60

Wilcoxon Signed Ranks Test

Ranks

		N	Mean Rank	Sum of Ranks
FileTx - Normal	Negative Ranks	11[a]	17.00	187.00
	Positive Ranks	26[b]	19.85	516.00
	Ties	3[c]		
	Total	40		

a. FileTx < Normal

b. FileTx > Normal

c. FileTx = Normal

Test Statistics[b]

	FileTx - Normal
Z	-2.490[a]
Asymp. Sig. (2-tailed)	.013

a. Based on negative ranks.

b. Wilcoxon Signed Ranks Test

7.0 References

[1] Coleman, David D. and David A. Westcott. *Certified Wireless Network Administrator Official Study Guide*. CWNP. Indianapolis: Wiley Publishing Inc., 2009.

[2] www.Cisco.com

[3] www.CaduceusWireless.com

[4] www.networkworld.com

[5] Meyers, Mike. *CompTIA Network+ All-in-One Exam Guide.* 4th ed. New York: McGraw-Hill, 2009.

[6] "Wi-Fi CERTIFIED™ for WMM™ - Support for Multimedia Applications with Quality of Service in Wi-Fi® Networks." *Wi-Fi Alliance* September 2004.

[7] Phifer, Lisa. "Using VLANs to compartmentalize WLAN traffic." *Search Networking.* 10 Apr 2006. Web. 16 July 2010. < http://searchnetworking.techtarget.com/generic/0,295582,sid7_gci1168965,00.html>

[8] "Wireless Networking Standards." *Classroom Connections 2010 Education Initiative.* Cisco Systems.

[9] Baker, Steve D. and David H. Hoglund. "Medical-Grade, Mission-Critical Wireless Networks." *IEEE* Engineering in Medicine and Biology Magazine March/April 2008: pp 89-95.

[10] "Wireless LAN Security for Healthcare and HIPAA Compliance." *Motorola White Paper*.

[11] "Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software." *Food and Drug Administration* January 2005.

[12] "Application of risk management for IT-networks incorporating MEDICAL DEVICES – Part 2-x: Guidance for wireless networks." *IEC 80001 committee* Preliminary Draft February 2007.

[13] Gibbs, Mike and Howard Quillen. "The Medical-Grade Network: Helping Transform Healthcare." Cisco IBSG 2007.

[14] "Wireless Considerations in Healthcare Environments." *Cisco Systems Inc* Version 1.0 May 2008.

[15] Barrett, Joel and Vinay Saini. *Dictionary of Wireless Terms and Acronyms*. CWNP. Brainslap Productions and CWNP Inc., 2009.

[16] Philip Levine. Personal Interview. 9 Jul 2010.

[17] Sundaresan, Namrata. "Wireless Medical Telemetry Service: Paradigm Shift Under Way." *Frost & Sullivan* 25 July 2005. <http://www.frost.com/prod/servlet/market-insight-top.pag?docid=43502991>

[18] Putnam, Eileen. “Stiffer Pressure to Move to WMTS Bands: Hospitals Face Higher Telemetry EMI Risks in 2006.” *FDA MedSun.* Web 8 August 2010.

[19] “Why WMTS.” *ASHE* Web. 8 August 2010 <www.ashe.org/resources/WMTS>

[20] “Improved outcomes and reduced costs with continuous monitoring of post-surgical patients on the general care floor.” Masimo White Paper.

[21] “Introducing Welch Allyn FlexNet™ for 802.11a life-critical wireless networks.” *Welch Allyn White Paper.*

[22] “Dräger Patient Monitoring Deployment in the Cisco Unified Wireless Network Infrastructure.” *Cisco* Deployment Guide.

[23] Chretien, Wendy. “Distributed Antenna Systems.” *Campustechnologies.com*, 1 Nov 2007.

[24] Baisa, Noel. “Designing wireless interfaces for patient monitoring equipment.” <*www.rfdesign.com*> April 2005.