The Impact of Next Gen Wi-Fi Technology on Healthcare

Ruckus Wireless | White Paper

Lowering infrastructure costs while improving performance and reliability. Is it possible?

Introduction

The mobile healthcare delivery model of 2010 and beyond demands critical business and clinical application performance. These demands place unique requirements on current wireless LAN (WLAN) systems for the healthcare market. Recent innovations in 802.11 technology can have a profound impact on improving healthcare mobile application performance and lower the total cost of ownership.

Life Critical Application Requirements

Life critical application performance has become an absolute requirement for the healthcare marketplace. A dropped call during a code-blue response or an alert/alarm not being received by a caregiver can impede workflow and result in negative outcomes or sentinel events. WLAN requirements for 2010 are vastly different than the requirement of 2008 or even 2009. So what are the requirements that will demand that this medium perform to the utmost?

WLAN deployments in hospitals are not just confined to one department or several departments. They are becoming ubiquitous within the hospital and across the Integrated Delivery Network (IDN). These application requirements have evolved beyond laptops on carts for the electronic medical record to voice over IP communication and other priority medical applications. These unique medical applications include the deployment of hundreds of wireless "smart infusion pumps" and "wireless enabled" patient monitors that traverse not just the step down unit, or single department, but provide "wireless transport patient monitoring anywhere in the hospital."

In addition, as standards and technologies evolve to enable the required QoS, there is a rapid evolution that is occurring as many

Data Rate Characteristics Per Application

Application	Packets (per sec)	kb/ packet	Peak (kb/s)	Average (kb/s)	Events/hr or Duty Cyle	Latency (max, ms)
Voice	28	3.1	86	86	Stream	.50
Telemetry	5	2.6	12.8	12.8	Stream	200
- *Diagnostic*	5	5.1	25.6	25.6	Stream	200
- *Alarms*	5	1.0	5.1	0.1	10/hr	
Clinician notifier	5	2.6	12.8	0.1	20/hr	200
BCMA	2	0.4	0.8	0.1	30/hr	500
Guest access	100	10	1,000	30	3%	1,000
EMR images	200	20.5	4,100	41	1%	200
- *Numerics*	4	12.3	49.2	0.1	40/hr	200
E-mail	200	20.5	4,100	41	1%	200
Infusion pump						
- *Status*	1	1.0	1	1	Continuous	200
- *Alert*	1	1.0	1	0.1	1/hr	200

Source: *IEEE Engineering in Medicine and Biology Magazine, March/April 2008, Medical-Grade, Mission-Critical Wireless Networks by Steven D. Baker and David H. Hoglund*

of the leading patient monitoring companies are offering 802.11a/b/g, "patient worn" telemetry to enable "housewide" enterprise monitoring over their existing wireless network.

This is also converging on the WLAN. Just like the growth of "wireless enabled" infusion pumps - from 10s to 100's of devices, the same is occurring with patient monitoring. Sometimes 150 or more 802.11a/b/g patient worn monitors can be anywhere within a hospital at any given time. The hospital enterprise of today, and tomorrow, will literally have hundreds and hundreds of data, voice, and wireless enabled medical applications and devices running over a shared network.

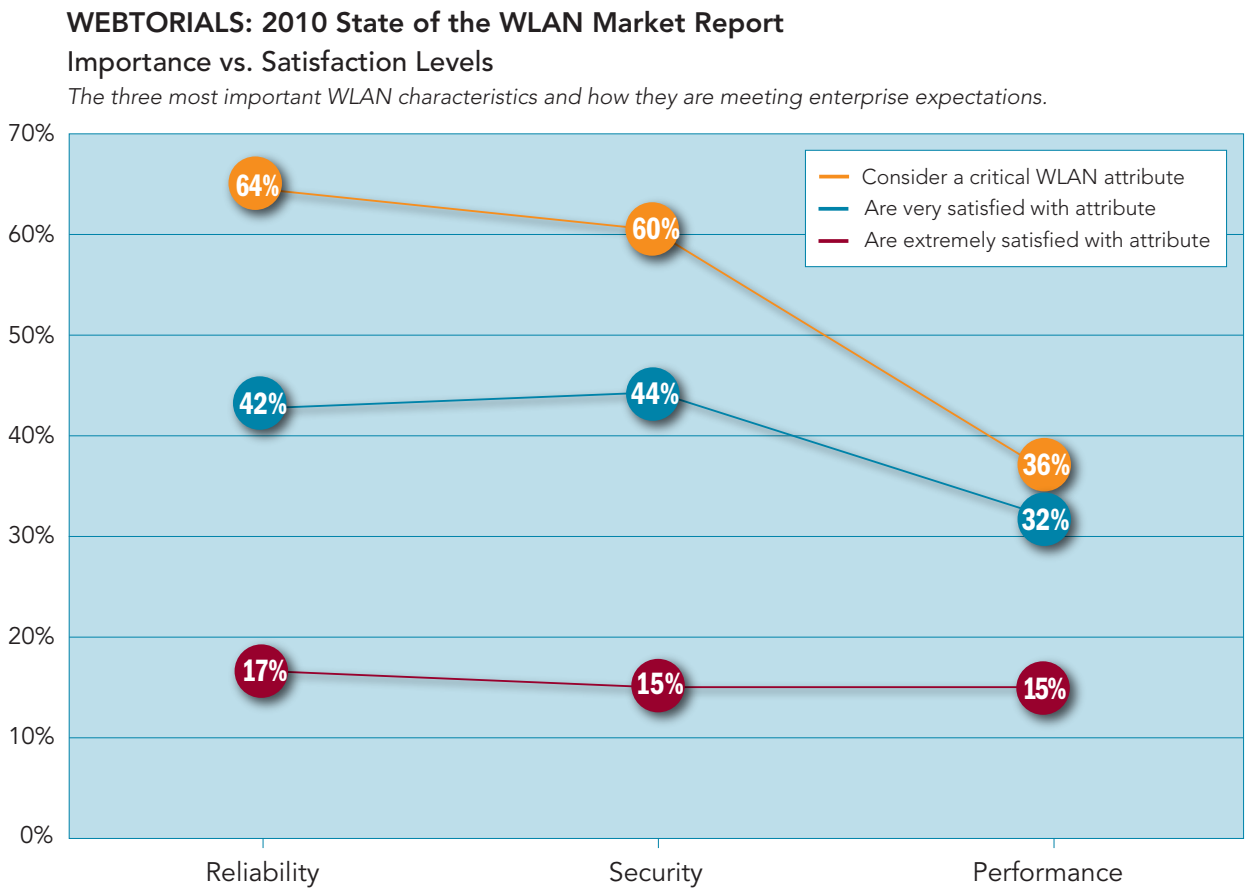
Life-critical applications that that transmit alarms, patient vital signs and waveform data; as well as the upload of drug libraries and the down load log files on the fly – require a wireless network with the same reliability and quality of service essential for latency-sensitive voice over IP applications.

Simply put, within the healthcare market, today's WLAN just cannot tolerate flaky network connections that incur packet loss, delays, and jitter, that often result in dropped voice calls, or worse yet a dropped waveform transmission from a patient monitor or patient worn monitor to a central station.

The WLAN must also now deal with the increased use of Wi-Fi enabled "smart phones" and smart phone applications like those found on the Apple iPhone — that shift traffic from the GSM network to the Wi-Fi network.

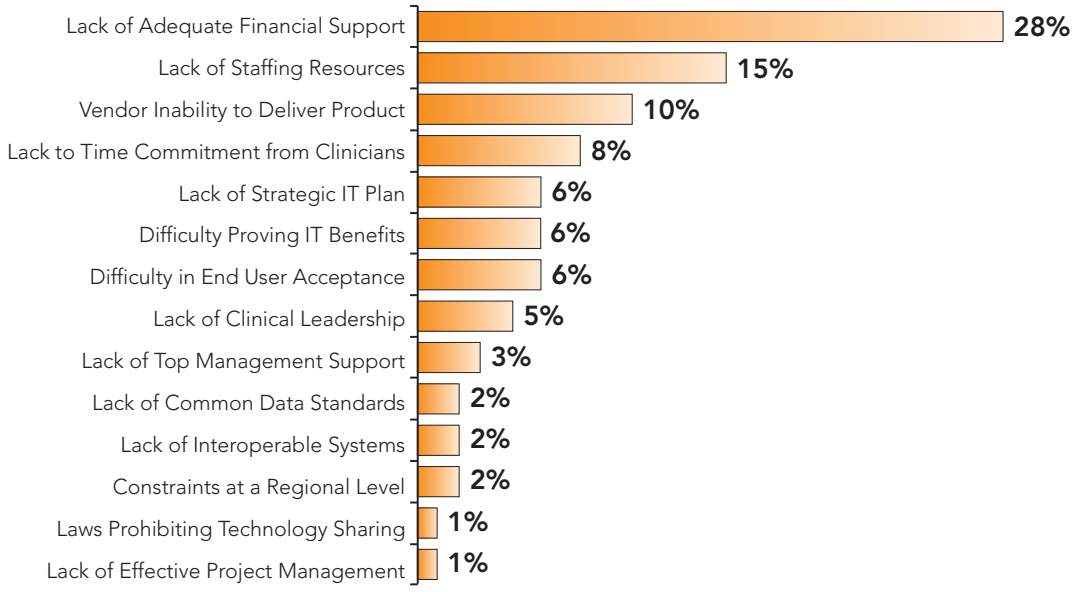
A recent 2010 WLAN report conducted by Webtorials (*see Figure 1*), identified the three most important WLAN characteristics, reliability, security and performance, and how they are meeting enterprise expectations. When it comes to wireless, these are the same three critical issues facing the healthcare market.

FIGURE 1: 2010 State of the WLAN Market Report: Importance vs. Satisfaction Levels



Ruckus WIRELESS

FIGURE 2: Most significant barriers to implementing wireless within healthcare



Source: HIMMS Leadership Survey, Healthcare CIO Final Report, 2009

WLAN Cost Pressures within Healthcare

The pressure on technology offerings in the healthcare market today, perhaps more so than in any other, is the requirement to deliver ultra-reliable performance 24 x 7 x 365.

Additionally, given the weak state of the economy, IT personnel are feeling increased pressure to show a solid and provable ROI for their technology expenditures. Compounding these problems is that the vast majority of IT departments generally do not have the resources to design and install, let alone manage new technology deployments — particularly with regard to the WLAN and latency sensitive applications such as voice over IP and medical Wi-Fi enabled devices, requiring uninterrupted connectivity. Often, there is a reliance upon third party integrators and there are costs involved for extensive site surveys, designs and the deployment of the WLAN. However, if these third party integrators can reduce network complexity and the needed infrastructure (e.g., fewer APs), there can be significant reductions in up-front costs.

The recent ratification of the 802.11n specification is helping companies that were holding back, to begin deploying wireless networks, reducing the overall need and costs of traditional Ethernet hardwired networks. A recent HIMMS Leadership Survey (*see Figure 2*) outlines some of the most significant barriers to implementing IT/wireless within the healthcare market.

Hospital Hell: A Challenging Place for Any RF

Hospital RF environments are arguably the most challenging and dynamic of any vertical market. Unlike more open environments like school classrooms, warehouses, or hotels, the hospital RF environment is vastly different.

Hospital buildings have a wide range of construction attributes from the very old to new renovations and buildings. Whatever the case, the propagation and penetration of RF signals are challenged by solid concrete, tile over chicken wire in concrete, lead-lined walls in radiology, vast cable trays of wire in the ceiling, isolation rooms, and newer construction methods such as poured concrete in metal pan construction from floor to floor. This newer type of construction often traps RF signals from propagating anywhere and can limit penetration of consistent and reliable RF coverage from floor to floor.

Unlike other markets where the business model is less dependent on mobility, healthcare workers and patients are frequently mobile during the care process. Vast amounts of metal (e.g. hospital beds, instrument trays), fluids (I.V. medication), pharmacy, (storage of IV medication) wreaks havoc with RF signals, especially those within the 2.4GHz band.

The combination of the hospital construction environment and healthcare mobility model places unique new challenges for

the healthcare WLAN to operate in a consistent and reliable fashion. Consequently the wireless network must be able to constantly adapt to change.

Making Wireless Reliable: Enter Smart Wi-Fi

New technical breakthroughs are helping define the next era of the WLAN for healthcare organizations of all shapes and sizes The recent introduction of "dynamic beamforming," or "Smart Wi-Fi" is one such breakthrough that solves the most overlooked aspect of making WLAN work reliably: predictable performance and stable RF connectivity at range.

Predictable Wireless Throughput: *Is it Really Possible?*

Wi-Fi throughput has always been inconsistent due to the mobility of users, interference between transmitters and receivers, obstacles and the fact that 802.11 is simply a shared medium.

The primary culprit to poor Wi-Fi performance and range is interference. Interference causes packet loss. Packet loss requires retransmissions. Retransmissions take time. In turn, Wi-Fi performance for everyone is lowered.

While many Wi-Fi suppliers now offer the capability to automatically detect noise on a given channel and automatically switch client communications to a better channel, it's not enough. Today nearly every Wi-Fi access point uses omni-direction antennas that radiate RF energy in all directions.

Traditional omni-directional static antennas might see multiple RF waves in phase at one point, but the mobile environment of the healthcare user or medical device is guaranteed to change, while static antennas cannot adapt to change. Mobile patient monitors, wireless infusion pumps are, and voice over IP appliances/handsets are always moving throughout the healthcare continuum. This is unlike wireless laptops on carts that are usually static outside a patient room environment.

Despite its location, if interference is experienced, a conventional Wi-Fi AP lowers its data rate so packet loss is minimized. This degrades overall throughput for all users and effectively eliminates the support for latency-sensitive applications such as a voice or streaming video.

These problems are exacerbated with 802.11n. With the advent of 802.11n these omni-directional transmissions by multiple radio chains can actually have a negative effect on system performance and reliability if the antenna elements are insufficiently spaced or improperly orientated.

Because 802.11n uses multiple radios and depends on multi-path communications to yield higher data rates, any interference or obstruction of the signal path minimizes the chances of spatial multiplexing or channel bonding — two of the fundamental techniques used to increase capacity.

Ideally, what is needed is the ability for each AP to know at a given moment, the best signal path to use for any transmission and to receive feedback from the client to assure the highest data rates are being achieved. Couple with this is the ability to detect and automatically avoid Wi-Fi interference by continually steering RF signals over paths that yield the highest data rates and lowest packet loss thereby adapting in real time to environmental changes.

The Art of Wi-Fi Beamforming

Beamforming is a new technique developed to solve some of these problems by focusing RF energy only where it's needed by either phasing signals at the chip level or through the use of intelligent antenna arrays that control the actual form and direction of Wi-Fi signals.

Dynamic beamforming takes this concept a step further by using client feedback to automatically switch the directional antenna used for any given packet. Dynamic beamforming also uses automatic interference avoidance techniques, similar to noise cancelling headphones, to nullify interference.

Smart Wi-Fi APs supporting dynamic beamforming use a number of physical antennas or antenna elements to create antenna patterns or paths between the AP and the Wi-Fi client. On the fly, the AP now can select the best path.

The best path will be the one where the radio waves radiating from at least two AP antennas combine to form still a higher signal at the Wi-Fi client; thus the signals are in phase.

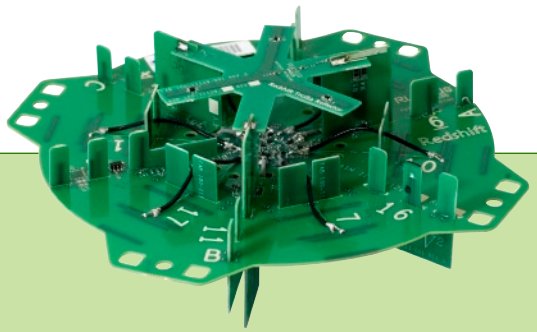
Contrast this with out of phase communication paths that interfere with each other, cancel each other, with resultant throughput drops. Smart adaptive antenna arrays offer thousand of antenna patterns from which to select and it is possible to control these multiple waves so that they are in phase frequently.

Ruckus Wireless is one vendor that has innovated such technology for the healthcare market through the use of dynamic beamforming.

By combining advances in miniaturized multi-element antenna design with sophisticated RF routing software, Smart APs are able to direct signals onto the best path in real time to deliver the highest possible performance and reliability in ever changing RF conditions. Smart Wi-Fi is based on Multiple In, Multiple Out (MIMO) antenna technology which provides unprecedented diversity, extended range, and explicit control over the RF paths that Wi-Fi signals take.

While the theoretical 802.11n data rate of 300Mbps or higher is constantly advertised, the actual and consistent user throughput can be an order of magnitude much less (*see Figure 3*). This is because current WLAN 802.11n products do not make use of Smart Wi-Fi technology.

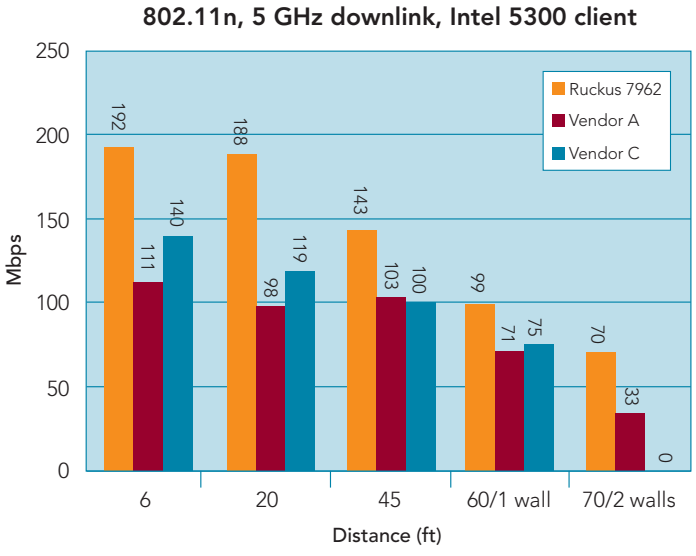
Smart RF routing software integrated within these systems continually learns the environment and re-configures the antenna array to select the best performing antenna pattern for each packet, switches to the signal path with the least interference, extends the range by focusing RF energy where it is needed most, and ignores or nullifies interference caused by other devices and environmental conditions. The Smart Routing software also learns from received packets as well as real-time 802.11 acknowledgements, thus maintaining an up-to-date ranking of the available antenna configurations for each destination.



Dynamic Beamforming with Smart Antenna Arrays

Smart antenna based beamforming actively addresses healthcare application and performance issues by selecting the best transmission path at any given time to sustain maximum data rates Integrated into all its "Smart Wi-Fi" access points, this miniaturized 19-element smart antenna array from Ruckus Wireless provides over 4,000 different antenna combinations that can be automatically selected for any given client. On a per packet basis, sophisticated best path selection software determines which antenna elements should be used at any time to yield the best performance possible. Antenna-based beamforming avoids existing interference and it uses directionality and antenna diversity to avoid creating it.

FIGURE 3: Comparing vendor 802.11n throughput at distance



Spatial Multiplexing in the Hospital

By controlling the RF signal path direction and timing; smart antenna arrays provide an important value add in multi-path operations for 802.11n. This is extremely important for multi-path healthcare environments of today. The availability of a large number of antenna configurations and the ability to select the best de-correlated patterns allow smart antennas to maximize successful spatial multiplexing operations to maintain the highest data rates.

The majority of today's 802.11n APs today utilize multiple omni-directional antennas polarized in a vertical orientation. This often undermines the potential of multi-path success — an essential element to achieve spatial multiplexing.

Ruckus™ WIRELESS

So Smart Wi-Fi APs support the use of smart antenna arrays that employ both horizontally and vertically polarized antenna elements to force de-correlation of different spatial streams. This effectively guarantees proper multi-path transmission regardless of the healthcare environment or mobility use model.

Getting the Most Out of 802.11n

With the recent approval of 802.11n (September 11, 2009), a lot of attention has been given to how best to upgrade from older 802.11a/b/g technology.

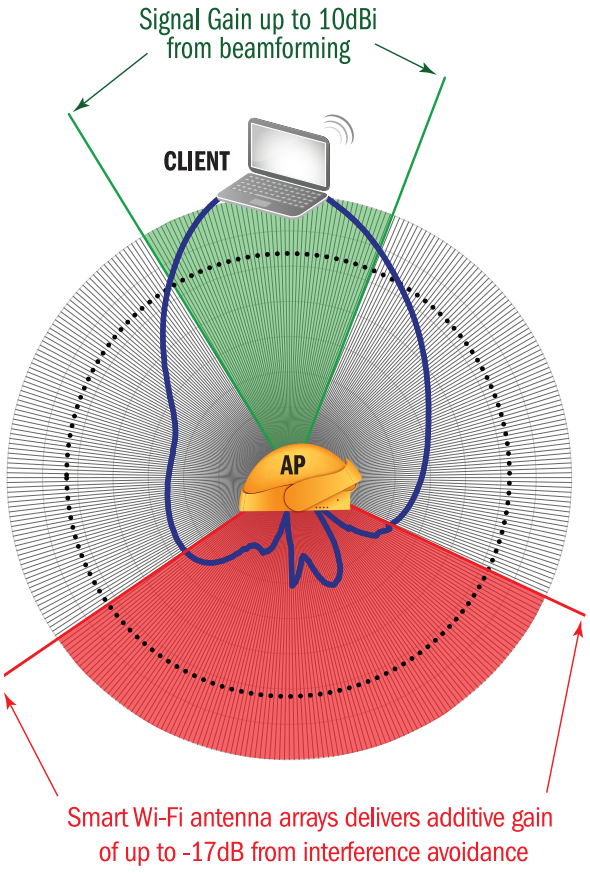
The migration in healthcare from wired to wireless, has now essentially left a lot (in cases up to 30%) of wired Ethernet ports not being utilized. With a theoretical throughput of 300 MB/second of 802.11n, the business case can made to no longer install wired Ethernet ports. This would save healthcare systems a tremendous amount of infrastructure costs, reduce port counts/decrease switches, as well as power and cooling requirements for this unneeded infrastructure. 802.11n is ideally suited to enable this migration if it can deliver reliable performance to every nook and corner of a medical facility.

To boost speed, 802.11n introduced a performance technique commonly referred to as channel bonding. Channel bonding boosts bandwidth by combining two adjacent 20MHz channels into a single 40MHz channel. Without channel bonding 802.11n is often compromised. The top data rate for an 802.11n system with two spatial streams is less than 150Mbps, instead of the theoretical maximum of 300Mbps.

For most 802.11n systems that use omni-directional antennas, channel bonding is often challenged or curtailed, by the presence of neighboring networks that are using the same channel. It is assumed that these 40MHz channels will only effectively work in the 5GHz band due to the large numbers of non-overlapping channels within that spectrum. Within the 2.4GHz band, there are only three non-overlapping 20MHz channels (1, 6, and 11). By combining two of those non-overlapping channels to create a wider 40MHz channel, produces only a single non-overlapping 40MHz channel. In the 5GHz band there are 23 non-overlapping 20MHz channels, therefore the risk of interference in using 40MHz channels is much lower.

Smart Wi-Fi's ability to select the best signal paths in combination with built in interference rejection and smart channel

FIGURE 4: Dynamic beamforming delivers both signal gains and gains from interference rejection.



utilization increases the likelihood channel bonding in both the 2.4GHz and 5GHz bands. Irrespective of whether the 2.4GHz or 5GHz band is used, 40MHz channelization is very sensitive to interference and packet loss. Most APs will react to signs of interference or packet loss by falling back to 20MHz channelization for a given client. This can result in the loss of more than half of the potential throughput for 802.11n. In contrast, Smart Wi-Fi allows the AP to choose among thousands of potential antenna patterns and paths resulting in specific antenna combination that will allow the use of 40MHz channelization, even in the presence of interference.

Robust, Simple Wireless Security Meets HIPAA

Enterprise grade wireless security for healthcare is an absolute necessity to meet HIPPA requirements. Securing a WLAN can be very complex and time consuming especially for hospitals that may have limited expertise to implement robust wireless security.

Two prevailing security methodologies include the use of pre-shared keys (PSK) and the 802.1X framework that combined encryption and authentication.

A pre-shared key is technique that uses a common encryption key or passphrase that is configured on the AP and on each respective wireless enabled mobile device. However the same PSK is used among multiple clients and tends to be a relatively short string that can be easily compromised.

Another option is using an enterprise-grade solution such as 802.1X. This is a highly secure framework that uses encryption and authentication to secure each client. Very complex to set up and configure 802.1X requires a RADIUS server to enable 802.1X supplicants on each wireless client. While 802.1X provides robust wireless security, the configuration and maintenance of 802.1Xis very time consuming for healthcare IT departments that do not have these resources.

New approaches to wireless security solve many of these problems by automating the generation of unique encryption keys, in the case of dynamic PSK as well as the configuration of complex certificate on clients, in the case of 802.1X.

A Ruckus patented approach called Dynamic PSK (*see Figure 5*) eliminates the risks associated with a shared PSK by automatically generating a unique encryption key for each client and installing that key and the requisite wireless configuration on the client. Here's how it works:

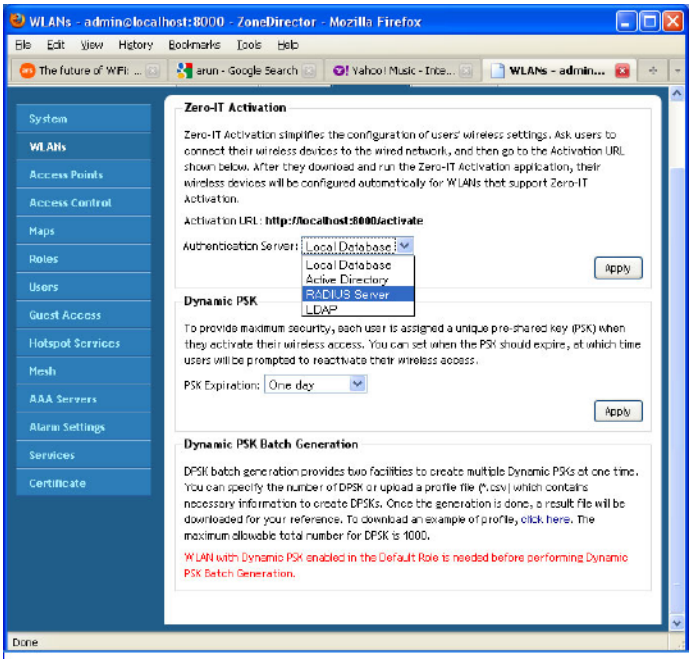
Once this is enabled for the entire wireless system, a new mobile user or medical device can connect and authenticate via a captive portal hosted on a centralized WLAN controller such as the Ruckus ZoneDirector.

The first time a user tries to connect to the wireless network, the user is challenged to login in with a valid username and password. The authentication is checked against any standard back-end authentication (AAA) server such as Active Directory, RADIUS, LDAP, or an internal user database on the Zone Director.

Upon the successful authentication of the user, the WLAN system dynamically generates a unique PSK for that client device, binding that dynamic PSK to the devices MAC address. The dynamic PSK is then automatically installed in the client device through a small application that also configures the requisite wireless settings to connect to the secure network.

The use of these dynamic PSKs can be limited in time, set to expire in minutes, hours or days. If the user leaves the healthcare organization, network administrators need only to expunge the user record from the authentication database. This same framework can be used with 802.1X, allowing 802.1X client configuration to be automatically pushed to and installed on client devices without human intervention.

FIGURE 5: Dynamic PSK is enabled by a simple checkbox within the Ruckus ZoneDirector GUI and automates robust Wi-Fi security



Fewer Smart Wi-Fi APs Provide Better Coverage, Capacity and Lower Site Survey Costs

A large part of the site survey and design methodology for traditional Wi-Fi deployments is to ensure adequate RF coverage and support capacity. The use of Smart Wi-Fi simplifies the deployment process to where the inherent intelligence and intuitiveness of the system simplifies the design, deployment and provisioning process.

Unlike conventional Wi-Fi APs, Smart Wi-Fi APs integrated a long-range intelligent antenna array (*see Figure 5*) that focuses RF energy in the best direction for the client. By doing this, signal coverage is extended by a factor of 2x to 4x (depending on the environment).

Understanding that hospitals are terrible multi-path environments and in a constant state of renovation, Smart Wi-Fi was developed to solve these issues. Smart Wi-Fi helps eliminate multi-path issues and is able to automatically adapt to environmental changes without human intervention. Renovation projects or additions will often require changes to the wireless network. Smart Wi-Fi helps eliminate or reduce the requirement to rely upon outside skilled technical assistance with another site survey and design.

From an applications perspective, this translates into the elimination of dropped voice over IP calls, reduced performance from having to fall back to lower data rates on 802.11a/b/g. Smart Wi-Fi systems are purpose-built to ensure consistent and reliable transmission of life critical patient monitoring information and alarms.

Summary

The majority of hospitals and IHN's have limited financial and human resources available to access, deploy, provision, and manage the proliferation of new mobile clinical applications and devices. These new mobile devices and applications are critical to improving the quality and efficiency of care delivery. There are also looming regulatory and industry standards which should be monitored that will raise the bar for running clinical applications over shared wired and wireless networks.

These dynamics highlight the importance of making intelligent and informed technology purchase decisions to ensure the optimal price-performance for investing a hospitals limited budget.

If you can do more with less hassle and the least amount of infrastructure, this just makes good fiscal sense. Also, if always works and allows your applications to work correctly 99.999 percent of the time, then productivity and the business of healthcare operates the way it should. These are hidden costs, but translate to the bottom line of creating a more efficient healthcare delivery system. Investing a small amount of time up-front to select the best solution can save a lot of time, frustration, and preserve scarce capital for other projects.

Smart Wi-Fi solves many of the technical issues that have traditionally plagued Wi-Fi deployments enabling healthcare organizations build a lower cost, higher performance and more reliable wireless infrastructure ideally suited to support life-critical applications. The tangible benefits include:

1. Reducing WLAN capital and operational costs by deploying fewer access points that yield a 2X to 4X improvement in range and capacity
2. A two-fold reduction in operational expense through the use of advanced wireless meshing techniques that enable APs to be deployed without Ethernet cabling
3. Purpose-built support for latency-sensitive applications such as IP-based streaming video, CCTV and voice over IP
4. Increased client connectivity from through the use of adaptive antenna arrays that constantly steer wireless signals to each client over the best performing signal path
5. Reducing port counts at the Layer 2 switch in the Intermediate Distribution Frame.
6. Reduction of warranty costs on access points, controllers and Layer 2 equipment.
7. Decreased need for extensive site surveys.
8. Decreased requirements for sophisticated and/or specialized integrators.
9. Decreased complexity of setting up security policies and procedures that decreases risk to the healthcare enterprise.

In the end, Smart Wi-Fi represents the newest generation wireless technology for the healthcare ecosystem of 2010 and beyond. Completely standard-based, Smart Wi-Fi reduces the overall amount of infrastructure required, decreases the costs for design and deployments, and delivers enhanced user and application experience for data, voice, and life critical medical applications.

Ruckus Wireless, Inc.
880 West Maude Avenue, Suite 101, Sunnyvale, CA 94085 USA (650) 265-4200 Ph \ (408) 738-2065 Fx