The Reality of the Life-Critical Wireless Healthcare Network

A SOLUTION WHITE PAPER

The Reality of the Life-Critical Wireless Healthcare Network

TABLE OF CONTENTS

Abstract

Today's healthcare CIO is under tremendous technical and financial pressure to deploy a secure and life-critical wired and wireless network to support data, voice, video and medical device applications. In the US, they are also required to satisfy the Affordable Care Act (ACA) and the deployment of Electronic Health Records (EHR) across the Integrated Delivery Network (IDN) in support of Meaningful Use. Add to this the new dimension of Bring Your Own Device (BYOD) to meet clinician demand and to support the myriad medical devices to include smart infusion pumps and patient monitoring. These requirements increase the level of risk for not only the design requirements, but the overall management.

Healthcare is by far the most challenging wireless environment. The wireless network must support data and voice, and beyond that, the various levels of quality service requirements and security. There is an urgent need to ensure the right Quality of Service (QoS) in multiple life and latency critical applications in a highly mobile environment. This paper addresses today's requirements for the Life-Critical Wireless Healthcare Network with a strategic focus on the following:

- The network must provide continuous and reliable availability throughout the integrated delivery network
- A high degree of enterprise visibility and security must be provided in supporting the myriad of medical devices, voice, video, and BYOD.
- Supporting this healthcare network must be cost-effective as EHR is rolled out to meet Meaningful Use requirements in the US

The Definition of the Life-Critical Wireless Healthcare Network

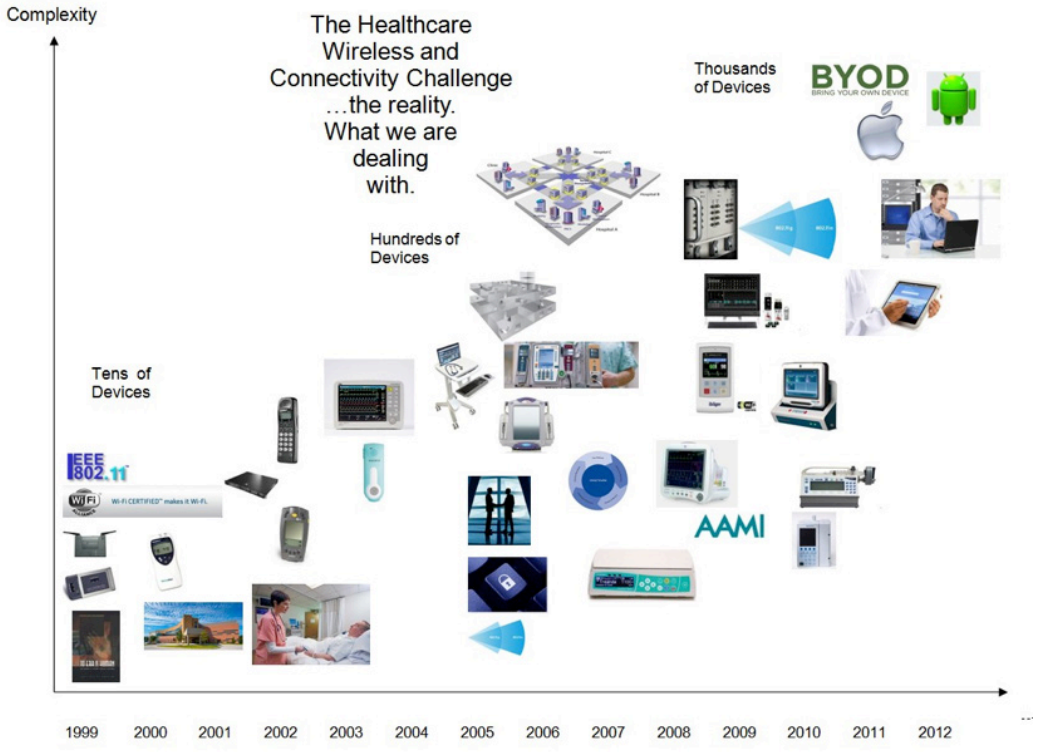
A life-critical wireless healthcare network is about providing the correct architecture that is continuously available and pervasive in a cost-effective fashion. This includes the ability to provide the healthcare institution of today with a technology infrastructure that is flexible, secure and scalable, while decreasing liability risk. Due to economic considerations that healthcare faces today, it needs to demonstrate – with hard numbers – the best Total Cost of Ownership (TCO).

Today's Wireless and Mobility Environment for the Healthcare CIO: The Challenges

Everyone associated with the healthcare enterprise today knows that wireless has to be everywhere. The productivity benefits of having wireless capability throughout the building environment are huge; but providing it presents challenges in design, implementation, and management. Additionally, wireless is not just confined to the WLAN, but also includes cellular, PCS and public safety. Just think of all the physicians carrying around their iPads and iPhones and add to this the proliferation of medical devices that are now becoming part of the healthcare WLAN. This consumerism of IT is driving today's healthcare requirements. The wireless network must not only support the myriad medical devices, but it must also support data, voice and video. This amounts to thousands of wireless devices to be managed in a visible, secure and cost-effective manner.

The reality is that this life-critical wireless healthcare network is supporting thousands of devices with a zero tolerance for downtime in a 24x7 environment. While using the wireless network for monitoring patients in real-time, either in transport or patient-worn telemetry, it is critical for the QoS to be assured; the alarms, waveforms and recordings involved in patient monitoring must be guaranteed to pass across the network. In addition, healthcare networks in the US must provide access to EHR for Meaningful Use compliance along with the requirement of supporting enterprise-grade security for HIPAA compliance. In light of this, questions that healthcare IT needs to ask include:

- Are there EHR disconnects or areas of the WLAN where devices have trouble accessing the network?
- What are the risks that BYOD brings?
- How do you manage the policies for security and device access across the wireless network?
- Do you experience unreliable voice or data connections due to network coverage?
- Does your facility provide continuously available Wi-Fi coverage for mobile devices?
- How can you manage this increasingly complex wireless network in a cost-effective way with a constrained staff size?



Today's and Tomorrow's Wireless for the Healthcare CIO: What are the Design Requirements?

To handle the proliferation of the data, voice, video, medical devices and BYOD devices, the actual wireless network has to be scalable, with built-in redundancy, and be able to grow with the needs and requirements of the modern integrated delivery network. The majority of, if not all WLAN medical devices, have shifted to 802.11a/g/n chipsets. There is also the tendency to move out of the 2.5GHz spectrum to 5.0GHz. However, with the rollout of 802.11n replacement to the enterprise, this issue is quickly being addressed. Right around the corner 802.11ac is being discussed, but in reality the wired network simply may not have sufficient capacity. Security and IDS are requirements because of HIPAA (in the US) and other medical device stringent security needs.

What is the Economic Situation Associated With the Integrated Delivery Network (IDN) Today and Beyond?

In the US, due to the pressure to comply with the mandated roll-out of EHR across the Integrated Delivery Network, a large amount of capital equipment dollars are being spent to meet regulations and take advantage of the monetary incentives provided by the US federal government. To support this initiative, often the wired and wireless network must be updated across the individual hospitals of the IDN to include clinics and physician offices. Infrastructure such as networking is now a necessity and because dollars are being allocated to other sources, pricing for networking and the accompanying support are under scrutiny. Hospitals no longer have a blank check for purchasing infrastructure, but they must validate and verify via a pro-forma for the purchase. Having a pervasive infrastructure can significantly reduce the risk associated with medical device integration on the wireless network. We are all familiar with the aviation industry as thousands of planes are in the sky each and every day. The reliability of the sub-systems of the aircraft, as well as the air traffic control system, is the reason for the high reliability of air travel. Healthcare networking architecture, both wired and wireless, just like the commercial aviation industry, must achieve this level of reliability and decrease risk.

Why a New Approach Toward an Increasingly Commoditized Wired and Wireless Infrastructure is Needed

The healthcare networking infrastructure has the burden of supporting more devices and more data traffic than ever before, both from a wireless and wired perspective in the most mobile 24x7 environment of any industry. IEEE WLAN standards for QoS and security (802.11e and 802.11i) have helped set the right baseline guidance in terms of what is needed in a healthcare wireless network today. However, this is only the baseline. The true performance comes down to the site design, the right architecture, deployment and management.

Since there is a very high priority in the US to support the roll-out of EHR due to Meaningful Use compliance, IT resources, especially in the areas of network management, can be very costly. Making networks more and more intelligent will have to be accomplished with the current number of FTEs or less to support network management and security. Because of the mission-critical requirements of the healthcare enterprise, the wireless network has to work flawlessly and must be continuously available. The right design of the overall network will ensure that as the network is increasingly utilized it maintains this high level of reliability.

The New Approach and Why This Should be Considered

There is a new converged wired/wireless network architecture that offers significant value to today's healthcare CIO. This design simplifies the overall management of the network. The uniqueness of this design allows for the assignment of single user or device specific configurations regarding traffic segregation, QoS and forwarding. This policy-based architecture keeps traffic from all different services segregated and isolated. The isolation of this traffic is irrespective of the port the traffic uses to enter the network, or the specific access point that provides the connectivity, or the wireless LAN ESSID being used to connect to the network. Having this policy-based design and isolation

of traffic is the necessary design that will address different medical device application requirements and the rush to BYOD in healthcare. In the era of BYOD, EHR security and access have become an important concern. Having the ability to provide access by location and by specific user policy is the ideal and necessary way to provide BYOD security.

What is the Value for the Healthcare Integrated Delivery Network in this Approach?

Network Management that Significantly Lowers the Cost of Ownership

It has become a fairly standard best practice to configure the overall wireless network with multiple ESSIDs. For example, what has become common practice is one ESSID for voice, one for data traffic and another for each wireless medical device service of operation. However in doing so, the management of the network design becomes increasingly complex. Creating a common ESSID and dramatically reducing the number of ESSIDS greatly simplifies the overall management of the network. As an example, a medical device connected through this new WLAN architecture can share the same ESSID with customer devices and its traffic will never be mixed with other network traffic and there is no possibility that one device can access another's traffic.

True Enterprise Visibility of all Wireless Traffic

For the first time, with this new design architecture, the network administrator has a heads-up display of all devices and network activity in one spot. No longer is an army of IT support staff needed to manage the network. A centralized end-to-end visibility and granular control of enterprise network resources is provided. This design and approach is distinctive because it provides granularity that can reach far beyond port control and VLANs, down to the actual users. Even when moves occur or add changes happen in the environment, everything is in view and under control via role-based access control.

Provisioning for Ultimate Cost Savings and High Reliability/ Redundancy of the Wireless Network

The ability to provide auto-discovery, profiling of BYOD devices and on-boarding, followed by real-time tracking of BYOD devices and users enables better control, as well as effective trouble shooting. This granular support for all devices, in all locations (both wired and wireless) can be provided across the entire Integrated Delivery Network in one easy-to-use interface. This ultimate cost savings and high reliability starts with the right foundational design of the networking infrastructure. It should be a requirement for today's healthcare network and should not come with additional costs either CAPEX or OPEX. These features that provide visibility and provisioning should be considered standard for today's life-critical healthcare wireless network.

Support for 400,000 Square Feet –
120 Access Points and 2,500 PoE Wired Ports

COMPONENT	ENTERASYS ONEFABRIC EDGE	LIST PRICE	CISCO	LIST PRICE	JUNIPER	LIST PRICE	CISCO/ARUBA	LIST PRICE
Edge Management including Guest Access	OneFabric Control Center (NMS-250)	$15,995	Prime NCS	$14,995	Ringmaster	$17,995	AirWave	$14,995
Additional Software (required to match features)					SmartPass	$1,265	Amigopod	$14,995
Wired Components	K-10 (10)	$630,150	Catalyst-4506 (10)	$847,025	Juniper-6200	$725,200	Catalyst-4506 (10)	$847,025
Wireless Controller	V2110 (2) + 104 AP	$22,390	Cisco-4400 (2)+100 AP	$54,985	WLC880 + 100AP	$26,205	Aruba 6000MC	$7,745
Access Points	WS-AP3610	$119,400	Aironet 3500p	$155,400	WLA522	$119,400	AP134	$155,400
		$787,935		$1,072,405		$889,666		$1,040,160
Price Compared to OneFabric Edge:				36%		13%		32%

Providing Peace of Mind to the CIO as Medical Devices Become Part of the Wired and Wireless Network

In light of IEC 80001 and risk management, for the first time the CIO has the ability to manage the entire network from a single pane of glass. IEC 80001-1 Ed.1: is an international standard that is defined as the application of risk management for IT-networks incorporating medical devices. It is a process standard; it tells you what to do, not how to do. It is a voluntary standard – unless formally adopted by regulatory authorities. Currently, many healthcare medical systems operate on isolated networks which (in the U.S.) are viewed as a component of a regulated medical device. Medical device manufacturers are held responsible for performing risk assessment and mitigation activities under current US federal requirements, thus ensuring these systems are safe and effective for their intended use.

Emerging technologies, such as wireless, hold the promise to allow medical device manufactures and healthcare facilities to begin combining these systems on the Healthcare Information Systems (HIS) network. When healthcare facilities use their HIS networks for medical device connectivity (instead of the manufacturer-provided networks), the healthcare facility becomes responsible for ensuring the proper operation of those medical devices and their availability over the wireless LAN. This drill-down ability to manage the network decreases risk and ensures the utmost in enterprise QoS and security, even in the case of biomedical device integration. This simplification of the network architecture significantly decreases the overall costs to manage the network. This has the ability to enable network resources to be better utilized and provide the best Total Cost of Ownership (TCO) of any networked-based wired and wireless solution in the industry.

Closing Thoughts

While today's life-critical wireless healthcare network is very complex, it has to meet the high requirements of continuous and reliable availability in very latency-sensitive applications. This network also has to be scalable, flexible and able to support literally thousands of potential devices in an integrated delivery network that spans multiple buildings and campuses. Finally, due to economic requirements, this network needs to be managed with the least number of resources that will demonstrate the best TCO. A new converged architecture has been discussed which can provide significant value to today's healthcare CIO.

This policy-based architecture not only simplifies the design but also enables complete isolation of traffic, enabling the better management of latency- sensitive applications. The simplification of this design and isolation of traffic by policies enables decreased costs for the enterprise management of the WLAN across the Integrated Delivery Network.

David Hoglund

Senior Design Consultant
Wireless/Medical Connectivity
www.integrasystems.org

Recognized as a Subject Matter Expert (SME) in wireless and medical connectivity, David is a nationally recognized consultant for venture funded clients, integrators, medical device companies, architectural firms, and Fortune 50 companies on a global basis.

Well known in the healthcare and wireless industries for his extensive knowledge of wireless ecosystems involving integrators, vendors, advanced technologies and specialty devices; he is also an expert in medical devices and clinical information systems involving patient monitoring, cardiology, anesthesia and respiratory applications. His experience includes working with the FDA, the Wi-Fi Alliance, IEC80001 and the National Institute of Health (www.nih.gov). He has created test plans, implemented product testing, led FDA 510K process approval projects, designed new product solutions and implemented M2M for corporate clients.

Internationally recognized as writer, speaker and professional blogger involving wireless/medical connectivity topics, he has given presentations, conducted web based event, and written for many technology companies, medical device companies and to include www.aami.org, www.himss.org, and www.ieee.org.

Currently the President / Senior Consultant of Integra Systems www.integrasystems.org, a boutique consulting firm, David provides strategic assessments and detailed planning services involving wireless and mobility technologies. He has worked with major corporate clients where he has developed strategic business plans, completed reseller agreements and executed technology agreements.

Member: IEEE, AAMI, HIMSS

Extreme networks

http://www.ExtremeNetworks.com/contact / Phone +1-408-579-2800