WHITEPAPER

Meru Uninterrupted Care Network

An Architecture Overview

Wireless Networks Designed for Hospitals

May 2013

Table of Contents

The Meru Uninterrupted Care Network

The Institute of Medicine (IOM) released a report in 1999 titled "*To Err Is Human: Building a Safer Health System*"[1]. According to the report, errors caused between 44,000 and 98,000 deaths every year in American hospitals, out of which 7,000 were attributed to medication errors. Within a short period, the industry responded by launching the first Wi-Fi-enabled smart pump to reduce medication errors. Use of Wi-Fi technologies grew rapidly from that point on.

Over the last decade, hospitals utilized Wi-Fi infrastructure to solve other problems. Voice over Wi-Fi, for instance, has enabled clinicians to coordinate care from anywhere in the hospital, wireless real-time location systems (RTLSs) are helping hospitals manage the wide range of medical equipment used in patient care, and "computers on wheels" (CoWs) are enabling clinicians to take advantage of decision-support systems to reduce errors while improving productivity.

In addition to the benefits Wi-Fi is delivering to hospital staff, it is also allowing patients, their families, and visitors to use tablets and smartphones to access the Internet, making their hospital stays more convenient and pleasant.[2] There is little wonder that over the past decade, the use of Wi-Fi technology in hospitals has increased rapidly.

Hospitals Are Ready for Wi-Fi—But Is Wi-Fi Ready for Hospitals?

The use of Wi-Fi in hospitals can be divided into three distinct categories: life critical, mission critical, and consumer critical.

- **Life-critical** applications such as telemetry require low bandwidth but exceptionally high reliability and stability. Interrupting the data flowing through these applications interrupts care and can jeopardize patient safety. Life-critical applications include devices such as infusion pumps and telemetry that are very sensitive to packet loss, require low latency, and tend to be operated for long periods—ranging from 7 to 10 years—without being upgraded. The primary concern for IT in delivering Wi-Fi support for life-critical applications is patient safety.
- **Mission-critical** applications such as voice over Wi-Fi, RTLS, and CoW require mobility and high bandwidth. They tend to be data intensive, and are subject to frequent patching, such as upgrades and security patches for Microsoft Windows systems or iOS for iPhones. Loss of connections and data affects staff productivity and interrupts daily care.
- **Consumer-critical** applications are used by patients and their visitors for researching their own medical conditions, staying in touch with family members, keeping their lives outside the hospital in order, and entertaining themselves with online video and other content. With public expectations for Wi-Fi availability rising rapidly, Wi-Fi is now a significant factor in patient satisfaction.

Partly because of this three-tiered Wi-Fi environment, hospitals present unique challenges for wireless deployments. Chief among them is the absolute urgency of maintaining the connectivity of life-critical devices. A typical ICU patient is connected to six to twelve medical devices in addition to numerous IV lines. These devices are hardwired to a central monitoring station.

[1] Kohn L T, Corrigan J M, Donaldson MS (Institute of Medicine), To err is human: building a safer health system. Washington, DC: National Academy Press, 2000.

[2] http://wellmont.newsroom.meltwaterpress.com/news/wellmont-invests-in-patient-satisfaction-boosts-wireless-internet-services-in-its-hospitals-97

According to a report published by ECRI,[3] The Pennsylvania Patient Safety Reporting System (PA-PSRS), a statewide adverse-event and near-miss reporting system, received 277 reports related to alarm response during medical telemetry monitoring between June 2004 and October 2006. All the reports described events in which patients were not consistently monitored for physiologic condition, and three events resulted in patient death. Unconnected telemetry transceivers, delays in connecting to patients, and transceivers taken off without orders constituted 66.9 percent of the cases. Such errors clearly establish the need for Wi-Fi-connected medical devices.

Another important factor is the teamwork involved in medical care. Doctors, nurses, lab technicians, and other staff need quick and efficient communication. Electronic health records and archived imagery have to be quickly available, no matter where caregivers are. Patients need to know that if they call for help, a nurse will respond promptly. According to a study conducted in a major academic medical center[4], a unit with 32 beds had an average of 320 nurse calls each day. Because nurses are mobile, responding to such a high number of nurse calls without a VoWiFi phone or pager becomes a daunting task.

Add to this the fact that hospitals are public places, with patients and their visitors coming and going constantly, and IT becomes responsible for providing wireless for a fluctuating collection of varied devices that send and receive data, audio, and video signals on the hospital premises.

Patient Wi-Fi traffic is no small part of this. In a time when everyone has become accustomed to and dependent on wireless devices for day-to-day activity, personal communication, and entertainment, patients and their family members need to use their devices while they're in hospital. This is not a simple matter of convenience. The ability of a patient to stay in touch with her children at school, update her family and friends, check in with her workplace, attend to household issues, read e-books, watch movies, and more is a major factor in patient satisfaction and well-being.

So more and more hospitals are investing in wireless technologies to:

- Improve patient care and safety
- Make doctors, nurses, and other hospital workers more efficient and effective
- Meet meaningful-use requirements of the HITECH Act
- Improve HCAHPS patient-satisfaction scores

Wireless connectivity can help hospitals accomplish these goals—and if it is done right, can help to ensure uninterrupted care for patients.

Addressing the Unique Challenges of Wi-Fi Implementation in Hospitals

A lot of hospital initiatives, including meaningful use, stroke protocol, and medication error prevention, rely on Wi-Fi connectivity. Because many of these initiatives require changes in work processes, they encounter a natural resistance from hospital staff. Well-implemented Wi-Fi can help lower this barrier to success.

Typically, hospitals have deployed traditional microcell-based Wi-Fi networks, which require significant time commitments on the part of a couple of IT network staff (for example, one hospital with over 900 access points had only one network engineer).

It takes so much attention to keep these traditional networks working well that IT doesn't have time to develop new applications and uses that can improve efficiency and patient care. So the smartness of smart beds never gets utilized to prevent events that must never occur, such as pressure ulcers or patient falls, even though hospitals have already paid for smart-bed technology.

[3] Alarm Intervention During Medical Telemetry Monitoring. A Failure Mode & Effects Analysis.

[4] Call Bell Requests, Call Bell Response Time, and Patient Satisfaction, J Nurs Care Qual Vol. 24, No. 1, pp. 69–75.

One specific technical challenge IT faces is that hospitals in general aren't particularly friendly to wireless systems. Hospital buildings tend to be added onto over a span of years, and so they incorporate many different types of construction. Things inside them move around—carts, equipment, patients, staff. Moreover, some of the medical devices are manufactured by specialized vendors with no Wi-Fi expertise and minimal to no interoperability testing.

Another hurdle to overcome is the potential for interference and its consequences. Competition for access and bandwidth among different types of devices is a fact of life in the shared world of wireless, but in a hospital the variations this can cause in network latency, connectivity, and application performance are dangerous. Imagine the outcome if the Academy Award–winning movie a patient is streaming to his iPad hijacks the bandwidth needed by his life-critical monitoring system.

This hazard is particularly hard to overcome in microcell-based networks, where client devices control access. In such a network, each device chooses the access point with the strongest signal, seizes all the airtime it can get, and then decides when it will shift from that access point to another as its user moves around. The network can't control roaming behavior, so connections can get dropped during handoffs, and latency fluctuates, interfering with the performance of devices and applications.

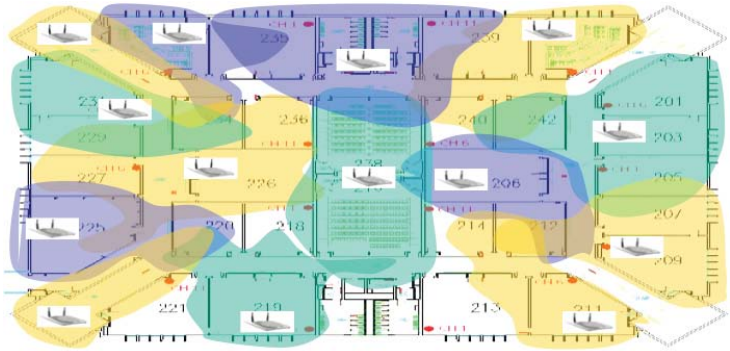

Figure 1 – microcells

To prevent co-channel interference, microcell-based networks put neighboring access points on different channels (Figure 1), and this means that AP locations have to be carefully planned, usually based on costly site surveys and repeated network tuning. Unfortunately, even with the best plan and with extensive deployment, it can be impossible to achieve coverage that is free of co-channel interference.

And finally, an important difference between life-critical hospital devices and administrative and personal devices is the length of their lifecycles. Life-critical devices tend to have long lifecycles, which is a good thing because it means that the wireless network that supports them doesn't need to be updated frequently. Networks that support enterprise applications and consumer devices, however, do, because of the frequent release of new features and functionality. If the life-critical devices share the network with enterprise and consumer devices, they are frequently at risk of interruption by upgrades, and the interoperability of the devices with new infrastructure software releases needs to be revalidated frequently.

These challenges and more make Wi-Fi systems for hospital environments a special case that demands a special architecture.

Introducing the Uninterrupted Care Network

Legacy microcell-based Wi-Fi networks don't deliver all the potential advantages that hospitals look to gain from wireless, and can actually put patient care at risk. Hospitals need a wireless LAN engineered specifically to deliver uninterrupted access that results in uninterrupted patient care. They need a network that enables IT to share responsibility for patient care with the medical staff by:

- Improving patient safety and quality of care by isolating life-critical applications from all other wireless traffic
- Increasing efficiency with reliable, pervasive Wi-Fi coverage for mission-critical applications and enabling clinicians to use the mobility platform of their choice in the hospital, clinic, or home
- Improving patient satisfaction by allowing patients to stay connected with family and friends, access the Internet, and enjoy entertainment such as e-books, music, and video

Meru developed the Uninterrupted Care Network with these requirements specifically in mind.

Reliable application delivery

Four characteristics of the Meru UCN enable hospital IT teams to step up to this responsibility: reliable application delivery, expansibility, assured service, and simplified network management.

The first characteristic of UCN is the ability to dedicate separate RF channels for the three different classes of applications found in the typical hospital:

Each class of applications has unique needs. In microcell-based, shared Wi-Fi environments, they compete with one another, and this can lead to the interruption of vital patient-care functions. Thus channel separation is an important capability of a UCN.

By allocating separate RF channels to application types, IT can guarantee performance for all types and at the same time keep them from interfering with one another. Channel separation makes it possible to grow the network incrementally, based on evolving requirements and budget fluctuations. It also addresses the issue mentioned above of longer lifecycles for life-critical applications by making it possible to upgrade mission-critical and consumer-critical layers of the network to keep pace with growing bandwidth needs, new devices, and so forth—without disrupting the life-critical layer.

Other factors in reliable application delivery that the UCN addresses are seamless mobility, constant connectivity and reliability, and controlled allocation of bandwidth to every client device based on the importance of its function and the type of data it sends and receives.

The ability to expand access to different classes of users and remote locations

Another potential interruption in patient care arises from the dependence on wireless personal productivity devices that hospital staff—like workers in almost every profession today—are beginning to develop. Doctors need to use their smartphones and tablets to access patient information remotely from their clinics and homes. Staff at off-site locations such as labs and clinics also need wireless access to hospital systems.

From IT's point of view, this means a constantly expanding Wi-Fi network that grows to include new classes of users, such as patients and guests, new locations, and new devices. That in turn requires more work as IT staff have to grant access and make sure it is controlled by policies, provision personal and hospital-owned devices, and make sure that all the data travelling back and forth is secure. The Meru UCN is not only expansible, it also has built-in management capabilities that enable IT staff to perform all these additional tasks efficiently.

Assured service

No system is perfect, and in the hospital setting, when glitches do happen, identifying and fixing them rapidly is paramount. That requires simple and efficient management tools that make it possible for IT to proactively assess end-to-end connectivity, performance, and latency issues, and fix them before patient care is affected—without shifting IT focus from supporting new applications to constant troubleshooting.

The Meru UCN Is Based on a Fundamentally Different Approach

The Meru approach to wireless local area networks (WLANs) is fundamentally different from the approach that underlies microcell-based Wi-Fi systems. Based on RF virtualization, this approach allows hospitals to realize the full benefits of Wi-Fi—and at the same time avoid problems that might interrupt patient care.

The Architecture

The unique hospital environment and the urgency of uninterrupted patient care demand a flexible architecture that can rapidly adapt to change. Ethernet-like network access is not enough. The architecture has to span multiple layers and give IT control and choice as they support life-critical, mission-critical, and consumer-critical wireless systems.

This multilayer control allows hospitals to grow their Wi-Fi networks incrementally as their needs evolve. Wireless access points can easily be added or channel-stacked when more coverage or capacity is needed, without IT having to rip out the installation or undertake the time-consuming channel mapping and reconfiguration required by convention microcell networks.

At the network layer

The Meru portfolio of access points and controllers enables IT to deliver ubiquitous network access. Unlike solutions from other vendors, the Meru RF approach gives IT multiple RF layer options for optimizing performance, mobility, and user experience. In addition, the Meru single-channel architecture (SCA) helps to realize the benefits of 802.11ac, because it reduces the number of available RF channels.

Enhancing the RF physical and MAC layers of the network has traditionally been Meru's unique innovation in the Wi-Fi space. Meru has always been a pioneer in the Wi-Fi market—first in the market to support unique Meru features like wireless virtualization and channel layering. Features particularly relevant to the hospital setting include seamless roaming, superior voice quality, and consistent connectivity. With Mobile***FLEX***, all the Meru unique capabilities built in at OSI layers 1 and 2 will not only be retained but extended.

In use cases where SCA and channel layering do not completely satisfy all requirements, Mobile***FLEX*** gives IT multiple RF deployment mode options designed to optimize performance and end-user experience based on the specific use case: native mode for small or distributed scenarios, and wireless virtualization plus virtual cell for ease of deployment for voice/mobility and channel layering to wireless capacity (especially in the 2.4 GHz band). This enables hospital IT staff to design their wireless networks in a way that best fits their specific requirements.

At the control layer

The Meru solution offers a choice between the simplicity of an on-premises controller appliance, the on-demand scalability of a VMware version of the controller software, or a WAN-optimization of distributed deployment for remote locations.

Within each wireless network, there must be a provisioning and configuration management control point, and the most popular architecture accomplishes this service via a network controller. Typically, this hardware server supports major control functions such as configuration and version management of AP firmware, secure client authentication and authorization, troubleshooting, zero-latency roams, application resource management, application gateway functions, and fault tolerance capability.

The network controller can also be a control point for integrated wired/wireless and network-health management. All of these functional elements are bundled into System Director, the Meru controller core software. Additionally, Meru offerings in the control category also include not only a broad choice of hardware controllers, but also virtualized controller options that can run under VMWare or distributed cloud service models.

At the policy layer

The industry's most widely deployed, integrated BYOD and guest-management solution can overlay any vendor's wired or wireless infrastructure to help IT define and enforce access policies.

As IT's responsibility goes beyond serving mobile employees to onboarding and managing visitors and patients as well, the wireless network needs a strong and flexible *policy* engine that can support a flexible network onboarding service and can apply diverse policy schemes to the various user/device classes needing support.

Meru recognized this problem and was first to market with our integrated guest onboarding with Meru Identity Manager. This single, integrated solution is deployed in several thousands of installations. IDM is now the basis of ***FLEX*** **Policy**, the policy service element of Mobile***FLEX***.

At the application layer

The Mobile***FLEX*** architecture delivers the services needed to support uninterrupted care in hospital environments. The most revolutionary aspect of this new architecture is its approach to supporting and integrating vertical-market mobile applications into the wireless fabric.

The real value of a WLAN has always been the value of the applications that hospital staff use to deliver excellent patient care. The enrichment of this aspect of the WLAN solution is a major goal of Mobile***FLEX***.

The Operating System

At the center of the Meru UCN is the Meru System Director operating system, which enables IT staff to easily and efficiently control traffic, allocate bandwidth, manage channels and access points, control access and handoffs, and more. The components of System Director, described below, work together to give IT control of an application-aware network with multilevel security and flexible deployment that supports voice and video services for life-critical, mission-critical, and consumer-critical traffic.

Air Traffic Control

Meru Air Traffic Control® manages all the transmissions that devices within the hospital send *and* receive, preventing system overload, helping to ensure reliability, and maximizing over-the-air system performance.

Airtime Fairness

Meru Airtime Fairness® addresses a major problem of Wi-Fi wireless networks—the tendency of the slowest traffic to determine the speed of the entire network. Airtime Fairness allocates time equally among clients, allowing every device to get optimal performance based on the speed of its connection. This makes the network equally accessible to all devices, lets bandwidth-hungry applications like PACs perform at peak capability, and allows latency-sensitive applications to have land-line quality.

Virtual Cell

In traditional Wi-Fi networks, client devices decide which access points to associate with, and when to hand off from one AP to another—sometimes chaotically fluctuating between access points or making choices that adversely affect their own performance and the performance of neighbors. Meru System Director creates a single, seamless Virtual Cell, which means client devices see one virtualized point of access for the entire network—providing uninterrupted roaming and transparent load balancing, so latency-sensitive applications like patient monitoring or nurse call can operate flawlessly.

System Director also allows IT to effectively manage co-channel interference without costly and time-consuming channel planning.

Channel Layering

With Meru Channel Layering, IT can deploy multiple channel layers that operate independently in the same area. This capability can be utilized to increase capacity, and in the hospital environment it is particularly useful for dedicating separate channels for life-critical, mission-critical, and consumer-critical environments, or for preserving legacy investments by layering a life-critical Meru UCN over an existing microcell-based wireless network.

Policy Enforcement

Meru Policy Enforcement extends wireless security, enabling IT to authorize, segregate, and control all wireless traffic.

Redundancy

A Meru Redundancy module provides high availability at the system level through controller redundancy. With N+1 redundancy, one controller can act as backup for many, ensuring cost-effective continuity in case of controller or back-end network failure.

The Management System

Meru E(z)RF® Network Manager gives IT staff control and single-console visibility over the Meru UCN, helping them to proactively identify and prevent issues before they interrupt patient care, and it streamlines management so IT staff can focus on developing new applications. The E(z)RF network management applications can be deployed on a VMware-based virtual appliance or on a Meru services appliance.

In addition, E(z)RF Network Manager shares an interface with Meru Service Assurance Manager and Meru Spectrum Manager:

Service Assurance Manager

Meru Service Assurance Manager delivers end-to-end service assurance for the network and its applications. By creating virtual clients on existing access points, it tests and verifies network performance without the use of physical clients.

Spectrum Manager

Meru Spectrum Manager detects and classifies sources of wireless interference to deliver optimal spectrum usage and high service levels—an important capability in hospital environments, where life-critical applications are deployed. Using the information captured from the RF environment, IT staff can qualify all Wi-Fi channels and quickly remediate interference issues.

BYOD and Guest Access

At the Meru UCN's consumer-critical layer, Meru Identity Manager (IDM) enables IT to easily manage the policies and provision patient-, guest-, and employee-owned devices, so their users can stay engaged with one another and connected to the outside world by browsing the Internet and streaming video and music without affecting other critical applications in the hospital.

IDM is a fully integrated software platform for managing visitor access and network access for employee-owned and hospital-owned devices. It supports onboardng for employee- or clinician-owned devices like iPads, Android tablets, smartphones, Apple Macs, and Windows- and Linux-based systems. IDM can be deployed over any vendor's wireless and wired infrastructure.

Role- and policy-based provisioning gives IT control over who and what devices get access, and over the level of access provided. And IT can delegate guest management to internal sponsors or allow guests to securely self-provision.

Mobility for Communications and Collaboration

Fast and reliable communication among hospital staff is a key requirement for uninterrupted patient care. Hospitals are implementing voice over IP (VoIP) and unified communication to meet this requirement, but legacy wireless solutions that depend on standards such as 802.11e and Wi-Fi Multimedia lack quality-of-service support at the application level and can't deliver zero-handoff roaming.

Because voice quality has to come paired with seamless mobility, the Meru UCN solution works with Lync Server to prevent the choppy audio and dropped calls during roaming handoffs that are characteristic of legacy LANs. The Meru Virtualized WLAN was designed from the ground up to overcome the challenges with roaming and scalability associated with voice over WLAN. Its unique single-channel architecture delivers voice packets reliably for mobile handoffs in 3 milliseconds—100 times faster than the 300-millisecond handoffs typical of legacy LANs.

Investment Protection

For life-critical devices, the UCN enables hospitals to create a stable Wi-Fi environment that, once optimized, requires very little intervention. Even hospitals with legacy microcell-based networks can get the benefits of the UCN, without sacrificing their investments or ripping out their existing network, by deploying the UCN's life-critical layer on a dedicated channel over the existing Wi-Fi infrastructure. This cost-effective approach enables hospitals to improve patient safety while continuing to derive value from their investments in microcell technology.

Summary

Whether you already have a wireless network in place or you're just beginning the process of planning one, we can help you take a cost-effective path to a wireless LAN that truly delivers the benefit you're after—providing uninterrupted care.

The Meru UCN is built on a unique architecture that frees your network from the limitations of client control, delivers seamless coverage and simple scalability that are only possible with a single-channel design, and virtualizes RF resources to ensure smooth, predictable performance.

So give us a call today, tell us about your unique requirements, and let us collaborate with you in your initiatives to improve patient safety, clinician productivity, and patient satisfaction.

Powering the Wireless Enterprise

Corporate Headquarters
894 Ross Drive
Sunnyvale, CA 94089
T: 1 408.215.5300
F: 1+1 408 215 5301
E: meruinfo@merunetworks.com

For more information about Meru, visit www.merunetworks.com.