

Wi-Fi Provides Rx for Healthcare Challenges

The healthcare industry is seeing a spike in wireless LAN deployments as Wi-Fi networks gain speed, medical records become digitized, and clinicians strive to improve the quality and reduce the cost of patient care.



Table of Contents

EXECUTIVE SUMMARY 3

Introduction: Providers of All Sizes Benefit from a Dose of Wi-Fi 3

Why Wi-Fi? 4

Challenges and Solutions 6

The Aerohive Advantage 10

EXECUTIVE SUMMARY

The healthcare environment naturally lends itself to wireless networking, given the inherently mobile nature of physicians, nurses, orderlies, and others who move from bed to bed or examining room to examining room, ministering to patients. This paper looks at how healthcare providers are using wireless LANs creatively to improve patient care and to realize much-needed cost efficiencies. It also discusses the primary challenges health organizations face in their deployments and offers up solutions for successfully addressing them.

Introduction: Providers of All Sizes Benefit from a Dose of Wi-Fi

The business of healthcare is both mission-critical and life-critical. Putting accurate, up-to-date medical information into a caregiver's hands at a patient's bedside can greatly impact the efficacy of an individual's diagnosis and treatment while also reducing the cost of care.

These are reasons that, according to a July 2010 study by Spyglass Consulting Group, 94% of U.S. physicians are now using smart phones to communicate, manage workflows, and access medical information¹. The widespread goal to improve care while containing costs is also a reason that the U.S. and other countries are attempting to get all medical records into an electronic format by mid-decade. Accessibility to current patient data from mobile devices at the point of care reduces the overall cost of health care delivery by alleviating much of the duplication of effort and inefficiency associated with hard-copy patient charts.

Another development: in the United States, the American Recovery and Reinvestment Act of 2009 (ARRA) has allocated \$19.2 billion in stimulus funds to develop standards around which a nationalized health IT system can grow. Under the ARRA, the U.S. government will provide direct financial incentives to providers receiving payments from Medicare and Medicaid if they adopt electronic medical records (EMR) and health IT systems.

Wireless LANs (WLANs) play a large role in all this activity. WLANs are quickly becoming the medium of choice for arming bedside caregivers with the up-to-date data they need to make important medical decisions quickly. Among the reasons are the generous network bandwidth WLANs afford and the sophisticated policy and security control that's inherent in 802.11 standards, which has also been enhanced by WLAN suppliers.

Another component of the standard Wi-Fi technology that's very important for healthcare is called secure fast roaming. This function allows mobile clinicians and others to stay connected while moving across coverage areas of different access points (APs). Secure fast roaming pre-authenticates users on nearby APs to which they might roam based on their initial authentication. This enables secure roaming without noticeable signal latency, which is mandatory for supporting deterministic, real-time communications such as voice over WLAN.

¹ "Healthcare without Bounds: Point of Care Communications for Physicians," Spyglass Consulting Group, July 2010

All these requirements and capabilities apply whether the facility is a large general hospital or a distributed medical or long-term care facility with remote sites. Especially challenging for the distributed organization is the typical lack of IT resources – both human and capital – at each distributed site because of the associated cost.

Here's a sampling of how Wi-Fi is being perceived and used at a few healthcare facilities:

- **LaVie Administrative Services**, an IT outsourcer to the long-term and post-acute care health facilities in Atlanta, Georgia, looks to WLANs as “a critical enabling technology for EMR applications,” says Marc Kane, the company's vice president of technology. EMR migration at the facility is expected to “improve cost efficiencies by reducing duplication of information capture and documentation,” Kane says.
- At **El Centro Regional Medical Center** in southeastern California, emergency room physicians using Wi-Fi-enabled handsets or laptops interview patients and simultaneously begin ordering lab work, radiology, respiratory therapy, or other tests and procedures over the network to speed up patient treatment, explains John Gaede, the medical center's director of information systems.
- And Wi-Fi in use at **NHS Lincolnshire**, a primary care trust based in Sleaford, Lincolnshire, England, means that “healthcare professionals can access and update medical notes on the run. Patients, in turn, are getting a far more efficient and informed service,” says Tony Arnold, senior network and systems manager.

These represent just a few real-world anecdotes that illustrate why ABI Research observed, in a June 2010 report, that the uptake of Wi-Fi within the healthcare industry had jumped 60 percent over the preceding 12 months². The researcher suggests that this trend is likely to continue with double-digit growth for the medium term.

Why Wi-Fi?

ABI Research cites the healthcare industry's need for staff mobility, transfer of digitized records, standardized administration of medications, and improved asset management as the primary reasons that wireless networks are starting to flourish in healthcare environments. Helping healthcare providers reach these goals are WLAN technology enhancements that qualify Wi-Fi as the most appropriate mobile network medium for these applications. Several are described below:

- **The arrival of higher-capacity networks.** Wi-Fi technology has gained the capacity needed to reliably transport large electronic patient medical files, images, and X-rays. The latest IEEE standard, known as 802.11n, was formally ratified last fall. 802.11n networks support data connect rates of 300Mbps per radio in AP infrastructure products. And many APs on the market support two or more radios. Actual throughput of about 120Mbps to 170Mbps per radio is generally possible when operating in the 5GHz band, depending on vendor implementation and the network environment.

² Press Release, June 22, 2010, “Wi-Fi Adoption in Healthcare Growing at 60%,” <http://www.abiresearch.com/press/1679-Wi-Fi+Adoption+in+Healthcare+Growing+at+60%25>

With such abundant capacity, these networks are enabling a new era in patient care. For example, the industry is seeing the proliferation of telemedicine, including the ability for emergency staff and others to consult with remote specialists who can even examine patients or supervise surgeries using videoconferencing. The Wi-Fi network can also be used for telemetry applications, whereby sensors can monitor patients and wirelessly alert a nurse if a patient's blood pressure, heart rate, temperature, glucose level or other vital sign indicates a dangerous medical situation.

- **Quality of service and reliability.** WLANs have gained the necessary quality-of-service (QoS) algorithms and tools needed to reliably support real-time traffic, such as the interactive videoconferencing consultations mentioned above and voice conversations among mobile medical personnel. Wi-Fi networks inherently use a shared network medium, and making these networks deterministic to emulate the switched nature of wired Ethernet networks has become a strong focus of QoS features and RF tools.
- **Security strides.** WLANs have embraced the security requirements of Health Insurance Portability and Accountability Act (HIPAA) privacy regulation, both within the IEEE standard and through innovation and security enhancements added by WLAN vendors.
- **The emergence of new applications.** The latest Wi-Fi applications in healthcare address patient care directly and indirectly as well as general efficiencies and cost.

For example, long-term care services provider Complete HealthCare Resources, in Dresher, Pennsylvania, has deployed an application called eMAR (electronic Medication Administration Record), which uses barcode scanning technology to monitor the bedside administration of medications. If the scanned information doesn't match the doctor's orders or a drug interaction is detected, the application triggers an alert, helping avoid medical crises, explains Martin Diller, the company's chief information officer.

Another growing application: Real-time location systems (RTLs) used with the Wi-Fi network are being deployed to track and quickly make available needed assets, such as beds and medical equipment. Low-power RF identification (RFID) "tags" are affixed to the assets to be tracked, and they continually transmit their location to an RTL application.

Such applications can make a big difference in patient care and alleviate wait times by helping staff immediately find a needed bed or infusion pump. These and other applications contribute to making the business of healthcare lean and efficient during a period when healthcare costs have skyrocketed out of control, spurring possible new regulatory policies and healthcare reform.

For example, at Riverside Health Care Systems in Westchester County, New York, a staff member wheels around a computer on a cart to handle patient insurance matters, says Niall Pariag, senior network administrator. The staff member is "in the elevators and on different floors, and she's always connected," he explains.

Challenges and Solutions

Perhaps one of the biggest challenges is that healthcare organizations have fundamental goals that are at odds with one another: Facilities need to be able to deliver confidential patient data immediately to highly mobile health professionals, particularly when circumstances are urgent. At the same time, though, HIPAA regulations dictate that they need to take extra precautions to protect the privacy of that data from unauthorized eyes, which is fairly challenging when data is no longer contained within the traditional borders of wired networks. Maximizing availability and access speed while also maximizing security is a tricky balancing act.

Many of these primary challenges for healthcare organizations are related to one another. Let's take a look at each, as well as how they can be met.

Challenge: High Availability

Healthcare organizations are tasked with making sure highly mobile caregivers can access patient data, including health and surgery histories, test results, drug allergy information, and dietary restrictions, on a 24x7 basis. Riverside Health, for one, listed high availability at the very top of its requirements list when it evaluated WLAN systems. One thing it discovered during its vendor evaluation was that WLANs that funneled all data traffic through a centralized controller created a single point of failure: the controller.

"Several vendors suggested installing redundant controllers. But when you fail over to a second controller, there is downtime," says Pariag.

In addition, there are potential WAN outages to consider in distributed deployments where facilities can't afford controllers at every location. Such organizations try to manage and control WLANs across WAN links from two or more redundant controllers in a central environment. However, downtime in the WAN service could result in users being unable to log on or roam among APs.

Solution

High-availability environments need a network solution that is inherently redundant and contains no single point of failure. That means first and foremost removing the controller from the configuration.

One cost-effective way to achieve inherent redundancy is to use over-the-air mesh networking, whereby APs talk directly to one another in the center of the WLAN. Most, but not all, Wi-Fi vendors support mesh. At this juncture, mesh is a capability not required by 802.11 standards.

In general, mesh works in much the same way that IP routers operate in the Internet: if one AP should fail or be decommissioned, the others around it will automatically direct traffic across an alternative route. This is much more efficient – both from a functional and cost perspective – than investing in multiple expensive controllers that must fail over to one another if an AP connected to it should go offline. And, as Pariag notes, the approach avoids incurring downtime during the failover process.

Challenge: HIPAA Confidentiality

While maintaining the highly available, highly reliable wireless environment above, complying with HIPAA patient confidentiality and EMR security is a must. This includes

preventing intrusions into the core data resources from would-be intruders outside the organization as well as from visitors who might be tapping into a guest network at the healthcare facility.

Solution

Ensuring that clinicians stay connected while keeping intruders out is desirable, so limiting the level of security exchanges that take place over the WAN is encouraged. The reason: for accessibility, a WAN outage could affect a clinician's ability to connect, become authorized, and access critical data. In addition, putting the security credentials and exchanges out across the WAN exposes them to other users on the public network and unnecessarily increases the risk of a breach.

Similarly, secure fast roaming, described earlier, requires preauthentication, either by the APs involved or a WLAN controller. Companies that don't put a WLAN controller at every location limit their ability to enable secure fast roaming across remote clinics, distributed long-term care facilities, and other sites in the event of a WAN outage. One alternative for these organizations is to create a backup service set identifier (SSID) that's local for user authentication in a fallback situation, should the WAN connection get disrupted. However, such a configuration uses something called a preshared key (PSK), which is known to be vulnerable to password cracking attacks.

From an industry perspective, Wi-Fi has made huge security strides. The latest 802.11n standards require the support of 802.11i/WPA2, a suite of encryption and authentication algorithms based on the robust Advanced Encryption Standard (AES). And the Wi-Fi Alliance, the industry consortium that certifies WLAN products for interoperability, is taking aggressive steps to phase out the existence of older and more vulnerable forms of security in new products being built.

In addition, a number of other security "layers" are available for Wi-Fi networks to further prevent data theft, either over the air or in networked data centers, and denial-of-service attacks, which can render data inaccessible. For example, firewalls and user authorization and authentication schemes built directly into distributed APs are now available (see Figure 1).

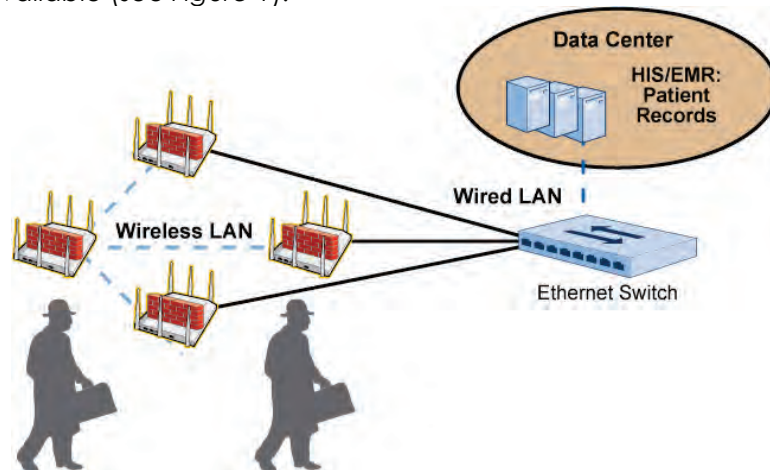


Figure 1: Privacy and Patient Confidentiality

Distributed wireless APs put key security functions, such as firewalling, authorization, and authentication, at the wireless edge to keep unauthorized users entirely away from all internal resources.

A fully distributed configuration means that unauthorized access is halted right at the wireless edge of the network rather than traveling further into the network, say, to a WLAN controller, posing a greater risk of penetrating the core network and consuming valuable network resources in the process. And 24x7 air monitoring systems are available that scan the airwaves for unauthorized APs that might be attempting to connect to the facility's network.

Challenge: RF Interference Avoidance for Reliability

Running a high-availability Wi-Fi environment requires managing the wireless environment around RF interference caused by neighboring Wi-Fi devices and other sources as well. "Noise" from a number of wireless sources can interfere with users' ability to use the network. Among the additional interference sources are medical equipment, guest devices, neighboring organizations with wireless networks, and everyday equipment that emits energy in the Wi-Fi bands, such as microwave ovens and wireless surveillance cameras.

Riverside Health, for example, found that it had a couple of challenges on this front: One of its buildings was across the street from an apartment complex in one direction and a medical park in the other direction – both running Wi-Fi APs and creating significant sources of interference.

Solution

As WLANs have matured, they have increasingly gained sophisticated RF management tools. These help tame the interference problem by using automation to detect the interference, dynamically adjust power levels and switch channels on the fly, if needed, to sidestep congestion in different areas. In addition, tools to enable solid RF planning upfront, when selecting locations for APs, are available such that the environment is optimized for interference avoidance upon deployment. RF environments, however, continually change, so automating the network to self-adjust and self-heal in the presence of interference and failures is valuable and time-efficient.

Such tools and automation are vendor-specific enhancements rather than inherent components of 802.11 standards. As such, they vary among suppliers.

Challenge: Cabling Sensitivities and Restrictions

It's becoming common for surgeons to refer to images delivered by the network in the operating room (OR). However, it can be a complex matter to bring a wireless AP into the OR if cabling or other access to the area above drop ceilings is required. This is because of strict limitations on the amount of dirt and dust that is allowed in hospital operating rooms and clean rooms.

Solution

Here, mesh networking is invaluable. In meshed Wi-Fi networks, it's possible to have some or nearly all APs exchanging information with one another about their state and forwarding traffic along the "best path" from AP to AP. In hard-to-wire environments – such as the restrictive OR – an AP can simply be mounted without the dust-inducing network cabling required to hard-wire the AP to an Ethernet switch. Note that at some point, one or more APs at the outside perimeter of the WLAN will need to connect to an Ethernet switch to provide access to the data resources residing in the wired data center (see *Figure 2*).

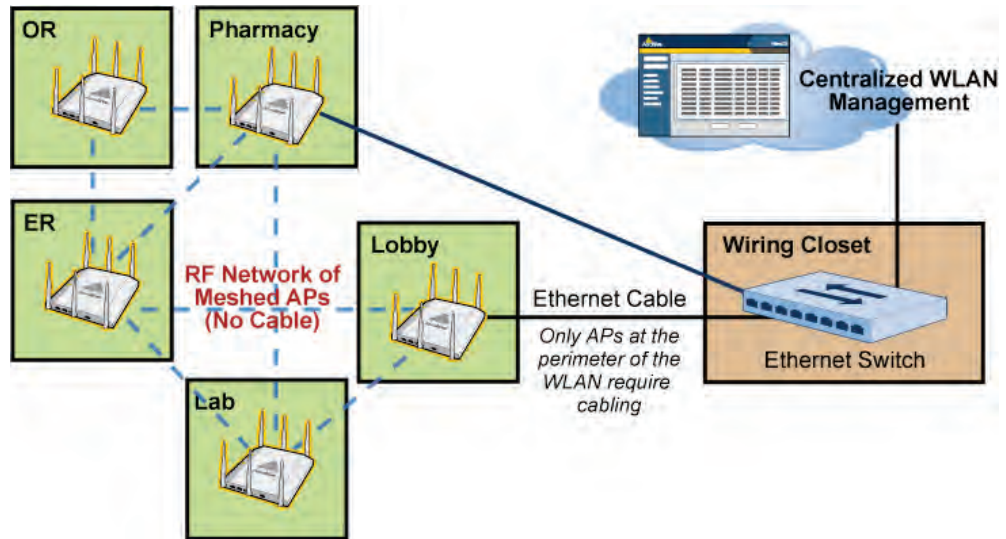


Figure 2. Use of Mesh in a Sample Healthcare Setting

Not having to cable each AP avoids drilling holes and opening up drop ceilings in required clean areas. Meshed APs are also inherently redundant. They discover one another, route around failures, and forward traffic to each other using the best path available.

Challenge: Migration-Performance Issues

There are migration issues to consider as facilities upgrade to the high-speed 802.11n from earlier versions of Wi-Fi that supported much lower speeds. When a mix of Wi-Fi APs and clients supporting different versions of the technology operate together during transition periods, it's possible for the slowest device in the group to bring down the performance of the inherently faster devices if steps aren't taken to ensure otherwise.

Solution

A number of vendors have introduced the concept of airtime fairness into their networks, a mechanism that prevents the slowest client on the Wi-Fi network from gating overall network performance. In general, this mechanism allows each client to transmit at the speed that it would if there were no slower-speed clients on the network holding it back.

Once airtime fairness has been accomplished, administrators can set priorities or weights for certain transmissions based on protocol, application, user, or other variable. To do this, they use a separate but related capability often called "policy-based QoS." Implementations among vendors and their effectiveness differ, again, because this capability is outside the functions that 802.11 standards specify.

Challenge: Guest Networking

A number of facilities are building logically segregated guest networks to give visitors and others Internet access securely, without mingling with any of the internal data resources. Some may wish to brand the guest network and perhaps even charge for the services, perhaps requiring compliance with Payment Card Industry (PCI) security standards.

Solution

In such cases, it can be beneficial to have a Remote Authentication Dial In User Service (RADIUS) server, stateful firewall, and captive Web portal distributed out to each location. Depending on vendor architecture, these capabilities could sit in a WLAN controller, if one is used at each site, or in each of a number of distributed intelligent APs that are also used for forwarding traffic. Again, these capabilities should be local to deter any service interruption or credentials exposure across a WAN connection.

The Aerohive Advantage

Aerohive WLANs have implemented many of the enhancements described that go above and beyond the 802.11 standards suite to automate, secure, and manage Wi-Fi networks. The Aerohive architecture uses self-organizing, mesh-capable APs that require no network controllers, for example. Software in the APs allows them to discover one another as they are added or removed and adjust to the environment accordingly in a fashion Aerohive calls "cooperative control." This discovery and inter-AP communication can take place over the air or over the cable attached to an Ethernet switch, depending on configuration.

In this way, Aerohive wireless networks eliminate the cost, performance, and availability issues associated with controller deployments, which create single points of failure, failover delays, and throughput bottlenecks.

The Aerohive architecture strikes just the right balance of distributed and centralized capabilities. Data forwarding, WLAN security, and performance-enhancement services such as real-time packet prioritization are distributed out to the individual APs to minimize latency and to ensure that a failed WAN connection to another location won't interrupt users already on the network.

The most important capability to be centralized – management – is handled from a single workstation, either in an appliance or in a service ("cloud") form factor. This enables IT staff to create a policy and push it out from one spot to any number of APs over the air. Administrators thus gain the flexibility to change policies back and forth to account for temporary situations and new users groups join the network.

Pricing and scalability are very easily calculated with the Aerohive solution. You simply multiply the number of APs you need by the per-AP price, then add the cost of the management for that number of APs (your choice of a management appliance, a VMware virtual appliance for your private cloud or Aerohive's cloud-based management service). There are no feature licenses or redundant components to worry about – and thus, no surprises. At the time of writing, a typical all-inclusive Aerohive 802.11n solution would cost approximately US\$750/AP list price.

To determine approximately how many APs are needed in your facility and where to place them, use this free online Wi-Fi Planning Tool: www.aerohive.com/planner. For more information about Aerohive's solutions, please visit: www.aerohive.com.

About Aerohive

Aerohive Networks reduces the cost and complexity of today's networks with cloud-enabled, distributed Wi-Fi and routing solutions for enterprises and medium sized companies including branch offices and teleworkers. Aerohive's award-winning cooperative control Wi-Fi architecture, public or private cloud-enabled network management, routing and VPN solutions eliminate costly controllers and single points of failure. This gives its customers mission critical reliability with granular security and policy enforcement and the ability to start small and expand without limitations. Aerohive was founded in 2006 and is headquartered in Sunnyvale, Calif. The company's investors include Kleiner Perkins Caufield & Byers, Lightspeed Venture Partners, Northern Light Venture Capital and New Enterprise Associates, Inc. (NEA).



Corporate Headquarters

Aerohive Networks, Inc.
330 Gibraltar Drive
Sunnyvale, California 94089 USA
Phone: 408.510.6100
Toll Free: 1.866.918.9918
Fax: 408.510.6199
info@aerohive.com
www.aerohive.com

EMEA Headquarters

Aerohive Networks Europe LTD
Sequel House
The Hart
Surrey, UK GU9 7HW
+44 (0)1252 736590
Fax: +44 (0)1252711901

WP1000908