Aerohive NETWORKS

Trends in Wireless Networking for Healthcare Organizations

Healthcare IT professionals are addressing new challenges and choices as their organizations increasingly rely on wireless networks to access critical applications.

Executive Summary

Healthcare organizations initially adopted Wi-Fi networking primarily for providing guest access to the Internet and other non-critical internal resources. Today, the trend is toward using Wi-Fi to support critical patient-care applications, provide mobile capabilities for care providers, and enable wireless clinical monitoring and tracking devices. This paper addresses trends in Wi-Fi usage and strategies in healthcare organizations. Based on findings from a survey to Healthcare IT professionals conducted by Spiceworks on behalf of Aerohive in March/April 2013 it provides valuable insights to the direction of Wi-Fi in healthcare.

Wi-Fi Increasingly Supports Business- and Life-Critical Applications

The business of healthcare is both mission-critical and life-critical. Putting accurate, up-to-date medical information into caregivers' hands at patient bedsides, in surgery suites, or at the emergency room can greatly accelerate diagnosis, enhance treatment efficacy, and reduce the cost of care. Wireless LANs (WLANs) have become the medium of choice for delivering and retrieving data from almost anywhere in a hospital, clinic, or operational and administrative department. Today, healthcare organizations are relying on their WLANs for:

- **Mobile access to data:** Giving caregivers bedside access to electronic medical/health records (EMR/EHR) applications.
- **Supporting remote monitoring:** Enabling patient monitoring devices to be read from a central location or while a patient is mobile.
- **Supporting highly responsive emergency rooms:** Accelerating lab work, radiology, and other tests and procedures for emergency room patients to hasten accurate treatment.
- **Faster information updates:** Enabling physicians and caregivers to update medical notes on the fly for the latest information.
- **Helping reduce medication errors:** Mobile barcode scanning for bedside medication administration.
- **Real-time asset tracking:** Using location-based services to quickly find and manage equipment such as wheelchairs, infusion pumps, and monitors.
- **Providing mobile voice services:** Delivering voice over Wi-Fi.
- **Providing guest access:** Providing Internet access for patients and guests to improve satisfaction.

Of the IT professionals who responded to the Spiceworks survey, EMR applications at the point of care ranked most important in terms of application traffic on WLAN. The second most important application is monitoring with Wi-Fi-enabled medical devices.

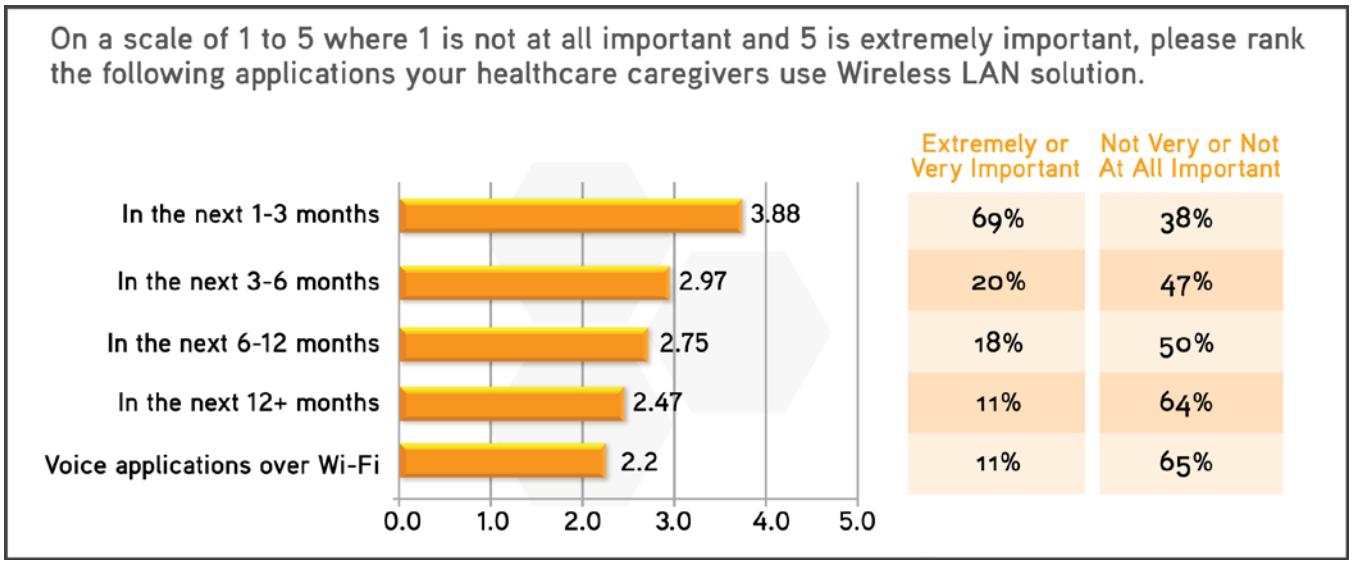

Figure 1: Spiceworks Healthcare Survey, March/April 2013

In addition to specific applications used in the clinical setting, 68% of respondents already support or plan to implement in the next 12 months a "bring your own device" (BYOD) policy on their WLANs. BYOD policies are spreading rapidly. In healthcare, these policies enable organizations to more effectively support physicians, specialists, and other caregivers who often move between facilities and private offices without the hospital having to procure, manage, and support mobile devices.

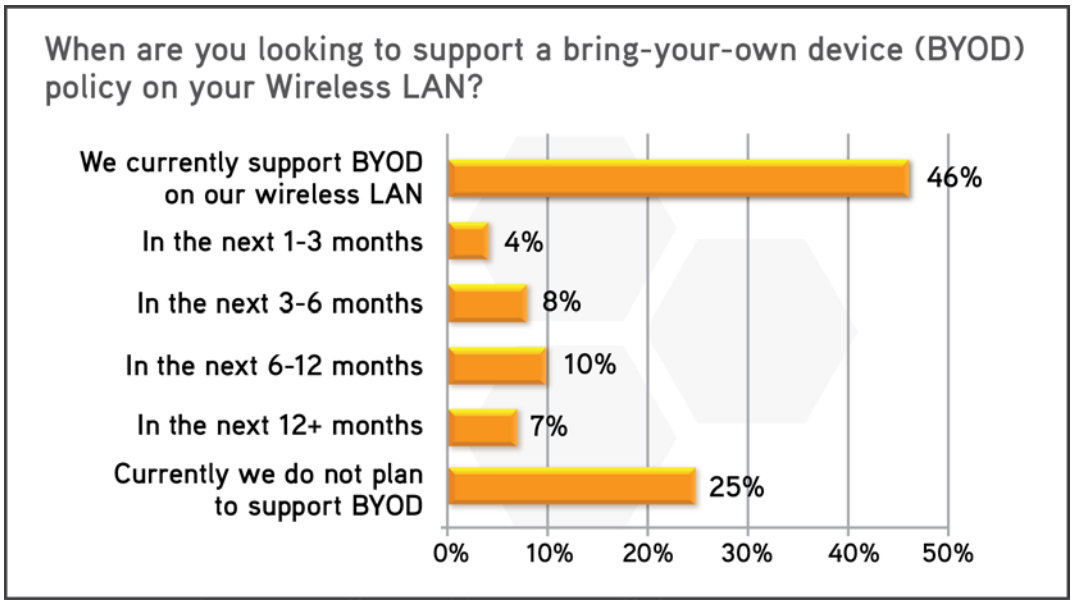

Figure 2: Spiceworks Healthcare Survey, March/April 2013

The WLAN Management Environment

The majority of respondents (95%) directly support or manage their WLANs, and 62% of all respondents were involved with implementing their current WLAN. This makes most respondents highly familiar with the architecture and infrastructure of their current networks. Most organizations surveyed—85%—have 1-50 wireless access points active across their locations. In addition, more than 80% manage 1-100 active Wi-Fi enabled devices in their largest site.

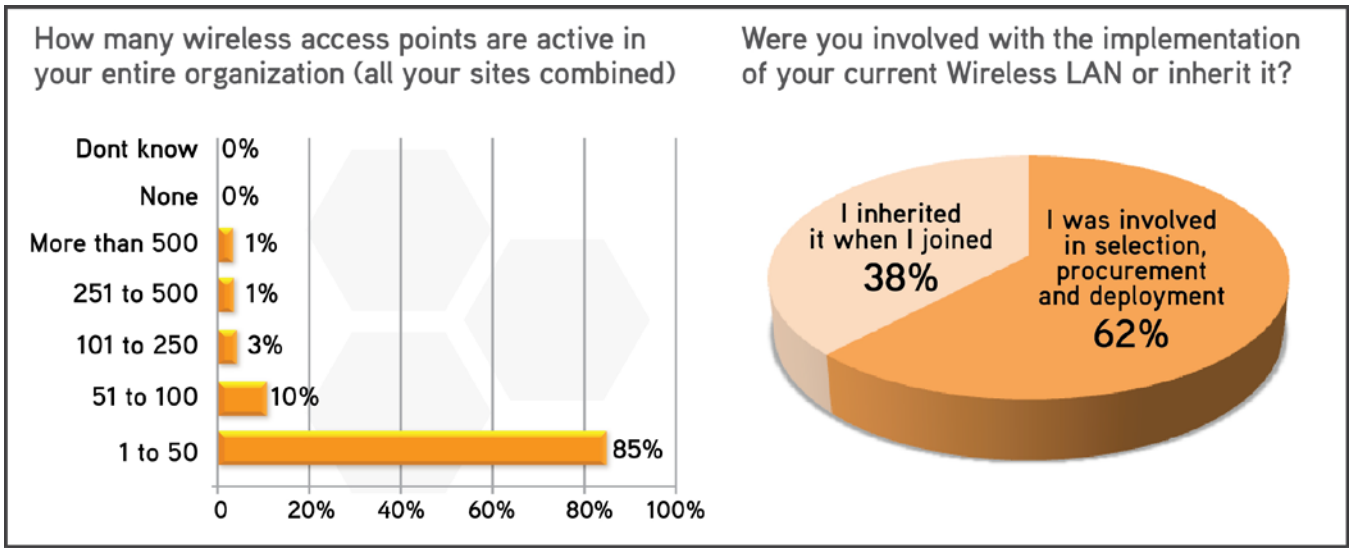

Figure 3: Spiceworks Healthcare Survey, March/April 2013

What Are Today's Challenges for IT?

Assuring High Availability

Healthcare organizations must make sure that mobile caregivers can access patient data, including health and surgery histories, test results, drug allergy information, and dietary restrictions on demand. It's no wonder that the IT professionals surveyed said that their top challenge when managing Wi-Fi enabled devices is ensuring acceptable Wi-Fi connectivity and performance.

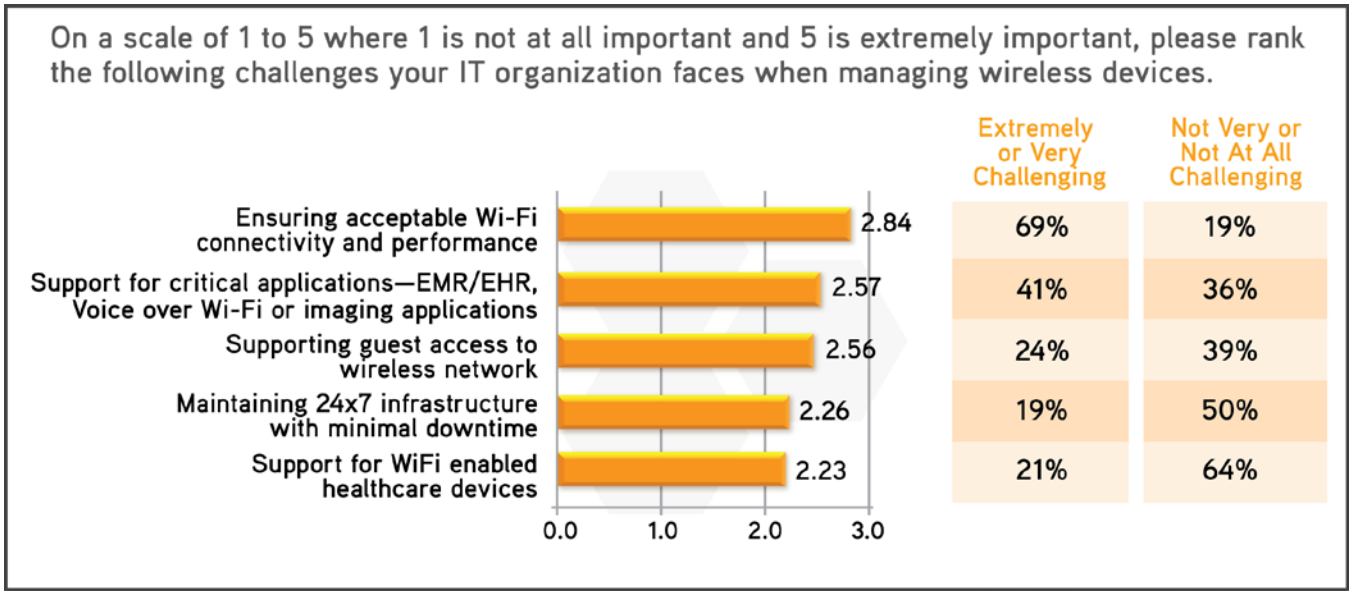

Figure 4: Spiceworks Healthcare Survey, March/April 2013

In deployments with a centralized controller, all data traffic funnels through the controller, creating a vulnerability and single point of failure. Even with redundant controllers, failing over introduces some downtime. In addition, wide area network (WAN) outages can introduce a risk of downtime into distributed deployments where it is too costly to place controllers at every location. Downtime in WAN service can result in users unable to log on or roam between access points (APs). Best practices encourage limiting the volume of secure exchanges that occur over the WAN. A WAN outage can affect clinicians' ability to connect, become authorized, and access critical data. In addition, allowing security credentials and exchanges to flow across the WAN unnecessarily increases the risk of a breach.

High-availability environments need a network solution that is inherently redundant with no single point of failure. This means removing the controller from the configuration. One cost-effective way to achieve inherent redundancy is to use over-the-air mesh networking. Many Wi-Fi vendors support a mesh networking approach, although a mesh capability is not required by 802.11 standards.

In mesh networks, if one AP's backhaul link should fail or be decommissioned, the AP can automatically direct traffic across an alternate route using surrounding neighbors' backhaul links. A mesh approach is much more functionally efficient and cost-effective than investing in multiple controllers and multiple switches to ensure that backhaul links are redundant.

Migration and Performance Issues

For healthcare providers, high performance is as essential as high availability. As facilities upgrade to high-speed infrastructures from earlier Wi-Fi versions, they often have a mix of Wi-Fi APs and clients operating together. In these situations, it is common for the slowest device in the group to significantly affect the performance of faster devices.

To combat this problem, many vendors have introduced the concept of airtime fairness into their networks. Airtime fairness mechanisms prevent the slowest client on the Wi-Fi network from gating overall network performance. Instead, each client can transmit at its maximum speed.

Once airtime fairness has been implemented, administrators can prioritize transmissions based on protocol, application, user, or another variable. To do this, they use a separate, but related, capability called policy-based quality of service (QoS). Not all vendors offer this capability or effective versions of it, because the 802.11 standards only require basic 802.11e, or Wireless Multimedia Extensions (WMM), which is a basic queuing mechanism but does not account for specific device, user, or protocol priority.

Patient Data Confidentiality

Health Insurance Portability and Accountability Act (HIPAA) requirements demand security for patient data. This includes preventing intrusions into core data resources from external intruders as well as from visitors who might be accessing a guest network.

Secure fast roaming features require pre-authentication by APs or a WLAN controller. Without a WLAN controller at every location, it is difficult to ensure secure fast roaming across remote clinics, distributed long-term care facilities, and other sites in the event of a WAN outage. 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). In addition, a number of other security layers are available for Wi-Fi networks to help prevent data theft over the air or in networked data centers and stop denial-of-service attacks, which can render data inaccessible. Firewalls and user authorization and authentication schemes built directly into distributed APs are examples of these additional security measures.

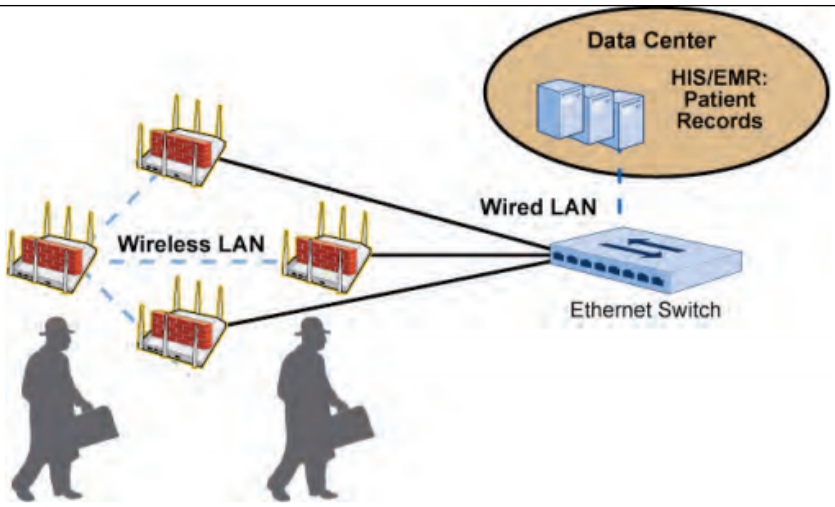

Figure 1: Privacy and Patient Confidentiality
Distributed wireless APs put key security functions, such as firewalling, authorization, and authentication, at the wireless edge to keep unauthorized users entirely away from all internal resources.

Figure 5: Healthcare Privacy and Patient Confidentiality

A fully distributed configuration means that unauthorized access is halted at the wireless network edge. This prevents an intruder from gaining access to a WLAN controller and possibly penetrating the core network. In addition, 24x7 air monitoring systems are available that scan the airwaves for unauthorized APs that might be attempting to connect to the facility's network.

RF Interference

Neighboring Wi-Fi devices and other sources can affect WLAN availability and interfere with users' ability to use the network. These sources can include medical equipment, guest devices, neighboring organizations with wireless networks, and any equipment that emits energy in the Wi-Fi bands, such as microwave ovens and wireless surveillance cameras.

Advanced WLANs have sophisticated RF management tools that can automatically detect interference, dynamically adjust power levels, and switch channels to sidestep congestion. Some vendors also have strong RF planning tools to select optimal locations for APs and avoid interference once deployed. However, because RF environments continually change, it is far more efficient to automate the network to self-adjust and self-heal in the presence of interference and failures. These tools vary among vendors.

Current Trends: Where Wi-Fi is Going

Closer to the Cloud

According to the survey, 68% of respondents are currently using a controller-based WLAN and 17% are already using a cloud-managed solution. However, of the respondents not using cloud at the moment, 18% are planning to implement or are evaluating a cloud-managed WLAN.

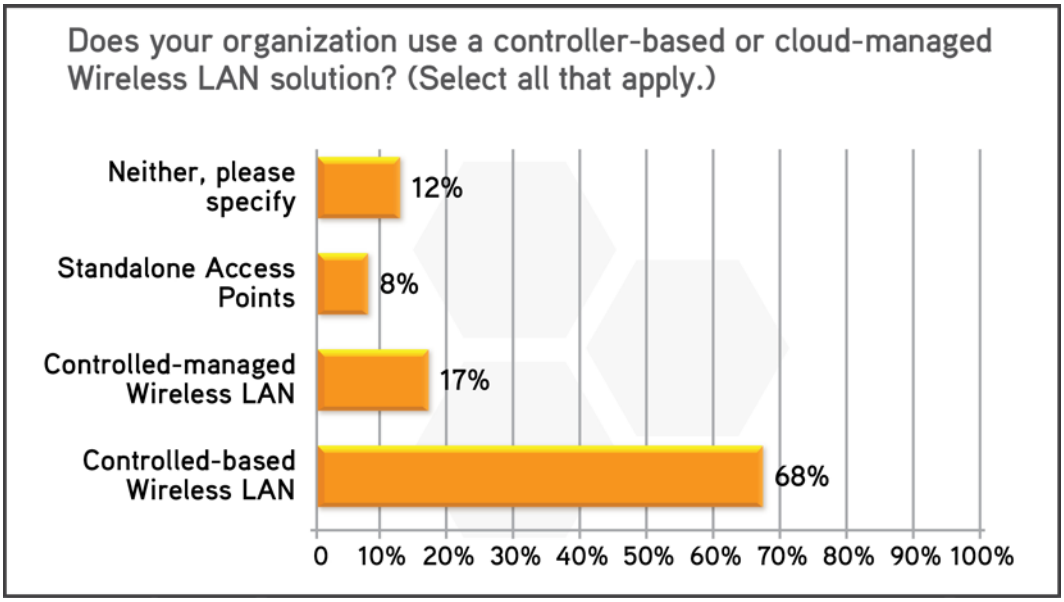

Figure 6: Spiceworks Healthcare Survey, March/April 2013

Moving To Simpler WLAN Management

With staff and resources in constant short supply, healthcare IT professionals are looking for ways to reduce the amount of time, staff, and effort required for managing their WLANs. Among respondents in the Spiceworks survey, 45% state that they are somewhat satisfied, not very satisfied, or not at all satisfied with their WLAN management platform.

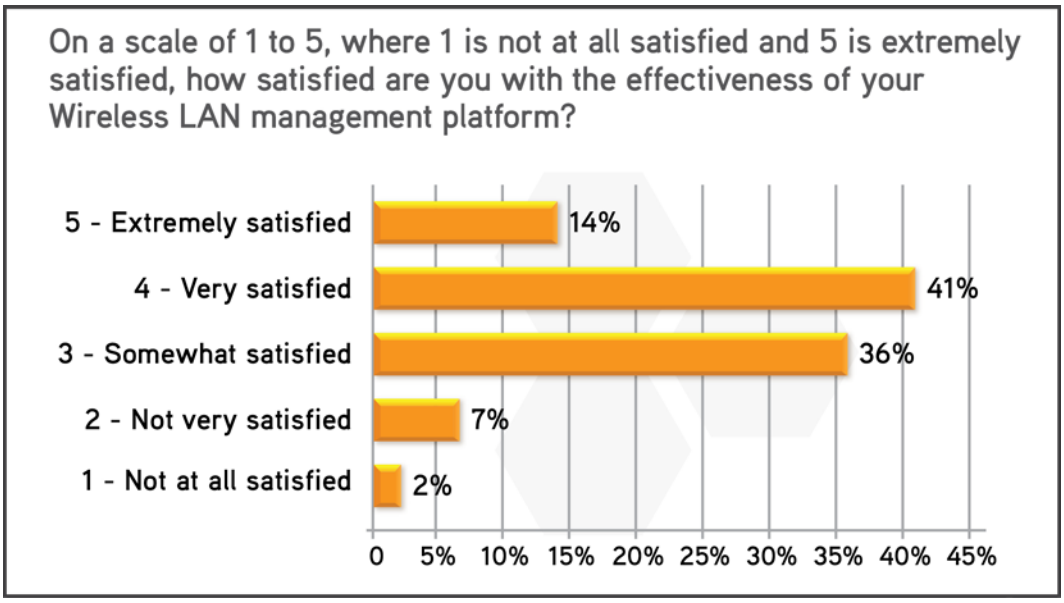

Figure 7: Spiceworks Healthcare Survey, March/April 2013

Some complaints about the existing solutions that are being used are that they lack useful features for simplifying operations and that the user interface is painful to use. Simplifying management can be achieved with management capabilities centralized to a single instance, either through an appliance or a cloud service. Centralization enables IT staff to create a policy and push it out to APs across the network over the air. Administrators thus gain the flexibility to change policies back and forth to account for temporary situations and allow new users groups to join the network.

Aerohive Delivers an Advantage

Aerohive's mission is to Simpli-Fi access to mission-critical applications with cloud-enabled, self-organizing, and automated Wi-Fi, switching, and routing solutions.

Aerohive delivers on this mission by providing automated, secure, and cloud managed Wi-Fi solutions that meet the requirements of even the most discerning healthcare organizations. For example, the Aerohive architecture uses self-organizing, mesh-capable APs that require no network controllers or additional hardware. HiveOS, the operating system that underpins all Aerohive products, allows Aerohive routers, switches, and Wi-Fi access points to discover one another as they are added or removed, share information to optimize network security

and performance, and dynamically adjust to network changes as needed. This capability is known as Aerohive's "cooperative control architecture." Auto-discovery and inter-AP communication can take place over the air or over the cable attached to an Ethernet switch, depending on network configuration.

In this way, wireless networks built on Aerohive technology eliminate the cost, performance, and availability issues associated with traditional controller deployments that create single points of failure, failover delays, and throughput bottlenecks. The Aerohive architecture strikes just the right balance of distributed intelligence and centralized management capabilities. Data forwarding, WLAN security, and performance-enhancement services, such as real-time packet prioritization, are distributed out to individual APs to minimize latency and to ensure that a failed WAN connection to another location won't interrupt users already on the network.

At the same time, network and system management capabilities are centralized through Aerohive's HiveManager Online Network Management Service. HiveManager Online is a cloud-based Software as a Service (SaaS) network management system for Aerohive network devices. HiveManager Online eliminates capital expenditure associated with dedicated network management appliances and shifts expenses into a pay-as-you-go model. This not only reduces the initial costs of network management, but also allows healthcare organizations to predictably grow the network to whatever size is needed. There are no management appliances to deploy, manage, or use rack space per location. Since it's a cloud-based solution, HiveManager Online simplifies an organization's ability to manage one or many locations. Network management can be done centrally by just one IT person using a Web browser from any location at any time. HiveManager Online offers the same simple policy creation, firmware upgrades, and centralized monitoring options as on-premises appliances without the need to deploy additional network devices. HiveManager Online is hosted within secure Tier IV SAS 70 Type II data centers, with scheduled backups and disaster recovery capabilities.

Pricing and scalability are very easily calculated with the Aerohive solution. Simply multiply the number of APs needed by the per-AP price, and then add the cost of the management for that number of APs. Customers have a choice of a management appliance, a VMware virtual appliance for private clouds, or Aerohive's cloud-based management service. There are no feature licenses or redundant components to worry about and no surprises.

For More Information

Data comes from a March-April 2013 Spiceworks survey of 109 IT professionals in the Healthcare industry that was commissioned by Aerohive. Of the respondents in the study, 36% came from companies with less than 100 employees, 51% from companies with 100-499 employees and 13% from companies with 500+ employees.

About Aerohive

People want to work anywhere; on any device, and IT needs to enable them -- without drowning in complexity or compromising on security, performance, reliability or cost. Aerohive's mission is to Simpli-Fi these access networks with a cloud-enabled, self-organizing, service-aware, identity-based infrastructure that includes innovative Wi-Fi, VPN, branch routing and switching solutions.

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, New Enterprise Associates, Inc. (NEA) and Institutional Venture Partners (IVP). For more information, please visit www.aerohive.com, call us at 408-510-6100, follow us on Twitter @Aerohive, subscribe to our blog, join our community or become a fan on our Facebook page.

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

International Headquarters
Aerohive Networks Europe LTD
The Court Yard
16-18 West Street
Farnham, Surrey, UK, GU9 7DR
+ 44 (0) 1252 736590
Fax: + 44 (0) 1252 711901