Healthcare Reference Architecture to Support Mobile Access for Point-of-care and Other Critical Applications
Healthcare Reference Architecture – Mobile Access Solutions for Point-of-Care Applications

Introduction .................................................................................................................. 4
Healthcare Reference Architecture................................................................................ 5
  Key Architecture Components.................................................................................... 6
Healthcare Use Cases................................................................................................. 7
  Application Performance and Availability............................................................... 7
  Security and Compliance.......................................................................................... 13
  Cloud-Enabled Networking for Remote Clinics......................................................... 18
  Management and Ease of Use.................................................................................... 17
Summary......................................................................................................................... 23
Introduction

Patient care is delivered from a growing number of places—some expected, others not. Of course, hospitals are the primary point of care delivery with caregivers needing access to patient records and data at the patient’s bedside, on nursing floors, outpatient exam rooms and emergency rooms. Treatment is increasingly being delivered through regional health centers, walk-in clinics, and urgent care facilities located in places such as supermarkets. And if current trends continue, patient monitoring and diagnostics via smartphone apps, such as AliveCor for monitoring heart rhythms, will enable patients to monitor conditions and receive care wherever they are located (The Future of Medicine is Now, Wall Street Journal, Dec. 31, 2012).

Wireless LAN (WLAN) and cloud networking technologies are dramatically changing care delivery. Initial WLAN deployments were driven by the need for reliable mobile voice and data access capabilities. Today, instruments ranging from diagnostic tools and monitoring stations to laboratory equipment are wireless, and caregivers access electronic medical records (EMR) applications and patient data from computer carts, laptops, tablets, and smartphones.

Healthcare IT administrators rely on wireless applications such as real-time location services for managing supply inventory; guest and patient Internet access to improve the care experience; voice applications, like Skype or Apple Facetime for easy personal communications; and data for enforcing security policies to meet HIPAA compliance. Advanced applications, such as medical imaging and biotelemetry, are driving further adoption—and demanding even higher performance and reliability from the WLAN. With wireless access central to many healthcare strategies, wireless networks are now considered critical healthcare infrastructure.

The Importance of a Healthcare Reference Architecture

Although standalone wireless networks have often been deployed ad hoc across healthcare organizations, many organizations are finding that they must implement a more comprehensive wireless networking architecture as a strategic asset. Reference architecture
Healthcare Reference Architecture – Mobile Access Solutions for Point-of-Care Applications

provides a blueprint for helping organizations construct secure, high-performance, and easy-to-manage wireless deployments across their entire organization—from the smallest remote clinic to (and throughout) the largest hospital.

Aerohive Networks’ award-winning wireless network architecture and solutions provide healthcare organizations with mission-critical reliability and remote site survivability to keep information flowing at the point of care. The Aerohive HiveOS operating system has a unique architecture that distributes intelligence throughout the wireless infrastructure, creating a naturally resilient and high-performance network. By fully using all of the available computing capacity, HiveOS can deliver all of the enterprise features required to support EMR and other critical applications, such as Voice over IP, guest access, and strong authentication and encryption capabilities needed for HIPAA compliance.
Reference Architecture for Healthcare

Figure 1 illustrates a wireless LAN (WLAN) deployment topology for a hospital, a data center, and one or more associated clinic. The data center hosts a premises-based version of the Aerohive HiveManager network management system, a HiveOS virtual appliance running the Layer 3 virtual private network (L3 VPN) gateway, authentication servers, and existing point-of-care applications. Although the clinic and hospital are displayed together, Aerohive’s flexible architecture allows either type of site to be deployed independently of the other without compromising features or functionality.

Remote Clinic

Data Center

Internet/WAN

Hospital

Figure 1: Point-of-Care Reference Architecture

The hospital’s wireless access points and switches are deployed according to Aerohive’s cooperative-control architecture to deliver unmatched application availability, security, and mobility. Aerohive access points identify, prioritize, and control application traffic at the network edge, helping ensure that critical medical applications are protected from performance degradation. The network supports 802.1x authentication against Active Directory or RADIUS and strong encryption, and Aerohive’s advanced private pre-shared key
(PPSK) technology enhances security for legacy wireless devices. Campus-wide seamless mobility is provided through Layer 3 tunneling. Users benefit from voice-grade roaming capabilities through embedded technology including 802.11i fast-roaming, 802.11r and 802.11k standards.

In Figure 1, the remote clinic’s Aerohive Branch Router (BR) provides a secure VPN connection to the data center. The router uses policies and configuration as the main hospital router and is managed from the same HiveManager application. With Aerohive’s cooperative control architecture, the local clinic retains all of its WLAN features and functionality in the event of an outage on the wide-area network (WAN) that breaks the connection to the data center. Access to applications is quickly restored over a backup 3G/4G link.

**Key Architecture Components**

Aerohive reduces the cost and complexity of hospital and distributed clinical deployments through cloud-enabled networking solutions based on Aerohive’s distributed intelligence architecture. Solutions include enterprise-class Wi-Fi access points, state-of-the-art gigabit switches, and easy-to-deploy routers.

| **Aerohive Access Point Family** | Aerohive’s 802.11n enterprise wireless LAN access points are an innovative class of wireless infrastructure equipment with cooperative control technology that provides the benefits of a controller-based wireless LAN solution, without requiring a controller or an overlay network. |
| **Aerohive Branch Routers** | Aerohive routers combine “work anywhere” mobility with enterprise routing functionality and complete security – all in a single device. The simple “plug and play” operation makes it easy for administrators to deploy hundreds or even thousands of remote/branch offices for their users. |
| **Aerohive Access Switches** | Aerohive Networks SR platforms combine enterprise-class access switching with cloud-enabled management, on-demand provisioning, and secure branch routing to provide the industry’s most advanced networking feature set to the edge of your network. |
Aerohive Virtual Appliance with L3 VPN Gateway

A lightweight, software-based solution that runs on VMware-compliant equipment, the gateway is designed to simplify VPN termination for thousands of remote branches.

Application Performance and Availability - Benefits of a Reference Architecture

Aerohive technology supports reliable, high-performance healthcare applications, security and HIPAA compliance, robust remote clinic networking, and simplified management. High reliability requires network design that effectively delivers redundancy and prioritizes traffic at key points in the network. Each network link—from the application server in the data center to a mobile caregiver—must be designed with resiliency and performance in mind. Aerohive’s cooperative control architecture enables:

24x7 Operation: Aerohive’s architecture avoids single points of failure and eliminates unnecessary maintenance windows.

User-based application control: Advanced application visibility, combined with HiveOS Quality of Service (QoS) features, deliver the control needed to ensure consistent application performance on a per-user basis.

Resilient RF: Advanced radio frequency (RF) management features and custom hardware design deliver exceptional performance in difficult environments.

Simple mobility: Standards-based roaming with 802.11i, 802.11r, 802.11k, and automatic Layer 3 tunneling deliver a simple and seamless mobile experience for critical applications.

24x7 Operation

Traditional WLAN designs unify multiple devices and present them to a “master controller” as a single device. This approach simplifies mobility and management but can create problems for maintaining the 24x7 operations required for healthcare.
Preventing Dead Zones
HiveOS is designed to distribute intelligence and traffic flows throughout the network, instead of centralizing them in a single device. HiveOS protocols dynamically organize devices into “hives” to enable redundancy and resiliency for roaming. These protocols enable HiveOS devices to automatically reorganize themselves around failures and effectively keep network interruptions localized. For example, if an access point fails or loses power, Aerohive’s Advanced Channel Selection Protocol (ACSP) automatically increases the transmit power of neighboring access points to prevent dead zones. Likewise, the Aerohive Mobility Routing Protocol (AMRP) enables redundant path calculations for mesh failover and redundant storage of client session information, including encryption keys, firewall, and QoS policies.

Maintaining Uptime During Software Upgrades
The traditional approach of concentrating data traffic and synchronizing software versions across the WLAN can create challenges to software upgrade processes. Typically, software upgrades on controllers automatically flow to the associated access points, effectively unifying downtime and maintenance windows across the campus or even across all remote clinics managed using the same system. Therefore, the impact of a single software upgrade can reach across the entire organization.

Aerohive’s cooperative control architecture gives network administrators flexibility to individually coordinate software upgrade maintenance windows for different areas on the campus or for each clinic.

Scaling a Deployment
The same flexible protocols that prevent dead zones and simplify upgrades make it easy to increase the scale and performance of an Aerohive deployment—while the network is operating. Adding capacity is as easy as adding access points. The access points will automatically discover HiveManager, and with auto-provisioning, are automatically configured and joined to the network. As each access point comes online, it augments the WLAN’s available processing and forwarding capacity, effectively upgrading total network
capacity without disrupting operations. There is no need to manage or balance AP capacity licenses, reconfigure the network, or re-test redundancy schemes. As new high-performance wireless technologies emerge, a distributed architecture enables organizations to completely avoid “forklift upgrades” of central controllers.

<table>
<thead>
<tr>
<th>24x7 Challenges</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Mobility without traffic bottlenecks or narrow points of failure</td>
<td>Aerohive’s Cooperative Control architecture enables the dynamic reconfiguration of network resources to reduce vulnerable stress points, enable selective network maintenance, and create a solution that automatically scales to the size of the deployment.</td>
</tr>
</tbody>
</table>
| Coordinating maintenance windows with caregiver staff in multiple locations | Advanced Channel Selection Protocol (ACSP): Enables automatic channel and power configuration, and protects against dead-zones in the event of AP failure.  
Aerohive Mobility Routing Protocol (AMRP): Client session and encryption key distribution for voice-enabled roaming, and protection against Ethernet faults by enabling redundant data-paths by meshing to peer access points. |
| Network Expansion and reorganization                | Dynamic Network Extension Protocol (DNXP): Automatically tunnel Layer 3 roamed clients between members of a hive, providing an inherently redundant and resilient method for campus-wide roaming of critical EMR and voice services. |

**User-Based Application Control**

Ensuring reliable application delivery over a shared mobile network can be challenging. Caregivers, consulting physicians, and patients or guests have different access requirements and usage patterns. The network must be able to identify applications, apply QoS settings to prioritize access, and block unwanted applications across both the WLAN and WAN.

As illustrated in Figure 2, Aerohive’s advanced application visibility and control capabilities deliver an unprecedented level of information about applications in use. With an advanced, deep-packet-inspection engine, HiveOS can identify even the most evasive applications, such as BitTorrent and Skype, without the errors and limitations found in other wireless network operating systems. Custom firewall rules can be added to prioritize specific applications, such as EMR, over other applications by using HiveOS’s advanced QoS features to identify traffic destined to specific application servers. Identified application traffic can be controlled on a per-user basis, allowing over-the-air prioritization; Differentiated Services Code Point (DSCP) or
802.1p marking for upstream network prioritization; bandwidth throttling; or even complete blocking on a per-policy basis.

Fine-grained control allows robust prioritization of network resources, enabling high availability and performance for critical EMR applications while also delivering less-critical applications without fear of disruption.

**Resilient RF**

Delivering the best possible wireless performance for healthcare applications requires a combination of advanced software features and purpose-built hardware. HiveOS
Healthcare Reference Architecture – Mobile Access Solutions for Point-of-Care Applications

incorporates a number of innovative features, which deliver the reliable performance required for always-on medical applications.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACSP</td>
<td>Enables automatic channel selection and adapts transmit power to minimize co-channel interference and dead zones.</td>
</tr>
<tr>
<td>Band Steering &amp; Client Load Balancing</td>
<td>Distributes clients across access points and radio bands to optimize performance of the entire system.</td>
</tr>
<tr>
<td>Wireless QoS with Wi-Fi Multimedia (WMM)</td>
<td>Allows prioritization between different classes of traffic to enhance application performance for VoIP, EMR, and other critical applications while still allowing lower priority applications to share the network.</td>
</tr>
<tr>
<td>WMM-Admission Control (WMM-AC) and Unscheduled Automatic Power Save Delivery (UAPSD)</td>
<td>WMM-AC allows voice clients to request bandwidth reservations from the network to ensure call availability and quality. UAPSD optimizes power-save communications between clients and the network to extend the battery life of client devices.</td>
</tr>
<tr>
<td>Airtime Fairness</td>
<td>Shares access among clients based on airtime consumed rather than bandwidth, effectively preventing older or more distant clients from affecting application performance.</td>
</tr>
<tr>
<td>Multicast to Unicast Replication</td>
<td>Converts unreliable multicast traffic, such as “push-to-talk” VoIP, into acknowledged unicast traffic, improving audio quality and range.</td>
</tr>
<tr>
<td>Advanced Hardware Design</td>
<td>High-quality discrete RF components deliver cleaner signals and higher receive-sensitivity, increasing the performance and range of low-power mobile devices.</td>
</tr>
<tr>
<td>Spectral Analysis</td>
<td>Quickly diagnoses and troubleshoots non-Wi-Fi interference that is adversely affecting application performance.</td>
</tr>
</tbody>
</table>

**Simple Mobility**

Caregivers are always on the move, needing access to applications, data, and voice capabilities regardless of where they are located. In small clinics with only one virtual LAN (VLAN) for clients, mobility is easy. Enabling applications to move seamlessly with users across network zones in a larger network has been a challenge in traditional WLANs.

HiveOS enables seamless roaming by using automatic tunneling to preserve IP address mobility across the network. For demanding applications, such as voice, HiveOS uses standards-based 802.11 fast roaming. For implementations requiring more than one VLAN, Layer 3 tunneling is required to preserve application sessions as the client moves across router boundaries. HiveOS automatically distributes responsibility for establishing tunnels to the access points at the network edge. This approach eliminates data round trips through the data center, preserving application performance, and scales by increasing the network’s forwarding capacity as new
devices are added. HiveOS uses the following technologies to enable fast, secure mobility for voice and critical healthcare applications:

- **802.11i**: Provides support for the widely implemented “fast-roaming” capability, including opportunistic key caching (OKC), which enables sub-50ms voice-grade roaming for 802.1x clients by proactively distributing keying material to the access points that a client can roam to, before it actually roams.

- **802.11r**: This newer standard focuses on increasing roaming performance and predictability. It more clearly specifies how keying material is distributed through a WLAN. 802.11r FT (fast transition) roams use fewer frames to authenticate and associate the client, resulting in faster roam times. Client support for 802.11r is not yet widespread but many vendors are beginning to adopt support.

- **802.11k**: Another IEEE standard typically mentioned with 802.11r, this focuses on enabling the network to inform clients of possible roaming candidates. Together, these two standard make up the Wi-Fi Alliance “Voice-Enterprise” certification program.

- **Customizable SSID and radio profiles**: Interoperability with legacy devices is an ongoing challenge. Dedicated medical devices may have special RF restrictions, so it is important to have low-level control over the WLAN. HiveOS allows advanced customization, like advertised data rates and power-save modes on a per-SSID basis, to enable maximum interoperability and smooth roaming for the widest variety of client types.

**Application Performance and Availability Use Case**

HiveOS brings 24x7 operation, user-based application control, resilient RF, and simple mobility together into an architecture that can deliver medical-grade application performance and availability. Figure 3 illustrates how the Aerohive healthcare reference architecture addresses each portion of the use case, forming reliable, scalable, and high-performance solution.
Figure 2: Application Performance and Availability Architecture
Security and Compliance
Protecting the network and patient data from unauthorized access is a critical piece of HIPAA compliance. Authentication, encryption, and security enforcement must be implemented in a way that still allows convenient Internet access by caregivers and guests. HiveOS provides the capabilities needed to safeguard electronic protected health information (EPHI) while still allowing needed access.

HIPAA-Compliant Security
HiveOS is fully HIPAA-compliant for:

- **Person or entity authentication:** HiveOS supports strong authentication through 802.1x RADIUS or direct Active Directory integration. In cases where legacy devices do not support the 802.1x standard, the HiveOS PPSK feature allows multiple Wi-Fi Protected Access (WPA) or WPA2 Pre-Shared Keys (PSKs) to be used on the same wireless network. Each PPSK can have a separate user policy, allowing entity or user-based authentication based on a unique encryption key.

- **Access control:** HiveOS supports per-user access controls by mapping authenticated users to user policies. The policies can specify stateful firewall rules (with application-aware control), VLAN membership, and QoS for the granular access control necessary to compartmentalize access to patient data and point-of-care applications. HiveManager includes multi-user access control, allowing administrators to define separate account roles that grant access to monitoring and troubleshooting data without the ability to reconfigure network access.

- **Audit control:** HiveOS supports RADIUS accounting and external syslog services to enable extensive auditing of user access and activity. HiveManager has extensive reporting capabilities available on demand or scheduled for regular email delivery.

- **Transmission security:** Aerohive access points are certified for WPA and WPA2 wireless encryption. They also include support for older and less secure Wired Equivalent Privacy (WEP) encryption. Branch routers, switches, and virtual appliances running HiveOS also support IPsec VPNs to securely transmit protected data across the Internet or 3G/4G mobile networks.
Consulting Physicians
Consulting physicians present a unique challenge. Not being full-time employees of the organization, they have their own laptops and mobile devices, which need to be provisioned for access to a set of the organization’s services. Typically, 802.1x authentication or simple PSKs have been used to enable wireless access. However, each of these methods has potential problems that can lead to operational or security issues.

HiveOS PPSK™ technology overcomes the security limitations of PSK, enabling a secure and easy-to-manage “Bring Your Own Device” (BYOD) option for healthcare organizations and their affiliated physicians.

<table>
<thead>
<tr>
<th>Feature</th>
<th>802.1x</th>
<th>PSK</th>
<th>PPSK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple configuration</td>
<td>☒</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Per-User policy</td>
<td>✓</td>
<td>☒</td>
<td>✓</td>
</tr>
<tr>
<td>AES Encryption</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Wide device support</td>
<td>☒</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Administrative staff can pre-generate PPSK keys, associate them with user profiles to provide access controls, and then distribute a single key to physicians for use on their own devices. Each key can be configured to be usable on a configurable number of simultaneous devices, effectively discouraging sharing.

If strong authentication using 802.1x is desired or required, HiveOS integrates with a number of mobile device management platforms, as well as device configuration utilities designed to automate much of the setup and certificate distribution required by the 802.1x standards.

Guest and Patient Access
Guests and patients are unauthenticated users who need network access to the Internet and some services. HiveOS features permit access while maintaining the security, privacy and performance of the rest of the network:
• **Per-user stateful firewall:** Each HiveOS device is capable of enforcing firewall rules at the network edge, preventing unauthorized traffic from entering the rest of the network. Firewall rules can be applied to both incoming and outbound traffic.

• **Guest tunneling:** In addition to the dynamic tunneling used for Layer 3 mobility, HiveOS also supports statically assigned tunneling. By placing a HiveOS device in the Internet DMZ enabling static tunneling for guest access, all guest traffic is completely isolated from the main network and tunneled back to the DMZ where it can access the Internet.

• **Captive web portal:** HiveOS includes default templates for captive web portal and “click-to-accept” pages that can be easily customized to match the organization’s acceptable use policy.

• **QoS and application control:** After security, the main concern about providing guest access is usually application performance. HiveOS has extensive QoS features to prioritize or de-prioritize traffic over the air. HiveOS can apply DSCP and 802.1p marking for appropriate prioritization over the wired network. Additionally, HiveOS’s application awareness and control allows the organization to throttle or block potentially disruptive or unwanted applications.

• **Peer-to-peer traffic blocking:** HiveOS can block communications between wireless stations, preventing viruses and malicious attacks between guest users. Additionally, a variety of security measures can prevent malicious behavior such as ping-scans, multiple IP address usage, and flood attacks.

• **Encrypted guest access:** If authenticated, encrypted guest access is desired, Aerohive’s ID Manager cloud-managed guest access system can be integrated with the WLAN. The ID Manager allows for self-service kiosk functionality with SMS, Twitter, or Email authentication to deliver time-based access guest credentials. Having the credentials delivered via an authenticated path verifies guest identities and can prevent fraud.

**Security Architecture**

The advanced security features in HiveOS provide a solid foundation for building a HIPAA-compliant network. Strong encryption and authentication, combined with advanced access control and auditing, provide the tools needed to safeguard electronic protected health information. Unique features, like PPSK, allow new ways to enhance security for consulting physicians and legacy medical devices while ID Manager enables encrypted and verified
guest options. Figure 4 illustrates how these elements can be utilized in the reference architecture to enhance security and compliance.

Figure 3: Security and Compliance Architecture
Cloud-enabled Networking for Remote Clinics Use Case

Aerohive’s cloud-enabled networking enables fast, easy WLAN deployment for clinics of all sizes. Automated provisioning and IP address assignment accelerate deployment by eliminating the need for extensive onsite technical expertise. Advanced security and encryption preserve patient privacy. HiveOS and 3G/4G-enabled backup WAN links maximize uptime for remote clinics, even during WAN link outages. The HiveOS distributed architecture supports full enterprise functionality, regardless of location, for seamless mobility and application access across sites.

Management and Deployment

HiveOS cloud-enabled networking greatly simplifies WLAN deployment for remote healthcare clinics. With Aerohive Cloud Redirector, administrators direct HiveOS devices to an on-premises version of HiveManager, where default configuration profiles are automatically installed based on device type, origination subnet, or unique device serial number. After provisioning, branch routers initiate IPsec tunnels to a HiveOS Layer 3 VPN gateway. Access switches and access points repeat the provisioning process until the entire network is up and running without technical personnel onsite. Once provisioned, HiveOS devices use one set of user policies to help ensure consistent security and privacy enforcement. Expanding a deployment is just as easy, whether it is adding additional sites or additional capacity at existing sites.

With multiple locations, both wired and wireless networks have to be easy to manage, maintain, and monitor. Typical solutions require multiple consoles for managing remote connectivity, security, and troubleshooting across routers, switches, and access points. However, HiveManager provides a centralized interface for everything from integrated IP address management to auto-provisioning and consistent policy deployment across all HiveOS devices. An administrator can manage thousands of devices as easily as one.

Security

One of the keys to a successful security policy is simplicity. Having to implement user policies across diverse devices and management systems is prone to error, due to different features across platforms. With HiveOS and HiveManager, administrators can easily configure and
manage unified user policies across all HiveOS devices and ensure enforcement—even during a WAN outage.

In remote clinics that do not have a dedicated Active Directory server, it is difficult to designate a secure access method to use in the event that the data center is inaccessible. Lack of connectivity to a domain controller prevents 802.1x clients from authenticating in most networks, disabling connectivity to all applications and the Internet. With cloud-based application services, the ability to preserve access to local and Internet resources becomes increasingly important. HiveOS allows a deep level of integration with Active Directory that enables Protected Extensible Authentication Protocol (PEAP-MSCHAPv2) authentication credentials to be cached. With this approach, previously authenticated clients can reconnect securely while a domain controller is unavailable. Additionally, Aerohive’s unique PPSK feature provides unique per-user encryption and policy enforcement without depending on data center connectivity.

**WAN Reliability**

Providing reliable access to critical medical applications at remote clinics requires a flexible and adaptive solution. HiveOS provides network designers with features that help maintain WAN uptime:

- **Redundant WAN interfaces**: The key to maximizing application availability is redundancy. Every WAN technology is subject to failures beyond the administrator’s control. Using HiveOS, administrators can designate up to three WAN uplinks for a resilient, cost-effective WAN redundancy scheme.

- **3G/4G support**: HiveOS includes built-in support for 3G/4G USB modems, allowing inexpensive redundancy or primary access in hard-to-wire or temporary locations.

- **Per-Interface IP tracking**: Each WAN uplink can be configured with a separate list of tracking IPs, allowing WAN failover determination to be tied to a specific network path instead of just the VPN gateway. This feature preserves Internet connectivity in the event of a data center outage.

- **Redundant VPN gateways**: HiveOS branch routing includes the option to configure a backup VPN gateway for VPN links or even full data center redundancy.
Implementing point-of-care mobile applications at remote clinics can be simplified by HiveOS easy deployment, distributed architecture, and advanced reliability features. Even the smallest, most remote clinic can operate with full enterprise features, security, and high availability.

Figure 4: Remote Clinic Architecture
Healthcare Reference Architecture – Mobile Access Solutions for Point-of-Care Applications

Deployment and Management Use Case

Deploying and managing remote clinic and mobile-optimized WLANs can be easy and cost-effective. Aerohive’s automatic provisioning process makes deploying access points or cloud-enabled remote clinic networks easy. Once deployed, HiveManager’s dynamic, interactive HTML5 interface enables unified configuration, monitoring, and troubleshooting of all HiveOS devices from any web browser. Unified policies for wired and wireless users across the infrastructure improve security and performance while reducing operating costs. Advanced tools for monitoring and troubleshooting also speed problem resolution to improve users satisfaction.

Deployment

Cloud-enabled networking greatly simplifies network deployment in any location. Deployment costs are directly tied to the amount of time it takes to move from unboxing equipment to turning on service. Automatic discovery and provisioning, unified wired/wireless profile support, and public/private cloud management enables rapid and reliable deployment of access points, branch routers, and access switches.

Configure profiles in HiveManager.
Import device serial numbers into Cloud redirector.
Ship devices to their locations.
Mount devices, connect, power on.
Wait for the LED to turn white.

Cloud-enabled HiveOS devices will automatically request a Dynamic Host Configuration Protocol (DHCP) address and can discover the IP address of their HiveManager management platform through IP broadcast, DHCP options, Domain Names Service (DNS) lookup, or over the Internet with the Aerohive Redirector. Once the device locates HiveManager, it automatically downloads its configuration and optionally upgrades the HiveOS software to a specific version.
Healthcare Reference Architecture – Mobile Access Solutions for Point-of-Care Applications

The HiveManager interface makes it easy to build configurations and manage user policies across all HiveOS access layer devices. HiveManager creates a single network policy that associates SSIDs with wireless devices, device templates with wired devices, and common user policies across the network.

With HiveManager’s Google Maps integration, administrators can quickly create scaled topology maps of buildings for planning WLAN coverage. Maps can be arranged in a customizable hierarchy for easy organization by city, region, campus, or other criteria. The hierarchy can then be used to customize location-specific configurations through HiveManager’s device classification feature. HiveOS devices on maps in one region can share the same configuration as devices in another region, but with region-specific definition of elements like VLANs and IP addresses. This capability allows one configuration policy to authenticate against one RADIUS server for devices on the West coast and use a different RADIUS server for devices on the East coast to reduce latency.

Auto-provisioning templates can be configured in HiveManager for rapid deployment with minimal chance of human error. Each template can be associated with specific device models or subsets of devices based on serial number or even local IP subnet. In addition to determining default device network and radio profiles, templates can automatically associate devices to specific areas on the topology hierarchy based on the IP subnet where they receive a DHCP IP address. When combined with device-classification rules that customize configurations per location, even complicated multi-site deployments can be completely automated.

Software upgrades are also greatly simplified. HiveOS distributed architecture enables organizations to avoid the problem of “unified downtime” since there is no master controller. Individual sites, or even individual devices, can be upgraded separately, streamlining new software release pilots and maintenance windows. Software upgrades can take advantage of topology maps to easily assign specific devices for upgrade while leaving the rest of the deployment unaffected.
Management
Successful deployments require monitoring tools that provide fast, accurate troubleshooting and resolution—especially for 24x7 healthcare environments. HiveManager tools provide at-a-glance information to quickly identify and resolve issues that might impact application performance:

- **Customizable dashboard**: HiveManager includes a customizable dashboard with up to six perspectives for filtering and displaying time, user, and device data. Widgets zoom in for more detail. Customizability simplifies creation of per-admin views and puts specific information right at administrators’ fingertips.

- **Scheduled reports**: Any perspective in the dashboard can be easily converted to a scheduled PDF report and delivered automatically by email. Additionally, HiveManager includes a range of canned and customizable reports for client Service Level Agreements (SLAs), security compliance, inventory, performance, and many other attributes.

- **Client health**: Quickly identify struggling clients with HiveManager’s Client Health indicator. Each client’s performance is monitored continuously, providing an at-a-glance summary of a client’s radio, network, and application health through an intuitive color-coded system.

- **Client Monitor**: Logging and debugging information for a single client can be aggregated across multiple access points to gain a unified view of client roaming and connection behavior. Intelligent filtering allows administrators to focus on DHCP, authentication, 802.11, or RADIUS messages for quick access to the data needed to resolve client connectivity issues.

- **Topology and custom filtering**: As deployments grow, so does the amount of monitoring information. HiveManager filtering tools save time by filtering device and client information by location, user-defined tags, VLAN, or even client operating system.

- **Spectral analysis**: The HiveOS real-time spectrum analysis capability enables rapid identification and location of non-Wi-Fi interference sources. Administrators can view spectral data from any HiveAP connected to the HiveManager through the web-based HiveManager interface. They can then use the spectrum analyzer to investigate interference at any location with supported HiveAPs.
• **Wireshark remote capture interface**: Direct integration with Wireshark makes packet captures simple. Aerohive access points can be configured as individual Wireshark remote capture interfaces (with authentication) from HiveManager, enabling start-and-stop frame captures from wired or wireless interfaces on multiple devices simultaneously, while the radios are still in service.

• **Remote diagnostics**: HiveManager provides a host of remote diagnostic tools for verifying network operation. Tools include LDAP server lookups, RADIUS authentication verification, and many other device-specific commands for displaying logging, status, and peer information.
Deployment and Management Architecture

Cloud-enabled networking changes the way networks are deployed and managed, as shown in Figure 6. Automated provisioning, profile- and location-based configurations, and unified wired and wireless user policies reduce operational cost and the need for onsite technical experts. Cloud management can be performed from any HTML5 device with advanced monitoring and diagnostic tools to reduce downtime and improve user satisfaction. Finally, the HiveOS intelligent distributed architecture eliminates “unified downtime” across the entire organization, enabling custom maintenance windows at each site or avoiding them entirely.

Figure 6: Deployment and Management Architecture
Summary

Aerohive’s mobile access solutions for healthcare provide a reliable, high-performance and easy-to-use infrastructure that meets the needs of mission-critical EMR and other applications used by mobile caregivers. HiveOS’s intelligent distributed architecture delivers on the promise of cloud-enabled networking today by bringing the following benefits to caregivers and network administrators:

• **Application performance and availability**: Enabled by advanced application visibility and control, combined with an intelligent distributed architecture that enables 24x7 operations.

• **Security and Compliance**: Backed by strong authentication and encryption, per-user unified policy for wired and wireless clients, and unique features like Private PSK to enable improved security and 1:1 user mapping for consulting physician and BYOD access.

• **Remote clinic deployments**: Without compromising available enterprise features or security, 3G/4G connectivity options for redundancy or rapid deployment, and continuing network availability when the data center is not available.

• **Management and troubleshooting abilities**: Lower operating expenses by enabling flexible deployment and upgrade options, a centralized HTML5 enabled dashboard, and advanced troubleshooting tools which allow rapid remote diagnosis of issues impacting client performance.
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 enterprise 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.