

The iEverything Enterprise

Understanding and Addressing IT's Dilemma
in a Bring Your Own Device (BYOD) World



Table of Contents

Introduction 3

The Impact To IT 4

Aerohive: Solving the Smart Device Dilemma 5

Cooperative Control: Eliminating Architectural Limitations..... 5

Identity-based Application Access: Your Device or Mine? 6

Simpli-Fi: Do more with less 9

Conclusion..... 11

Introduction

Virtualization, cloud computing, and wireless technology are fundamentally changing enterprise computing, providing revolutionary gains in productivity and cost savings. Powerful enterprise applications can now be delivered to almost any device, anywhere, at any time and take advantage of tremendous computing power available in consumer devices, such as smartphones and tablets. Regardless of whether these devices are corporate issued or personally owned, almost every IT department is experiencing the effects of unprecedented smart device and "Bring-Your-Own-Device" (BYOD) policy adoption in their enterprise.

These changes demand that IT organizations think strategically about their Wi-Fi™ infrastructures, so that they can maximize the benefits of mobility and virtualization while helping ensure the flexibility needed to accommodate rapid growth and changing user needs. Integrating this new world of mobile, virtual computing begins with selecting the right wired and wireless access infrastructure that can:

- Scale to support many high-speed devices without service interruption
- Easily integrate users' diverse devices, whether company-issued or BYOD
- Provide secure, reliable access to enterprise applications based on the users' identities
- Help eliminate inconsistent wireless performance
- The Computing Paradigm Shift - Mobility Changes Everything

Just a few short years ago, if you claimed that "everything will access the network wirelessly and wires will be obsolete from the network access layer," you would have been laughed out of the room. Since the 1990s, Wi-Fi has been implemented in laptop computers and by sheer momentum usage grew rapidly. However, wireless access remained little more than a convenient way to access basic services while away from your desk. Desktops and laptops continued to have wired network connections for their primary access and no IT manager in his right mind considered delivering mission-critical applications wirelessly. In 2007 about 300 million Wi-Fi devices were shipped, according to the Wi-Fi Alliance, and still Wi-Fi was not broadly leveraged for primary access.

However in 2007, Apple's introduction of the Apple iPhone™ and iPod™ Touch changed everything. Although these devices did not greatly increase the number of Wi-Fi devices shipped, they demonstrated distinct use cases for how users could change their daily routines to incorporate mobility and increase productivity both at home and at work. The iPhone™, the iPad™, and the many smart devices that have followed since all have enough computing power to run business applications and enable robust, simultaneous voice and video communications. These devices, their inherent computing power, and their ease of use spurred all new use cases for smart devices and drove Wi-Fi adoption by consumers, who began bringing them to work and demanding to use them to become more productive which is the genesis of the BYOD phenomenon. Additionally, commercial enterprises began to realize that leveraging virtualization on these low-cost devices would allow users to securely and reliably run mission critical operations.

A second trend, cloud computing, is contributing to a seismic change in how IT delivers services and applications and how users access them. When IT-enabled capabilities are delivered as a service ubiquitously to multiple users, they open the door to almost unlimited computing power on any device, anywhere, at any time.

Enterprises are not wasting any time taking advantage of BYOD and consumer device productivity enhancements. Analysts forecast that the number of devices shipped into the enterprise without any wired Ethernet ports exceeded the number with Ethernet ports at the end of 2011. The total

number of Wi-Fi devices shipped in the enterprise will quadruple from 2009 to 2014¹. IT organizations are beginning to recognize that Wi-Fi is a strategic, primary-access platform for application delivery, instead of just a convenient wireless connection. Users are relying on their smart devices, together with public or private cloud applications, to access business-critical information anywhere, anytime.

The Impact To IT

As wireless becomes the primary mode of application access, it changes IT's approach to selecting and implementing the network's access layer. IT departments must ensure reliability, security, and scalability for a wide range of devices as users' work migrates from PCs, laptops, local applications, and wired local area networks to smart devices, cloud applications, and wireless access. At the same time, with little budget for adding staff, IT must somehow manage everything without over-taxing existing resources.

This transformation presents multiple challenges:

- BYOD and company-issued smart devices are no longer simple text-based email readers. Rather, they are high-resolution, video-capable devices that are purely wireless and mobile.
- Applications being run on smart devices are robust, real-time, and mission critical. Recent studies indicate that almost 66 percent of the world's mobile data traffic will be video by 2014. Mobile video will grow at a CAGR of 131 percent between 2009 and 2014². Demanding applications combined with rapid growth can quickly overwhelm existing wireless local area network (WLAN) architectures, significantly affecting users' experiences and productivity.
- Although IT budgets are increasing slightly, implementing a wireless network that can handle rapid growth and maintain optimal user experience must remain affordable and manageable.
- Wireless infrastructure introduces a connectivity methodology that is more unpredictable than IT departments have managed in the past. Decades of wired network usage have streamlined IT into an efficient operation capable of solving many networking problems with the least expensive resources. In fact, a best practice for IT is achieving 65 percent to 80 percent of trouble tickets being solved by inexpensive level-1 support teams. With wired networks this was relatively easy to do because wires eliminated many variables. However, traditional wireless networks require wireless experts, not level-1 support staffing, making it difficult for IT departments to support a massive influx of smart devices and a new access network with the same resources.
- CIO initiatives must balance the cost savings of "bring your own device" initiatives and virtual desktop infrastructure (VDI) with allowing employees to access business critical applications on the same devices as their personal apps and data. In some cases, consumer-grade devices are replacing expensive specialized hardware for specific applications. However, CIOs do not want these devices used for non-business purposes.

¹ "Market Analysis Perspective (MAP) Enterprise Communications Infrastructure Market" IDC Nov 2010

² Cisco Visual Networking Index: Forecast and Methodology, 2009-2014

Aerohive: Solving the Smart Device Dilemma

Life in a post-PC world has begun, and the combination of enterprise applications with triple or quadruple the existing number of smart devices and BYOD corporate policy adoption has created numerous challenges for IT. Aerohive Networks, a networking company with a history of innovation, reduces the cost and complexity of wireless networks with cloud-enabled, distributed Wi-Fi and routing solutions for commercial enterprises, including their branch offices and teleworkers. Aerohive's award-winning cooperative control Wi-Fi architecture, public or private cloud-enabled network management, routing, and virtual private network (VPN) solutions give IT mission-critical reliability with granular security and policy enforcement, and high scalability.

Aerohive built the future into its system and removed the architectural limitations of the wireless access layer. Aerohive delivers an access infrastructure that connects users to mission-critical applications reliably on any device and leverages patent-pending cloud infrastructure to revolutionize wireless operations to allow IT departments to do more with less. Aerohive eliminates architectural limitations of traditional WLANs, supports identity-based access, and enables delivery of mission-critical applications and services to any user and device, anywhere, at any time.

Cooperative Control: Eliminating Architectural Limitations

There are currently three kinds of wireless LAN architectures available today which attempt to deal with the architectural challenges of the post-PC enterprise:

- Centralized
- Hybrid: Some functions are centralized and some are distributed to the network edge
- Distributed: No central appliance. Control functions are distributed among a grid of edge devices

The controller-based, centralized model for enterprise Wi-Fi systems, developed in the late 1990s and popularized around 2003, enabled companies to deploy hundreds or thousands of access points (APs) without requiring manual administration of every device. Faults, wireless and network configuration, Quality of Service (QoS), and security management could be handled from a single, centralized device known appropriately as a "controller." It was an innovation for network management.

In 2003, when enterprise Wi-Fi usage began to be driven by laptop usage, the 802.11a/b/g Wi-Fi standards supported data rates reaching a theoretical maximum of only 54 Mbps per device. As a deployment architecture, controllers delivered sufficiently high performance and network bottlenecks were rarely noticeable because data throughput was relatively low per client, Wi-Fi was only available in laptops, and wireless was not heavily used for delay-sensitive applications like voice or video. Additionally, application demands were relatively low, even the best laptop could only run 1.13 Ghz with a single-core processor, and video communication was non-existent.

Today, three forces have combined to make this centralized model a severe architectural limitation:

- **Faster speed:** Wi-Fi can now achieve data rates of 450 Mbps per client—833 percent faster than in 2003.
- **Distributed access:** Access to enterprise applications is increasingly distributed among end devices, users, and locations.
- **Powerful smart devices:** Smart devices sport dual-core, 1Ghz processors with graphics co-processors and increasingly use the latest video and voice applications.

Some Wi-Fi vendors have built colossal controllers to keep up with increasing throughput demands. However these super-controllers do not address the limitations imposed by the increasingly distributed nature of users connecting to applications. The combination of massive growth in wireless usage and increasingly distributed nature of work simply destroys the centralized model.

Another approach to dealing with centralized systems is to retrofit the architecture using distributed data forwarding, also called local forwarding. This technique allows the system to forward network traffic at the AP without going back to the main controller, alleviating controller and WAN bottlenecks. However, this approach means that the devices controlling security and QoS never act on the data. Without the controller applying stateful security and QoS policies, application performance can be disrupted.

Non-stop Networking

Aerohive has relentlessly focused engineering on realizing a vision of “non-stop wireless.” Its Cooperative Control Architecture is an inspiring reinvention of the control model for wireless networks. The Aerohive Cooperative Control Architecture creates a wireless network that maximizes network availability by removing any single points of failure. Every Aerohive device participates in grid-computing to process data and control and manage the network as a group, sharing state and other information through control protocols. This is the same model of control and inherent redundancy used in the largest network on earth – The Internet. Just as routers in the Internet use control and routing protocols to create the inherent capability to route around trouble and maintain the state of every communication even when a single routing node goes down, Aerohive’s Cooperative Control Architecture doesn’t force any single AP to be responsible for all management and security, and therefore, the system is inherently redundant with no single points of failure.

This architecture provides the benefits of centralized management of fault, wireless and network configuration, security, and QoS but with the actual data forwarding and policy enforcement occurring at the point closest to the client. The Cooperative Control Architecture inherently relieves the requirement to re-architect the enterprise network for the massive influx of smart devices while allowing the scale of the wireless access layer to be limited only by the coverage area and not the total throughput of the users.

Identity-based Application Access: Your Device or Mine?

Is it possible as an IT department to simultaneously decrease capital expenditures while increasing productivity? That is exactly what has the IT world buzzing today. There are many fancy names for it—“Consumerization of Enterprise IT” or “Bring your own device.” Powerful, inexpensive consumer devices purpose-built for productivity on the move have many CIOs looking for the best way to use these devices for reliable delivery of mission-critical applications.

Achieving simultaneous cost savings and process and productivity improvements can happen only with answers to important questions:

- Who owns the device? How is the user's identity established?
Security is always a top concern. With smart devices, the user's identity is key because it determines which resources they can access and from where.
- How do you enforce non-work related application usage policies?
With consumer devices, users can sometimes run applications that detract from business objectives. If there is a policy against non-business usage, how is that prevented?
- How does one make sure the devices have deterministic access?
Mission critical means mission critical—the device must have access when called upon and the bandwidth and priority to perform as required when pressed into service.

Applications Delivered To Any Device: A Single, Seamless Solution for Smart Devices

Company owned (or company liability) and personally owned (or personal liability) devices may have different levels of application access granted by the secure wireless system in place. Networks designed for smart devices should be able to ascertain users' identities and the types of devices used. These two factors offer a multitude of possible security options and require a system that can work directly with an organization's authentication infrastructure and restrict access to resources when needed.

The easiest scenario, and one typically associated with smart devices, is providing wireless guest access for devices that are personally owned and being used by a non-employee. Guest access on Wi-Fi networks has traditionally been controlled through captive web portals. Web-based enforcement of network access does not require new client-side software or extensive user training, because it depends on familiar metaphors. It does not, however, protect data flowing over the wireless link, which may leave guest users vulnerable.

Aerohive has evolved secure guest access, because security cannot be a part-time job. For example, consultants at a firm may be guests, but the information they are working on can be every bit as sensitive as that of a regular employee. Aerohive networks are engineered to seamlessly marry corporate use policy with network and data security for users' preferred devices. Aerohive provides one simple system capable of implementing multiple device liability scenarios.

With an Aerohive system, every wireless client is secure. Aerohive has developed Private Pre-Shared Key (PPSK) security. This allows registered guests to receive the same encryption levels that authorized employees have, without requiring complicated configurations to back-end systems. Once a guest registers on the Aerohive guest portal, device communication is encrypted and safe.

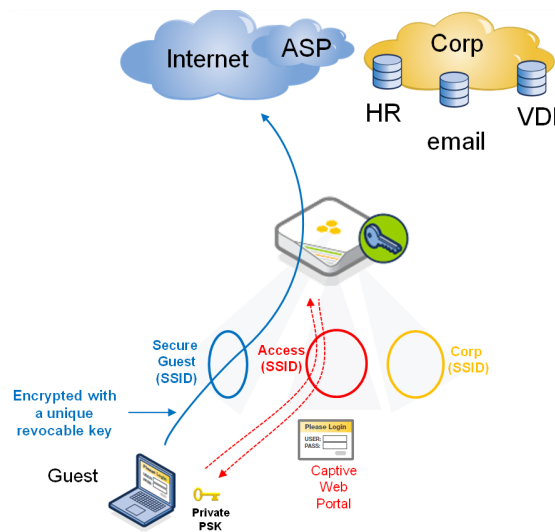


Figure 1 - Guest user with fully encrypted connection

For companies looking for a single solution for "Bring Your Own Device" policies, Aerohive provides a single architecture that allows corporate use policies, network security, users' personal device preferences, and the wireless network to seamlessly converge.

As shown in Figure 2, the same system that allows guests' devices to connect securely to the wireless network and to the Internet also effortlessly integrates with existing corporate authentication services. Once a user's identity is understood and authorized, the Aerohive system identifies the type of device in use and automatically enforces the corporate use policies in place. For example, if a user is authorized to access all the applications from his laptop, but the corporate

use policy states that iPhones may only access email, then this usage policy will be enforced on that user's device (see Figure 2).

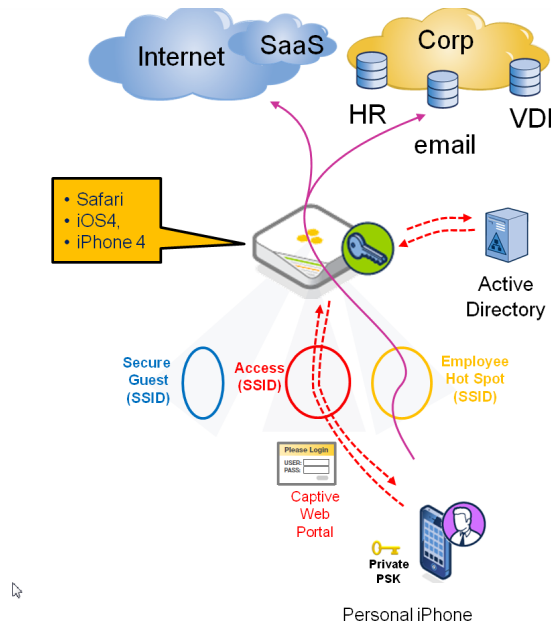


Figure 2 - "Bring Your Own Device"

Smart devices and device virtualization vendors like Citrix, VMware, and Microsoft are enabling corporate-owned smart devices to be used in place of highly specialized, very expensive computing devices. Many industries use specialized devices for their inherent security and reliability, for example, a hardened laptop used in a hospital for Electronic Medical Record (EMR) applications. With VDI, an inexpensive tablet can now reliably and securely replace these devices, running a secure, private application on a virtual desktop.

The Aerohive system is specifically designed to recognize virtual desktop environments and allow corporations to enforce usage policy even when the user identity is authorized to use the device. This means the network actually recognizes the device type, prioritizes the VDI application running on that device, and routes the traffic to the appropriate server allowing even a wireless network that is loaded with traffic to reliably deliver mission critical applications to the device running the virtual desktop environment – a key requirement for replacing expensive, specialized devices.

Figure 3 represents a deployment example. The corporate iPad is used to access corporate applications, whether they are on-site datacenter applications or cloud-based software as a service (SaaS) applications. While the iPad is capable of running other applications, the corporate usage policy states that these devices will only access the VDI server and/or specific SaaS applications on the Internet. Aerohive's infrastructure checks the identity of the user upon login and enforces this usage policy on the specified device.

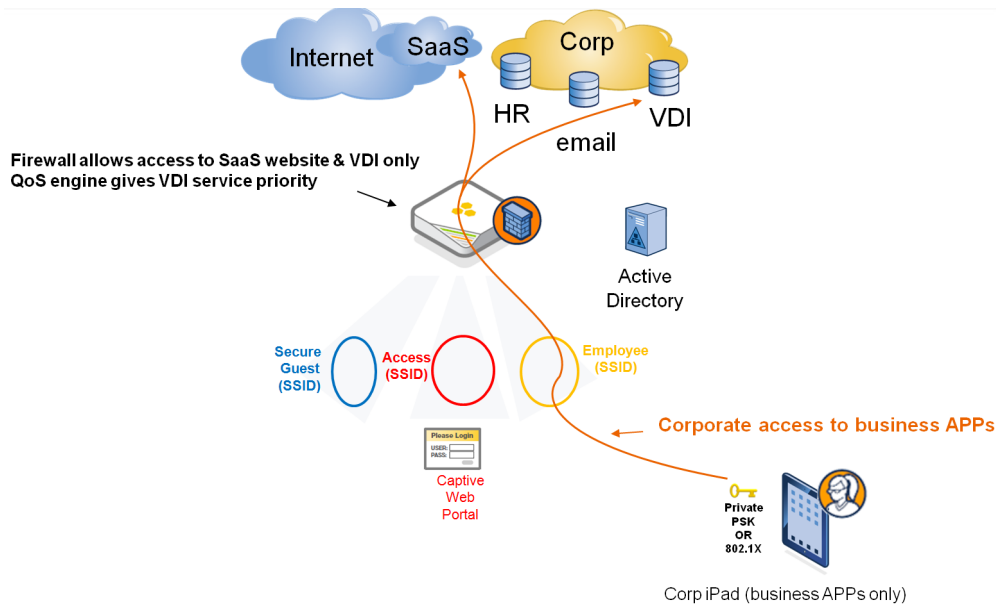


Figure 3 - Corporate Owned

The unique advantage of this seamless marriage of technology and corporate policy is the flexibility to employ any of these usage scenarios simultaneously for smart device deployments. It can finally provide application services and enforce bring-your-own-device-policies with corporate-owned smart devices with every one having application services based on the users' identity.

Simpli-Fi: Do more with less

With conservative estimates predicting skyrocketing numbers of Wi-Fi devices and ubiquitous wireless connectivity, how do you handle this growth in Wi-Fi clients from an operational standpoint?

Systems, training, and processes were all designed assuming the user was connecting to a wired interface. Now that wireless usage is skyrocketing, staff that are not wireless experts are being called upon to solve complex RF problems. Any high-level RF experts that you do have will be forced to handle most of the workload. Worse, you may have to retrain your entire IT staff.

When Aerohive set out to build its network infrastructure, the goal was not to simply make a highly scalable, highly secure, non-stop enterprise Wi-Fi system. The objective was to make Wi-Fi simple to deploy, simple to maintain, and simple to scale as your business grows. To achieve this we have engineered a solution that:

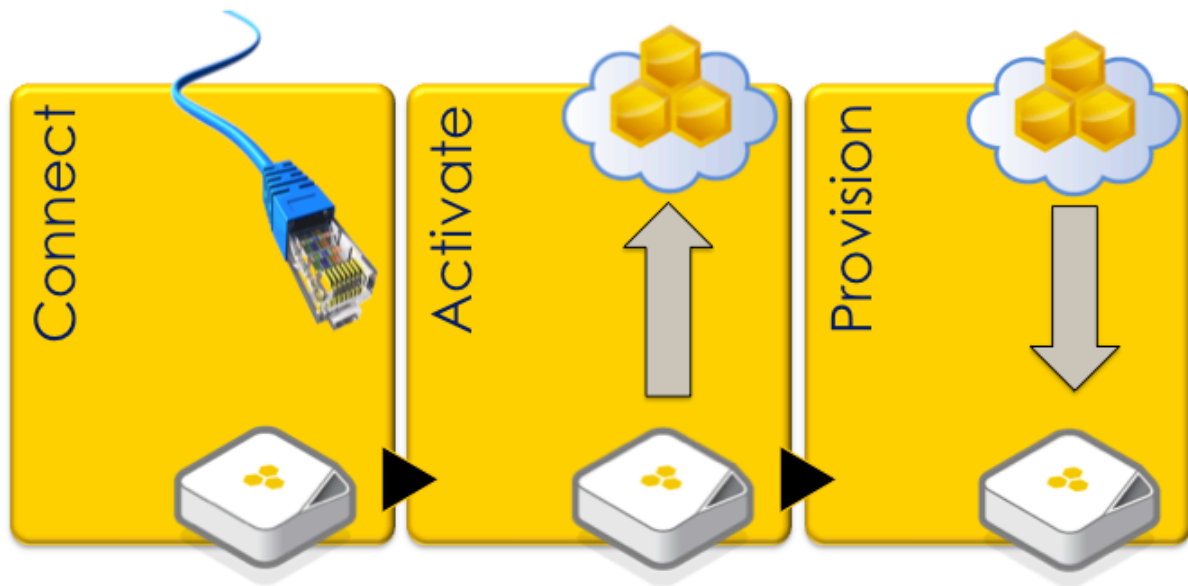
- Relies on cloud computing to provide instant provisioning and elastic management capacity
- Uses advanced wireless technologies to enhance visibility and control over every connection of every device on the network and automate client connection healing
- Uses web application technologies to provide health reports, client health scoring, and Wi-Fi SLA management

Simply speaking, using Wi-Fi with cooperative control and moving network operations to the cloud simplifies enterprise networking, even in the face of a massive influx of Wi-Fi enabled smart devices.

Save on Operational Costs: Installation

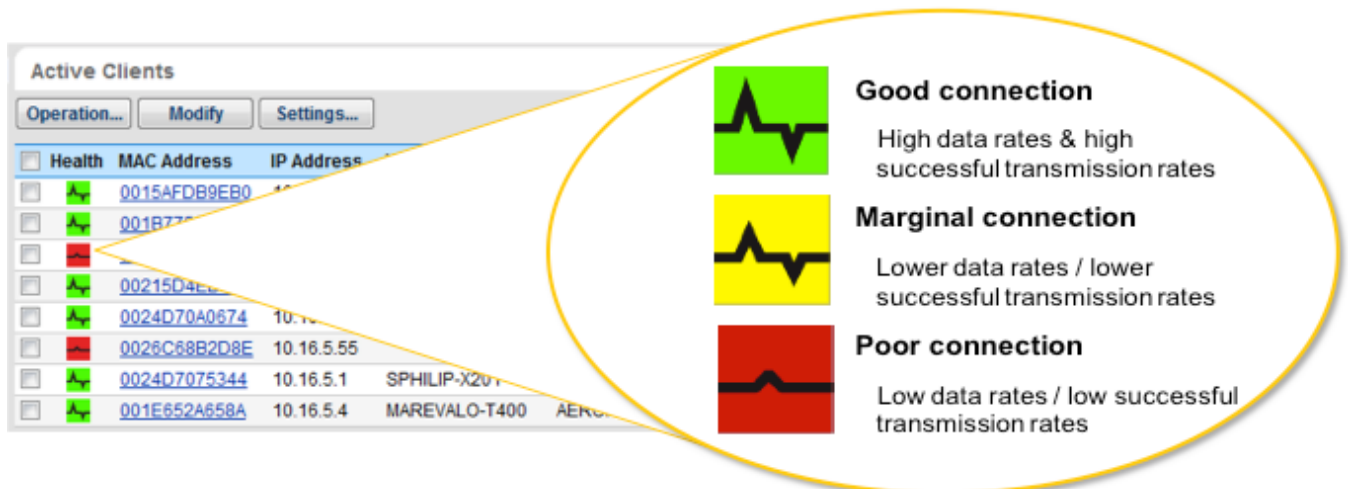
Cloud computing is revolutionizing application delivery. Aerohive's patent-pending cloud services platform allows you to instantly provision high-performance, controller-less Wi-Fi that is limited only by the area you choose to cover.

Simply plug in your Hive device, whether AP or Branch Router, and the cloud services platform does the rest. Your Hive devices find the Aerohive HiveManager Online, the enterprise management service, and are instantly provisioned and joined into the local Hive. There are no truck rolls, no installation experts, no RF experts, and no controller rebooting needed to bring the network online. Using your existing IT resources, you can increase coverage of high-performance Wi-Fi instantaneously. Additionally, since this is provided by Aerohive's cloud services platform, you only pay for what you use. You can increase or decrease service or coverage without any complicated licensing issues.



Save on Operational Costs: Automatic Problem Remediation

With smart devices, diagnosing the root cause of a network problem can be extremely difficult, even for RF experts. The very nature of wireless communications often make problems transient and difficult to pin down. Aerohive's cloud-based HiveManager Online provides high-level dashboard analysis of client connections, giving network managers the information they need in a dashboard form.



In parallel to this client health dashboard, HiveAPs coordinate the communication of the clients connected to them. This enables them to automatically adjust performance through techniques such as band steering, airtime boosting, and others and remediate problems before clients notice a degradation in application performance. As smart devices penetrate the enterprise, automatic remediation increases in importance as low-power radios are more sensitive to noise and interference. The Aerohive architecture and client health dashboard allow network managers to locate and escalate application-affecting problems without chasing transient, non-recurring problems from a single Client Health SLA report.

Conclusion

IT departments can prepare their companies for the wireless transformation with the right Wi-Fi architecture. With Wi-Fi as the primary network access layer, IT can balance the bring-your-own-device requirements of today's business with the high performance, security, control, and manageability required for delivering mission-critical applications to a host of wireless clients. Aerohive's award-winning cloud-enabled networking solutions eliminate complexity, cost, and single points of failure for today's enterprise wireless networks.

See how easy it is to migrate to an Aerohive network. Begin with Aerohive by visiting the Building Your Network page at <http://www.aerohive.com/build-your-network> today.

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).

iPhone, iPad, and iPod Touch are registered trademarks of Apple Inc.



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

WP1104009