Aerohive NETWORKS

white paper

Retailers Gain Simple, Budget-Friendly WLAN Options

The retail industry faces highly distributed IT deployments, which carry unique cost, manageability, and security challenges.

Executive Summary

Retailing companies often must support many geographically dispersed sites on a shoestring IT budget. The wireless LANs (WLANs) in these sites are often small, but they nevertheless need business-class capabilities, such as advanced security protection and centralized management, which often add a premium to the price tag. New WLAN architectures and deployment models, however, have emerged to offer more options to help retailers get what they need while sticking to their budgets.

Table of Contents

Copyright ©2011 Aerohive Networks, Inc.

Introduction: Adventures in Retailing

Retailers were among the pioneering users of wireless LAN technology, back when formal standards were just a gleam in the tech industry's eye. That's because retail has long had requirements for local user mobility, whether it was employees scuttling around warehouses picking orders or in-store personnel checking inventory or scanning prices at checkout counters.

For a long time, these specialized, low-bandwidth applications didn't rely much on interoperability with other company IT and communications systems. So islands of small, proprietary WLANs worked just fine.

Retailers still run similar picking, scanning, and pricing applications. But the context is very different. Today, warehouse and in-store WLANs are segments of companywide wireless deployments that also span office buildings and data centers. Inventory and transaction systems are an integrated component of enterprise resource planning (ERP) business application suites that store a company's confidential data, including private customer credit card numbers.

Because wireless has now become mainstream, you can no longer take for granted that unauthorized users can't – accidentally or on purpose – clamp onto your warehouse or in-store wireless network and steal or view data that they shouldn't.

In addition, there's a trend toward running in-store multimedia wireless application traffic and the use of higher-speed, 802.11n networks to accommodate it. These advances open up plentiful opportunities for retailers but in doing so, also ignite a few new considerations. The remainder of this paper will explore new wireless opportunities for retailers, then discuss several considerations associated with modern WLAN decision-making.

802.11n: A Secure Path to New Opportunities

Wireless networking has matured in many ways, and security is one of them. The current IEEE 802.11i security suite uses a derivative of the revered Advanced Encryption Standard (AES) for encrypting authentication and authorization messages. The algorithm is required by the latest, high-speed standard version of Wi-Fi, 802.11n, and is at work in current products.

In addition, enterprise-class vendors have layered supplementary security capabilities onto their systems, including wireless firewalls and air monitors, to make sure unauthorized users don't sneak onto the network and that transaction and credit card data are segmented from other business traffic.

These advances help greatly with Payment Card Industry Data Security Standards (PCI DSS) compliance. Retailers must abide by PCI DSS or risk hefty fines when PCI auditors come calling. In addition, though, today's enterprise-class WLAN providers often go far beyond the basics needed for PCI compliance to fully minimize retailers' liability risks.

On the coverage and capacity side, the Institute of Electrical and Electronics Engineers (IEEE) standards body ratified high-speed 802.11n in late 2009. 802.11n reaches farther

Copyright ©2011 Aerohive Networks, Inc.

than its predecessors, so fewer APs are required to achieve the network coverage you need in uncongested areas. 802.11nis also the first Wi-Fi version to deliver Ethernet-like wireless network speeds to the mobile industry. Most of today's 802.11n WLANs support 300Mbps connect rates with approximately 150Mbps+ actual throughput rates. That move has opened doors to new in-store multimedia opportunities. Some are described below.

Customer Engagement Experiences
A number of retailers are set to jump on the so-called "customer engagement" bandwagon to enhance the customer in-store experience. This involves taking advantage of the fact that most shoppers now carry smart wireless devices, which retailers can use to answer FAQs and push in-store promotions to shoppers. Merchandising professionals can also use wirelessly connected Web cams to remotely view shopper behavior patterns and make changes to displays based on what they see.

Queue Busting
Another emerging application is known as "queue-busting." Small-footprint properties that experience seasonal or time-of-day peaks in business can equip employees on the floor with wireless handheld point-of-sale (POS) devices. Armed with these devices, they can "ring up" customers and email receipts to them to alleviate wait times at cash registers. A prime example of this application is in force at Apple Computer retail stores, where employees on the floor offer general assistance, product consulting, and checkout services.

Restaurant Applications
Similarly, when the line backs up at a drive-thru restaurant, an employee with a handheld POS terminal can walk the line, vehicle to vehicle. The employee can catch up on order taking and get the line moving by beaming orders to the kitchen over the WLAN.

Considerations and Tradeoffs

These are just a few opportunities for retailers to differentiate themselves using wireless. However, low-margin retailers must closely consider, perhaps more than other industries, the following:

- The price tag of new solutions and associated operations
- How to provision, configure, manage, and update lots of geographically dispersed WLANs with little or no local IT staff budget
- Whether the local, in-store network will continue to operate if a wide-area network connection to a data center should fail
- How to manage performance levels when mixing older customized scanning devices with newer, faster 802.11n APs
- Growing security threats to customer-confidential credit card data and compliance with PCI security and auditing mandates, as mentioned

There's a significant trend among enterprise-class 802.11n WLAN suppliers to distribute at least data forwarding functions to local wireless access points (APs) while retaining

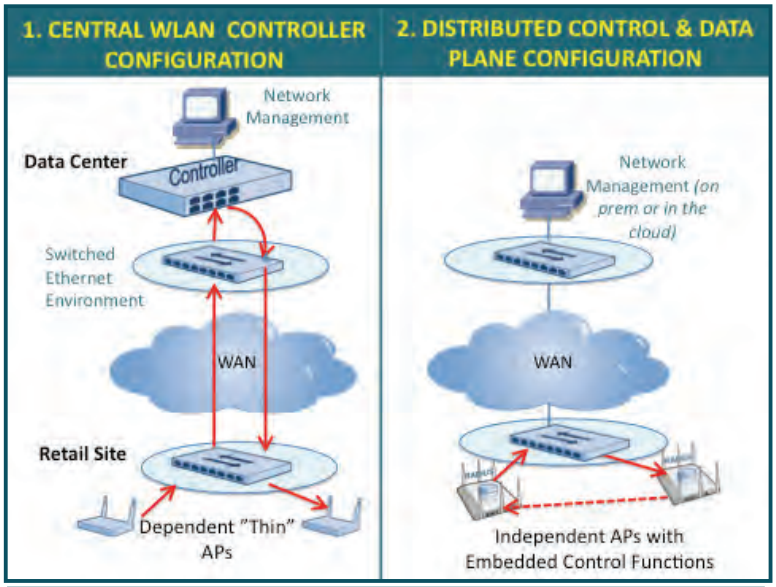
Copyright ©2011 Aerohive Networks, Inc.

centralized management systems. These efforts make significant strides in reducing the sensitivities described above for retailers. Let's take a look.

Cap-Ex Busting Measures

Affordability is a prime factor in retailing companies' selection, design, and management of the WLANs they deploy at distributed stores and warehouses.

For example, a retail store with a fairly small footprint may need only one or two APs to fully cover the area with network connectivity. But it might need extra APs for adding capacity as the multimedia in-store applications described become part of the network mix and require more bandwidth.



The red line indicates the data-forwarding path traffic takes once it has reached an AP from a mobile device. It also indicates the necessary path for authentication and other control services to be applied. The dotted red line in Configuration 2 indicates a mesh connection – a direct over-the-air connection between independent APs.

A warehouse, conversely, may not require lots of capacity. But, depending on its square footage, it might need more than one AP to ensure coverage and user network accessibility throughout the entire facility, though 802.11n helps improve this situation with its longer transmission distances.

One way of getting extra capacity, coverage, or both in a cost-effective, scalable manner is eliminating a costly component known as the WLAN controller. WLAN controllers came on the market in the 2002-2003 time frame. Some organizations with growing headquarters WLANs welcomed them as a way to streamline and automate how they provisioned, managed, and secured quickly growing numbers of wireless APs. Some highly distributed retailers with small numbers of APs per site, however, avoided controllers because of their hefty cost.

The functions of a WLAN controller – wherever they reside – are important for avoiding interference and enforcing quality of service (QoS) and security policies.
In the most modern architectures, the control functions are distributed out to APs just like data forwarding. Distributing the capabilities has become important for several reasons.

One is that most data in business access networks now traverses the WLAN, rather than the wired LAN, and the volumes are growing. Dell'Oro, for example, predicts that

Copyright ©2011 Aerohive Networks, Inc.

enterprise WLAN market revenues will increase more than 75 percent in the next five years1. The point is that, with such large volumes of data, much of it becoming latency sensitive, passing all data and control information through a remote WLAN controller causes congestion and latency problems. This is especially true for highly distributed sites that connect to the controller over a WAN link that is vulnerable to failure.

The controller adds latency to traffic that must pass through it before being forwarded onto its destination (see figure) and is a significant added expense. WLAN controllers come in sizes that support a specified maximum number of APs. When you install more APs than the maximum, you need to add another controller. Controllers cost anywhere from $15,000 to $40,000, depending on how many APs they support. Still more are required for redundancy in companies that want high-availability configurations. In addition, some vendors charge "twice," by also taking a licensing fee per AP that you connect to the controller.

Distributing control functions, along with data forwarding functions, out into the APs eliminates the controller from the picture entirely, as shown in the figure. It's a particularly good deal if you can get the AP for a price that doesn't have a premium attached for the control functions.

Case in point: The Charmer Sunbelt Group, a wine and spirits distributor, was growing its warehouse locations and worried that its existing controller-based network would soon exceed the number of APs that its legacy vendor's controller could support. This would mean installing an expensive second controller, plus one more for resiliency due to the mission-critical nature of its order processing system.
Instead, the company turned to the distributed model, moving data forwarding, control-plane, security, and QoS functions out into the local APs.

Eliminating controllers means simply doing away with all controller-related costs. What does remain centralized is the management and provisioning component. This enables central IT staff to provision and update far-flung WLANs remotely, but, should the WAN link to the management system fail, live APs and clients can continue to use the control, security, and forwarding capabilities available to them locally, so the system keeps running.

This was a factor for 7-Eleven Stores in Oklahoma City, which wasn't keen on purchasing a controller to sit alongside the single AP it deployed in each of its stores. Sharing a remote controller was more affordable, "but we rejected that option because it was vulnerable to failure" across the WAN, explains Gayle Crouch, director of IT at the chain.

OpEx: Performance and Management

Centralized management is critical to keeping WLANs live and high performing in sites where no IT personnel are located. If you're like most retailers, you have a headquarters location and one or more data centers, then also support a number of geographically

[1] Source: Dell'Oro Group, February 3, 2011

Copyright ©2011 Aerohive Networks, Inc.

distributed sites that are relatively small; say, from 600 to 3000 square feet. So you need remote provisioning and updating capabilities.

In traditional environments, provisioning and management – as well as tools and automated capabilities for managing RF interference – have been packaged alongside the control and forwarding capabilities in the WLAN controller. That works fine in a single location that's not going to grow. But in multi-location organizations, you either need local controllers at each site (overly expensive for most low-margin retailing companies) or require a remote WLAN controller that's big (and expensive) enough to accommodate all your remote APs. The rub with the controller, aside from cost, is that it retains critical services – such as security, data forwarding, and QoS – in the remote location. If a branch connection to that site fails, local WLAN service becomes unavailable.

Acuity Brands Lighting wasn't willing to take that risk. It runs a 24x7 operation and a custom-developed inventory distribution system that is "literally the company's lifeblood," says Way Brunson, network engineering project lead. "Downtime for any reason is simply not acceptable." So it went with a fully distributed, controller-less system.

And, of course, if data forwarding relies on trips in and out of the remote controller, that adds latency and creates bottlenecks, particularly if the backplane speed of the controller can't keep up with the 802.11n throughput. If it can't, you might need to invest in one or more additional controllers to split up the traffic to keep it moving.
It's far more reliable, secure, and high performing, however, to simply bundle the control capabilities into the distributed APs so that you don't have to face this situation.

Mixed-Client Effect on Performance
Another performance issue to consider is that your WLAN might run mixed types of WLAN clients. Inventory management, customer POS, and order processing systems have traditionally required specialized mobile devices that are pricey, compared to general-purpose computing devices. Given the prices of the purpose-built devices and the retail industry's notoriously thin margins, those devices don't get refreshed with newer technology as often as in some other industries.

As a result, these devices might run older, slower versions of Wi-Fi, while you are introducing high-speed 802.11n into the environment. 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.

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, airtime fairness 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."

Copyright ©2011 Aerohive Networks, Inc.

Centralized Management: On Premise or in the Cloud?
As noted, retailers should be able to provision, configure, manage, and maintain APs in all their sites from a central place. The very latest WLAN architectures give you a choice of how you want to do that. The premises-based choices are VMware-compliant software management applications and standalone management appliances. Alternatively, you could use a cloud service, which entails accessing a Web portal to provision, configure, manage, and secure each site from any remote location.

Depending on your organization's IT philosophy, you might choose any of these methods. What are the tradeoff considerations?

Appliances that run hardened, proprietary operating systems are often considered the most secure option. So it's worth asking whether your vendor's appliance is hardened or instead runs a general computing OS that hackers are likely to be familiar with. In addition, there are cost considerations in terms of capex, real estate, and power associated with appliances.

Using a virtual server instance, or VM, of a management application eliminates the capex and associated costs of the dedicated appliance yet leaves you in control of overseeing the physical access to components in your own data center.

The cloud service option avoids any capex for management whatsoever; you simply pay a flat fee per month for access to the cloud and its sophisticated management tools. These are early days for cloud services. There have been no documented reports of cloud services being less secure than on-premises equipment or software, yet some might perceive Web-based access to your WLAN topology as more "breachable" than using software and hardware in your own data center.

PCI Compliance and other Security Issues

As mentioned earlier, the PCI watches retailers that accept credit cards carefully. And the organization recently added a couple of requirements to its DSS. PCI DSS now require not only over-the-air data encryption of customer credit card data, but also network admission control and the ability to associate a cable connection with a legitimate device.

The latest version of the PCI DSS, Version 2.0, went into effect in January 2011. That means that if you work for an entity that stores, processes, or transmits credit card data in electronic form, your organization is required to comply with the standard or risk being fined or, in very extreme cases, being cut off in your ability to accept credit card payments.

This is where some of the security capabilities outside of 802.11 standards come in handy. Integrated stateful firewalls embedded in APs, for example, fulfill the wireless segmentation required by the PCI DSS specification. Such firewalls have multi-level response mechanisms that can log, block, disassociate, or disassociate-and-ban wireless clients in response to particular attacks.

Copyright ©2011 Aerohive Networks, Inc.

And while compliance is very important for lowering your liability with the PCI, PCI standards aren't particularly comprehensive or stringent. For example, it can be beneficial to also have a Remote Authentication Dial In User Service (RADIUS) server so as not to expose credentials across a WAN connection.

In addition, 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 to a WLAN controller. Moving in and out of the controller poses a greater risk of "bad traffic" penetrating the core network and consuming valuable network resources in the process.

Newer systems also contain built-in 24x7 air monitoring systems called wireless intrusion detection and prevention systems (WIPS), which scan the airwaves for unauthorized APs, known as "rogues," that might be attempting to connect to your network.

The Macaroni Grill restaurant chain, for example, recently deployed WLANs under the supervision of a VP of IT that joined the company from a security background.

"The biggest piece of compliance was to be able to perform rogue access scans," says Drew Stafford, who ultimately selected a controller-less system. "We have a strict threshold on our AP signal levels. If we see a fairly strong signal coming from an unauthorized device, we are alerted and can immediately investigate the issue. We can also see if traffic from an unauthorized AP is connected to our wired network, indicating a possible breach, and take immediate action to shut it down."

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 distributes all data forwarding and control mechanisms out to the APs – at no additional cost – so that you can avoid the expense of WLAN controllers at each site or the vulnerability and bottlenecks they impose when using them remotely across a WAN link. WLAN security and performance-enhancement services such as real-time packet prioritization, airtime fairness, and policy-based QoS are also distributed out to the individual APs to minimize latency.

In fact, Aerohive offers an implementation option to one 802.11i security requirement that is friendlier to companies that don't have the staff, funding or setup to run certificate-based systems and 802.1x security frameworks. Aerohive's patent-pending Private Pre-Shared Key system generates and manages separate pre-shared keys for every client. This enables multiple users, each with a unique key, to access the same WLAN, providing one-to-one authentication and strong encryption. Clients cannot eavesdrop on each other in a Private PSK system, and network access can be revoked on a per-client basis.

The Aerohive system uses self-organizing, mesh-capable APs that 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

Copyright ©2011 Aerohive Networks, Inc.

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. Aerohive makes retail deployments straightforward and less costly. You simply total the number of APs you need for each site, perhaps adding in one or two spares, multiply that by the cost of the AP you choose, and you have calculated your WLAN system cost. Adding the price of management – in the form of VM software, hardware appliance or monthly cloud service fee – to this number plus an annual vendor support fee delivers the total cost of ownership (TCO).

There are no hidden licensing fees or costs for extra features.

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.

Copyright ©2011 Aerohive Networks, Inc.

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

WP1101203