Transforming Retail Business using Cisco Unified Wireless Network Mobility Services

This whitepaper describes how Retail Businesses can employ mobility services to improve business efficiency, boost profitability, and increase Customer satisfaction.

Summary

Initially adopted as a method of increasing productivity in warehouse and storage areas, wireless networking is emerging as a critical component in the retail business. Having been one of the earliest adopters of the technology, retail enterprises have gained tremendous understanding of wireless networking and are now using it to transform how they buy and sell products, service customers, and conduct their day to day business.

Aberdeen's 2004 research revealed that just as the foundation of a house is intrinsic to its value, real-time networking (wired and wireless), as the foundation of real-time communication, is intrinsic to the value of the retail enterprise.[1] In today's world, when the in-store experience is critical to capturing the hearts and minds of consumers, mobility services built upon a pervasive, reliable wireless network have become the underpinning of most customer-facing initiatives to drive incremental sales and revenue growth results, and are the foundation of programs to reduce costs and increase profits. Cisco® Wireless LAN Mobility Services allow retail enterprises to gain business benefits from more informed customer-employee interactions, up-to-date inventory and sales information, and the ability to analyze store and employee performance more rapidly, all while ensuring intellectual property and proprietary information is protected.

Trends Driving Retail Enterprise IT Departments

Retail is a behemoth among industry sectors. Across all major world economies, its size as a percentage of gross domestic product (GDP) ranges from 20 to 33 percent. Despite its size, the retail industry's net margin of approximately 3 percent[2] is among the lowest of any sector. Consequently, improvements and efficiencies are paramount and can mean billions of dollars in savings, avoided costs, or both. Until recently, a solid return on investment (ROI) case for data connections between stores and corporate offices was difficult to make in retail chains, especially in those with a store footprint of less than 10,000 square feet. The monthly cost for T1 or Frame Relay lines to individual stores was disproportionately high and was exacerbated by the requirement for up-front capital for hardware investments.

Today, however, connections to even the smallest offices or outlets cost a fraction of what leased lines cost. These cost reductions have enabled retail stores and outlets to become integrated into the overall IT infrastructure, allowing retailers to take advantage of IT systems to become much more customer-centric by gaining near real-time information from stores, employees, supply chains, and customers. A pervasive, secure wireless network frees this information from the confines of desktop computers and allows it to be used anywhere, anytime to improve the

---

[1] "Real-time Networks: The Foundation of the Empowered Store," Aberdeen Group, December 2004
[2] 2002 U.S. Economic Census: Advanced Comparative Statistics for U.S. based on 1997 NAICs

customer experience and store performance and to transform how retail enterprises conduct operations.

Benefits of Cisco Unified Wireless Network Mobility Services for Retail Enterprises

Retail enterprises are deploying the Cisco Unified Wireless Networks pervasively throughout the organization as a critical component of intelligent retail network architecture. Cisco Wireless LAN Mobility Services are a combination of guess access, enhanced security, location, and voice capabilities, uniquely delivered by the Cisco Unified Wireless Network, that allow retail businesses to deploy value-added mobility applications. Cisco Wireless LAN Mobility Services build on the existing mobile data capabilities inherent in any pervasive wireless deployment.

In order to improve operations and customer satisfaction, retail enterprises need to be able to move beyond simple hotspot or point wireless deployments, and move to a pervasive deployment. Once pervasive, the wireless network becomes a platform for the delivery of intelligent services. These mobility services serve as the middleware between business applications and the infrastructure, allowing existing and new applications to take advantage of the flexible connectivity inherent in wireless networking.

With an infrastructure designed to support wireless LAN mobility services, retail enterprises can:

- Enhance the shopping experience
- Boost productivity by connecting people, places, and information wherever they are located
- Protect brand images and assets securely and reliably
- Decrease the time it takes to react to market shifts

The rest of this paper will discuss potential applications for each mobility service and the associated benefits. This paper will also briefly describe the implementation of the Cisco Unified Wireless Network.

Guest Services

Retailers rely on the network to provide dependable access to real-time information on inventory, customers, and operations, with the goal of ensuring that customers are satisfied with their purchases and level of service. In this way, the retailer can create brand loyalty and build long-term customer relationships. The top priorities for achieving this are inventory on hand when the customer wants it, information available to customers to answer immediate questions, and providing complimentary services that deliver a richer shopping experience to the customer.

With pervasive wireless access in stores and corporate offices, IT departments can provide guest access services for partners, vendors, and customers. Guest access that is secure and isolated from the corporate information enables suppliers to gain real-time visibility into stock levels and to reorder to avoid losing sales because of lack of inventory. Additionally, partners can "push" promotions to in-store advertising venues, keeping customers apprised of the latest offers. Extending quick access to information on products not only to managers and employees but also to customers through Wi-Fi access or in-store kiosks increases the value of the information that retailers have about products. Ultimately, access to product information helps customers feel comfortable with their purchases. In addition, certain retailers can increase the length of customer visits as well as brand loyalty simply by providing wireless Internet access to customers.

Of course, a primary concern for any IT administrator is how to offer guest access in a secure, controlled way, ensuring that the corporate network and information on it remain isolated.

The Cisco Unified Wireless Network supports up to 16 independent wireless LANs and allows multiple user groups to utilize the same infrastructure. In this context, a wireless LAN is defined by a unique network name (Service Set Identifier or SSID), security, and quality of service (QoS) setting. This allows the administrator to define separate SSIDs for different user groups. As an example, the SSID "guest" might be created for visitors who wish to have wireless Internet access. Another SSID "office" could be set up for employees, while a third named "shipping" might be established for business-specific devices such as bar code scanners.

Furthermore, each wireless LAN can be directed to a specific VLAN, ensuring that only the necessary resources are available to the users of that wireless LAN. Administrators can set the SSIDs to broadcast or not broadcast, at their discretion. This provides an additional level of security. By broadcasting only the guest network SSID, fewer attempts will be made by unauthorized users to access the internal, private wireless LANs.

For some retail enterprises, guest traffic isolation through a VLAN does not provide a sufficient level of security. In this case, the Cisco Unified Wireless Network can create a Layer 2 tunnel to direct all guest traffic outside the unsecured network area to a controller dedicated to guest services. Figure 1 shows an example of such a topology. Even remote and branch office guest users can be tunneled to a wireless LAN controller for guests, which then applies the appropriate policies before Internet access is granted. Employee wireless usage policies are managed by the wireless LAN controller(s) internal to the enterprise

Figure 1.   Directing Guest Traffic Outside the Unsecured Network Area Through a Layer 2 Tunnel
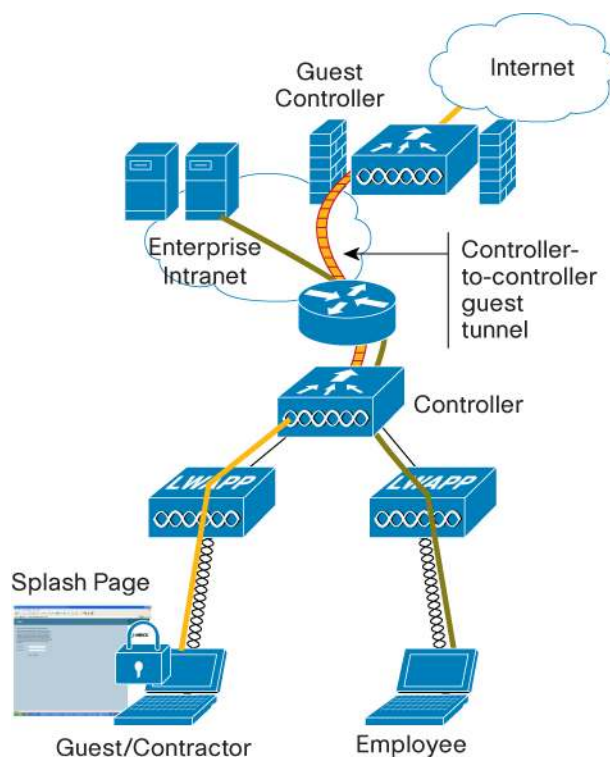
Users enter the guest network by opening their browser. A captive portal redirects the browser to a specific address where a customized login page can be presented. For tracking purposes, unique user names and passwords can be required. Administration is greatly simplified through the Cisco Guest Access Lobby Ambassador. Endpoint control, for both employees and guest users, to ensure that viruses, spyware, and worms are not introduced can be managed through Network

Admission Control. For more detailed information about setting up a secure guest network, see *Achieving Business Goals and Enhancing Customer Relationships with a Secure Guest Access WLAN*.

Security Services

Security and privacy are paramount for retail enterprises. In addition to violating corporate secrets, breaches can cause severe damage to brand equity, as demonstrated by recent Internet attacks in which thousands of customer records were stolen. If customers associate a major violation of private information with the retailer's brand, it becomes far more difficult to win their loyalty. Further, the payment card industry (PCI) has created requirements for data security designed to be implemented by any businesses that accepts or facilitates credit card transactions or the handling of sensitive credit card and user information. Cisco's Wireless LAN Security Services were designed to strictly adhere to the most stringent industry regulations and enable the full business-enhancing potential of wireless networks to be realized while encrypting, firewalling, and protecting all sensitive data, whether that data is corporate or private customer information.

When the most recent security standard, IEEE 802.11i, is employed, wireless networks are as secure as many wired network implementations (and in some cases, more secure). However, because wireless LANs can penetrate beyond the physical boundaries of buildings, wireless threats can exist from unauthorized infrastructure and clients that aren't even on premises. The good news for retail IT managers is that these threats can be detected and prevented using the Cisco Unified Wireless Network while it simultaneously provides service to wireless clients.

The most common threat is the rogue client or access point. Rogues are typically consumer-grade access points that are brought in by employees anxious to provide wireless service to their general surroundings or clients with dedicated software deliberately trying to access network resources they are not authorized to access. Unfortunately, while the consumer-grade access points are deployed on premises with the best of intentions, because the default mode for most APs is to have security disabled, they become an unsecured portal to the enterprise network for anyone within range of the signal. And because wireless LAN signals can pass outside the building, unauthorized rogue clients may gain access to the network.

To address this security risk, the Cisco Unified Wireless Network provides advanced security services that continuously monitor, identify, and prevent wireless threats. Cisco Unified Wireless Network lightweight access points, whether servicing clients or configured as air monitors, scan for all Wi-Fi activity. If a managed access point detects another access point over the air, and it is not managed by a Cisco Unified Wireless Network controller, it is classified as a rogue. As Figure 2 shows, the location of the rogue will be immediately plotted on the floor plan map in the Cisco Wireless Control System (WCS). This technique ensures the quick physical removal of the rogue without the need for time-consuming inspections using a handheld analyzer. Similar techniques are used for ad hoc networks, client misassociation, denial of service attacks, and penetration attempts.

Figure 2. Plotting a Rogue Access Point on a Floor Map
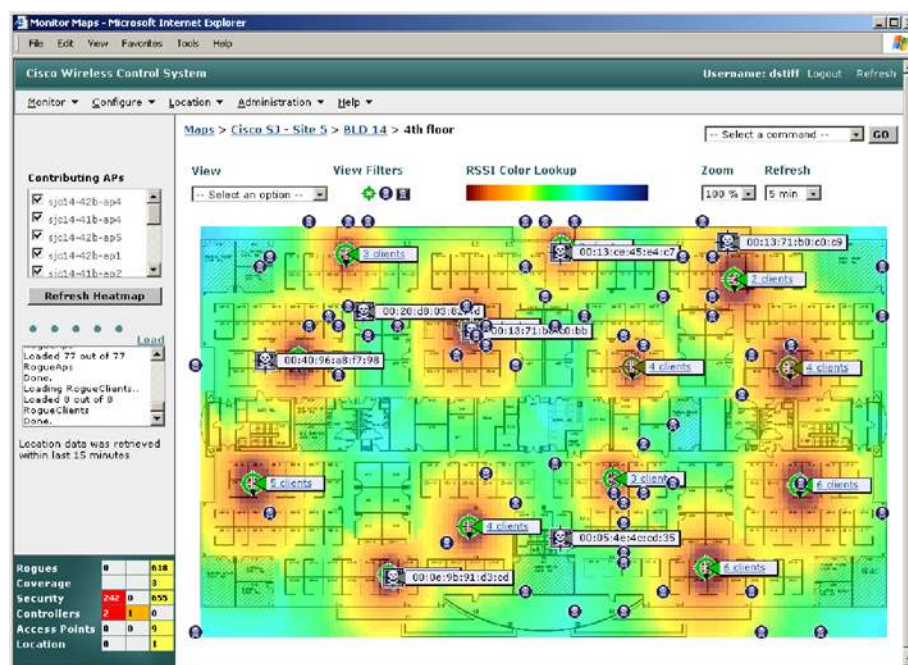
In addition, only Cisco offers the ability to integrate wireless intrusion detection system/intrusion protection system (IDS/IPS) services with wired network IDS capability, endpoint compliance, and offsite endpoint protection, delivering a truly unified IDS/IPS solution.

Location Services

One of the greatest transformational forces in retail today is the ability for a pervasive wireless network to provide information on the location of assets in near real time. Knowing exactly where an asset is can enhance productivity, improve customer satisfaction, reduce cost overruns, and increase security. Instead of spending resources looking for an item or wasting capital by purchasing it again, location tracking immediately identifies exactly where it is. Devices or people that should not leave a specific site, building, or floor can be monitored so that alarms are triggered if the device or person leaves its designated area. And precise location tracking enables quick physical removal of wireless threats such as rogue access points. Furthermore, location tracking can facilitate process improvements leading to long-term efficiency gains. As a history of asset utilization is developed, new procedures can be put in place to more effectively utilize the asset.

Cisco Unified Wireless Network Location Services create the ability to quickly locate any Wi-Fi device to support enhanced network security, management, and troubleshooting as well as enable location-based applications. Using the Cisco Unified Wireless Aironet access points, Wi-Fi clients, and active RFID tag signals, the Cisco Location Appliance calculates device locations, which are then displayed in real time through the Cisco WCS on site-specific floor plans. A standards-based application programming interface (API) allows integration of the location information into business-specific security, enterprise resource planning (ERP), or workflow applications. Additionally, the appliance provides location-based alerts for business policy enforcement, and it records rich historical location information that can be used for location trending, audit trails and regulatory compliance, rapid problem resolution, and RF capacity management. For retail

enterprises, this means improved asset utilization, and improved protection against theft and inadvertent release of sensitive customer data, as well as reduced inventory management costs.

Voice Services

Voice over IP is rapidly gaining ground as the preferred method to deliver voice communications within enterprises. By delivering voice and data over a single converged IP network, acquisition and operational costs are significantly decreased. When voice over IP is deployed over wireless LANs, these same benefits are multiplied by making mobile workers reachable anywhere and anytime. Unlike cellular phone service, which is not economically feasible for large retail organizations operating on extremely thin net margins, voice over wireless LAN (VoWLAN) provides inexpensive, continuous, high-quality service when a pervasive wireless LAN is deployed.

Retail organizations can realize many benefits from deploying VoWLAN, including:

- Improved customer service by freeing personnel from having to provide personalized service only from fixed locations
- Increased profits through operational efficiency and improved customer satisfaction
- Improved communication by giving phone services and voicemail to each store employee
- Improved responsiveness by making business applications, like inventory management, mobile with wireless phones

The Cisco Unified Wireless Networks delivers voice services through unique enhancements that support demanding real-time communications capabilities, including the following:

- Industry-leading quality of service (QoS) and Call Admission Control (CAC) on the wireless voice network, enabling voice and data applications to peacefully coexist
- Power saving for extended handset talk-time battery life
- Real-time RF scanning and monitoring of the RF environment, delivering a self-configuring, self-optimizing, and self-healing wireless network to ensure the quality and availability of voice services
- Fast secure roaming across the campus while maintaining Wi-Fi Protected Access 2 (WPA2) security
- Access points with MAC layer enhancements to intelligently handle voice and reduce voice packet delays caused by retries

The Cisco Unified Wireless Network supports the widest variety of voice clients in the industry. The Cisco Unified Wireless IP Phone 7920 is an easy-to-use IEEE 802.11b wireless IP phone that provides comprehensive voice communications in conjunction with Cisco Unified CallManager and Cisco Unified Wireless Network. In addition, the Cisco Compatible Extensions program gives voice client manufacturers the ability to design current and future voice wireless innovations into a wide variety of devices.

The Cisco Unified Communications system provides a full-featured, scalable, distributable, and highly available IP telephony call-processing solution. The Cisco Unified Communications system and its application partners, combined with Cisco's voice-capable wireless infrastructure, together enable retail employees to move around freely within their environments to support customers and to maximize asset utilization. Employees have individualized voice extensions with only an incremental cost increase over current retail enterprise voice costs.

Conclusion

Pervasive wireless LAN deployment supports new services that enable applications to significantly improve the operational efficiency as well as customer satisfaction in retail enterprises. Deploying the Cisco Unified Wireless Network pervasively across retail enterprises enables comprehensive guest, security, location, and voice services. Through a pervasive guest network, vendors, customers, and employees can gain access to and use valuable information anywhere and at any time to improve operations and increase customer satisfaction.

Security services are a critical piece of any IT security strategy to protect against wireless threats, such as rogue client access points. Immediate identification and prevention of such threats is critical to maintain network and data integrity. As retail enterprises are likely holders of confidential customer information, it is imperative that these potential vulnerabilities be fixed before customer trust is violated and brand equity is damaged as a result of a security breach.

Location services can be coupled with security to provide fine-grained authentication of users based on their physical placement within a building, creating an even higher hurdle for would-be hackers. And tracking assets and inventory, from hand scanners, to registers, to in-store inventory, to individual employees, ensures that people and resources are used efficiently, and security of valuable items or people is maintained.

Voice services complete the picture by providing real-time communication for every employee so that customer responsiveness can be improved without adding the cost of a cellular phone to employee overhead, a cost that would be unacceptable in the 3 percent net margin world of retail..