In-Store Mobility — Realize Your Vision
# Table of Contents

- Introduction 3
- Retail mobility landscape: Business challenges & opportunities 3
- Resulting technology requirements 4
- Aruba’s integrated mobility solution for retail 5
- Meeting in-store mobility requirements 7
- Conclusion 7
- About Aruba Networks, Inc. 8
Introduction

Mobile applications in retail are not new. Over the years, barcode scanning enabled mobile applications in the retail storefront, in the back room and in warehouse locations that have helped retailers reduce operating costs by improving productivity and providing greater supply chain visibility. Mobile applications such as inventory tracking, shelving, labeling, etc. started as competitive differentiators and now have become an integral part of how retailers conduct business. Leading retailers have even used in-store mobility technologies to improve the sell-side of their business with customer-facing applications and store manager applications to foster a better in-store experience.

The rapid rate of evolution in mobility technology and elevated concerns regarding credit card data security, are bringing about a new phase in retail mobility with a brand new set of challenges and opportunities. The most urgent and compelling issue that retail IT faces today is to keep existing applications running. Aging mobility infrastructure and, more importantly, legacy investments in mobile devices are no longer supportable. Add to that recent compliance mandates and it is clear that retail IT has a major overhaul of its mobility infrastructure in sight. The good news is that the costs of making such changes can be easily contained by choosing the right IT strategy and the right in-store mobility infrastructure.

Another upside of this situation is that the new phase in retail mobility also brings exciting opportunities for retailers to further improve their business process and competitiveness. Mobility technology has improved significantly since the last major wave of adoption in the early 2000s and now can enable a host of new applications involving multimedia or based on data about the location of assets and people. New mobile applications to improve the in-store experience (such as kiosks) and productivity applications (such as the Manager’s device) have shown impressive ROI by improving store and staff productivity and building customer loyalty. Other major technology improvements have been in the areas of reliability and management. Leading mobility infrastructure products have the necessary tools to reduce IT expenses related to managing hundreds, or even thousands, of remote sites from one centralized location.

This paper provides a detailed look into the retail mobility landscape – including the key business challenges and opportunities that retailers face and the technology required to address them. We will also define the requirements for a cost-effective in-store mobility solution.

Retail mobility landscape: Business challenges & opportunities

IT managers in retail mobility environments face several important business challenges and opportunities today, including PCI compliance mandates, disruption of existing mobile applications and the need to introduce new applications to stay competitive.

**PCI Compliance Mandates:** The PCI security standards council has released an updated PCI data security standard that went into effect January 1, 2007. To address the changing security landscape, the updated standard requires additional wireless LAN security to be implemented at the store-level. The mobility infrastructure used today does not have the necessary security capabilities required to address PCI security requirements. Retailers urgently either need to add security components, which would require new capital and operational investment, or upgrade to a mobility infrastructure that offers built-in security.

**Disruption of Existing Mobile Applications:** Many wireless LAN access points and mobile devices used in retail environments today have been discontinued and are no longer supportable/serviceable. To continue to run existing mobile applications, retailers must upgrade their legacy wireless LAN infrastructure and installed base of legacy devices. Given the large investment already made in legacy mobile devices, retailers are looking for a cost-effective migration path that allows a phased upgrade. To support such a phased approach, retail IT is looking for a mobility infrastructure that can simultaneously support both legacy and new devices.
Stay Competitive: The next-generation of mobile applications based on voice and RFID technology is now available and offers an attractive business value proposition. Voice and RFID applications have been shown to improve in-store staff productivity by getting store managers out of their offices and onto the floor and by supporting customer-facing technologies to enhance the overall shopping experience. Accordingly, retailers are looking for a mobility infrastructure that can be used for existing mobile applications and can easily support new voice and RFID applications – without requiring hardware and software upgrades.

Resulting technology requirements

Upgrading legacy in-store mobility infrastructure is the most viable solution to meet the unique needs of retail environments today. A replacement mobility infrastructure must meet the following requirements:

Scales for a distributed network environment: The retail environment is unique in that there are hundreds or thousands of remote locations, where no IT personnel are located. Instead, the network for the entire chain is managed from a central data center at the company headquarters. Therefore, an in-store mobility network must scale to multiple thousands of locations and must be centrally manageable. This includes:

- Plug-n-Play deployment tools to make the installation process as simple and sure as possible.
- Centralized configuration and software management to roll out upgrades and changes to hardware platforms used in a retail store.
- Centralized support and help desk tools that provide the necessary visibility into the store network, applications and devices.
- Centralized troubleshooting for network engineering to quickly diagnose and fix problems without requiring a trip to the store.

Meets PCI Security Requirements: The new PCI data security standard – v1.1 – consists of 12 major requirements. Nine of these requirements have a wireless LAN security component, and the mobility infrastructure must meet these requirements. Given the capabilities of mobility and wireless LAN products available today, retailers must ensure that the infrastructure provides the following three security capabilities. The absence of these technologies would require additional hardware investments.

- Wireless analyzers that can detect all unauthorized (a.k.a. rogue) access points and devices on the network. The goal is to prevent accidental or malicious backdoors to the payment card network – requirement 11.1. In addition to wireless analyzer capability, the classification and reporting system must be capable of distinguishing between a rogue device or access point on the store network versus one in a neighbor’s network (e.g., other stores in the mall with wireless, new hot-spots, etc.)
- Firewall for segmenting wireless and wired networks to prevent the threat of attacks to the payment card network from the wireless network – requirement 1.3.
- Latest wireless encryption standards such as WPA/WPA2 for applications such as wireless point-of-sale applications that carry credit card data over the wireless link – requirement 4.1.

Simultaneously support new and legacy devices: To provide a cost-effective migration path from legacy devices to newer devices, the mobility infrastructure must be able to simultaneously support both legacy and new devices. Supporting legacy devices is a challenge given that such devices do not support the desired security mechanisms that new devices can. Therefore, the mobility infrastructure must be able to support new and old security mechanisms simultaneously. Additionally, the mobility infrastructure must be able to segment legacy mobile devices running with poor security to provide added protection.
Integration with Existing Systems: The replacement mobility infrastructure must integrate with existing network, security and management systems. This includes the wired LAN, WAN links, security infrastructure and mobility management platforms such as Wavelink’s Avalanche, etc.

Supports upcoming applications: The mobility infrastructure must support latency-sensitive applications such as voice and video as well as Wi-Fi RFID tags. Although these applications are not a mainstay in retail storefronts, they are definitely on the near horizon. When these applications are ready for deployment, no changes or additions to the mobility infrastructure should be required.

Cost-effective: Cost is a particularly important factor for chain stores, where purchase decisions impact so many locations. The in-store mobility infrastructure must not be too costly for a small location that requires only a few devices and it must not have hidden costs. These hidden costs could include the hard costs of additional products to meet defined requirements, as well as the soft costs of management. Mobility infrastructure products must have built-in security, management capabilities and application control to eliminate the need for additional products at a store-level.

Aruba’s integrated mobility solution for retail

To better meet the needs of in-store mobility, Aruba has pioneered a new approach to network infrastructure called user-centric networking. In contrast to traditional network architecture, Aruba takes a user- and application-centric approach to enterprise mobility. Aruba’s user-centric networks provide secure mobility, improved application performance in mobile environments, greater ease of integration and deployment, and cost-effective scalability. They offer the most flexible platform for legacy and new mobile devices and the highest level of support for existing and emerging mobile applications.

Aruba offers the only integrated in-store mobility infrastructure that offers PCI-level security and wireless LAN access for a wide variety of mobile applications. The Aruba architecture is designed to easily scale to hundreds or thousands of remote sites and to offer centralized management and control. Aruba’s architecture features a device-agnostic approach that can simultaneously secure and support a heterogeneous set of device types - legacy and new mobile devices, different vendors’ devices, etc. The open-standards system combined with mobility performance capabilities ensures the highest levels of mobile network reliability without requiring any device-side software or proprietary hook-ins. In addition, built-in application awareness future-proofs the mobility infrastructure investment with support for upcoming applications – voice, video and RFID-based applications.

The Aruba solution consists of two key components – thin Access Points (APs) and Mobility Controllers, and an optional component – Mobility Management Server (MMS). APs connect to any Ethernet Switch in the wiring closet and provide a wireless link to devices. APs tunnel all wireless LAN traffic (over a GRE tunnel or IPsec tunnel) to a Mobility Controller installed in the data center or the distribution layer of the network. The Mobility Controller handles all of the wireless intelligence: user authentication, RF monitoring, wireless IDS, policy enforcement, encryption, location services, VPN termination, etc. A Mobility Controller can be configured as a stand-alone device or as a member of a hierarchical setup in which a master controller communicates with local controllers. For small to mid-sized networks, the Mobility Controller also acts as the single point of configuration and management. For larger networks that require more than one master controller, the MMS can be used for multi-controller management and assumes the role of a single point of configuration and management.
**In The Data Center:** Depending on the number of remote locations and total number of APs, one or more master Mobility Controllers are installed in the data center. These controllers can also terminate APs used for wireless connectivity in the HQ and remote APs used in small-sized retail stores. A master controller can support up to 700 remote controllers and is the single interface for configuration and management. A master controller can also back up a controller in a remote location in the case of an outage. To scale for larger deployments, multiple master controllers can share the load of connecting to remote controllers and APs, and the MMS can be used as the single interface for management and configuration.

**In Warehouses, Large-Sized Stores and Medium-Sized Stores:** Depending on the number of APs required in each location, a different model of Aruba controller (called a local controller) may be installed. Controller models are available to support from as few as four to as many as 2,048 APs. All Aruba controllers run the same software and have the same functionality.
Each local controller gets its configuration from the master controller. Service and security levels for multiple applications and device types are enforced at a per-user level by the local controller. Local controllers enable Wireless Intrusion Protection security and have the capability to offer local authentication services and/or pass-through requests to the data center. Each local controller automatically calibrates the RF coverage to optimize application performance and to address any coverage holes.

In Small-Sized Stores: Remote APs are a cost-effective solution to provide secure and centrally managed wireless connectivity to locations that only need one or two APs. Remote APs can connect directly via Ethernet to a public/private Internet connection or to the LAN. Remote APs automatically discover the master controller and establish a VPN tunnel to the data center. All traffic is tunneled back to the data center, where the security and management services described above are provided by the Mobility Controller. For local applications such as printing, remote APs support split-tunneling where specific application traffic is bridged locally.

### Meeting in-store mobility requirements

<table>
<thead>
<tr>
<th>Key Requirement</th>
<th>Aruba Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scales for a distributed environment</td>
<td>Aruba’s user-centric network architecture is designed to scale to remote sites with capabilities to centrally manage &gt;10,000 access point networks.</td>
</tr>
<tr>
<td>Meets PCI requirement</td>
<td>Aruba’s user-centric network architecture satisfies PCI v1.1 security requirements with a built-in per-user firewall, comprehensive wireless intrusion protection services and support for all standard wireless security technologies.</td>
</tr>
<tr>
<td>Simultaneously supports legacy &amp; new devices</td>
<td>Aruba’s user-centric network architecture is fully interoperable and enables the highest levels of “mobility performance” for the widest range of mobile devices. The Aruba architecture uses a device- and vendor-agnostic architecture to simultaneously support and secure legacy and new devices.</td>
</tr>
<tr>
<td>Integration with existing systems</td>
<td>Aruba’s user-centric network architecture can be added on top of any existing wired network and can be managed by systems used by retailers such as Wavelink.</td>
</tr>
<tr>
<td>Supports upcoming applications</td>
<td>Aruba’s user-centric network architecture is voice- and RFID-ready such that voice and Wi-Fi RFID applications can run simultaneously with other data applications. No change to hardware or software is required.</td>
</tr>
<tr>
<td>Cost-effective</td>
<td>Aruba’s user-centric network architecture is an integrated single product solution for mobile access that meets PCI security requirements, and provides centralized managed and application awareness. Aruba offers the most cost effective solution for in-store mobility with right-sized options for different retail environments including products that scale for headquarters, warehouses, large stores and small stores.</td>
</tr>
</tbody>
</table>

### Conclusion

Regulatory compliance issues, combined with the discontinuation of legacy access points and mobile devices, is driving the need for a wide-scale upgrade of in-store mobility infrastructure. Retailers are looking for a cost-effective solution that minimizes disruption to existing applications, reduces IT opex costs of managing a mobile network and supports new applications to improve operations. Aruba offers the only integrated in-store mobility solution that meets PCI v1.1 requirements and simultaneously enables a cost-effective migration path to new devices and emerging applications.
About Aruba Networks, Inc.

Aruba Networks is a leading provider of next-generation network access solutions for the mobile enterprise. The company’s Mobile Virtual Enterprise (MOVE) architecture unifies wired and wireless network infrastructures into one seamless access solution for corporate headquarters, mobile business professionals, remote workers and guests. This unified approach to access networks enables IT organizations and users to securely address the Bring Your Own Device (BYOD) phenomenon, dramatically improving productivity and lowering capital and operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at http://www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook.