

Retail



Best Practices to Simplify Retail Mobility Operations

Table of Contents

Executive Summary	2
Retailers Face Unique Enterprise Mobility Challenges	3
The Antidote to Complexity: Create an Operating Model that Leverages Industry Best Practices	3
Best Practice #1: Choose the Right Metrics for Success	4
Best Practice #2: Put Users at the Center of Operations	5
Best Practice #3: Standardize and Automate	7
Best Practice # 4: Focus on Interference Management	8
Best Practice #5: Delegate Responsibilities and Empower the Right People	9
Best Practice #6: Make Investment Decisions with a Solid Foundation of Data	10
Best Practice #7: Use Existing Infrastructure to Address PCI Compliance	12
Summary: Use AirWave to Minimize the Burden of Complexity in the Retail Enterprise Mobility Infrastructure	16

Executive Summary

Enterprise mobility has been and continues to be essential to retail operations. With mission-critical wireless applications to support and locations distributed across regional and even global geographies, they must put effective processes in place to ensure the uptime of their wireless LANs (WLANs). However, a number of factors create significant complexity for network management in retail environments:

- Remote store and warehouse locations with limited or no on-site IT staff
- Application-specific mobile devices such as printers and barcode scanners are the primary computing device on the network and are used by non-technical users.
- Payment Card Industry (PCI) compliance requirements that mandate wireless scanning, even if a WLAN is not present at a location
- Relatively long replacement cycles for wireless infrastructure, with multiple generations of products in deployment

To simplify their mobility operations, retailers need an effective operations model that encompasses planning, management, and troubleshooting processes across the entire infrastructure. Based on our work with more than 10,000 customers, Aruba has identified seven best practices make up such an operations model:

1. Chose the right metrics for success
2. Put users at the center of operations
3. Standardize and automate
4. Focus on interference management
5. Delegate responsibilities and empower the right people
6. Make investment decisions with a solid foundation of data
7. Use existing infrastructure to address PCI compliance

In this white paper, we will discuss each of the best practices in detail and describe how leading retailers have used the AirWave Wireless Management Suite™ from Aruba Networks to put them into practice. AirWave is the only integrated, multivendor operations management solution that manages wireless networks, wired infrastructure, and client devices in a single, user-centric interface that operates across multiple generations of products from more than 15 enterprise mobility infrastructure vendors, including Aruba, Cisco and Motorola.

AirWave helps retailers to ensure uptime of mission-critical networks, make better use of their valuable network engineering resources, protect the store more effectively, and manage PCI compliance with significantly fewer hassles.

1 Retailers Face Unique Enterprise Mobility Challenges

According to Gartner, retailers that are serious about mobility spend up to 10% of their overall IT budgets on these types of projects.¹ With mission-critical wireless applications to support and locations distributed across regional and even global geographies, they must put effective processes in place to ensure the uptime of their WLANs.

Remote troubleshooting is crucial, since stores and warehouses may have limited or no on-site IT staff. The workforce consists of a relatively high proportion of non-technical users working with a variety of handheld devices. Recent security breaches across a variety of industries have put protecting the store at the top of executives' worry lists. Finally, relatively long replacement cycles mean most retailers have multiple generations of wireless infrastructure running across different locations or even side-by-side.

All of these issues have led to an unprecedented level of wireless network complexity. Taken together with the volatile business environment over the last several years and new PCI compliance requirements, this complexity can potentially lead to escalating costs and a negative impact on the bottom line.

2 The Antidote to Complexity: Create an Operating Model that Leverages Industry Best Practices

While most retailers are striving to minimize wireless network complexity, their efforts can take them only so far. Even those retailers that are able to standardize on a common set of infrastructure from a single vendor cannot eliminate the biggest source of complexity: the mobility, unpredictable usage patterns, and diverse client devices of end-users themselves. Furthermore, most retailers simply have far too much invested in prior generations of WLANs to replace everything at once.

A more realistic approach is to minimize the burden of complexity with an effective operations model that encompasses planning, management, and troubleshooting

“When we upgrade our network, the new equipment is rolled out gradually across our locations, not overnight. We needed a way to configure and control our newer hardware without sacrificing manageability on our existing Cisco and Motorola infrastructure.”

James Lersch, Network Services Engineer for Giant Eagle

¹Gartner, “Market Trends: Enterprise Wireless LAN by Vertical Industry, Worldwide,” May 2010

processes across the entire infrastructure. Based on our work with more than 10,000 customers, Aruba has identified a number of best practices make up such an operations model. In the following sections, we will discuss those best practices in detail.

3 Best Practice #1: Choose the Right Metrics for Success

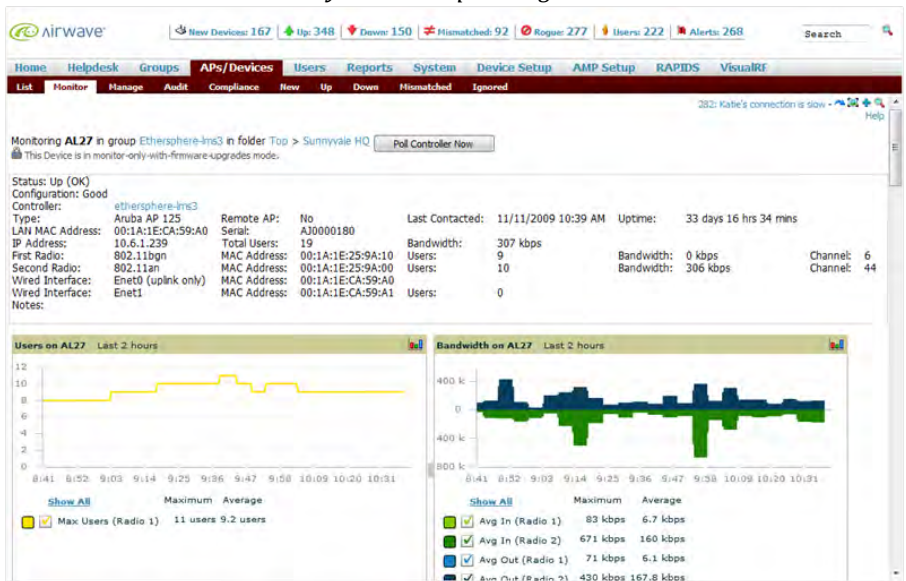
Ensuring uptime for mission-critical networks requires a laser focus on mean time to problem resolution (MTTR). After all, even the best-designed networks can behave unpredictably when you add mobile users, diverse client devices, and the physics of wireless communications into the equation. The bottom line is: How quickly can you repair a problem, regardless of where the fault lies?

AirWave gives you a complete picture of the devices on the network, including each device's current status and operation history. Visual dashboards in AirWave let you distinguish between what's normal for your network and what's not. You can then drill down into detailed information in just a few clicks. AirWave includes monitoring views for individual users, access points (APs), controllers, and switches, with upstream relationships mapped to enable root cause analysis.

For example, the AP monitoring page shown to the right provides a set of summary charts, data, and diagnostics that let network engineers and even service desk personnel identify potential problems and take action quickly. In addition, AirWave has

configurable alerts that automatically notify you about important conditions, including: down APs or radios, misconfigured devices, new devices discovered (including potential rogues), excessive AP usage, excessive numbers of connected clients, excessive bandwidth usage by individual clients, and IDS events. All of these alerts can be sent to you via email or directly to your existing network management system via SNMP, further accelerating time to response.

Figure 1. The AirWave AP monitoring page gives you a complete view of how your AP is operating.



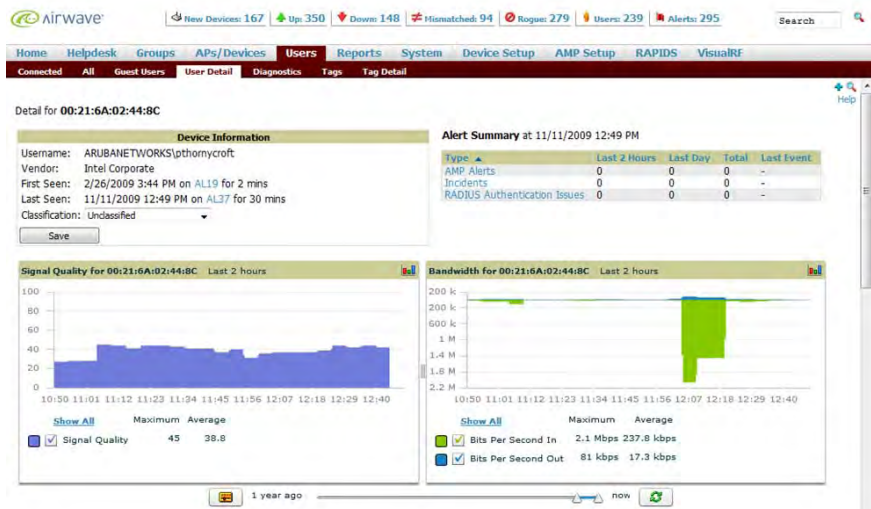
4 Best Practice #2: Put Users at the Center of Operations

Traditional network management paradigms center on ensuring uptime of APs and controllers. However, APs and controllers don't call the service desk with connectivity problems; users do. A user-centric approach to troubleshooting is easier and faster than an infrastructure-centric one, and it leads to higher user satisfaction. So, what does it really mean to be user-centric?

User-centric management is about looking at all of the issues that could affect service quality, from the user's standpoint. You may need to look at coverage in the user's area or how the closest APs are functioning. You may also need to be able to investigate root causes in the wired network or even outside of the network infrastructure. Regardless of the source, information about the potential causes of connectivity problems should be easily accessible to your staff while they are talking to users and investigating problems.

User-centric management is one of the key advantages cited by AirWave customers over using their element management systems for troubleshooting. Staff members can search for a user through a simple text search interface and gain instant access to a wealth of diagnostic information displayed on an intuitive dashboard. In addition, AirWave is able to map upstream relationships between APs, controllers, and switches. It also tracks RADIUS authentication failures because user connectivity problems are frequently caused by incorrect passwords or RADIUS servers that are down.

Figure 2. The AirWave user details page displays critical network information from the standpoint of a single user.



“The interface is very intuitive.... We can understand what's going on in our network visually rather than having to dig into the guts of our equipment. All of the information we get — including client connection history — has sped up the troubleshooting process for my team.”

*Gary Putman, Enterprise Network Manager
Cabela's, the world's largest direct marketer of hunting, fishing, camping and related outdoor merchandise*

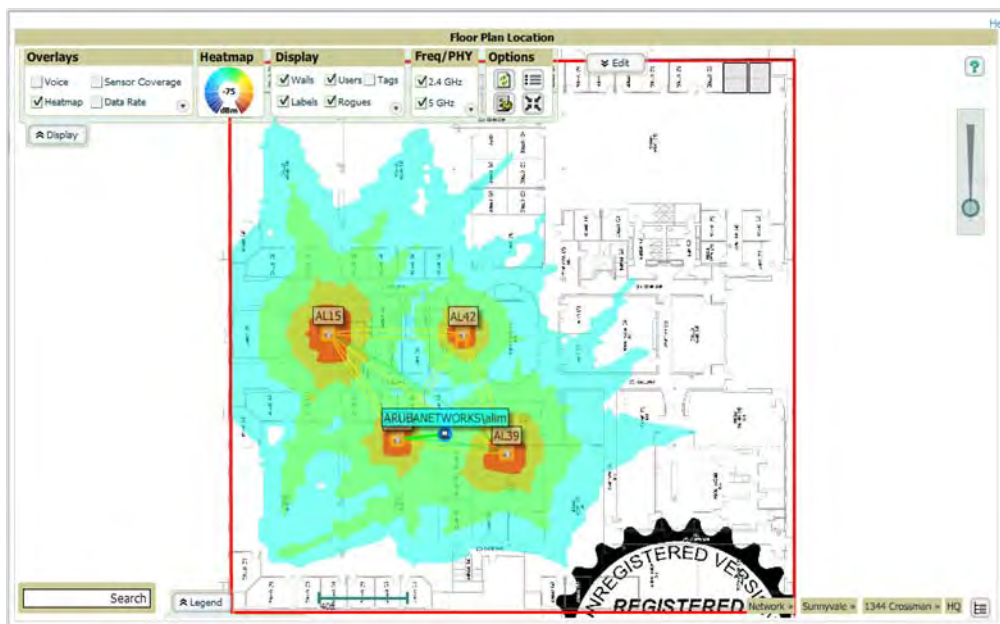
For retailers in particular, location information is an absolute necessity for user-centric management. Many of the connectivity problems that Aruba customers see in store and warehouse environments are caused by users' movements – either because of unforeseen coverage gaps or sticky roaming, a problem common with some handhelds where the handheld remains associated with one AP after the user has moved to a distant location. In order to solve these problems, you can't look only at what AP a user is connected to; you also have to have insight into his or her location and movements. With AirWave's VisualRF module, you can determine exactly where a user is and what the RF environment looks like in his or her area.

Furthermore, you can track the user's movements for a period of up to 24 hours to see if his or her movements explain the connectivity problems being experienced.

Potential actions to take with AirWave data: A user complains about intermittent slow connections during the work day. Looking at the AirWave user details page, you see that signal quality has varied significantly. You can then use VisualRF to track his or her movements and determine that the connectivity problem was caused by sticky roaming rather than coverage holes.

In summary, Aruba customers have found user-centric network management saves time during the troubleshooting process, increases user satisfaction, and improves service quality by shifting resources from reactive problem resolution to proactive problem avoidance.

Figure 3. VisualRF's heat map view depicts the strength of the RF coverage in each location.



5 Best Practice #3: Standardize and Automate

Even for wireless networks that comprise of equipment from multiple vendors or multiple generations from the same vendor, AirWave can help you standardize configurations. AirWave provides a simple, easy-to-use configuration interface that operates across firmware versions for different products and product generations. In fact, one customer told Aruba about a situation when its vendor sent out an early version of a firmware update that changed SNMP object identifiers (OIDs). Working with the customer, AirWave was able to accommodate this change faster than the vendor's own element management system was able to do so! AirWave also supports APs that may have been discontinued by the manufacturer. Furthermore, AirWave simplifies the process of finding non-standardized devices through an audit report that lists all misconfigured devices across the network. This makes the task of ensuring compliance much easier.

Figure 4. The AirWave Config Audit Report provides a complete list of misconfigured devices to investigate, independent of vendor or product.

Name	Folder	Group	Mismatches												
00:0b:86:66:18:a7	Top > Sunnyvale HQ > HQ-RAP	HQ-RemoteAP	<table border="1"><thead><tr><th>Current Device Configuration</th><th>Desired Device Configuration</th></tr></thead><tbody><tr><td>Master Discovery Type (failed to fetch)</td><td>AP Discovery Protocol</td></tr><tr><td>Name aankumah-RAP-5WN</td><td>00:0b:86:66:18:a7</td></tr><tr><td>PPPoE Authentication (failed to fetch)</td><td>No</td></tr><tr><td>Remote AP (failed to fetch)</td><td>No</td></tr><tr><td>Use DHCP (failed to fetch)</td><td>No</td></tr></tbody></table>	Current Device Configuration	Desired Device Configuration	Master Discovery Type (failed to fetch)	AP Discovery Protocol	Name aankumah-RAP-5WN	00:0b:86:66:18:a7	PPPoE Authentication (failed to fetch)	No	Remote AP (failed to fetch)	No	Use DHCP (failed to fetch)	No
Current Device Configuration	Desired Device Configuration														
Master Discovery Type (failed to fetch)	AP Discovery Protocol														
Name aankumah-RAP-5WN	00:0b:86:66:18:a7														
PPPoE Authentication (failed to fetch)	No														
Remote AP (failed to fetch)	No														
Use DHCP (failed to fetch)	No														
00:0b:86:66:21:1c	Top > Sunnyvale HQ > HQ-RAP	HQ-RemoteAP	<table border="1"><thead><tr><th>Current Device Configuration</th><th>Desired Device Configuration</th></tr></thead><tbody><tr><td>Master Discovery Type (failed to fetch)</td><td>AP Discovery Protocol</td></tr><tr><td>Name alim-5wn</td><td>00:0b:86:66:21:1c</td></tr><tr><td>PPPoE Authentication (failed to fetch)</td><td>No</td></tr><tr><td>Remote AP (failed to fetch)</td><td>No</td></tr><tr><td>Use DHCP (failed to fetch)</td><td>No</td></tr></tbody></table>	Current Device Configuration	Desired Device Configuration	Master Discovery Type (failed to fetch)	AP Discovery Protocol	Name alim-5wn	00:0b:86:66:21:1c	PPPoE Authentication (failed to fetch)	No	Remote AP (failed to fetch)	No	Use DHCP (failed to fetch)	No
Current Device Configuration	Desired Device Configuration														
Master Discovery Type (failed to fetch)	AP Discovery Protocol														
Name alim-5wn	00:0b:86:66:21:1c														
PPPoE Authentication (failed to fetch)	No														
Remote AP (failed to fetch)	No														
Use DHCP (failed to fetch)	No														
00:0b:86:c3:58:98	Top > Sunnyvale HQ > HQ-RAP	Aruba HQ	<table border="1"><thead><tr><th>Current Device Configuration</th><th>Desired Device Configuration</th></tr></thead><tbody><tr><td>Master Discovery Type (failed to fetch)</td><td>AP Discovery Protocol</td></tr><tr><td>Name dpeterson-RAP-2WG</td><td>00:0b:86:c3:58:98</td></tr><tr><td>PPPoE Authentication (failed to fetch)</td><td>No</td></tr><tr><td>Remote AP (failed to fetch)</td><td>No</td></tr><tr><td>Use DHCP (failed to fetch)</td><td>No</td></tr></tbody></table>	Current Device Configuration	Desired Device Configuration	Master Discovery Type (failed to fetch)	AP Discovery Protocol	Name dpeterson-RAP-2WG	00:0b:86:c3:58:98	PPPoE Authentication (failed to fetch)	No	Remote AP (failed to fetch)	No	Use DHCP (failed to fetch)	No
Current Device Configuration	Desired Device Configuration														
Master Discovery Type (failed to fetch)	AP Discovery Protocol														
Name dpeterson-RAP-2WG	00:0b:86:c3:58:98														
PPPoE Authentication (failed to fetch)	No														
Remote AP (failed to fetch)	No														
Use DHCP (failed to fetch)	No														
00:0b:86:c3:59:03	Top > Sunnyvale HQ > HQ-RAP	HQ-RemoteAP	<table border="1"><thead><tr><th>Current Device Configuration</th><th>Desired Device Configuration</th></tr></thead><tbody><tr><td>Master Discovery Type (failed to fetch)</td><td>AP Discovery Protocol</td></tr><tr><td>Name mathieson-RAP-2WG</td><td>00:0b:86:c3:59:03</td></tr><tr><td>PPPoE Authentication (failed to fetch)</td><td>No</td></tr><tr><td>Remote AP (failed to fetch)</td><td>No</td></tr><tr><td>Use DHCP (failed to fetch)</td><td>No</td></tr></tbody></table>	Current Device Configuration	Desired Device Configuration	Master Discovery Type (failed to fetch)	AP Discovery Protocol	Name mathieson-RAP-2WG	00:0b:86:c3:59:03	PPPoE Authentication (failed to fetch)	No	Remote AP (failed to fetch)	No	Use DHCP (failed to fetch)	No
Current Device Configuration	Desired Device Configuration														
Master Discovery Type (failed to fetch)	AP Discovery Protocol														
Name mathieson-RAP-2WG	00:0b:86:c3:59:03														
PPPoE Authentication (failed to fetch)	No														
Remote AP (failed to fetch)	No														
Use DHCP (failed to fetch)	No														

Furthermore, conditions can change rapidly. Given the mission-critical nature of most retailers' wireless networks, it is essential to have a system of early warnings to prevent problems before they occur. AirWave includes a number of alerts that let staff know immediately when certain thresholds are met. These triggers include high channel utilization, excessive AP usage (bandwidth in/out), number of connected clients exceeding a threshold you set, and excessive bandwidth usage by individual clients. You establish the trigger points for and criticality of each alert yourself, so that you only get notified about meaningful events.

Potential action: A network administrator at a retailer receives several alerts about high user counts on January 25. His organization conducts annual inventory during this period in preparation for its January 31 fiscal year-end; scanner gun usage is always extremely high. He knows that inventory is the primary cause of the high user counts but that some new VoIP phones are also in operation. After looking at the last six months' data, he knows that he'll need to increase capacity significantly before the holiday season.

6 Best Practice # 4: Focus on Interference Management

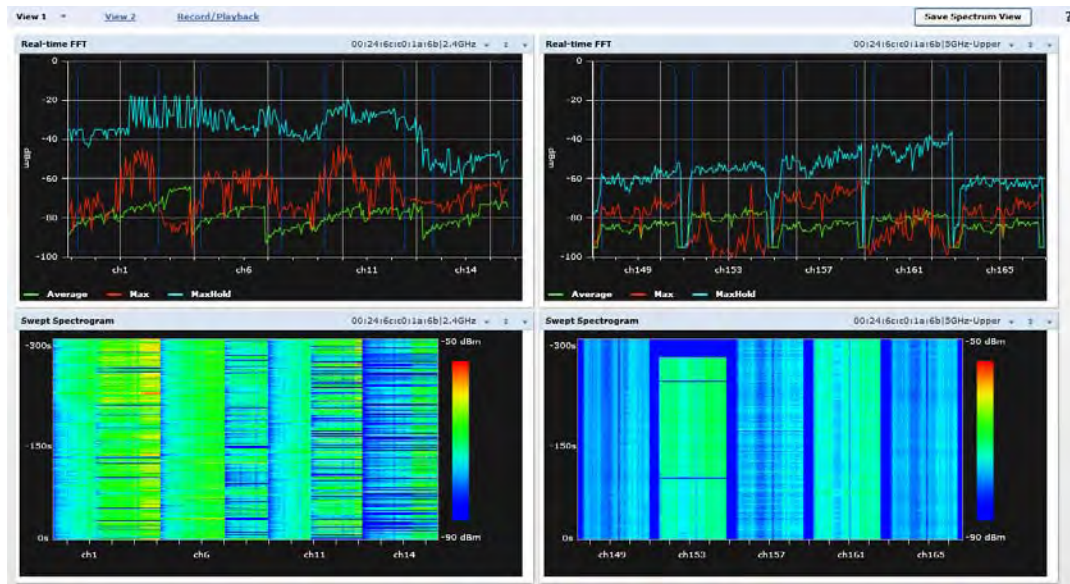
Interference management is an area that deserves a special focus for retailers. Retail environments — particularly those situated in high-density areas like malls or shopping centers — suffer from dirty air filled with interference from a variety of sources. To help automate interference management, AirWave provides visibility into RF performance across the network.

Organizations using Aruba APs can take advantage of advanced capabilities, including Aruba's new Spectrum Analyzer Module and its Adaptive Radio Management (ARM) technology. Enabled in ArubaOS, the Spectrum Analyzer quickly identifies potential sources of interference and jamming that could affect network reliability. The Spectrum Analyzer module, which can be enabled post-installation on any Aruba 802.11n AP, includes new capabilities such as interference charts, channel quality, and spectrum recording and playback. These data help isolate packet transmission issues, over-the-air quality-of-service (QoS) problems, and traffic congestion caused by contention with other devices operating in the same band or channel. Appropriate remediation measures can then be put in place to return the network to full performance. Aruba's ARM technology uses automatic infrastructure-based controls to take the guesswork out of RF management and maximize the performance and reliability once your APs are deployed. With these controls, ARM can adjust your network around the sources of interference — 802.11 and non-802.11 — whenever possible.

Figure 5. Setting up an alert in AirWave.

The screenshot shows the 'Trigger' configuration window in AirWave. It is divided into several sections: 'Type' (Device User Count), 'Severity' (Major), and 'Duration' (10 minutes). The 'Conditions' section shows 'Available Conditions: User Count' with an 'Add' button and a table with columns 'Option', 'Condition', and 'Value'. The table contains one row: 'User Count', '>=', and '10'. The 'Trigger Restrictions' section includes 'Folder' (Top), 'Include Subfolders' (Yes selected), and 'Group' (- All Groups -). The 'Alert Notifications' section includes 'Additional Notification Options' (Email and NMS checkboxes), 'Logged Alert Visibility' (By Role dropdown), and 'Suppress Until Acknowledged' (Yes selected). 'Add' and 'Cancel' buttons are at the bottom right.

Figure 6. The Spectrum Analyzer dashboard offers a summary update of all spectrum analyzer functions.



Potential actions: A retailer is running 802.11n voice handsets and 802.11b handheld scanners in its stores. Because of their inefficient use of the spectrum, the scanners can decrease performance on the handsets. Because the stores have Aruba APs, the retailer is able to implement ARM’s “airtime fairness” feature, which limits how much time is allocated to the 802.11b clients. As a result, it is able to increase throughput and reduce the RF utilization in the air.

Did You Know?

WLAN disruptions often occur because the plethora of Bluetooth devices, wireless cameras, and other consumer technologies that are present in retail environments operate in the same ISM (industrial, scientific and medical) bands. This is why spectrum analysis tools are critical to identify and mitigate interference.

7 Best Practice #5: Delegate Responsibilities and Empower the Right People

Few retailers have the resources to place skilled network engineering staff in every store and distribution center. These valuable resources often have to cover multiple locations, while working with on-site non-technical staff to get problems resolved. Depending on the size of your organization and the makeup of your wireless network, it may make sense to delegate responsibilities geographically or by type of facility (retail stores, distribution centers, and corporate offices).

AirWave lets you provide data access to people across the IT organization – network engineers, network operations center staff and service desk personnel – without sacrificing security or control. Each staff member is assigned a role that specifies whether he or she has read-only, read-write, or audit privileges. In addition, you can restrict administrative privileges to a location and/or a set of devices in addition to role. Team members may not view monitoring or configuration information for portions of the network for which they do not possess the appropriate permissions.

Potential action: Give on-site or geographically assigned IT staff read-only access to AirWave, along with basic training on troubleshooting. Create separate folders in AirWave that correspond to how you define your business (for example, corporate, distribution centers, stores-east, and stores-west) to restrict information to the areas that each staff member covers and to facilitate escalations from on-site staff to network engineering.

Did You Know?

Many AirWave customers estimate that less than ten percent of wireless trouble tickets are escalated to WLAN engineering, a much lower rate than before they implemented the solution.

8 Best Practice #6: Make Investment Decisions with a Solid Foundation of Data

With tight budgets and many competing priorities around enterprise mobility, every dollar invested needs to count. The best way to make good decisions is with a solid foundation of data about what users are actually doing on the network and how it is performing. The seasonal variations in retail mean that 30 or 90 days of data is rarely enough; every decision needs to be made with the context of both peak and average usage, taking the Christmas holiday season into account.

AirWave captures over one year of historical data. It makes information immediately accessible to IT through dashboards, alerts, and standard or customizable reports.

The **User Session Report** is particularly useful for gaining insights on how users are using the network. It displays information such as the number of users, average session duration, and average session traffic. You can break this information down by connection mode (802.11a/b/g/n). The report can analyze your entire network, or it can focus in on a specific portion of the network or even a single AP.

Potential actions you can take with AirWave data: If you see a lot of legacy 802.11b connections, you may need to upgrade clients or consider changing supported 802.11 data rates in order to increase network performance.

Figure 7. The AirWave User Session Report.

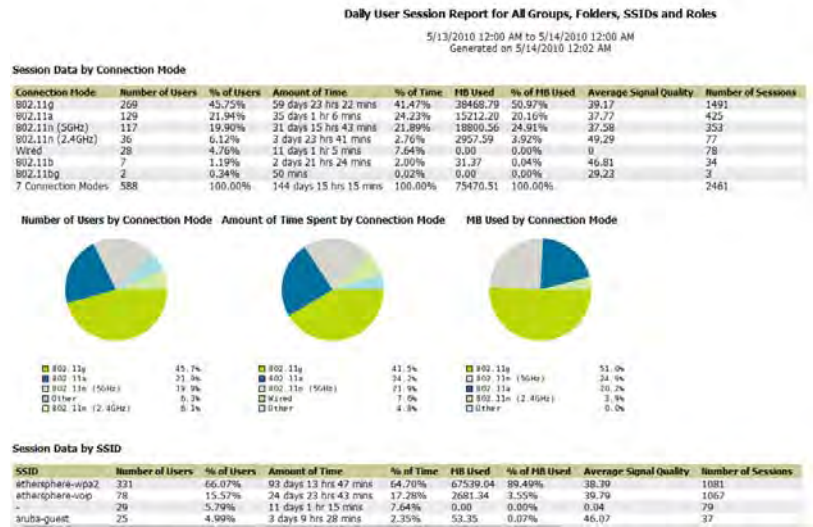
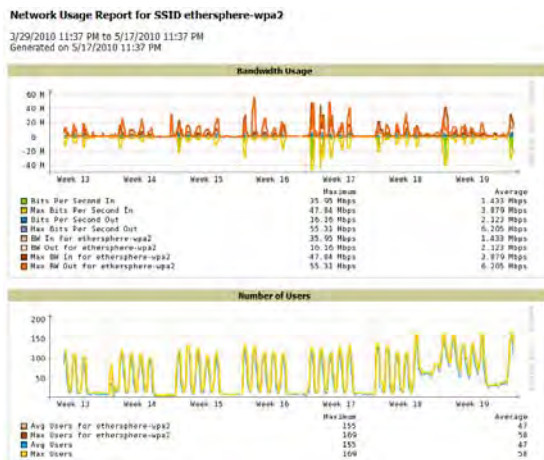


Figure 8. The Network Usage Report.



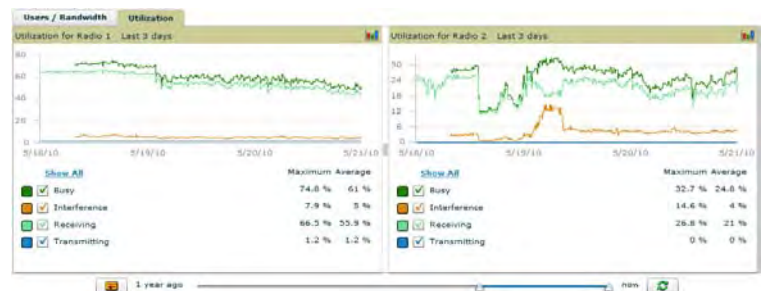
The **Network Usage Report** provides you with a snapshot of your users and the bandwidth that is being used on all or part of the network. It gives you an at-a-glance view indicating how network use is growing.

Potential action: Plan your future network expansion or rightsizing with a clear picture of user adoption trends.

Channel Utilization metrics available on the AP monitoring page help you identify APs and areas that are exceeding capacity, as well as the reasons for high capacity. An intuitive set of graphs breaks down the percentage of time that radios are transmitting data, receiving data, listening, and experiencing interference. Using AirWave's device summary report, you can identify the APs with the highest channel utilization and then drill down on each individual AP for further detail.

Potential action: Target upgrades from 802.11 b/g equipment to 802.11n for areas where channel utilization is the highest.

Figure 9. Channel utilization metrics in AirWave.



“Being able to see what our users are doing on the network, having a single view of information across all 300 stores, and analyzing historical data to find trends – all of this helps us to make better decisions.”

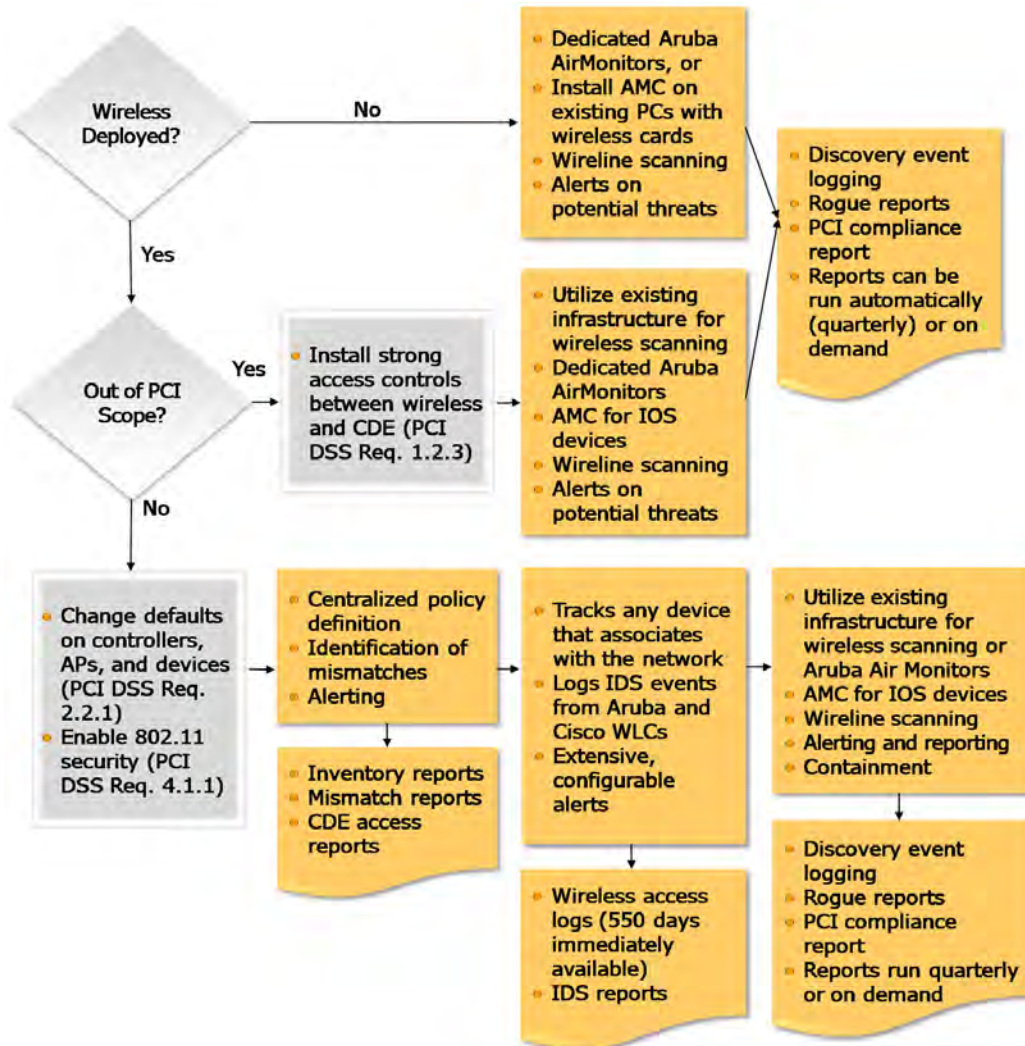
Security and Architecture Manager, Major Canadian Retailer

9 Best Practice #7: Use Existing Infrastructure to Address PCI Compliance

Compliance with the PCI Data Security Standard (DSS) is a top concern of virtually every retailer. With numerous guidelines intended to help organizations proactively protect customer account data and extensive reporting requirements, retailers need to think carefully about how to stay in compliance and how to prove compliance on an ongoing basis without breaking their budgets.

As the flowchart on the next page illustrates, the Wireless Guidelines (Requirements 11.1 and 11.2) mandate wireless scanning and an incident response plan on the part of every merchant, even if that merchant is not using a WLAN. Those retailers that operate a WLAN for non-cardholder transmissions and those that transmit cardholder data over their WLANs face a number of additional requirements. For a deeper review into the requirements of PCI DSS 1.2, refer to Aruba’s [white paper](#) available on www.arubanetworks.com.

Figure 10: Key Requirements from PCI DSS 1.2 Wireless Guidelines



Retailers have several choices for how to implement wireless scanning. They can meet the requirement simply by performing a physical scan at each site every quarter, or they can automate the process using solutions such as AirWave RAPIDS™. The automated scanning approach is less costly for retailers with many remote stores and significantly more secure than a quarterly manual check.

The Aruba solution takes much of the repetitive, manual work out of PCI compliance and reporting. It is the most cost-effective solution available because it can leverage your existing wireless network – utilizing data from any APs made by the 15+ vendors that AirWave supports – to act as wireless sensors. In cases where the wireless network cannot be leveraged or where no wireless networks are present, Aruba's affordable 802.11a/b/g/n APs can serve as dedicated sensors that locate rogue

wireless devices, monitor for attacks, and shield clients from attaching to rogue devices. In both cases, RAPIDS does not require any changes to be made to the existing wireless or wired networks.

All of Aruba's APs are multi-purpose devices. They can be used as hybrid sensors/APs or as dedicated sensors. They can be used for spectrum analysis, identifying and mitigating interference. Finally, retailers that do not have immediate needs for a WLAN can deploy Aruba APs as dedicated sensors today and easily convert them into APs should wireless connectivity be required at a later date.

An oil and gas company with no wireless networks deployed for operational purposes needed to perform scanning for wireless devices at its retail gas stations. After evaluating a number of IDS vendors, the company found Aruba's AP-105, centralized 6000 Controller with M3 controller modules and AirWave solution to be the simplest to deploy and the most cost-effective solution to operate.

Deployed in conjunction with Aruba APs or with your existing wireless network, RAPIDS provides a practical, cost-effective solution for enforcing security policies and managing PCI compliance. Using a patented combination of wireless and wired network scans, RAPIDS automatically detects and locates unauthorized APs using your existing, authorized APs and air monitors to scan the RF environment for any unauthorized devices in range. Unlike many other wireless security solutions, it also scans your wired network to determine whether any unknown devices have been connected. RAPIDS then correlates all of this data and uses a set of rules to highlight only those devices that are truly a threat to your organization. Companies can set up automated, prioritized alerts that can be emailed to a specified distribution list the instant that rogues are detected.

RAPIDS is able to classify potential threats based on rules you customize to define what a rogue device is. Given that retailers often see an overwhelming number of unidentified devices coming from neighboring businesses, these rules save significant amounts of time for network engineering and security staff. RAPIDS significantly reduces the number of false-positives so that your security team can focus on the most significant threats first.



Rogue Detection and Mitigation at Cabela's

Cabela's is a leading specialty retailer, and the world's largest direct marketer, of hunting, fishing, camping and related outdoor merchandise. Because its stores are in central shopping areas, the company captures huge quantities of rogue data – as many as 20,000 events per day, mostly from neighboring businesses. RAPIDS, along with location tracking in AirWave VisualRF, has helped the security team to remove actual threats much more quickly. "With AirWave being able to monitor Cisco switch ARP/ CDP tables, we know exactly where a rogue client may physically be plugged into the network," says Matt Perry, an engineer in the Enterprise Network Group. "Then, we can proactively close security holes."

The PCI auditing capabilities of RAPIDS allow organizations to monitor, audit, and demonstrate real-time PCI compliance on the network. The system can alert network staff whenever a configuration error is detected, providing complete information as to how the configuration violates defined policy.

RAPIDS creates a full report listing all suspected rogues for compliance reporting. Reports can be run on a scheduled or ad hoc basis to meet the organization’s specific requirements. As staff investigates potential rogues, RAPIDS provides an Acknowledge Yes/No flag for every device as a workflow management feature. RAPIDS provides a grade for the network as a PASS or FAIL for each PCI requirement that is enabled, allowing security teams and auditors to quickly confirm compliance in an easy-to-use report.

Figure 11. The PCI Report provides an at-a-glance view of compliance status, along with detailed information about what issues need to be addressed.

Daily PCI Report for Groups Ethersphere-lms3, Aruba HQ, Cisco Gear

11/5/2009 11:00 PM to 11/6/2009 11:00 PM
Generated on 11/6/2009 11:02 PM

This report covers sections of the Payment Card Industry (PCI) Data Security Standard (DSS) Version 1.2 requirements that are relevant to security in your network. PCI DSS standard requirements are available at <https://www.pcisecuritystandards.org>.

Disclaimer: The PCI Compliance Report must be completed by an authorized QSA. The sole purpose of this report is to provide IT administrators with an on-demand internal audit of components that are visible to AirWave Wireless Management Suite.

Summary

PCI Requirement	Description	Status
1.1	Configuration standards for routers. A device fails if there are mismatches between the desired configuration and the configuration on the device.	Fail
1.2.3	Install firewalls between any wireless networks and the cardholder data environment. A device passes if it can function as a stateful firewall.	Pass
2.1	Always change vendor-supplied defaults. A device fails if the usernames, passwords or SNMP credentials being used by AWMS to communicate with the device are on a list of forbidden credentials. The list includes common manufacturer defaults.	Pass
2.1.1	Change vendor-supplied defaults for wireless environments. A device fails if the passphrases, SSIDs or other security-related settings are on a list of forbidden values. The list includes common manufacturer defaults.	Pass
4.1.1	Use strong encryption in wireless networks.	Pass

Furthermore, because RAPIDS seamlessly integrates with AirWave, it has a complete view into default password enablement and wireless association information. RAPIDS provides detailed user tracking and session history, showing who is connected to your network, when they connected, and where they have roamed. These capabilities support the additional DSS requirements for retailers with WLANs in the cardholder data environment (CDE).

For more detailed information about RAPIDS works, please refer to the [white paper](#).

Summary: Use AirWave to Minimize the Burden of Complexity in the Retail Enterprise Mobility Infrastructure

The best practices described in this white paper all serve to simplify retail mobility operations despite the use of multivendor, multigeneration wireless networks that must support a diverse range of mobile client devices. They help retailers to ensure uptime of mission-critical networks, make better use of their valuable network engineering resources, protect the store more effectively, and manage PCI compliance with significantly fewer hassles.

AirWave is the key to putting the six best practices into effect today. Regardless of whether your network consists of equipment from a single vendor or multiple generations of products from multiple vendors, AirWave gives you a single operational view with data that guides you to better decisions. AirWave brings a number of advantages to your organization, including:

- **A better user experience:** Unlike element management systems, AirWave has been designed from the ground up as an operations solution for the whole IT organization, from the service desk, to the network operations center to network engineering. Each team member has role-based access to relevant information such as the dashboards and reports shown throughout this white paper, and they can use the system productively with minimal training.
- **User-centric management:** AirWave gives you a single, accurate picture of everything that affects service quality for your users — from wired infrastructure, to the RF environment, to individual mobile devices. It also integrates easily with existing IT service management tools for faster problem resolution.
- **Intelligence for better decision-making:** With the wealth of information available in AirWave and data that spans days, months, and seasons, you always have what you need to spot trends, plan capacity, and craft the right strategies for your company.
- **Easier PCI compliance:** AirWave provides practical, cost-effective solutions to meet PCI requirements with less hassle and to protect the store.

AirWave can be used in a variety of deployment modes to meet your specific needs, whether you have 10 stores in a 100-mile radius or 2,000 stores across the globe. Whether deploying on-premise, using an AirWave appliance, or in the Cloud, many retail organizations have simplified their mobility operations within weeks of their purchases. AirWave can bring you the operating efficiency you need to stay ahead in today's economy.

About Aruba Networks

Aruba is the global leader in distributed enterprise networks. Its award-winning portfolio of campus, branch/teleworker, and mobile solutions simplify operations and secure access to all corporate applications and services – regardless of the user’s device, location, or network. This dramatically improves productivity and lowers 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, Facebook, or the Green Island News Blog.



1344 Crossman Ave. Sunnyvale, CA 94089-1113
Tel. 408.227.4500 | Fax. 408.227.4550 | 1-866-55-ARUBA
info@arubanetworks.com | <http://www.arubanetworks.com>