



# Runaway

**IT'S EVERY LOGISTICS MANAGER'S NIGHTMARE:** On the eve of the close of a critical quarter, wave after wave of rush orders for shipments hit, straining logistics personnel and systems to the breaking point. Suddenly, the already stressed warehouse manager receives a phone call from one of his foremen: the new wireless handheld terminals that were installed three months earlier as part of an upgrade of the company's Wireless Local Area Network (WLAN) inexplicably are working one minute and then quit working the next. Shipments are arriving late on the shipping dock with vital elements missing from orders, and it's unclear whether out-of-stock positions exist in some key products. The warehouse manager places a frantic call to the head of IT, who is already aware of the problem and is hurriedly trying to determine the cause in order to implement a fix on the fly.

# WLAN:

## Managing Wireless in the Open Standards Environment

IT WASN'T SUPPOSED TO BE LIKE THIS. AFTER ALL, WLANs have been integral parts of warehouses and manufacturing for years now and continue to spread to other fields. Radio frequency (RF) equipment and wireless devices have become more sophisticated and robust. So why do nightmares continue to plague users' WLANs? And how can users protect themselves from such meltdowns?

In part, this type of problem occurs with frustrating frequency as a by-product of how the wireless arena has evolved, as well as how users have approached upgrades. It used to be that companies adopting a wireless system for tying together sales, manufacturing, and logistics only had to deal with a single vendor who provided an end-to-end system. These systems most often relied on proprietary technology only offered by that vendor. While the single-source solution often insured compatibility, such systems were expensive and left companies wedded to a single vendor. If a new device or software tool came along that the user wanted, but wasn't compatible with the installed system, the user was out of luck.

### EVOLVING TO OPEN STANDARDS

Enter the brave new world of open systems operating on a standard platform. This shift from proprietary to open standards has put greater power in the hands of customers, enabling them to shop among various device and software features.

While open standards reduced equipment cost, it made the design and management of WLANs much more complex. Instead of an end-to-end system supplied by a single vendor, today's WLANs typically rest on a multi-vendor platform. It's not uncommon for today's WLANs to incorporate features from four or five vendors. This has dramatically increased the complexity of WLANs, not to

mention the potential for problems, particularly when upgrades, new applications, or new devices are installed.

"Problems today are much more common than is generally realized," says Tom Barber, business development manager at PEAK Technologies. Indeed, when a serious problem crops up on a WLAN today, the result can be disastrous. As Barber explains, "It's really the case today that companies can't do without their WLANs. A typical item moves through the manufacturing or warehouse system so quickly that the company might not have even paid for it by the time it's out the door and on the way to the customer."

WLANs have enabled users to maintain lower inventory levels, hold down their costs, and dramatically shorten the time from order to delivery. The danger of this tighter supply chain is that there is little margin for error. "Any hiccup in the system and you can have major problems," adds Barber.

Phil Ballai, director, network sales, at Symbol Technologies, explains that WLAN technology—and industry standards—continue to mature and improve. Having said that, Ballai adds, "There is much work to be done in many areas such as security, standardized management, and mobility attributes, such as Fast Roaming. While the 802.11 protocol is roughly 10 years old, today's variants are much more recent, and some are still not fully ratified. Some vendors elect to implement pre-standard versions in products, which carry inherent risk with the eventual ratification being potentially different or slightly modified." While users are aware of the benefits of WLANs, Ballai says, "most don't fully grasp the immaturity of technology from a standards and multi-vendor environment viewpoint."

### NAVIGATING THE NEW ENVIRONMENT

Ken Whelan, director of partner sales at Wavelink, echoes that assessment. "The wireless environment today is less

and less homogenous. The vast majority of users have a mixture of Cisco, Intermec, Symbol, Zebra, and any number of devices from other manufacturers. Moreover, wireless today isn't just about access points and wireless devices. It's about peripherals, too, such as mobile printers. You've got to think about managing the complete wireless domain environment."

Unfortunately, many companies' IT departments are ill equipped to cope with the kinds of problems that can develop on the newly expanded WLANs. Most enterprise IT groups were set up to deal with desktop computers in a wired network environment. With the advent of WLANs, many IT departments are still learning the differences and nuances of WLAN environments. "It's no real fault of the IT group," Barber adds. "They're geared to fight a different battle."

Ballai explains, "In my experience, most IT professionals are eager to learn new technologies and do so readily. That said, 802.11 is evolving very quickly and often IT professionals are involved with many other projects. This makes it difficult for them to stay on the 'leading edge' of technology developments in general. I strongly encourage IT professionals to seek out experts in each area of interest and ask questions. Leverage the experience of others and build relationships that will ultimately benefit everyone."

Smart users of WLANs acutely understand two basic

### ➤ WLAN: A Different Animal

**Beyond the simple fact that radio waves are used in place of cables, WLANs differ fundamentally from wired networks of desktop computers. Some of these differences include:**

- **Most WLANs utilize a shared access or "hub" architecture, rather than a switch architecture for a wired network**
- **The bandwidth of a WLAN is far less than a wired network**
- **Data transmission over a WLAN is less reliable than over a wired network**
- **Additional attention needs to be paid to the security of a WLAN**
- **Devices on a WLAN need to be able to seamlessly and reliably roam between access points**

**For further Wireless RF Services, go to [www.peaktech.com/html/solutions/wireless\\_rf\\_services.htm](http://www.peaktech.com/html/solutions/wireless_rf_services.htm)**



facts: One, wireless mobile computing systems today are mission critical to the organization. If all the transaction data gathered by a WLAN running SAP software, for example, suddenly had to be done by hand, it would be impossible to handle all the paper. The workload would be crushing.

Secondly, wireless systems are fundamentally different creatures from wired ones. Take the terminals, the most obvious part of the system to any user. Desktop terminals

on wired networks contain tremendous computing power, display enormous quantities of information, and run on a robust, reliable power supply. Handheld terminals on wireless computing networks function in a completely different environment and can present new challenges, including displaying a limited amount of data on a small screen and running on batteries that have to be recharged.

### WITH WLAN, A DIFFERENT SET OF CHALLENGES

Those are just the differences that meet the eye. Inside the systems, the differences are even more profound. A wireless network carries with it these additional considerations: The bandwidth, or volume of data that can be transmitted in a period of time, is far less with a wireless system. Unlike wired networks that are based on a switch architecture, most wireless systems utilize shared access or "hub" architecture. Moreover, data transmission over a wireless system can be less reliable than information transferred on a wired one. And like a cell phone, wireless systems "roam" between access points. Finally, there is the issue of security. Unless properly secured, a wireless system's signal can be picked up and used as an unauthorized method of accessing an organization's wired network and servers.

The challenge of implementation is highlighted by the experience of Ruth Landes, IT project manager for Intermec Technologies Corp., a leader in supply-chain systems. In 1999, Intermec implemented a wireless management system for its 50,000-square-foot warehouse using a best-in-breed strategy that featured a bolt-on wireless system to its SAP system. The company decided in 2003 to convert to SAP

Warehouse Management (WM). The new system promised the capability of cutting hours out of the time required to fill rush orders and an end to the reconciliation issues.

### PLAN AHEAD FOR WLAN IMPLEMENTATION

Even with eight months of diligent preparation for the

**continued on page 13 ...**



**Running PEAK IntelliField on handhelds empowers a customer-service engineer with point-and-click workflow software that supports all of their tasks.**

tracking, customer sign-off, access to inventory and customer account data, communicating over a wireless network to a server that interfaces with PEAK's ERP system, and viewing prompts with suggestions for cross-selling opportunities.

Before traveling to the customer's site, a CE can pull up contact information, a listing of equipment, a history of service calls, and the status of service contracts on each piece of equipment. If parts are needed, the CE can instantly access a database that shows the location of every part in PEAK's local inventory. As the CE clocks in and out of the application, recording the time and parts used, the application automatically tallies the costs, captures customer sign-off, and allows the CE to perform a short customer satisfaction survey.

The bottom line is a substantial improvement in cash flow as the bill can now be printed and mailed before the CE leaves the customer's site. According to Shriane, "We are projecting that as we roll the solution out to our entire field-service force, we will increase our first-time repair percentage by 15%, reduce service time per call by 20%, reduce inventory by 15%, reduce costs by decreasing field-service support staff hours, and increase sales revenues generated by CEs by almost 60%."

... continued from page 6

transition, Intermec did encounter a problem with its mobile printers: they were programmed to communicate with the first access point instead of roaming to the closest access point. Fortunately, the problem was caught and corrected during the two-week shakedown of the system prior to going live. "The implementation was very seamless," Landes says. "No one realized that we had done it." The benefits of expanding the system were immediate to Intermec. "We have better control of our assets and better customer service, so we're not making promises to clients that we can't keep."

In the end, a successful WLAN expansion boils down to planning and preparation. Ballai offers users the following advice: "Do your homework. Just because you plug wireless access points/ports into your wired Ethernet does not mean your wired Ethernet vendor understands the concept of wireless mobility. Consider all the factors typically involved like: Which mobile devices will be used now and in the future? What operating systems will they run? How much bandwidth will these various devices need and where? What type of security will you want to run? How will you maintain a secure connection in a highly mobile environment with good quality of service?"

PEAK's Barber says the extra planning and preparation upfront for upgrades over the life of a WLAN is worth the investment. "Compared to the cost of fire alarms, in terms of lost productivity and angry customers, the cost of wireless network and mobile computer monitoring software and making certain upgrades are applied in the least disruptive manner over the life of the system pays for itself," says Barber.

That's a mission-critical lesson best learned with well constructed plans, not 20/20 hindsight.

