

**Five Reasons Why You Should Upgrade
Your Wireless Network to 802.11
And what you need to consider once you decide to upgrade.**



Introduction

It's time to upgrade your old 900 MHz wireless backbone and terminals. We know how attached you are to them. They've been a reliable companion for so many years and were likely your first venture into wireless data collection. But technology has come a long way since you and your wireless network first met. And making the transition from 900 MHz to 802.11 has become a straightforward task that offers many incremental benefits. We've written this white paper to help you understand life without your legacy equipment. A life that is simpler, faster and more secure.

1. Open Standards

802.11 is an extremely robust open standard, and as we all know, open standards encourage competition among manufacturers to develop better and more cost-effective solutions.

So for starters, today's wireless computers are simply much easier to operate than what you are currently using. They have easier to read color LCD touch screens versus dim mono displays. Their keyboards are better organized and more rugged with function keys and wild card keys, and some are fully programmable. Modern handheld computers are also lighter & better balanced.

Today's wireless computers and access points have more built-in diagnostics which makes them easier to troubleshoot. Remote configuration features are also common in newer technology. Off-the-shelf remote management software for 802.11 hardware is readily available so upgrading 200 wireless units with the latest version of your application is as simple as a click of a mouse?

It's also easier to find experienced IT workers that are fluent in the newer technologies so problems that require a complicated solution are much easier to resolve.

Battery technology has improved from NiCad or NiMH to Li-Ion, a much higher capacity battery with no more "memory effect."

And many of today's wireless computer are Bluetooth enabled which means you can get rid of those pesky cables for your scanners, printers and headsets.

2. Speed – The Backbone Technology

Today's wireless technologies are faster, allowing you to run more sophisticated applications including:

- Voice-directed applications

- RFID
- Voice over IP (VOIP) Walky Talky

There are, in fact, three high speed open standard options available: 802.11(b), 802.11(a) and 802.11(g).

802.11b is by far the most widely used open standard within the supply chain/logistics field. It utilizes the 2.4 GHz frequency band and provides 11 megabits per second (Mbps) data throughput. This is sufficient data transfer speed for almost all wireless data collection applications in warehouses, distribution centers, ports and manufacturing facilities. 802.11b systems can be used throughout the world.

802.11a operates on a wider band of the frequency spectrum, between 5.15 GHz and 5.35 GHz. 802.11a products can transmit at 54, 48, 36, 24, 18, 12 or 6 Mbps, so they can be significantly faster than 802.11b networks. The 54 Mbps speed is necessary for large file transfers such as streaming video. This frequency band offers fast data throughput but limited coverage ranges. This frequency band also is limited in its ability to travel through material. It is not interoperable with 802.11b. Although fine for the office, these limitations do not make 802.11a a viable choice for enterprise wireless networking.

802.11g is a newer standard that also offers a data rate up to 54 Mbps. However, it utilizes the 2.4 GHz band and by definition is backward-compatible with 802.11b systems. That means 802.11g devices can function on 802.11b networks; however, using an 802.11b device on an 802.11g network will not improve its throughput. Because 802.11g is compatible with 802.11b and is significantly faster, it will end up being its replacement.

Sure, IEEE 802.11g's data throughput of 54 Mbps seems sufficient for current WiFi networks, but IEEE is already looking ahead to boost that to 100 Mbps and possibly even 320 Mbps. Why? Because applications are becoming increasingly complex and bandwidth hungry. It's good to know that WiFi throughput won't be a constraint in the future.

3. Speed – Client Technology

Today's wireless computers are equipped with faster processors, faster radios and more efficient Windows® operating systems. They can run more robust applications many times faster than your 900 MHz terminals.

The scan engines found on today's wireless computers are also significantly better. You'll find "all range" scanners versus scanners that only work at short range or long range. And they are better at reading damaged barcodes which will make your operators much happier and more efficient.

4. Upgradeable

If you've been reading the trade pubs recently, you've likely read about the productivity benefits that voice directed applications can deliver. You've also read that RFID technology is coming, with many pundits predicting that it will be the primary data collection technology of the future. VOIP, Bluetooth – it seems like everyday some new technology is being pitched that will improve performance and productivity in your warehouse. The problem is that with your old 900 MHz technology you can't take advantage of any of them. You need Windows and you need the bandwidth provided by 802.11.

And to take advantage of browser, Java and client server based applications that are becoming more prevalent – you'll need a modern operating system.

5. Reduced Maintenance Costs

As you are probably fully aware by now, hardware service contracts get more expensive with age and parts only get harder to find. Companies sometimes lose sight of the expense associated with keeping older equipment in service. Think about the steps involved in repairing a broken computer.

1. Troubleshooting the unit on the floor.
2. Removing the equipment from the floor.
3. Troubleshooting on the phone with vendor.
4. Pulling broken unit out of circulation.
5. Configuring replacement unit.
6. Admin costs to pick pack and ship.
7. Returning repaired equip into circulation.

This process gets set in motion more often as terminals get older. And with the older 900MHz equipment, parts are becoming harder to find which extends the repair time – which begs for more standby terminals which may or may not be available – which...you get the picture. It may feel like you are saving money by continuing to maintain and operate your 900 MHz technology, but with further analysis you may find that you are not. At some point the cost of keeping the older equipment alive becomes very expensive, particularly when you take into account softer cost items such as the disruptions in your operator's momentum and deliveries that are late or go unfulfilled due to hardware issues.

Many 900 MHz terminals are no longer serviceable through traditional means. If your terminal's time hasn't come yet, it will. And aftermarket repairs can be thorny – if you can even get your terminal repaired. So be careful not to back yourself into a corner when it comes to repairing (or not being able to repair) older equipment.

Planning for an 802.11 Upgrade

As with any significant upgrade, a project team representing all functions within the enterprise should be assembled and empowered. This is particularly important when implementing 802.11, because it is highly likely that the wireless backbone will extend well beyond the shop floor, warehouse or yard to include a wide range of management functions.

A project team might benefit from input from other departments that might benefit from the system such as: Accounting, Facilities Management, IT/IS, Operations, Personnel, Planning, Purchasing, Sales, Traffic, and Warehousing.

The membership of a project team depends on the nature of each company's operations but should solicit needs requirements from every functional department within the company. While every department may not see an immediate need for implementing 802.11, it is important to understand possible future users to design a scalable, robust system.

In a typical installation, 802.11 will require additional access points. Placement of access points will be determined not only by a site survey but also by a "user" survey. The project team can perform a "user" survey by looking at every part of the enterprise to determine who will (or might) access the wireless network. Once potential users have been identified, a site survey will provide an access point map.

You will likely have 900MHz propagation experts in house that may feel that a professional site survey is unnecessary. Be careful. 802.11 networks behave much differently than a 900 MHz network.

For example, unlike 900 MHz signals that are absorbed or attenuated by metal, 2.4 GHz signals can be reflected by metal. When signals from a mobile terminal are reflected by metal obstructions, a situation called multi-pathing exists. When this happens, the same signal from the mobile terminal reaches the access point antenna by several different paths. Each reflected path has a slight time delay from the original signal. These multiple signals can confuse some systems and significantly reduce system range and performance. LXE has addressed this problem with its patented Spire® antenna technology that filters out multi-pathing signals and provides superior 360° coverage.

Also be aware that higher speed does require some trade offs. With 802.11(b) for example, the maximum 11Mbps data transmission speed is available closest to the access point, out to approximately 130 feet (39.6m). Beyond that distance, data transmission speed drops to 5.5 Mbps, 2 Mbps and 1 Mbp at the maximum 350 foot (106.7m) range.

Data transmission speed drops to compensate for reduced signal strength and additional electromagnetic interference (EMI) or "noise" in the environment. The reduced data

transmission speed assures error-free operation even at the extreme edges of the system's range. (Systems will go "silent" before they produce errors.)

These figures are generally for open environments with typical amounts of "noise" in the 2.4 GHz band. In environments with heavy concentrations of metal or liquid obstructions (e.g., freight containers, paper rolls) or where there is more noise in the 2.4 GHz band, data transmission speeds will drop more quickly and maximum range may not be achievable.

As with 900 MHz systems, "dead spots" can also be created by the proximity of obstructions or EMI-generating equipment (e.g., arc welder, other equipment operating at 2.4 GHz).

It is critical to have a professional site survey to determine access point placement to avoid dead spots and to ensure a high level of system performance.

Next, you'll need to determine whether to expand an existing wired network to include these access points or whether to install a new wired network for the 802.11. In some companies, a single wired and wireless network will suffice. In others, it may be desirable to have several wired and wireless networks to physically limit access to certain applications.

In some applications, particularly freight or container yards, possible access point locations may be limited and wiring to these points may be difficult. In these situations, the use of a "wireless bridge" may be desirable to connect distant access points or subnetworks to the main network. Again, a site survey will help determine effective coverage range and access point location.

Finally, an analysis of legacy and current software applications needs to be done to determine whether any changes will be required. Typically, host applications can run unchanged although some applications on mobile computers may need to be updated.

Ownership

An 802.11 wireless network poses some additional challenges – not in a technology sense but in a business sense. Whereas a 900 MHz wireless network was traditionally a manufacturing, warehouse or yard operation, it was typically implemented and owned by that department.

However, because an 802.11 can theoretically be used by all departments of a company, the wireless network may be considered the property of the IT department, as is usually the case with the Ethernet network. Individual terminals accessing the 802.11 network would be owned by each department.

While this may seem to be an intuitively sensible approach, it can create interdepartmental issues when purchasing equipment, maintenance, repairs and upgrades. Part of the planning process, therefore, must include a solid understanding of which department owns what equipment and how to efficiently handle maintenance, repairs, upgrades and so forth. Most companies prefer to have a single source for all 802.11 related issues. This simplifies contractual agreements and provides a single point of contact for any problem.

Security

There have been a lot of reports in the trade media about security threats to WiFi systems. While some of these concerns are valid, closer examination shows that the majority of reported security problems occurred in systems that:

- a) were early implementations that did not include even basic security protocols,
- b) used only very limited, first-generation security protocols,
- c) also had inadequate wired network security, or
- d) are more theoretical than actual.

Protecting wireless networks from security breaches requires much of the same diligence as protecting a wired network. Recent surveys have shown that network security in general is not as good as it should be. Implementing rigorous wireless security can help spur implementation of better network security in general.

Among the tools available for wireless security is the use of virtual private networks (VPNs), firewalls designed specifically for wireless networks (that may be applied to the outside of the network or between authorized terminals and host only), and a wide range of other standard wireless and hardwired security access protocols. For more information on wireless security, see LXE's white paper entitled "Keep The Bad Guys Out of Your 802.11 Wireless Network."

Implementing 802.11(b or g)

Once the site survey and user surveys have been completed and network wiring issues have been decided, installing 802.11 hardware is relatively straightforward. Newer access points already have an 802.11 (b/g) radio and can easily accommodate a possible future upgrade.

Once the 802.11 backbone has been installed and tested, mobile computers can be upgraded as required. This can be as simple as a radio and software upgrade to the existing mobile computer hardware. Some companies have added an 802.11 backbone for management use and anticipated future shop floor/warehouse needs but have not upgraded mobile computers. In other installations, some mobile computers have been

upgraded to 802.11 in order to handle particular applications, but the existing 900 MHz network and computers are run in tandem with the 802.11 network until all mobile applications have been upgraded. Still other companies have completed the transition to 802.11 even though the existing applications run quite satisfactorily on the previous 900 MHz network.

And most WMS host applications are Terminal Emulation based so they typically port to new devices seamlessly. With Windows based TEs, the transition can be seamless and painless for your operators.

In short, the pace and level of 802.11 implementation depends on the specific concerns and needs of each company.

Conclusion

With the increasing complexity of many enterprise application packages, the lines between data collection and data management are blurring. Where production workers historically might have only entered data or received simple “green screen” work orders, they may now receive many of the same graphical status reports, quality data and other relevant information previously accessible only to management at desktop work stations. Management now requires this data on mobile platforms and many companies have found that providing this same information to workers can enable improved productivity and performance. It only makes sense, therefore, to adopt a standard solution to wireless communications.

An 802.11(b or g) wireless backbone provides a solid platform upon which to build any future data collection and data management applications. That means that when new enterprise application solutions are rolled out, the wireless network won't pose any implementation constraints. Implementing 802.11 now, before it becomes a critical need or before maintenance becomes too costly, just makes good sense. You should see an immediate bump in efficiency. We have several case studies (www.lxe.com) of companies just like yours that made the transition and are glad they did. Check out Dayco, Mercury Marine or FMI International.

While it's important to consider implementing 802.11(b or g) now, it's equally important to choose the right technology supplier. A company with the right experience and the right products will ensure a smooth installation and the most efficient coverage. Look for products that provide a path to the future, even if you are not sure what your future might be.

Stay current with new technology - keep a “new technology” lab. Play with new products and test for compatibility. Participate in your vendors development efforts and most importantly, don't be intimidated by new technology.