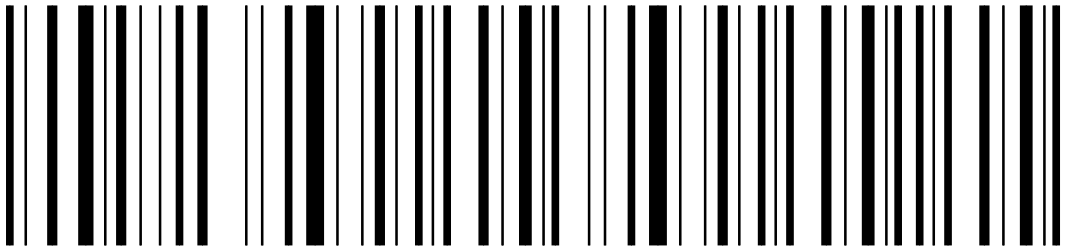
The Benefits of Wireless Printing

An Overview of Applications, Connectivity Options, Security, and Wireless Networking Technology



APPLICATION WHITE PAPER

Zebra Technologies

Executive Summary

Wireless printing systems are rapidly maturing, making it easy for users to print bar code labels on demand wherever they are needed. Because wireless printers are independent of cabling and a wired network infrastructure, they can be used virtually anywhere and relocated in minutes—without incurring additional costs. Wireless printing provides the responsiveness and flexibility that modern manufacturing and supply chain operations demand. These benefits come without performance trade-offs or a premium price. In fact, the total cost of ownership for wireless printing systems can be lower than traditional, wired-network configurations.

There are few limitations on where bar codes can go. The compact patterns of lines and spaces can be read on assembly lines, shipping and receiving docks, patient bedsides, retail checkouts, offices—anywhere information is needed. The traditional limitation on bar code systems has been the location where the symbols could be produced. By eliminating the need for a physical network connection, wireless printers remove the final obstacle to creating bar codes in real time where they are needed.

This white paper introduces prospective users to the basics of wireless printing, including applications, benefits, wireless networking technology, connectivity options, and security. For this paper, "wireless printers" refers to printers in which a radio frequency (RF) interface is used to connect the printer to a network. In many mobile printing applications, a wireless interface replaces the cable connection between the computer and mobile printer carried or worn by the operator. This paper deals with wireless networking and does not address mobile, cable-replacement applications except as noted.

Wireless Flexibility & Benefits

More than 70 percent of all bar code printers in use around the world are connected to a network.[1] The network may be Ethernet, Token Ring, or some other older technology, but in almost all cases the connection is made by a physical cable. There are literally miles of Ethernet cable in use throughout the world connecting label printers to networks, and additional miles of replacement cable and connectors yet to be purchased. Wireless printers are quickly gaining acceptance and popularity because they eliminate this expense.

When you remove cables, you gain flexibility. Once the network administrator assigns an IP address to the printer and turns on the unit, it is ready for use. Wireless printers can be relocated in seconds if the work area is being reconfigured for new production equipment, warehouse space allocation, or a redesigned retail selling floor. Wireless printers also can be put on carts or forklift trucks and moved throughout the day without ever losing their network connection, saving reboot time. Removing cables also improves ergonomics and workplace safety.

Freedom from network cables also makes it easy to add new printers to the workplace. If operations expand, or more printing capacity is temporarily needed, new printers can be up and running in minutes, instead of waiting hours or even days for busy IT staff to run cables to the work area. This is especially valuable to businesses that experience seasonal or end-of-quarter spikes in sales that challenge their existing shipping systems. Demand spikes can be satisfied by temporarily moving printers from other areas instead of buying new units. This increases asset utilization and may reduce the total number of printers needed within a facility.

[1] **Source: Venture Development Corp., Natick, MA.**

Wireless printers use a radio to communicate with the network over airwaves instead of over cable. On the network side, the radio transmissions pass through an access point (or base station) that is physically wired to the main network. The access point decodes the wireless data and passes it to the wired network. The wired network infrastructure equipment does not "know" the printer is wireless; the printer appears as any other device on the network.

Radio signals can travel through walls and other physical objects—no line of sight is required between the printer and access points. Entire factory floors, distribution centers, retail stores, and shipping yards are often completely covered by only a few access points. The same network and access points used to connect wireless printers can also be used with mobile computers, scanners, and other devices.

Most industrial wireless networks have far more bandwidth than is required for their applications, so adding additional printers rarely results in network congestion or slow response times. For example, wireless warehouse management systems usually operate at 1 or 2 megabits per second (Mbps) wireless transmission speeds, but the most commonly used industrial wireless networks operate at 11 Mbps.

Printers can connect with a wireless network either through native wireless support or by adding some type of radio peripheral. The different configurations are explained below.

Native Wireless Support

Printers with native wireless support have a factory-installed radio inside the printer that matches the user's wireless network. When the power is turned on, the printer is available to the user's wireless network. No external interface ports are used for the wireless network. The internal configuration provides security against radio theft, but limits the user's flexibility to choose and change radio cards.

PC Card (PCMCIA)

Printers with a PC Card (PCMCIA) expansion slot can be included in a wireless network by inserting a radio card. The PC Card serves as the radio for communication with the network. If users upgrade their networks, all that is needed to make the printer compatible with the new network is to insert a new radio card. The ZebraNet® Wireless Print Server provides 802.11b-standard wireless connectivity for Zebra 105*SL*™, *Xi*III*Plus*™, Z4Mplus™, Z6Mplus™, 110*PAX*™, and 170*PAX*™ printers, plus R110*Xi*™ and R170*Xi*™ multi-protocol RFID printer/encoders. It accepts six different 802.11b and Spectrum24 networking cards from leading manufacturers, including Cisco Systems and Symbol Technologies.

Except for the network connection, there is little difference between wired and wireless printers. In fact, wireless printers perform just as their wired counterparts, offering the same speed, graphics, resolution, and other performance qualities.

Applications

Any printing application can be made wireless, but the technology is most beneficial in situations where cabling is impossible or inconvenient. The greater the difficulty in running network cable to the desired print location, the greater the value of wireless printers. In all wireless printing applications, users enjoy total-cost-of-ownership benefits from not having to purchase, install, and periodically replace network cable and connectors.

As with most technology, many of the benefits users receive from wireless printing are derived from new business processes it enables. Wireless network connection allows printing to be done in places where it was not possible before. Changing procedures and business practices to take advantage of this capability can produce strong efficiency and quality improvements. Following are some examples of how different industries can benefit from wireless printing.

Manufacturing

Many manufacturers apply tracking labels to work in process after certain production operations are completed. Assembly line workers typically walk to a central computer and printing station to pick up the labels, or use preprinted labels stored at their workstations. Installing a wireless printer at the point of activity is an improvement over either of these procedures.

Requiring workers to leave their assembly stations to pick up labels guarantees that nonproductive time is built into every product. Even if the printing station is nearby, label pickups may serve as unscheduled breaks as workers converse around the printer. If workers pick up labels for several items at a time, they run the risk of mislabeling, which defeats the tracking system. The results may seem inconsequential when observed during a few shifts, but over the course of time the minutes saved for each worker translate into significant productivity gains and labor cost savings.

Using preprinted labels at the workstation eliminates distractions and lost productivity, but at a cost. Preprinted labels cannot carry variable information, such as the date of manufacture or identification of the worker who made or inspected the product. The ability to produce variable-information labels in real time is critical in many automated production environments, particularly ERP or ISO-certified environments. In addition, preprinted labels must be held in inventory to ensure adequate supplies, leading to ordering, processing, and storage expenses.

Wireless printers are advantageous to manufacturers that change their production lines or use flexible work cells. By not having to retool and set up workstations based on the availability of cabled network connections, manufacturers can greatly reduce their changeover time and take full advantage of their facility space and flexibility options.

Manufacturers also can use wireless printers at testing and quality control stations to ensure items are identified and tracked correctly. More applications exist for materials management, finished goods inventory, asset management, and other operations.

Shipping and Receiving

Wireless printers are valuable when used to support cross docking. A wireless printer at the receiving area can be used for relabeling incoming shipments. By eliminating the need for workers to go inside for labels, wireless printers provide the time savings and responsiveness demanded by cross-docking operations. The printers also can be used to generate manifests, safety labels, or temporary ID badges for delivery drivers.

For traditional receiving, wireless printers can be used to relabel incoming pallets or create new identification labels for cases and individual items when pallets are broken down for item putaway. For large items stored outside of the warehouse, wireless printers can be installed in the receiving yard to label items as they enter the facility—without requiring a trip inside to pick up a label.

Wireless printers can aid busy shipping operations. If a surge of orders exceeds the capacity of a company's shipment labeling system, wireless printers can be temporarily deployed to meet the increased demand. Operations and IT professionals appreciate how quickly wireless printers can be set up and configured in busy times, especially when compared with traditional wired models.

Retail

Mobile wireless printers are widely used by retailers for shelf price labeling, returns processing, inter-store transfer labeling, price auditing, portable POS, item marking, signage, and other applications. Wireless printers may also be installed with scales for bulk-food sales or other self-service applications to create accurate price labels. Retailers that frequently reconfigure their stores or set up temporary POS or returns processing stations after the holidays are good candidates for wireless printing. More retail application ideas and a cost-benefit analysis are detailed in Zebra's "Wireless Technology: Solutions for Retail" white paper, which is available on Zebra's Web site: www.zebra.com.

Office

Offices are among the fastest growing environments for wireless networking. Busy IT departments appreciate time saved from cabling; facilities managers like the flexibility to reconfigure offices that wireless networks provide; and users like their workspaces free from cable clutter. Wireless label printers are a welcome addition to many offices to facilitate mailing labels, shipping labels, file tracking, visitor badging, and other applications.

Hospitality

Hotels, conference facilities, and convention centers easily can set up extra registration and VIP check-in stations virtually anywhere by using computers and printers on a wireless network. For example, hotel guests could check in and receive their room key at curbside from a staffer using a mobile computer and printer with magnetic stripe encoder. Wireless printers can produce name tags, admission tickets, and other materials on demand, saving the expense of printing and transporting materials for preregistered guests who never check in. At front desks and other check-in locations, wireless networks enable multiple users to share a printer without running a tangle of ugly cable. With their advanced bar code and graphics capabilities, wireless printers also can be used to create short-term security passes, eliminating the security risks associated with keeping an inventory of preprinted, nonpersonalized passes.

Networking Technology

The boom in wireless adoption started in late 1999 when the IEEE 802.11b standard was created, and it has continued unabated. Even though wireless technology has been available for years, it was used mostly in niche applications until the standard provided users an open interoperability option. Until just a few years ago, wireless networks bore little resemblance to their wired counterparts. Personal computers from Dell, IBM, Gateway, and other manufacturers routinely are used on the same network as HP laser printers, Compaq servers, and other devices from mainstream IT providers. But wireless networks were proprietary, with a single vendor providing all the access points, computers, and peripherals. Each vendor developed its own radio technology at one of three available frequency bands (450 MHz, 916 MHz, and 2.45 GHz), making interoperability impossible. These proprietary systems, from vendors such as LXE, Lucent Technologies, Proxim, Symbol Technologies, Telxon, Teklogix, and others usually performed quite well, but locked the customer into using a single vendor for the life of the system. This environment kept system complexity and prices high, leading to adoption mostly by large companies or those with specialized needs.

Today's wireless environment is much more user-friendly. In the past few years, most vendors have abandoned their proprietary offerings and developed interoperable products governed by internationally recognized standards. The most important and widely used wireless network standard is the Institute of Electrical and Electronics Engineers (IEEE) standard 802.11b. (The IEEE 802 committee has a more famous standard, 802.3, which we know as Ethernet). Soon after the 802.11b standard was ratified, prices for wireless networking equipment began falling dramatically, users enjoyed many new product options, and advanced network security and management tools were developed. Now wireless networks can be configured and managed using familiar tools and techniques that network administrators have used for years to maintain their wired Ethernet systems.

Other 802.11 (pronounced eight oh two dot eleven) standards are in use and in development, and older, proprietary technology is still used successfully in many legacy systems. Some of the most widely used non-802.11 wireless networking technologies are Aironet, Bluetooth, OpenAir, Spectrum24, and WaveLAN. However, 802.11b accounts for the vast majority of new deployments, is supported by the largest number of vendors, and faces no viable challenge to remaining the dominant wireless networking technology of the next several years. Please see the Glossary beginning on page 7 for definitions of these and other wireless networking technologies.

Zebra Technologies is a leader in standards development and works directly with all leading wireless technology companies to ensure its customers are offered the most appropriate wireless technologies and new features as they become available.

Wireless Security

Wireless networks have developed an undeserved reputation as being insecure, making security the top concern of potential wireless users. Exaggerated stories about wireless security breaches have played to these fears and obscured the fact that wireless networks process millions of mission-critical transactions in manufacturing, defense, healthcare, government, retail, logistics, and other industries every day.

Wireless security presents a unique challenge. The features that attract users to wireless—freedom from cables and freedom of movement—create new security challenges. The characteristics of wireless technology can both enhance and inhibit network security. Policies and systems used to secure traditional wired networks do not adequately satisfy wireless network needs. Fortunately, there is a wealth of available security tools and system architecture options for securing wireless networks, and new security standards are on the horizon.

With the notable exception of wireless credit card authorization, protecting data usually is not the most important aspect of wireless network security. In most applications, data transmitted over the wireless network has no value to anyone outside the enterprise. In industrial environments, the wireless transmission might indicate that a part has left a testing station, or convey a putaway location to a warehouse worker. The data has limited value outside of the enterprise.

Hackers who use wireless devices to gain network access are often a more serious threat than data pirates. Users value wireless technology because their network access is not restricted by walls, ceilings, or cables. These qualities are also attractive to hackers. Using homemade antennas connected to common laptops, hackers can search databases, steal files, or shut down applications that reside on wired host systems without ever setting foot in the building by gaining access through the wireless network. Interoperability standards provide a road map for hacking systems; there are comparatively few security problems with proprietary radio technology.

Three things must happen to make a wireless network secure: data must be protected while it is in transmission; access must be denied to unknown or rogue devices; and devices must be protected from communication with outside hackers and unauthorized access points. Simply put, the security system must ensure the integrity of both the data and the hardware on the network.

Data transmission is protected by **encryption**, which uses algorithms to encode the data. The transmitting and receiving devices have matching encryption keys that enable them to decode and process the encrypted data.

Authentication prevents rogue and unauthorized devices and access points from gaining access to the network. Authentication can be performed with a simple password or more sophisticated algorithms. The most secure networks employ **mutual authentication,** in which the mobile device and access point must each authenticate themselves with the other before any network transmission can take place.

Commonly used wireless security protocols include WEP, Kerboros, LEAP, MAC, virtual private networks (VPNs), WPA-PSK, WPA-LEAP, 802.1X, and 802.11i. (These protocols are defined in the Glossary beginning on page 7.) Wireless networks may also include security protocols commonly used on wired networks, including Internet Protocol Security (IPsec), Secure Socket Layer (SSL), third-party password, encryption, and network management products. One third-party product that is gaining support in the enterprise wireless environment is Funk Software's Odyssey Client. The product is used in conjunction with security servers to provide authentication and additional password security, and supports subnet roaming so users do not have to reestablish security credentials when they come in range with new access points on the same network.

Zebra supports up to 128-bit WEP and 802.1X LEAP authentication throughout its wireless printer products. Zebra mobile printers support several additional security implementations, including VPNs, Wi-Fi Protected Access (WPA), and Kerboros. Zebra continues to offer advanced wireless security features as they are introduced through its involvement with international standards committees and strong relationships with leading wireless technology developers.

Many excellent white papers about wireless network security are available. Visit the Resource Library section on Zebra's Web site, www.zebra.com, to download "Closing the Loop: Extending Wireless LAN Security to Wireless Printers." The Wireless LAN Association Web site (www.wlana.org) is a good starting point for further information.

Conclusion

Wireless printing offers all the capabilities and performance of traditional printing, with the added advantages of flexibility and convenience. Including printers on a wireless network adds only a small incremental expense that reduces the total cost of ownership for the enterprise printing system and accelerates the return on investment for the wireless network. Using a sound network architecture and available security tools makes wireless networks more secure than their wired counterparts.

Zebra Technologies was the first printer manufacturer to offer integrated wireless capabilities, and its products work with products from all of the leading network technology vendors. Zebra has the experience, partners, and comprehensive product line to help you create the optimal wireless printing system. Contact Zebra at +1 800 423 0442 or visit its Web site at www.zebra.com for more information regarding wireless printing.

802.11a—802.11a offers throughput up to 54 Mbps. It uses 5 GHz frequency and is incompatible with 802.11b technology. The 802.11a standard was ratified after 802.11b; thus far there have been few deployments of the technology.

802.11b—The most widely used and supported wireless networking standard, 802.11b uses the 2.45 GHz frequency band, which is available in most of the world, and offers 11 Mbps data transfer rates. There are dozens of interoperable 802.11b products, including handheld, forklift-mounted, and stationary computers; access points; PC Cards (PCMCIA); printers; and other peripherals in industrial, home, and office models. Zebra Technologies supports 802.11b with the ZebraNet Wireless Card Socket, a PC Card adapter that enables the *Xi*III™ products to operate in a wireless environment. The ZebraNet Wireless Card Socket supports wireless networking cards from leading manufacturers, offering different features and security levels. The Cameo®, Encore®, and QL 320 printer families have native 802.11b support.

802.11g—There is no 802.11g standard yet. The 802.11g committee is attempting to create a standard that is compatible with 802.11b technology but would allow faster data rates with a minimum of 20 Mbps. Ratification and available compliant products are likely to be years away.

802.11i—802.11i is a work in progress that has not been ratified as a standard. It is intended to strengthen the encryption of WEP keys and to shore up their well-publicized deficiencies. The 802.11 standard committee's Task Group I is developing 802.11i as an interim standard that will be backward-compatible with existing 802.11 networks until a more secure encryption standard is developed for future versions.

802.1X—The 802.11 committee developed the 802.1X standard, which covers device authentication for network access control. The standard builds on WEP and other security features in the 802.11b standard by strengthening security of MAC addresses on client devices. 802.1X is supported in Windows XP.

Access Point (AP)—Also referred to as base stations, access points act as the gateway between wireless devices and enterprise systems. Access points include an antenna for communicating with wireless devices, coordinate all wireless traffic, and communicate with enterprise systems as needed over a physical (cabled) network connection.

Aironet—Cisco Systems offers the Aironet® brand of wireless networking products. The Aironet family was originally developed by Telxon Corp., an industrial wireless networking pioneer, which sold the line to Cisco. The current generation of Aironet products complies with 802.11a or b specifications. Older Aironet systems from the Telxon era operate on proprietary network technology and are still used in many facilities.

Base Station—See Access Point.

Bluetooth® Technology—Bluetooth is not truly an enterprise networking technology but is often confused with one. Bluetooth uses low-power, short-range (about 30 feet or 9.1 meters maximum) radio transmissions to create what has been dubbed personal area networks (PANs). It enables peer-to-peer communications among computers, printers, and peripherals without using a server or access point. Bluetooth could be used for networking in homes or small offices, but lacks the robustness and features required for enterprise applications. Bluetooth does have a place in the enterprise as a replacement for cables in mobile applications. Workers who use handheld computers and mobile printers can use Bluetooth for the printer-computer interface, improving ergonomics by eliminating cumbersome cables.

When Bluetooth first surfaced, interference with other wireless LANs was a major concern, but the fears have been put to rest. The Bluetooth connection does not prevent the handheld computer from also connecting to a wireless LAN through an 802.11b or other interface, even though both technologies operate at 2.45 GHz. Extensive testing and real-world experience have proven that Bluetooth and 802.11b devices can operate in the same space without interference. Interference is avoided because of differences in how radio signals are transmitted, power output, and anti-collision protocols that are built into each technology. For a definitive study on this topic, visit the Learning Center section of the Wireless LAN Association Web site: www.wlana.org.

EAP—Extensible Authentication Protocol. EAP is an extension that allows wireless client adapters to communicate with RADIUS servers.

IPSEC—IP Security Protocol Working Group, an Internet security standards group. IPsec is a widely supported standard for protecting data packets transmitted over the Internet.

Kerboros—Kerboros is a network authentication protocol that can be used with WEP. It is supported by many vendors, including Apple Computer, Microsoft, and Symbol Technologies. Kerboros uses mutual authentication (both wireless access points and wireless devices are authenticated) and has stronger data encryption than WEP.

LEAP—Lightweight Extensible Authentication Protocol. LEAP is a proprietary technology developed by Cisco Systems that provides mutual authentication at user-selectable intervals. If desired, access points and devices can be authenticated every second the network is in operation. LEAP can be used with 802.11 networks.

MAC—Media Access Control. One security technique is to limit access to the network to devices with specific MAC addresses. MAC management performs device authentication, but does not provide strong security because MAC addresses can be hacked.

RADIUS—Remote Authentication Dial-In User Service. RADIUS is a protocol for carrying authentication, authorization, and configuration information between a Network Access Server that desires to authenticate its links and a shared Authentication Server. Wireless network authentication can be improved by employing a RADIUS server because it provides mutual authentication and blocks traffic from unauthenticated devices that are trying to reach the wired network. RADIUS servers are fully compatible with 802.11b systems and use WEP keys for some authentication functions.

OpenAir—A widely used family of wireless networking products that predates 802.11. OpenAir is a proprietary technology developed by Proxim and supported by multiple vendors that manufacture compatible PC Cards, access points, and other products. OpenAir uses 2.45 GHz frequency-hopping RF technology and offers 1–2 Mbps data rates.

SSL—Secure Socket Layer. SSL is an open encryption protocol used to secure Internet transmissions that is supported in common browsers.

Spectrum24—A family of proprietary wireless networking products developed by Symbol Technologies, the Spectrum24 line includes fully compliant 802.11b offerings as well as other products created before the standard was ratified. Spectrum24 users may add Zebra mobile and tabletop printers to their networks with native support or the ZebraNet Wireless Print Server and Spectrum24-compliant and Spectrum24 High Rate-compliant PC Cards.

Subnet Roaming—The ability of wireless users to move freely in and out of the coverage areas of different access points without having to reestablish network connection or security authentication.

VPNs—Virtual Private Networks. VPNs create a secure "tunnel" to pass data between network devices and access points. VPNs authenticate users (by password) and specific devices so that only authorized personnel can use specific computers or other equipment, eliminating threats from lost or stolen equipment. Data is authenticated so all traffic in the tunnel originates from authenticated devices. Transmitted data is also encrypted, improving data security.

WaveLAN—The brand name for wireless LAN products from Lucent Technologies. The line includes 802.11b products and older, proprietary systems that predate the standard.

WEP—Wired Equivalent Privacy. WEP is the main security feature in the 802.11b standard and is intended to provide wireless users the same base level of security found in wired Ethernet (802.3) networks. Researchers at the University of California-Berkeley demonstrated that the WEP algorithm could be broken, raising concerns about overall wireless security.

WEP is used for both data protection and network authentication. A security key is used on the wireless server (access point) and on each device on the network. Data transmission is protected by encryption that is encoded and decoded by the keys. The standard calls for 40-bit encryption, but individual equipment makers offer compliant networking cards with up to 128-bit encryption.

Encryption keys are also used to authenticate the device to the network. However, WEP does not support mutual authentication—the access point does not authenticate itself to the server. Without additional security provisions, WEP systems are vulnerable to hacking through rogue access points. It is important to note that many wireless LAN users fail to activate WEP security features when configuring their networks, leaving themselves open to attack.

WEP is an imperfect security solution, but it should not be dismissed. At a minimum, users should activate their WEP features and change the default network name (SSID). As the Berkeley team demonstrated, the security keys can be decoded. Users can change the keys and should do so regularly.

WLANA—Wireless LAN Association. WLANA is an industry group made up of wireless networking technology providers that supply education and resources about the technology.

Zebra Technologies

333 Corporate Woods Parkway
Vernon Hills, IL 60061-3109 U.S.A.
T: +1 847 793 2600 or +1 800 423 0442
F: +1 847 913 8766
www.zebra.com

GSA#: GS-35F-0268N

13033L Rev. 4 (11/05)