Wireless Serial Device Servers:

Leveraging Investments in Legacy Equipment While Upgrading Network Accessibility

By Lisa Hephner and David Johnson

SERIAL communication is at the heart of many I/O intensive applications in a broad variety of industries. From the bar code scanners at POS stations, to card readers in ATMs, cash drawers at teller stations, CNC machines on production lines, access control gates and warehouse inventory systems, serial communication is the interface of choice because it is a reliable, robust, and time-tested solution. However, as newer PC technologies are introduced to accommodate more sophisticated application software demands, and as wireless computing becomes more practical, affordable, and convenient, IT managers increasingly need to leverage their investment in existing serial equipment while increasing accessibility. Wireless device servers solve this problem by embedding a wireless Ethernet client into a standard Serial Device Server, thereby enabling RS-232 and RS-422/485 serial devices to communicate over local and wide-area networks without routing Ethernet cables. This article discusses the technology behind wireless device servers, and explores some common system implementations. It also provides information about product features, Access Point location, antenna selection, and other key issues to consider when deploying wireless device servers on a network.

WHAT IS A WIRELESS DEVICE SERVER?

A wireless device server is the combination of two connectivity technologies—Serial Device Servers and wireless communication protocols such as 802.11b. Both these technologies on their own are used to greatly enhance options for i/o intense applications by eliminating the need for lengthy cable runs, communication distance limitations, and the one-to-one relationship between a peripheral device and the PC to which it is typically connected. When joined together in a wireless device server, the benefits are exponentially increased as any computer on the network can wirelessly access previously isolated devices.

A Serial Device Server (SDS) is a computer in a very robust and compact package (approximately the size of a deck of playing cards) that contains a built-in operating system and TCP/IP stack. State-of-the-art SDS models also contain a built-in web server that allows configuration and monitoring through a client PC's web browser.

An SDS serves a very specialized purpose: sending data to and from a serial device and a client PC over an Ethernet network. The application software on the client PC, whether in the same room or across the country, communicates with the SDS as if connected locally to a "virtual" COM port and cable. The fact that the data is moving around the network and not a short serial cable is invisible to the client PC and the serial device. Practically any serial device having a software application to monitor it locally on a PC can be accessed remotely using an SDS —without changing a single line of code.

The next step in developing the SDS is to cut the cord on the Ethernet connection and enable completely wireless communication. This is accomplished by embedding a wireless Ethernet client adapter into the SDS. This client adapter, or wireless radio, connects the device server to an Access Point which bridges the wireless network to a wired LAN, enabling resources to be shared across an entire network. The technology used to create a Wireless Serial Device Server (WSDS) is identical to the wireless radios used to enable a desktop or notebook PC to access a wireless network.

Almost all WSDS units are designed to use the ubiquitous 802.11b standard, because for the majority of applications this is the best and most economical choice. Typically the Intersil wireless chipset, the standard used by major networking hardware companies such as Linksys® and Cisco®, is utilized to create a WSDS. However, security protocol support, antenna strength and sensitivity (range) vary greatly among WSDS models. Basic units are compatible with 2.4 GHz DSSS (Direct Sequence Spread Spectrum) Access Points, provide support for 128-bit WEP security protocols, and have built-in mid-range multi-purpose antennas. High-end units provide increased transmit power of up to 100-milliwatt (mW), enhanced receive sensitivity, support for premium security protocols such as Cisco® Aironet® LEAP or WPA, and offer a flexible RP-TNC or RP-SMA connection compatible with a wide range of external antennas.

WHY USE WIRELESS DEVICE SERVERS?

A large percentage of the equipment accessed, monitored or maintained by organizations around the world is equipped with an RS-232 serial communications port. In fact, the RS-232 protocol has existed since the 1960s and is included in millions of devices that contain an electronic communications interface. It is estimated that only 10% of the serial ports available worldwide are connected to a network, and of those only a small fraction can be accessed wirelessly. However, the

potential exists for a wide variety of serial-based equipment (for example, medical equipment, CNC machines, and access control systems) to be monitored wirelessly using a wireless device server.

While increasing access to previously stand-alone devices is important, the real benefit of wireless device servers is connecting these devices to networks without running cables. This is particularly useful in manufacturing and other tight environments where long lengths of cable can be particularly cumbersome to install. It is also extremely useful for connecting devices that are moved often, or when field staff using laptop or handheld computers must access equipment in multiple locations.

In addition, when a traditional network is converted to wireless, there are typically a great many peripheral devices and software applications that cannot directly communicate via the new interface. Instead of scrapping these devices—which in all likelihood are still in perfect working order—a wireless device server can be used to connect them to the network. And, since the WSDS can do this without requiring any changes to application software, it is an extremely cost-effective solution that leaves IT budgets free to be used in areas where added investments can yield increased performance.

Not only can wireless device servers enable multiple computers to access a single device, they can completely eliminate the need for a PC to be involved in the process. This capability, called serial tunneling, enables two serial devices to communicate directly with each other—for example a serial barcode reader can transmit data directly to a serial printer that generates inventory reports. When serial tunneling is used, each serial device is connected to its own WSDS, which allows them to communicate wirelessly with each other over a network just as if connected by a short serial cable. That is, the WSDS units work behind the scenes to add and then remove network routing packet information around the serial data to invisibly send and receive data between the two serial devices. When used within range of each other, two WSDS units can connect in Ad-Hoc mode, that is, without an Access Point between them. If the serial devices are far apart, however, the Access Point at each location puts the data received wirelessly from the WSDS onto the wired network, which can then transmit the data back and forth across great distances. In effect, serial tunneling can allow two serial devices designed to connect to each other over a short cable to be placed thousands of miles apart, communicating over Intranets, VPNs or even the Internet.

SYSTEM PROBLEMS SOLVED WITH WIRELESS DEVICE SERVERS

Wireless device servers are used in a wide range of industries and applications to streamline applications and to enable networking connectivity while preserving legacy peripherals and the applications written for them. In addition, wireless device servers are used to enable remote access, monitoring and control of serial-based equipment that cannot be easily connected to a wired network. Serial tunneling saves resources and manpower by enabling peripheral devices to communicate directly, thereby eliminating the need for a human or PC interface.

Preserving Legacy Serial Peripherals

Automated factories often have computer numerically controlled (CNC) machines in the production line. DNC software companies write applications that create and download control codes to CNC-operated machine tools. Rather than storing the codes on a floppy disk or tape and walking it out to the machine tool, many machine shops are implementing wireless SDS networks to drip-feed these instructions to the CNC. This eliminates the expense of a special ruggedized PC installed at each workstation, and of having a technician physically access a particular workstation to implement changes or troubleshoot problems. While one solution would be to connect these devices on the factory's Ethernet network, that is not always feasible because of tight quarters, moving parts and enclosed spaces. Using wireless device servers and a network of 802.11b Access Points, each CNC can be remotely programmed from any PC on the network.

Retail Point-of-Sale systems such as cash register banks and kiosks also rely heavily on serial based equipment. For example a car rental return kiosk might employ an RFID reader connected to a wireless device server that can be used to record the return of a particular automobile and wirelessly transmit that information via a local Access Point to a data collection point located nearby or at a home office. If the automobile is also programmed to transmit mileage information, a serial-based receiver connected to the WSDS can capture and transmit that data. A receipt can be generated for the customer on the spot, while the data is transmitted to the central processing computer. While this same system could be implemented using peripheral devices designed for wireless communication, using a wireless device server is typically a more cost-effective choice because the devices themselves are less expensive when purchased with a serial interface, and because the software applications used to process the sale are generally designed for serial, not wireless, communication.

PROVIDING REMOTE ACCESS TO SERIAL-BASED EQUIPMENT

In some systems it is not practical to have a PC located near a serial-based peripheral device that is collecting data. Further, it may be difficult to route a wired-Ethernet network to these locations because of potential interference, or because there are too many other systems in the way. In addition, when data collection equipment is not based in a single location, but must be moved from station to station, a wired solution is not practical. Medical monitoring systems must overcome these exact environmental challenges, and wireless device servers are an ideal, unobtrusive way to connect them with hospital networks.

Medical monitoring equipment such as vital signs monitors, EKG machines, and fetal monitors must all be connected to a hospital's central system for monitoring and control. However, these machines are often mobile, and are wheeled from patient to patient as tests are performed. Or, they are placed at the bedside of a patient when monitoring is required, and then moved to a different location when needs change. Using a series of well-placed 802.11b Access Points, a hospital or care facility can create a network over which medical devices can communicate wirelessly. A WSDS attached to each piece of equipment can be moved freely throughout the network while maintaining a link with a base nurses' station or with a central computer.

Serial Tunneling Eliminates wires for Device-to-Device communication

There are many applications in which serial devices are connected directly to each other but not necessarily to a PC. Traditionally, these devices needed to be located in close proximity of each other, because standard RS-232 communication was restricted to 50 feet, and the more

flexible RS-422/485 could extend only 2000 feet. With wireless device servers, serial devices can be located anywhere within the range of a wireless Access Point, and behave exactly as if they were physically wired together.

With the advent of RFID-based inventory systems, this capability is becoming increasingly useful. For example, an RFID reader attached to a WSDS can be located at a plant entrance or loading dock. It can read inventory tags from cargo as the truck passes, and transmit that information via an 802.11b wireless Access Point back to a report printer and a thermal label printer inside the warehouse (connected via a wired Serial Device Server, or with another WSDS). Staff can then know in advance the cargo they are about to unload, can bring the equipment necessary to unload it, and can prepare properly tagged storage space with the labels generated before the load arrives at the door. This ability enables a company to accurately check inventory while in the truck, and then verify that the appropriate amount of merchandise was actually stocked on the shelves. It also streamlines and speeds up the entire delivery process so that drivers are not kept waiting as staff determines how to unload and where to place merchandise. In large plants, a scanner located at the entrance might give warehouse staff more than a 15-minute head start on preparing for a delivery.

CONSIDERATIONS WHEN IMPLEMENTING A WIRELESS DEVICE SERVER

There are essentially two portions to consider in the selection of a wireless device server—the device server portion and the radio portion. Wireless technology, and in particular the 802.11b technology used in most Wireless Serial Device Servers, is fairly mature. It's becoming increasingly popular for SDS units to incorporate a wireless radio into a Serial Device Server, but the key to a superior product is the transmit power, receive sensitivity, compatibility with a range of Access Points and the security protocols supported.

The Device Server Component

The most important feature to look for in a WSDS is low latency—the time it takes to deliver a data packet from the serial device to the receiving computer and back. Serial devices themselves are slow when compared to communication across a busy network. They also are often sharing bandwidth with critical network applications such as security monitoring stations or customer service applications such as a cash register check out stands. Clearly it is imperative that the device server be completely unobtrusive on the network in order not to cause bottlenecks that cripple vital systems. Some wireless device servers are available with power processors and ultra low-latency modes that enable round-trip data transfer, using standard TCP/IP protocols, in under 2.5ms.

Another key feature for a wireless device server is an MEI interface component, especially for multi-port models needed to network a number of serial devices using one WSDS. MEI—or Multi-Electrical Interface—designates the WSDS' ability to connect to different serial protocols, such as RS-232, RS-422 or 485. There are two types of selectable interfaces, switch-selectable and software selectable. Switch-selectable models require manually setting a small dipswitch selector on the SDS. Software selectable means that the interface desired can be programmed using a software utility or, better yet, remotely through a Web interface.

One should also keep in mind that while designed primarily to run as a virtual COM port in most popular operating systems, WSDS units should support a variety of operating modes. Depending on the application, support for serial tunneling may be a requirement for the WSDS. Other operating modes such as Raw TCP, IP broadcasting/multicasting and TCP Client modes are several methods that can be used to connect a WSDS to a non-standard or specialized application.

Finally, ease of installation of the wireless device server should be an important factor, particularly if you are implementing a large multi-platform system. In the past, device server configuration could be a long, complicated, and cumbersome process. Today, while some manufacturers have yet to refine the process, others have made installation a simple task. Using an Installation Wizard approach in conjunction with an automatic search for local and remote subnets, Serial Device Servers can be installed quickly and easily. Network settings automatically assigned by DHCP networks are displayed for confirmation, or a static IP address can be assigned during the installation process. Watch out for those that require Telnet sessions, MAC address data entry or special cables to configure through the serial port. Higher-end Serial Device Servers also contain a built-in web server that can be accessed through the Windows® Device Manager interface or a Web browser, for continued ease of configuration and maintenance long after the initial installation is completed.

The Wireless Component

The embedded wireless radio component of the wireless device server you choose must be compatible with your overall wireless network. These decisions are largely independent of the device server decision, and should generally be made to serve the needs of the network as a whole not simply a single serial device application.

However, for optimal performance of your serial device application, it is just as important to select good wireless Access Points and antennas, and to locate them properly, as it is to select a high-performance, low-latency device server.

When selecting Access Points, key considerations are path length and antenna power. It is important that wireless links are not over-extended beyond the distances for which they are designed. Typically, short communication distances of a few hundred feet can be accomplished with small "rubber duck" type antennas. Communication distances of several hundred to several thousand feet are implemented with "flat-plate" antennae attached to the side of buildings or inside windows. For distances of several miles, "yagi" antennae or reflector dish type antennae mounted on towers are required.

To insure high reliability, use the lowest bandwidth that meets your needs, because lower speed links are more forgiving of external interference on long paths. Directional antennae are typically more reliable than omni antenna, which should be used only for a very short path or when specifically required by a multi-drop application.

The key factor to keep in mind is that high-power, long-distance Access Points are typically more expensive, but large networks typically require fewer of them to cover required distances. These antennae can be easily attached to any Wireless Serial Device Servers that provide the proper connection. Most high-end models offer a bulkhead mounted antenna connector so that if the one antenna provided does not meet your needs another one can be connected easily. The most common antenna connectors are RP-TNC or RP-SMA (these types are commonly found on wireless routers, gateways, and Access Points as well).

Once wireless Access Points and antennae are selected, they must be located appropriately in order for systems to function properly. To minimize signal loss between the antennae and the Access Point, the

cable that connects them should be a high quality, low-loss cable and should be as short as possible.

For long distance communication, such as between buildings, antennae must be within line of sight of each other. The antenna should be mounted to a rigid structure that will not be affected by wind or ice. And, obstructions of any kind should be avoided because they can seriously compromise the signal. There are a number of ways to deal with these obstructions such as adding repeaters to circumvent them.

Once the wireless environment is established, the device server can be easily incorporated. Wireless Serial Device Servers then "cut the cord" between device and computer, thereby allowing remote access to any serial device from any other serial device or any computer—even when that device is located at a great distance from a wired network. This provides tremendous savings by eliminating the need for on-site data acquisition, removing the requirement of one-to-one PC to device connections, streamlining i/o intense applications and enabling remote monitoring and servicing of equipment.

NaSPA member David Johnson is the product marketing manager at Quatech. His primary responsibility is the marketing and continuous development of device networking product lines.

NaSPA member Lisa Hephner is Quatech's media manager. She specializes in technical writing that explains Quatech device networking and device connectivity technology to both novice and expert audiences.