Wireless - The perfect solution for cutting costs in industry

Wireless communications has been a hot topic in recent years. Hundreds of applications have been fulfilled by wireless technologies using commercially available products or specialist, custom-designed solutions. In this article, *David Evans, Product Manager at Amplicon*, looks at Wireless LAN, a protocol that has seen widespread adoption by home and office users, and is now starting to be employed in industrial environments. Exposure within the consumer markets has helped reduce the cost of this technology, which today, makes it a very affordable solution for industrial applications.

So what has made wireless become such a widely talked about topic? What are the real and genuine benefits? Fundamentally, going wireless cuts costs in three key ways. Firstly, it is a cable replacement solution. It is well known that the cost of installing data cables is often prohibitive. Wireless is the perfect solution, especially in hard-to-cable areas, hazardous environments, listed buildings or where temporary installations (e.g. concerts / conferences) are required.

Wireless also provides increased mobility. Forklift trucks, instrument trolleys and cranes are just a few of the devices that need freedom of movement and where wireless can save on the cost of armoured or specialist cabling systems.

Wireless protocols designed to work with TCP/IP can seamlessly extend existing systems without software or hardware changes. It is possible to interchange wired and wireless segments of IP networks at will.

Apart from the tangible cost savings, there is also an element of prestige for anyone using leading-edge technology. Both system integrator and end-user can benefit from marketing opportunities generated by new and innovative wireless applications.

Wireless LAN

Wireless Ethernet, WiFi and WLAN are all references to the IEEE802.11 specification for wireless communications based on a 500 page specification completed in 1999. Although the bulk of the specification text seems heavy going at first, it contains an introduction that is legible and comes highly recommended for those getting to grips with wireless technologies. It can be downloaded at http://standards.ieee.org/getieee802/802.11.html.

One of the key benefits of WiFi (IEEE802.11) as a wireless protocol is its seamless compatibility with the abundance of wired Ethernet (IEEE802.3) systems currently in place around the world. Because wireless Ethernet has a radio physical layer, it needs to employ a collision avoidance system, rather than the famous (or infamous?) collision detection used by its wire-bound counterpart. Keeping Ethernet's Logical Link Control (LLC) interface to the TCP/IP protocols the same means that the MAC layer has to be changed to accommodate transmissions across a wireless medium. Forgetting the intricate details, the average user can simply enjoy the ease of use of this high-speed cable replacement technology, inter-changing wired and wireless segments as required.

Despite the potential for interference on the 2.4GHz band (which is also used by Bluetooth), the 802.11b & 802.11g variants are proving the most popular and account for the vast majority of wireless LAN infrastructure product sales. The table below describes the Wireless LAN standards that are currently in use around the world. Other 802.11 standards with improved security and data rates are also in development.

Wireless Standard	**802.11b**	**802.11a**	**802.11g**
Ratified	1999	1999	2003
Raw data	11Mbps	54Mbps	54Mbps
Frequency	2.4GHz	5GHz	2.4GHz
Av. actual throughput	4.5Mbps	27Mbps	27Mbps
Channels/non-overlapping	11/3	12/8	11/3

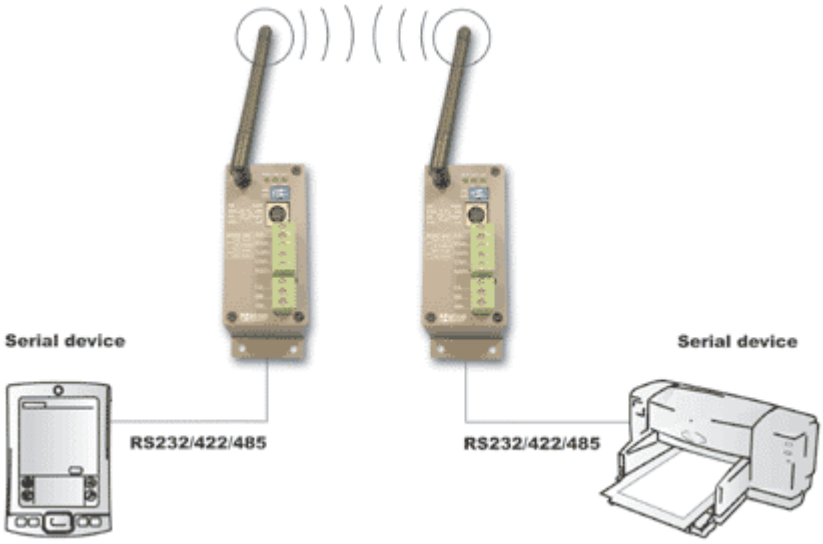
Applying Wireless LAN – *Wireless Device Servers*

Devices servers (also known as terminal servers, serial servers or serial to Ethernet converters) have been used for several years to encapsulate serial data (RS232, RS422 or RS485) within an Ethernet frame, allowing serial information to be distributed across a TCP/IP network. This innovative gateway capitalises on the high bandwidth of Ethernet to piggyback diverse industrial (serial-based) protocols, such as Modbus, onto and across an existing network. Device servers are used extensively to cut costs in cabling where an existing Cat 5 network already exists.

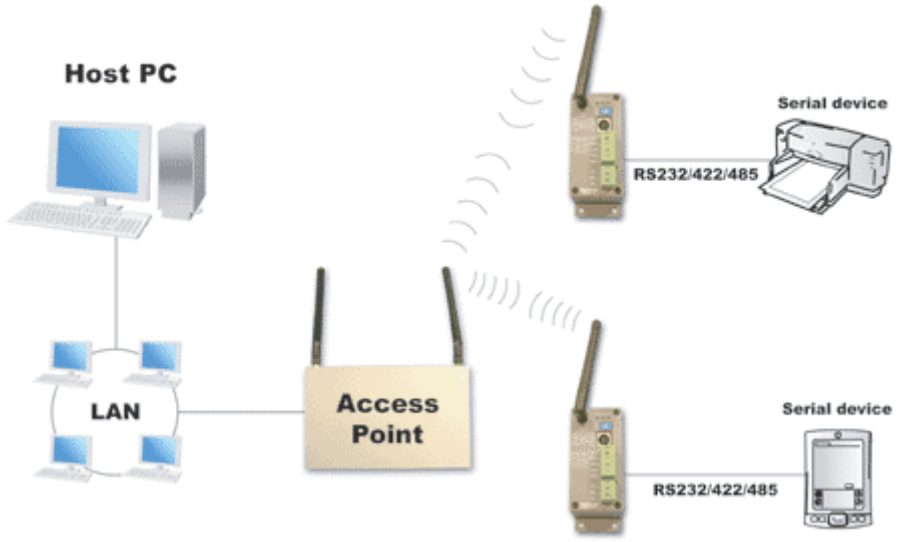
Wireless device servers do the same as a device server but use an integrated wireless (802.11b or 802.11g) interface instead of the standard RJ45 wired Ethernet connection. This allows serial data to be sent across a wireless LAN network and provides cable-free solutions that were not previously possible.

There are a variety of ways that a Wireless Device Server can be implemented; the following two are the most popular:

An ‘ad-hoc’ connection, as illustrated in the diagram below acts as a point to point cable replacement – what goes in one end, comes out the other.



In ‘infrastructure mode’, a wireless access point is used as the gateway to a wired network (a LAN, WAN or even the internet), where a host PC with driver software installed manages the connection to the remote wireless device servers. This mode of operation allows existing application software to be used as the wireless device server is simply addressed as an RS232, RS422 or RS485 COM port that is directly attached to the host PC. The diagram below shows an infrastructure mode example.



Some early adopters of this technology can be found in the CNC machine control market. Most CNC machines are programmed via an RS232 port which previously would have required a cable to be run across the shop floor (or ceiling) connecting it to a host PC. This PC needs to be in a relatively clean and safe environment, potentially tens of metres away from the CNC machine itself. With a wireless device server connected to each serial port, it is possible to simultaneously send serial data to the CNC machines via a commercially available wireless access point transmitting from a nearby office.

Interest has also emerged in the RFID market. A dual port wireless device server is used, with one RS232 port reading the input from an RFID scanner and the RTS pin of the other port acting as a digital I/O line to control an entry gate as required. This allows the addition of an RFID system in an environment where it is impractical to lay new cables, such as distribution depots or warehouses.

A major UK energy generation company is currently examining the possible use of wireless device server technology to connect to industrial electricity meters. The meters are often sited in inaccessible locations in the darkest corners of the UK's power stations, making wireless access to the RS485 port a very cost-effective and practical solution.

Applying Wireless LAN – *Wireless Bridge*

The vast majority of commercially available Access Points support a “bridge” mode of operation. This allows TCP/IP traffic to “bridge” a span between two networks or two devices where no cables exist. On its own, a wireless bridge is a useful network infrastructure tool but when combined with the following Ethernet gateway devices, total wireless solutions can very quickly be realised:

Video encoder / decoder – Send PAL or NTSC signals wirelessly. This is especially useful when connecting a DVR to an existing analogue camera in a hard to reach location.

Ethernet to Digital I/O – Access Control applications can be extended across greater distances without cables.

Ethernet to analogue I/O – Analogue signals such as the 4 – 20mA output of a valve can be digitised and sent back to a monitoring PC on the other side of a process plant – often required for insurance purposes.

USB to Ethernet gateway – Can be used to allow wireless access to remote USB devices such as cameras or data loggers.

GPIB to Ethernet gateway – Connect to legacy Test & Measurement busses from a conveniently located PC.

Industrial applications of wireless LAN are not suitable for flimsy, off-the-shelf access points. For this reason, a number of Industrial access points with hardened metal enclosures, DC power supplies, screw terminals and DIN-rail mounting capability have recently emerged.

Applying Wireless LAN – *Wireless Client*

Whilst most Access Points support wireless “bridge” operation, a much smaller number support a wireless “client” facility. This allows Ethernet devices without a wireless interface to participate in an existing Wifi network. This can be especially useful if an expensive piece of monitoring or test equipment needs to be added to a wireless network, saving the costs of buying a newer wireless model.

Wireless worries

No discussion of wireless LAN is complete without a mention of the classic pitfalls, namely, security and reliability. Media frenzy regarding a lack of security in Wifi has not helped to develop a reasoned approach to deploying wireless networks. It is wise to consider whether the data being sent actually needs to be secure. In an office environment, emails and strategic documents need a high level of protection, ensuring that company confidential information is not inadvertently broadcast to passers-by. In an industrial environment, the data transferred is more often a reading from a thermocouple, pressure sensor or other instrument. Does this data warrant extreme security measures? If the intruder deciphers the meaningless numbers to be a temperature measurement from an oven - what can he or she do with them?

The basic level of encryption in Wifi is WEP (Wired Equivalent Privacy) and is designed to offer exactly what it claims, the equivalent security to putting your data down a wire. At a recent security event in the US, members of the FBI cracked a randomly generated WEP key ‘live on stage’ in around 2 minutes. To combat this, WPA (Wifi Protected Access) encryption is available, employing a dynamic key and several other improvements. Whilst this too has been cracked, the process is far less easy and WPA remains a respected security measure.

If security is a real concern, then it is crucial to not rely solely on any of the encryption methods supplied with wireless LAN. Implement other security measures, usually higher up the protocol stack with passwords, authentication (such as RADIUS 802.1x) and MAC / IP address filtering.

The 2.4GHz ISM band on which most Wifi systems operate is license exempt and available for anyone to use (within certain guidelines). For this reason, interference is a possibility leading to transmission rate reduction or even lost data. One of the simplest ways to avoid these problems is to perform a site survey prior to installation. Rudimentary site surveys can be achieved with free wireless network tools such as the classic “Netstumbler”. Available for download at www.netstumbler.com, this software can be installed on a wireless enabled laptop and will alert the user to any existing networks in the vicinity, facilitating the choice of a clear Wifi channel and removing the prospect of interference.

Another approach is to assume the worst of the wireless network and build simple acknowledgment systems into the application software. In this way, intermittent network performance need not result in the loss of any data.

If the application can be described as mission-critical, real-time or high security then wireless may not be the right tool to use. There are, however, a plethora of other applications where the benefits of wireless connectivity far outweigh the genuine concerns or misguided paranoia that stand in the way. If someone wants to compromise security, there are far easier and more destructive ways than accessing your wireless network.