

Airborne™ 802.11b Wireless LAN Node Module Embedding Industrial Wireless Networking



Introduction

Extending the capabilities of existing industrial devices onto wireless networks is significantly different than simple Ethernet enabling. Adding a Client device to bridge between WiFi wireless networks (IEEE 802.11) and existing factory equipment are inherently more complex and require different configuration than simple Ethernet-based network Clients. Managing the various configurations and parameters over the life cycle of the equipment requires additional features, such as distinct login IDs to restrict access to configurations, parameters and data to those entities entitled access. Integrating the equipment onto the network, complete with applications is essential for productive use of the data.

Standards vs. Proprietary

There are certainly a number of different approaches to wireless data. Proprietary solutions provide point-to-point, or limited networking capabilities between equipment and

PCs. Standard Internetworking protocols are provided by additional software on the PC, and make deployment more complicated. Standards based networking, such as WiFi (IEEE 802.11) provide an extension of the corporate infrastructure down to the device itself. This allows the use of all of the power and global reach of the network to be utilized.

Wireless Complexities

Wireless adds additional complexity to networked devices. Not only do you have the traditional IP address and TCP/IP stack requirements, but also you have to concern yourself with how to get to the network. WiFi networks have both unique channels and Service Set Identifier (SSID) that need to be configured before data can travel over the network.

Unlike traditional Ethernet connectivity that only provides one channel to the network, WiFi provides up to 14 distinct channels for networking. The Client device must be on the same channel as the Access Point in order to associate and begin data exchange. Depending on where you deploy the devices, each Client device may need to use a different channel.

Issues, such as interference and multiple access points, require each Client device to be agile and programmable in its communication to the Access Point.

Embed Quatech's Airborne™ 802.11b Wireless LAN Node Module into OEM applications in as little as 6 weeks.

- Highly integrated 802.11b wireless module with radio, base-band & application processor
- Built-in web server enables drop-in LAN and Internet connectivity
- Quick time-to-market & reduced development costs
- Reduces need for RF and communications expertise
- Integrated RTOS and TCP/IP Stack
- Configurable serial, digital & analog I/O ports

Each Access Point has a Service Set Identifier (SSID) which is unique not to the Access Point, but to the network service the Access Point provides. The SSID is the "name" of the subnet or service. Any Client device wanting to associate with the Access Point must be configured with the same SSID. If the Client and the Access Point have a different SSID, they will not be able to communicate.

Finding embedded wireless devices can also be a challenge. It is not possible to just walk-up and plug into the network port and communicate with the device. A wireless-based device discovery mechanism must be available in order to find Client

devices during deployment or, later, for upgrades and operation. The discovery mechanism should not only be able to locate the IP addresses on the wireless network, but also find some human-readable description, or name, of the device.

Security is a paramount feature in a wireless LAN. Since direct physical interaction is not required to gain access it is important to secure the network logically. The standard mechanism for this in a WiFi network is using WEP. Although WEP is not perfect, there have been numerous enhancements to it. These enhancements, including individual keys per Client, and periodic re-keying are primarily implemented in the Access Point, and significantly increase the privacy of network data. Upcoming enhancements such as 802.11i and WPA will make the system significantly more robust.

Managing Access

Managing access to the functionality and data of both the Client and the equipment itself is a common practice in the IT industry, but seems fairly rare in the industrial environment. The IT industry has long-ago learned that restricting access to information and services not only prevents malicious use, but also “keeps honest people honest” by managing what kinds of information and control curious users can have access to. Many of the parameters under control, even though simple, can cause headaches in understanding the changes, locating the Client over the network, and recovering the devices. The best way to manage these changes is by distinct login/password accounts for the manufacturer, network deployment and daily operation.

Existing applications

Most existing data interfaces have software written specifically to manage the equipment or retrieve production-related data. In the case of serial interface devices the applications are typically written to use the serial device interface (COMx:) in Microsoft Windows. In order to provide a seamless transition from direct-wired RS-232 interfaces and wireless networks, the appropriate drivers and services must be provided in the operating system. It should be the responsibility of the drivers and services to understand about wireless networking, not the application program.

This allows existing applications to use advanced wireless networking features without re-writing the application code.

Many times a web browser interface is desired for the equipment. This provides a standard interface to the equipment for multiple users, without additional software development. The addition of a web browser interface requires that the Client device have not only a web-server, but a data interface to the equipment as well. Many networked client devices have a static web-server for configuration, but few have a dynamic web-server capable of building web pages containing dynamic equipment data. This is an essential feature for rapid deployment of equipment with new capabilities.

Implementation Tradeoffs

There are certainly a number of different approaches to adding wireless networks to existing products. The most tempting is to take existing off-the-shelf networking products such as PC Cards, Compact Flash or USB adapters. While this approach is feasible, it doesn't come cheap. In addition to the wireless adapter hardware, you have to figure in the TCP/IP stack, web server, and the configuration and management software. Even licensing these software components, there is still a fair amount of integration costs including both hardware and software. The cost tradeoffs between tackling the wireless networking yourself and buying already proven modules needs to be weighed carefully. The dollar difference in unit costs may be more than offset by the development costs and production delays associated with learning complex new technologies.

Conclusion

While WiFi Client devices and Ethernet Client devices may seem, on the surface, to be the same horse with different stripes, they are very different beasts. The complexity of configuration and deployment are exaggerated by the fact that there is no “plug” to connect directly into in the case of problems. A properly designed Client device, capable of managing the peculiarities of the network, is a must. Instead of simply a device that expands on a modem “AT” command set, or a wireless addition to an Ethernet product, a WiFi Client, designed from the ground-up, is necessary to manage and simplify the various complexities of wireless.