SMARTPHONES & M2M

CONNECTING MADE EASY, FINALLY.

by Bill Conley

You could argue that wireless data communications began in 1782, when Claude Chappe used semaphore towers to send messages between Paris, France, and the city of Lille, 220 km away. Called the 'Telegraph," Chappe's system was the origin of the word used for electrical messaging systems developed in the following century. It didn't work in bad weather, it didn't work at night, there was no network security and the data rate between Paris and Lille was roughly one symbol per minute. But it was the cutting edge of technology in its day, and an instant success. New telegraph lines soon sprang up all over Europe. When Morse code and electrical signaling came along they were faster and more efficient than the Chappe Telegraph, but the name stuck.

Data communications have continued to improve ever since. And just as happened with Chappe's telegraph, it would seem that new technologies must automatically supplant their predecessors.

But sometimes that's impractical. For example, in spite of the improvements of things like USB and Wi-Fi, there are still millions of perfectly serviceable serial devices in the world. And new serial devices are still coming on line. Serial technology is reliable, it's still very useful and so many people have so much invested in existing serial devices that the standard won't be disappearing any time soon. But as tablets and smart phones become more ubiquitous in the corporate and M2M business world, connecting to serial ports has become a bit more complicated. Tablets and smart phones don't have serial ports. In fact they tend to have limited wired connectivity of any kind, largely relying upon wireless communications for their interaction with the rest of the world. They're wonderful devices, but they're not natively designed to interact with serial equipment. Manufacturers, suppliers and integrators 2M equipment – as well as their customers - have a continuing need for serial communications.
So what can they do about the communications gap?

HOW IT WORKS

Serial device servers can be wired or wireless. The most popular types are network or TCP/IP device servers. In either case, wired or wireless, the serial server translates the serial data into an Internet Protocol (IP) format that can be transmitted across a network.

Wired serial device servers use Ethernet cable to connect to the local area network (LAN).

Wireless device servers contain a Wi-Fi client similar to the one in your laptop and connect via Wi-Fi, or 802.11. (The most common standards are 802.11b/g and 802.11b/g/n.) Wireless servers can connect to either an infrastructure network or to an AdHoc network.

When the Serial Device Server (SDS) network interface is connected to a LAN it provides an IP address that all other network devices can use for sending and receiving information. This address is unique to the SDS. Since this address is the location for all interactions, a secondary reference is used to locate the information or resource required for the specific interaction. This is called a port number.

Using the combination of IP address and port number it is possible to uniquely locate any serial port on the network.

It works like this: A serial device server has a physical serial port connected to port 8023 on the network interface. The network interface connects to the network and gets an IP address of 192.168.2.100. After combining the two pieces of information the full address of the serial port would be 192.168.2.100:8023. Any network-connected device capable of accessing that address can receive data from, or send data to, the serial port.

So what's the problem?
Current network SDS devices are designed to be used with an existing network infrastructure. If you have a manufacturing facility, warehouse or office, odds are that you already have a network installed - wired, wireless or both. Connecting to these networks has become much easier with the latest versions of SDS technology.

But what happens when you want to talk to a device that isn't covered by an existing wireless network? A large portion of the desired serial data may come from remote locations that are out of the coverage range of the corporate Wi-Fi network, or in an area where access to the available network is restricted because of IT policy and security rules. How can users access the data from these devices?

EMBEDDED HOTSPOTS

There is emerging technology that supports embedded Access Point functionality without changing the SDS functionality. As an example, B&B Electronics' SDS technology features an embedded AP device that creates a small, self-sustaining Wi-Fi network around the remote equipment that isn't all that different from the hotspot in a coffee shop. As your technician comes into range of the network, his Wi-Fi tablet or smart phone sees the network, connects to it and receives an IP address from the embedded AP. His device can then access the serial port on the AP using the appropriate IP address and port number. It doesn't change the way the SDS devices are used, it just makes them easily accessible to tablets and phones. Benefits of embedded AP:

- Tablets and smart phones will be able to access serial data in addition to existing network devices like laptops.
- Network devices won't need reconfiguring to use static IP addresses.
- A self-maintaining network won't lose devices or compromise their access.
- Users can simultaneously add and access wireless and wired devices on the embedded hotspot.
- There is no change to the existing use paradigm of networked serial device servers.

The example B&B device can support up to two serial devices, an Ethernet 10/100 network and multiple wireless clients simultaneously. It provides WPA/WPA2 security and an embedded DHCP server. Both external box and embedded module versions are available.

Serial ports have been around for a long time, and they represent an earlier generation in communications engineering. But that doesn't mean that tablets and smart phones shouldn't talk to them. They still have a lot of information to share.

TALK BACK!
Visit Bill's wireless blog and chat it up!
We'd love to hear from you!
www.bb-elec.com/Tech-Support/Bill