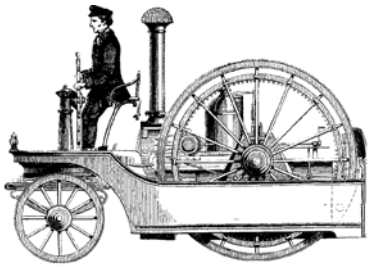
Changing the Rules of the Road – How to Make Legacy Devices Communicate in A Wireless World

The Ford Model T started rolling off the assembly line in 1908. If you'd purchased one you would have found yourself sharing the right of way with Stanley steam cars, battery-powered Baker coupes, horses and buggies, mule trains, ox carts, Indian motorcycles, bicycles and trolley cars. There was more than one way to get around and each one had unique advantages. The result, quite often, was sheer bedlam.

Modern digital communications may appear to be in a similar state of disarray. Newer protocols like USB and Wi-Fi haven't driven older protocols like RS-422/485 off the streets; they merely share the right of way. There are still some things that serial communications do so well – connecting the pumps at your corner gas station to the cash register would be a good example -- that the total number of serial-equipped devices deployed around the planet is actually continuing to grow. They'll be out there on the road for a long, long time.



Inconveniently, few computer manufacturers bother to support the serial protocol anymore, as its IT and desktop functions have largely been replaced by USB and wireless. It's getting harder and harder to find a new computer with a serial port. Tablets and smart phones are even worse. Some don't even have a USB port; they largely depend upon wireless for their communications purposes.
They're useful tools, but what do you do if you need to connect to older devices and protocols?

The Current State of Affairs

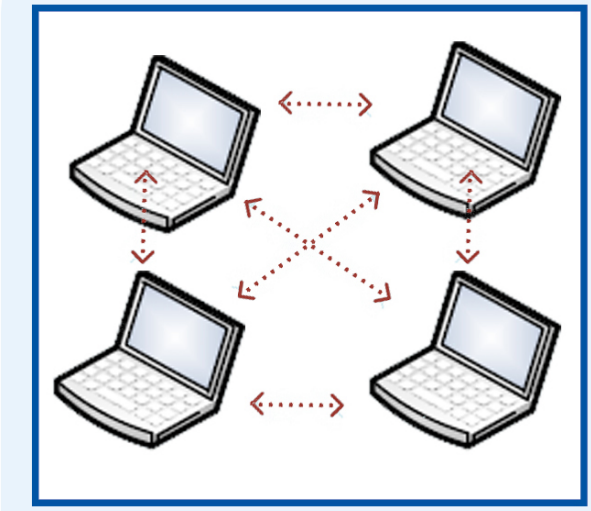
Ethernet and serial communications started cooperating with one another when the Ethernet serial server came along. The serial server translated the serial data into TCP/IP formats that could be transmitted across a network. The serial devices could then be network-enabled, and the device servers could use ordinary Ethernet cable to connect to a local area network (LAN).

The next step was to go wireless. A wireless device server contains a Wi-Fi client very much like the one in your laptop, usually 802.11b/g or 802.11b/g/n these days.

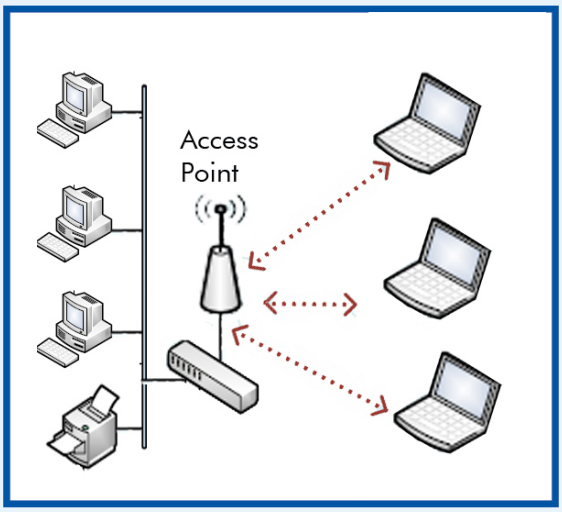
When a device server connects to a LAN it provides an IP address that is unique to the SDS. The other network devices can then use that address to send and receive data. Since this IP address is the location for all interactions, a secondary reference is added to locate the information or resource required for the specific interaction. The secondary reference is called the port number.

The IP address/port number combination makes it possible to uniquely locate any serial port on the network. Here's a typical scenario: 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 adding the second piece of information the full address of the serial port becomes 192.168.2.100:8023. Any network-connected device capable of accessing that address can establish two-way communication with the serial port. So far; so good.



AdHoc Network



LAN

What Happens When a Device Goes Off-Road?

A serial device server needs a network connection to do its job. But some serial devices are placed in remote locations where they not only lack access to wired infrastructure; they're also outside the range of any potential wireless connection. Sometimes access is available, but it's restricted because of IT policy and security rules. The need to communicate with these devices still exists, but the connection isn't there.

Where there's no available network infrastructure it's possible to set up an AdHoc network. (A wireless device server can connect to either an infrastructure network or to an AdHoc network.)

An Adhoc network is a peer-to-peer based network that doesn't use a central resource (Access Point) to manage the network connections and structure. AdHoc networks can be established when just two clients are within range of each other. Groups of devices can also be connected, with each group being referred to as a "cell". The AdHoc network uses the Internet Protocol Suite for data communication between the devices.

But an AdHoc network has some drawbacks:

- You have to use Static IP Addresses. A service called DHCP, which larger networks often use to provide IP addresses to connected devices, is not normally available on an AdHoc network. That means you'll have to manually assign and distribute unique addresses to each device.

- AdHoc creates a static subnet for the network and for all devices on the AdHoc network. This restricts interaction between different networks. You'll have to manually configure your IT (laptop) equipment when connecting, and enter a static IP address.

- AdHoc networks are not self healing. Even if you have multiple AdHoc networks within the same geographical location, and they're all using the same network name, devices in one network still can't talk to devices in the other.

There's another problem with AdHoc networks, which is that the latest Android™ tablets and smart phones can't connect to them without advanced modification. And certain iOS devices can't connect to AdHoc networks that employ wireless SDS's.

So How Do You Get Things Moving Again?

Just as the Model T Ford eventually gave way to newer, sleeker vehicles, Wi-Fi technology keeps getting better and better. There is now technology that supports embedded Access Point functionality without changing the SDS functionality. For example B&B Electronics has developed an embedded Access Point that creates a small, self-sustaining Wi-Fi network around remote equipment wherever that equipment may happen to be. It's quite like the hotspot in a coffee shop. Your technician can use that network hotspot to connect his Wi-Fi-enabled laptop, tablet or smart phone and acquire an IP address from the embedded AP. His portable device can then communicate with the serial port on the AP. This doesn't change the way the SDS devices are used, it just makes them easily accessible to tablets and phones.

B&B Electronics' embedded wireless access point network-enables legacy devices

Embedded AP has numerous benefits. Tablets and smart phones can now access serial data. Network devices don't need to be 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. Networked serial device servers can be used just as they always have been.

The Stanley Steamer was only sold for about two decades. Serial ports have already been around a lot longer than that, with no end in sight. Embedded wireless AP ensures that you'll be able to keep yours running smoothly for as long as you need to.