Make Your Tablets and Smart Phones Smarter – Add Serial Capability for Seriously Remote Data

Andrew C. Ross (aross@bb-elec.com), Director of Wireless Applications for B&B Electronics (www.bb-elec.com)

 To paraphrase Mark Twain, rumors about the demise of serial ports are greatly exaggerated. Serial ports are everywhere, in everything from industrial automation systems to scientific instrumentation. Too many people have too much invested in serial-equipped devices for the standard to disappear any time soon. But as data communications technology continues to evolve, the humble serial port is sometimes left behind. This article will review serial device server technology, its usefulness and drawbacks, and then demonstrate how to access serial data from locations that are either remote or restricted and therefore out of range of a WiFi network.

Back when the first serial device servers were introduced they closed a connectivity gap between connected devices and remote networked PCs. The development of the serial-to-Ethernet device server in the late 90’s was another huge step forward. Later, the advent of USB made accessing serial data from desktops and laptop PCs easier than ever.

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 of M2M equipment – as well as their customers -- have a continuing need for serial communications. So what can they do about the communications gap?

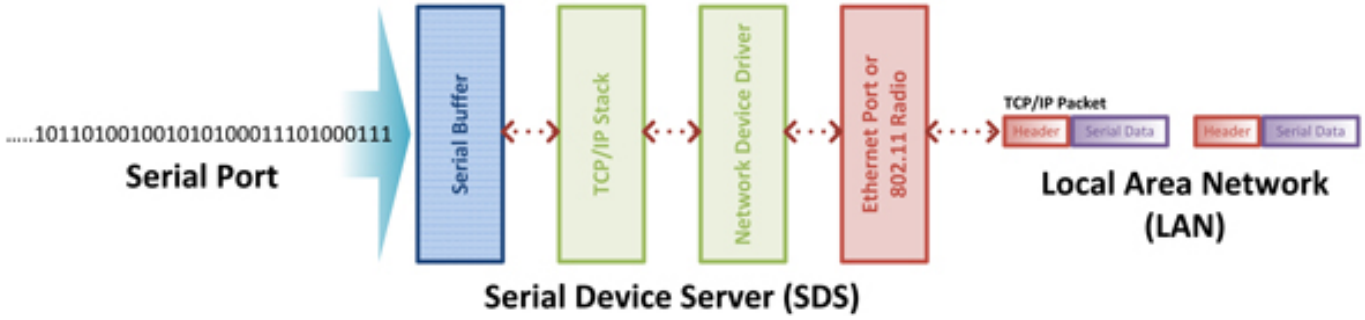
How does it work now?
Serial device servers can be wired or wireless. The most popular types are network or TCP/IP device servers. In either case -- wired or wireless -- the serial server translates the serial data into an Internet Protocol (IP) format that can be

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

Wireless device servers contain a WiFi client similar to the one in your laptop and connect via WiFi, 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 (see sidebar for explanation of network types).

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. (See Fig.1)



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. (See Fig. 2)

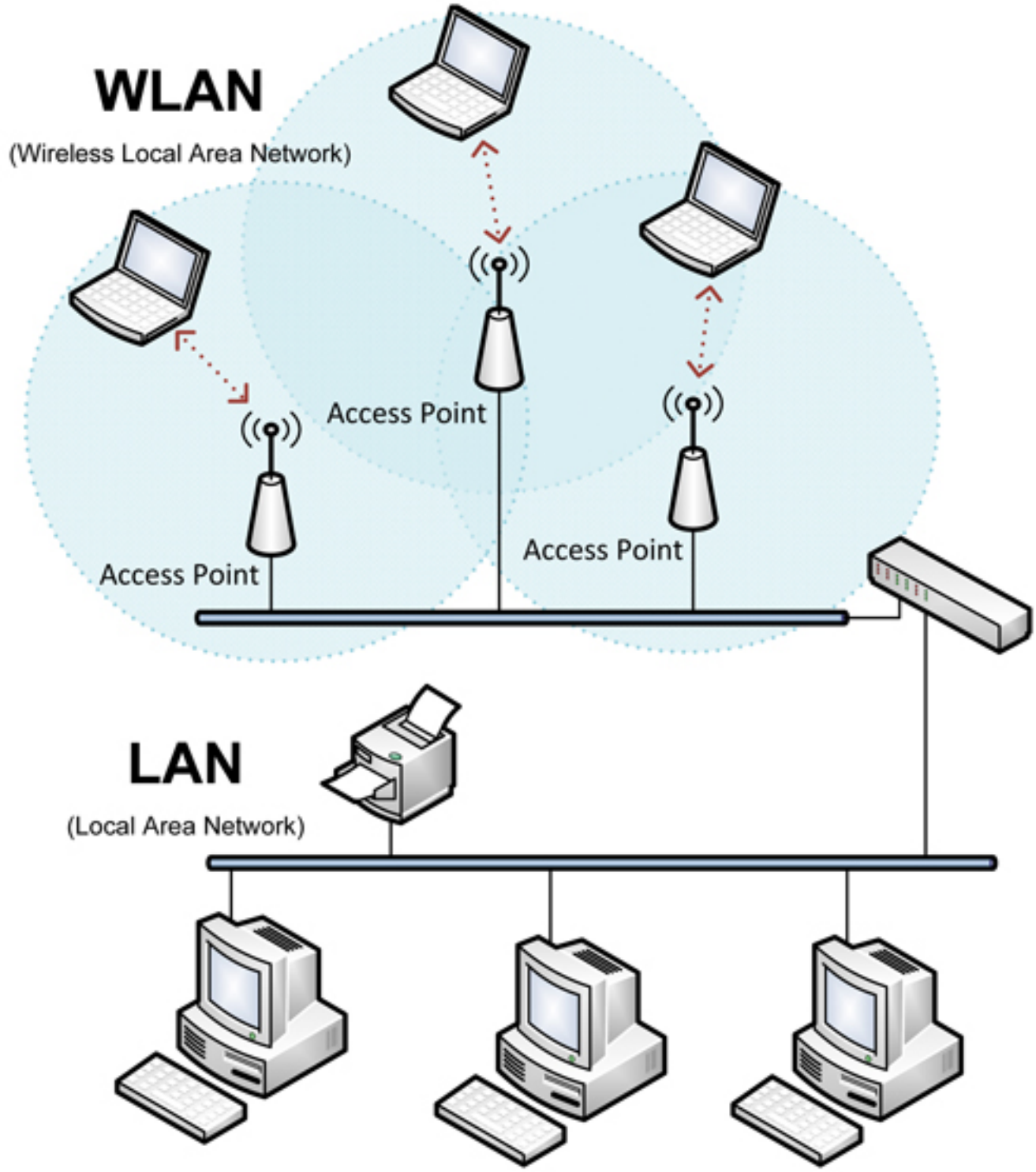


Figure 2. Infrastructure: A wireless network uses Access Points to connect a variety computers and equipment, allowing them to share resources and information. Referred to as Wireless Local Area Networks (WLAN) they use the Internet Protocol Suite for data communication between computers, networks and devices.

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 WiFi 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?

Historically, a wireless network type called AdHoc has been used where no available infrastructure network exists. (See Fig. 3)

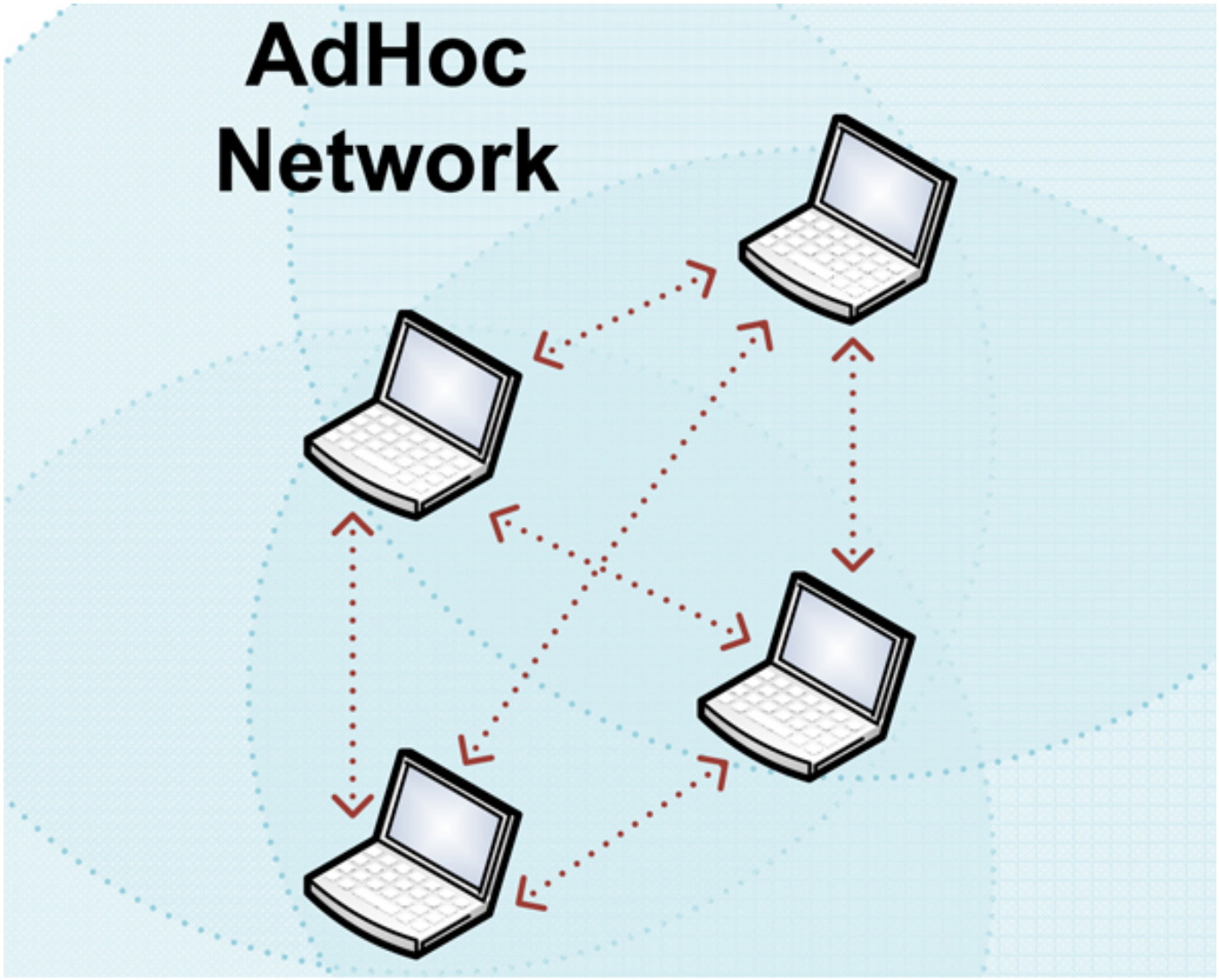


Figure 3. AdHoc: A peer-to-peer based network that does not use a central resource (Access Point) to manage the network connections and structure. AdHoc networks can be established when just two clients are within range of each other, with each group of devices being referred to as a cell. They use the Internet Protocol Suite for data communication between the devices in the AdHoc network.

AdHoc, however, has certain issues:

• **Static IP Addresses are needed**: A service called DHCP, often used on large networks to provide IP addresses to the devices connected to the network, is not usually available on an AdHoc network. This has several drawbacks:
  o It requires manual assignment and distribution of unique addresses to devices.
  o It creates a static subnet for the network and for all devices on the AdHoc network. This restricts interaction between different networks.
  o It requires manual configuration of IT (laptop) equipment when connecting to the AdHoc network. Personnel are required to 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 are utilizing the same

network name, devices in one network cannot talk to devices in the other. This can therefore limit or prevent access to serial data.

There's an additional issue with AdHoc networks. The latest Android tablets and smart phones don't connect to them without advanced modification of the devices. There are also known issues with certain iOS devices that make it impossible to use them with AdHoc networks that employ wireless SDS's, which forces users to carry bulky laptops for remote access.

How about an embedded hotspot?
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 (See Fig. 4) that creates a small, self-sustaining WiFi 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 WiFi 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.

Figure 4. Embedded wireless module from B&B Electronics.

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.

Application Example – Tablet Accesses Serial Data Using Embedded AP for Remote Security-Monitoring

Homeland Security has expanded the need for camera-based monitoring systems in extremely remote locations, and many security-monitoring applications will have both remote sensors and vision systems. In one such application, a B&B Electronics customer has installed an IP camera, barometric pressure and temperature sensors and a microcontroller capable of storing event or time-based scenarios. It can record a picture or a short video coupled with a time code and a record of environmental conditions. The remote location is not accessible from an existing network, so an officer visits it once or twice a week and downloads the data to a tablet that accesses the embedded AP attached to the serial port on the controller.