

Demystifying Wireless Ethernet

Jim Gardner, Business Development Executive, Oil and Gas, FreeWave Technologies

Many SCADA (Supervisory Control and Data Acquisition) managers are looking to convert their telemetry systems from serial communication (RS-232, or RS-485) to Ethernet. Many IT supervisors are comfortable with Ethernet, but have not had much experience with wireless technologies. The world of wireless Ethernet still is new enough that a lot of myths are associated with it. Sorting through this maze of misinformation can be daunting, even unnerving. The following is a list of common questions that seem to be the most mystifying for the average SCADA expert, IT professional or instrumentation technician.

So What are These Mysteries?

- How do I integrate Ethernet into my serial network?
- Can I get IP addressability to the wellhead?
- What advantages can I expect?
- What does it cost?
- Can I have mobile connectivity for my vehicles?
- Can I speed up my polling times and by how much?
- Can I have multiple sites polling the network?
- Can I talk to legacy serial devices?
- Can I bring Modbus data through my Ethernet network?
- Can I talk to instrumentation via Ethernet?
- What frequency Ethernet backbone should I use?
- How do I plan an Ethernet backbone, what are the considerations?
- How many repeaters can I use?
- Who can design, install and deploy this for me?
- Is it secure (encryption, authentication)?
- Is it reliable?

The trend in data communication clearly is moving to Ethernet, since the advantages are too compelling to ignore. Security, faster polling times, mobile communications, Internet accessibility and IP addressability all provide benefits previously unavailable with serial communications.

So Who Will Care About the Answers?

IT Supervisors, Measurement Managers, Automation Managers, SCADA professionals, I & E Technicians, Systems Integrators, Communications Providers, Electrical Engineers, Electronics Technicians, Digital Security Personnel, Production Optimization teams, Facilities Engineers, RTU Manufacturers, EFM Manufacturers, PLC Manufacturers, Instrumentation Manufacturers.

Radio manufacturers are building an increasing number and variety of wireless Ethernet radios. RTU, PLC and EFM manufacturers are including Ethernet ports on all their latest generation devices. The transition has begun, but the process of matching the right products to the right applications still is in the early stages. Here are typical questions that usually arise with possible solutions to each.

How do I Integrate Ethernet into an Existing Serial Network?

With millions of dollars invested in legacy serial systems, this is one of the most common questions. Many radio manufacturers are building terminal servers (protocol translators) into their Ethernet products. If needed, an external terminal server also can be used to convert serial data to Ethernet. The entire system does not have to be replaced to gain the benefits of Ethernet. The end user can start by changing the master radio and the repeater sites to Ethernet and leave the slave sites as serial to still gain many of the benefits. (See Diagrams 1 and 2.)

Diagram 1 and 2 are the same system. Diagram 1 is a graphic representation of changing the master and

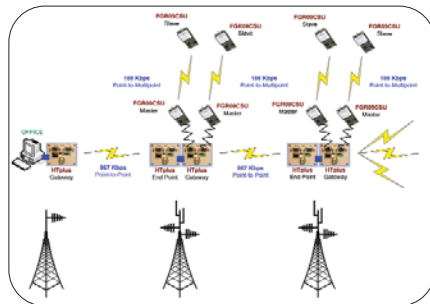


Diagram 1

repeaters to a high throughput Ethernet system, while Diagram 2 is a block diagram of the same system.

By using the high-throughput Ethernet radios as a "backbone" between repeaters, IP addressability for all data traveling through the network is realized. Also port identification is available via numbers that route the data to both the correct IP address and the proper port number. If this data were being delivered by the post office, the IP address would be the equivalent of the regional post office, and the port number would be the mailbox within the post office. With multiple ports on every IP address, the one system can begin to be divided into multiple systems. (See Diagram 3)

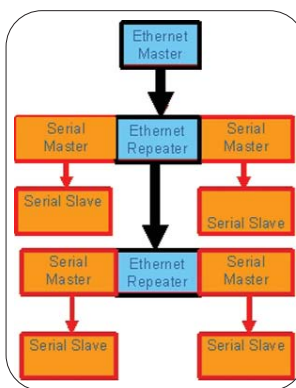


Diagram 2

repeaters to a high throughput Ethernet system, while Diagram 2 is a block diagram of the same system.

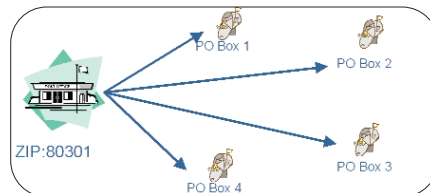


Diagram 3

In this scenario, each Ethernet radio now can have two serial master radios connected to its two serial ports. Each master has its own group of slaves or, in other words, its own network. By adding three high-throughput Ethernet radios at three repeater sites to an existing network of 600 radios, the network could then be split into six separate networks of 100 radios each, dividing polling times by six. If the polling time was 120 minutes in the old serial system, it now would be 20 minutes in the new Ethernet system. This represents a huge technical advantage for a relatively small capital expenditure (about \$6,000).

Can I Get IP Addressability to the Wellhead?

The way to get IP addressability to the wellhead is to install Ethernet radios at each well. The RTU or EFM at the wellhead does not necessarily need to have an Ethernet port or IP address. The radio can convert the Ethernet traffic to serial and vice versa. The radio can be a simple wire replacement device if your wellhead equipment has IP addressability, or it can act as the protocol translator between serial devices and Ethernet networks.

If older, licensed radio technology is being used, then the same holds true and the master radio for the licensed system is moved to the repeater and tied to the system (tail-end) into the Ethernet network.

What Advantages Can I Expect?

The most common advantage managers can realize is speed, which translates to faster polling times. Other advantages include: real time alarms, mobile connectivity (access to the network from the truck), connectivity to devices that have serial connections but do not have an Ethernet connection, security, encryption, access to data from multiple offices and peer-to-peer communication.

What Does it Cost?

While this is an open-ended question, there are many high throughput radios that deliver approximately one megabit over-the-air throughput that sell for \$1,000. However, as a general rule, the higher the throughput, the more expensive the solution. Don't overlook an important, often overlooked cost: the associated cost of installing the system. Many of the highest throughput devices assume that there is AC power available everywhere a radio is installed. One end user recently paid \$20,000 for solar panels and batteries for a high-throughput repeater site that did not include the cost of the radios, the antennas or the coax cables. Obviously, he had the wrong tool for this application, because other products could have accomplished the same thing using \$500 worth of solar and batteries.

When considering product options, end users should look closely at power consumption needs of the products, their range and throughput to ensure they are selecting a product that will meet all of their requirements.

Can I have Mobile Internet Connectivity for My Vehicles?

The short answer is "yes," but not everywhere. Just as cell phones are prone to interference and lost signals, radios also can suffer similar maladies. Radios rely on "line-of-sight" to communicate. There will be areas in every application where the person in a vehicle will not be within the line of sight of a repeater tower. Sometimes, a technician will have to drive to a nearby hilltop or open area to get line of sight back to a repeater.

Can I Speed up my Polling Times and if So by How Much?

The short answer here also is "yes," but the "how much" answer is a function of two variables. First let's look at one of the advantages of Ethernet and IP addressability. In a serial system there only is one conversation allowed at a time much like a telephone call where the master has to hang up with one slave before it can call the next. In Ethernet, the rules change. Multiple slaves can be called at the same time. The IP addresses of these multiple slaves allow the master to route the conversation to the right slave, receive multiple messages back at the same time and then de-scramble the messages by using the IP address. Again, it is like the mailman looking at the address and putting only the right mail in the right mail box. (See diagram 3)

So the question now becomes, "If I have a 'hybrid' serial and Ethernet system, how many serial networks can the system be broken into?" As previously stated, by moving the masters to the repeater sites, two masters at each repeater site can be created. However, in an all Ethernet system, the question becomes, "How many conversations will your host software (polling engine) support at one time?" It is common to see polling times reduced by six or even eight times in "hybrid" systems.

Can I Have Multiple Sites Polling the Network?

Yes. The IP addressing ability of Ethernet allows conversations to be routed from one point to another point within the network. The best example of this is at the office. Multiple work stations can poll the server for information at the same time. The server knows which station made which request, by identifying the particular IP address it has, and sends the right response to each. In the case of an IP-based radio network, the regional office (in Tulsa, OK, for example), can poll the field and the corporate office (Houston, TX) has the same privileges once the system has IP addressability.

Can I talk to legacy Serial Devices?

As discussed earlier, this can be done in two ways: with Ethernet radios at the wellhead or by combining Ethernet and serial in a "hybrid" system.

Can I Bring Modbus Data Through an Ethernet System?

Yes, the radio system is just the messenger. In most cases, the radio acts like a replacement for wire and transmits the message from the slave to the host. In the case of Modbus, the radio "packets" the message and puts it in an Ethernet "wrapper" for transmission. At the master site, the packet and Ethernet wrapper are removed and the data, in its original format, is handed to the host. Many radios have a Modbus feature, allowing the radio to "spoof" the Modbus device into waiting a little longer than normal before it breaks its link. This allows the host and the Modbus device to have a two-way communication or "full duplex communication." Originally, Modbus was designed for one-way communication only.

Can I Talk to Instrumentation on an Ethernet System?

Yes. Many instruments have RS-232 or RS-485 communications, but do not have a unique device ID. The Ethernet radio can take the place of the device ID by using its IP address. In this way, the host can communicate to level sensors, chromatographs, provers, correctors, etc. Additionally, with many of the new wireless I/O radios now available, it is possible to communicate directly from the host to an analog device in the field. An example of this is a pipeline company with offices in Tulsa that recently polled-over the Internet a pressure transducer located in McAllen, TX. The communication went over the Web and the radio system without any RTU's or PLC's in the link.

What Frequency Backbone Should I Use?

The best technical answer to this may not always be the best practical answer. Most radio manufacturers have Ethernet radios in 900 megahertz (MHz), 2.4 gigahertz (GHz), and some have 5.8 GHz available also.

The lower the frequency of the radio, the more forgiving it is for line of sight issues such as penetration of trees, buildings, etc. But the lower the frequency, the more congested the spectrum, typically. Most data communications in this country are in the 900 MHz band. Therefore, usually it is better to have the "high-speed backbone" in a different frequency band than the SCADA, or gas measurement, systems. It always is advisable to get an RF (radio frequency) expert to take a spectrum analyzer tool to the area where you intend to install a high-speed backbone and get feedback on what will work best in that environment.

How Do I Plan a Backbone? What are the Considerations?

The first consideration is towers and line of sight. These are referenced together because you need to ensure that the towers have line of sight to each other and to the locations where the slaves are located. The first step with towers is to determine if you

are going to purchase or build. The purchase option often is the quickest, and that is to identify commercial towers in the geographic area you are interested in and contact the owners for lease space on the towers. Typically rent is at least \$1 per foot, per month, so if you rent space at 100 feet, it would cost at least \$100 per month. The build option is to identify high ground where you can erect a tower of your own. Prices vary, but a 100-foot tower would cost about \$10,000 in most areas. Once you have identified the sites you want to use, a path study should be completed to determine if you can communicate to all of your proposed towers. All you need for a path study is the GPS coordinates of the proposed towers and the heights where your antenna will be installed. Many communications companies that act as resellers for radio manufacturers will provide all of these services for you as part of a turnkey service, along with the purchase of the radio equipment.

How Many Repeaters Can I use?

The answer may vary depending on the manufacturer you are using but many manufacturers have no limit to the number of repeaters you can use. It is important to have a qualified technician design the system because one of the most common problems in radio systems is poor design where two repeaters interfere with each other.

Who Can Design and Install This For Me?

This may be the hardest question of all to answer. In most cases, the companies that design and install radios are aligned with specific manufacturers. They only sell one brand of radio. Often, the best choice is to discuss products and applications with a manufacturer and pick the products you want and ask the manufacturer to recommend factory trained and certified resellers in your area.

Is It Secure?

Not all radios are created equally, so be sure you look for security when picking a product. The commonly accepted security features to look for are:

- 128 bit AES encryption
- RADIUS Authentication
- MAC Address filtering
- Dynamic Key substitution
- VLAN Tagging

If the product you use has all of these features you should never have any concerns about security.

Is it Reliable?

A properly designed and installed wireless Ethernet system should be 99 percent reliable. There will be "acts of God," such as lightning, floods and hurricanes that can affect a radio system, but if you ask your potential supplier for return rates on the products you are looking to purchase, they should have a less than one percent return rate from all causes.

Summary

The advantages of wireless Ethernet are too numerous to ignore. Many speculate that serial communications will go the way of the black and white television. We now are seeing the way that the world of data communications is changing. It is early in the adoption phase, but Ethernet is quickly becoming the standard for many oil and gas producers.

When looking to implement your first system, asking all the right questions is a great place to start. Wading through the misty moors of myth and legend about new products is an unpleasant and tedious job, but all change has some risk and some pain associated with it. The change only will happen when the pain of remaining the same is greater than the pain of change.

Jim Gardner is the business development executive of oil and gas for FreeWave Technologies, Inc., a designer and manufacturer of spread spectrum radios. Gardner brings more than 30 years of management experience in the oil and gas industry, including the last five years at FreeWave. Prior to that, he served as director of business development for ABB TotalFlow and as vice president of sales and marketing for Remote Operating Systems and Pipe Renewal Service. He is a graduate of the University of Washington. He can be reached at 281-799-8643 or jgardner@freewave.com.

Visit the Freewave Booth At the Remote 2008 Conference and Expo!

Sign up today at: www.RemoteMagazine.com

Remote 2008
CONFERENCE AND EXPO

SCADA, Device Networking, M2M, Wireless Technology, Onsite Power, And Security for Remote Sites and Equipment

No other industry conference brings together technology users that manage remote sites like the Remote 2008 Conference and Expo. Over 50 conference sessions will provide cutting-edge technology direction and application strategies from the companies and users driving the growth in SCADA, M2M, device networking, data communications, system & site security, emerging wireless technology, remote monitoring and automated control, and onsite powering of distributed equipment, networks and facilities.

www.RemoteMagazine.com

NOVEMBER 5-6, 2008 - ATLANTA, GA.