UNDERSTANDING THE ADVANTAGES OF IP NETWORKS

Burke P. Miller

CenterPoint Energy / TCT
Houston, Texas 77041

Introduction

Convergence in the Oil and Gas Sector

Today's oil and gas industry faces increasing pressure to maximize the capability of its wireless infrastructure while minimizing operational and developmental costs. Unprecedented uncertainty and business volatility are transforming the landscape, as the oil and gas industry becomes more competitive, profit-oriented, and responsive to a fickle and savvy clientele. *The key to developing a successful enterprise-wide networking strategy is to recognize that it is only part of a larger strategy-one in which modern oil and gas facilities must literally reinvent themselves.*

Several key factors are driving this transformation:

- **Consolidation** - Corporate mergers and acquisitions both mandate and complicate the task of unifying workforces and infrastructure. Many companies have dozens of disparate wireless networks supporting both voice and data; these legacy systems, which are often comprised of a mixed technology base, must be unified, integrated, and standardized with emergent technology.
- **Competition** –Regulatory changes are fueling price and service competition where less previously existed. Consumers are seeking value, reliability, and flexibility, and are exercising choice with increasing frequency.
- **Security** - Post-9/11 security analyses have revealed widespread, systemic opportunity for improvement.
- **Technology Evolution** - Consolidation and competition are forcing corporations to do more with less. Applications enabled with intelligent networking infrastructure are increasingly necessary to service a larger, more diverse, and more demanding clientele. Workforce automation and mobility capabilities are extending oil and gas networks beyond conventional SCADA and front office functions.

Collectively, these factors represent high-level convergence across the industry - in administrative functions, in technology, and in business processes. Industrial wireless infrastructure is a vital component in addressing and mastering each of these factors; it permits unprecedented levels of technological integration for both new and old technologies, for SCADA and corporate networks, and for fixed and mobile applications.

Managing an enterprise mobility strategy, then, consists in managing convergence. And at the network level, this means adopting, and migrating to, an IP-based networking infrastructure. The corporate LAN/WAN computer network has become the common access medium for this data.

IP vs. Serial Interfaces

Migration to IP Networks

Wireless networks have traditionally supplied serial RS-232 interfaces for landline network connectivity. The oil & gas industry in particular has used serial connectivity for over 25 years to attach an automation device, such as an EFM or RTU, to a wireless communications device (radio).

In the last several years, however, more and more companies are using the IP/Ethernet interface instead, for a variety of compelling reasons.

- The merger of the I.T. computing departments with field telecom and wireless engineering groups within the oil and gas sector is creating a need for practical technical standardization. Information technologists want a computer network standards protocol to acquire the field data. IP (Internet Protocol) is the most common of these, with Ethernet as the most common communications medium.
- This gives rise to an implied need for common troubleshooting and diagnostics standards. In the computer networking world, the most widely used standard is SNMP, or Simple Network Management Protocol. Today most computer network devices, (both wired or wireless), are designed to comply with SNMP diagnostics standards.
- Other network management tools found in the IP/Ethernet domain (Ping, TELNET, HTTP, etc.) give network managers a broad spectrum of tools to monitor and control corporate networks.

Advantages of Serial Interface

Serial interfaces have been widely used and highly successful for decades. Here are few reasons why:

1. **Understanding**: Serial interfaces are well-known and understood by field personnel. Most field technicians have been trained to use the RS-232 or RS-485 interface.

Ubiquity: Nearly all automation devices, EFM, RTU, PLC, etc. have a serial port, while most devices in service now do not have an Ethernet network port. However this is changing as many offer both now.

2. **Configuration**: It is simple and easy to configure serial devices. The connector pin out functions, such as RXD, TXD, RTS, CTS, etc., are straightforward. Setting up the baud rate and data byte configurations, such as 9600 8N1 or 4800 7E1, are usually accomplished with simple pull-down menu screens. No addressing of the IP network, subnets, or ports & sockets is needed in an all-serial system.

3. **Efficiency**: There is very little overhead data associated with a serial network. In a typical asynchronous serial system, such as 8N1, a 10-bit byte would consist of a start bit, 8 payload data bits, no parity bit and a stop bit.

4. **Latency**: End-to-end data throughput delay is very low due to the simplicity and the small amount of overhead data.

5. **Narrowband**: Narrowband radio systems, (using a 12.5 Khz channel) are adequate for most serial polling systems. Most EFM/SCADA systems operate between a 1200 and 9600 BPS baud rate.

6. **Power Supply**: The typical remote serial radio has a lower current drain than a comparable IP/Ethernet radio. For remote EFM/SCADA sites that are solar powered, the lower current drain serial radios mean a less costly power supply is necessary.

7. **Price**: The typical serial remote radio has a lower price than a comparable IP/Ethernet remote radio.

Disadvantages of Serial Interface

1. **Homogeneity**: It is difficult to mix different equipment types and protocols on the same wireless network at the same time. For example, using Modbus at 9600 bps and HART at 1200 bps in the same radio system would be difficult to implement.

2. **Access**: Enterprise wide access to the field data is cumbersome in a serial network.

3. **Speed**: Slower data speeds using serial, 115.2 kbps is maximum for RS-232 interface. IP/Ethernet wireless networks typically run at data rates of 256 kbps and higher.

4. **Services**: Other types of network services, such as VoIP, wireless video, QoS, VLAN tagging, email, and mobile data are difficult or impossible to implement on a serial network.

Advantages of IP/Ethernet Interface

1. **Heterogeneity**: It is easy to mix different equipment types and protocols on the same wireless network at the same time. With IP networks, protocols such as Modbus and HART are each encapsulated in a data packet and then routed to the appropriate destination. See figs. 1,2.

2. **Protocols**: It is possible to mix polling systems with 'report by exception' systems on the same radio network, at the same time, without causing data collision on the radio channel. This is possible because IP networks can utilize a variety of protocols, such as TCP (transmission control protocol), that guarantee delivery of the data packets and correct any errors that may occur during transmission. See fig. 3.

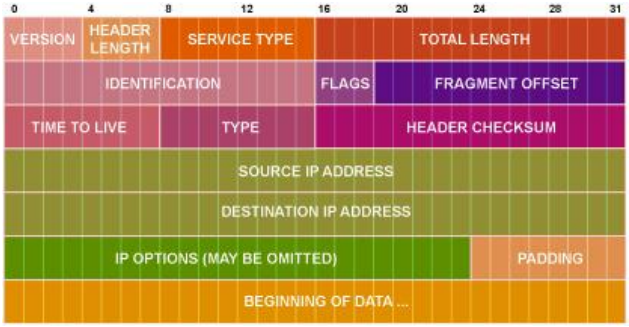

Figure 1. IP Packet Structure

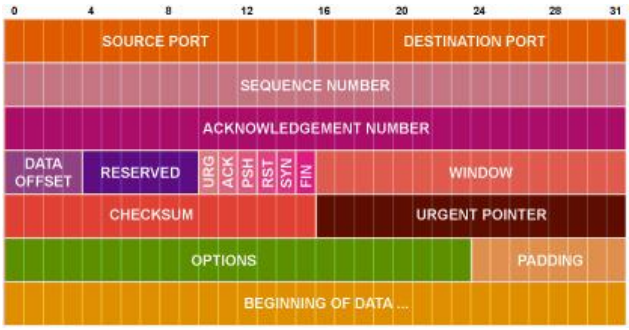

Figure 2. TCP Structure

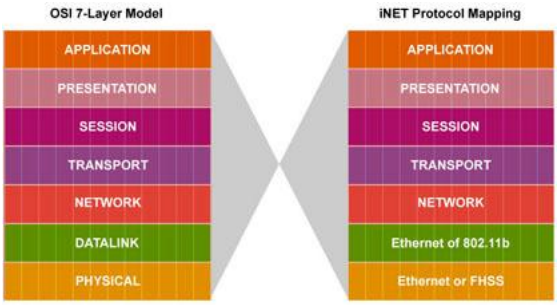

Figure 3. 7-Layer OSI Stack

3. **Compatibility**: The enterprise can get access to field data easily because it is part of the company LAN/WAN network. The field data is in a IP/Ethernet packet form that is compatible with the enterprise network.

4. **Flexibility**: Many types of network services can share the same wireless network at the same time. Because the data is all in IP/Ethernet packet form, VoIP (voice over IP), video, email, the Internet, WiFi 802.11a/b/n networks, mobile data & GPS (global positioning system) can be provided.

5. **Speed**: Much higher data rates are possible. A typical IP/Ethernet radio network operates at 256 kbps or higher, with the backbone networks operating at 10 mbps, 100 mbps or 1000 mbps.

6. **QoS**: IP/Ethernet packet types can be prioritized for QoS (quality of service), such as giving SCADA packets priority over voice or video packets. This insures that the most important data will have sufficient bandwidth available for transmission.

7. **Security**: IP offers much better data security, such as 128 bit encryption, two way authentication, user name / password protection, provision lists, dynamic encryption key rotation, remote port /radio disabling 'over the air', and others. VLAN tagging also provides a way to isolate each user's data from others on the same network.

8. **Tools**: Better diagnostics and management tools, such as Ping, Telnet, SNMP, FTP, HTTP, and many others are unavailable for serial networks. For example, SNMP can be used to track every device on the network, be it an RTU or a radio. It can determine what the device is, when a device communicates, when it is added or dropped from the network, indicate status of alarms, and many other functions. The FTP protocol can be used to download new firmware to upgrade the device (a meter or radio). With HTTP, service personnel can use their web browser to access the administrative interface of the radio to perform programming and diagnostics functions.

9. **Addressing**: TCP/IP offers virtually universal addressability out to the end field device.

10. **Standards**: TCP/IP/Ethernet is almost universally accepted in industrial applications.

11. **Accuracy**: The IP/Ethernet radio system, independent from the EFM/SCADA protocols, ensures data accuracy by doing CRC error checking, retries, CSMA/CD (carrier sense multiple access/collision detection), and in some radio systems, also use CSMA/CA (collision avoidance).

12. **Efficiency**: The MAC (Media Access Control) function in radio systems provides a means to avoid collision over the air, thereby making the radio channel much more bandwidth efficient, which means faster data throughput and more remotes per master access point.

Disadvantages of IP/Ethernet Interface

1. **Understanding**: IP/Ethernet is less well known by field personnel than the serial interface.

2. **Complexity**: IP/Ethernet is more complex to set up and configure.

3. **Installed Base**: Most existing field devices do not have a network port (Ethernet), or it is an optional feature.

4. **Efficiency**: IP/Ethernet has 25%-50% more overhead data than a serial system.

5. **Latency**: It has more end to end data delay than a serial system.

6. **Power**: A typical IP/Ethernet remote radio has a higher current drain than a serial remote radio.

7. **Cost**: A typical IP/Ethernet remote radio has a higher cost than a comparable serial remote radio.

The Value of IP Network Convergence

Combining Serial With IP/Ethernet Networks

Most installed field automation equipment and the radios systems interfaced to them are RS-232 serial devices. With the trend slowly moving towards IP/Ethernet networks, there is an increasingly compelling need to combine these serial systems with emerging IP/Ethernet networks.

IP Terminal Servers

The IP terminal server is a device that is designed to bridge these two communications architectures. It is a gateway device that transparently encapsulates serial payload data into the IP protocol, thus bringing serial payload data onto the enterprise network. This is an ideal solution for preserving investment in legacy serial devices (both measurement devices and radios) while facilitating migration to, or expansion of, an IP enterprise network for data collection. The terminal server may be a standalone device, or it may be one of many functions included in a wireless device (radio). The terminal server may also provide SNMP, TELNET and Web browser functions to the serial devices. See fig. 4

Communication Devices

Private vs Public IPs: In public IP systems, the carrier provides the end user with a list of public IP addresses to be used for the communications device, such as a network radio, cellular modem or satellite device. Using the carrier supplied IPs is the easiest and cheapest method, however it is less secure, because the device can be accessed by anyone on the Internet, if they knew the IP address, e.g., 148.63.1.5 If a private IP is used, the end user supplies their own list of corporate IPs that fit into the corporate addressing scheme being used, and this IP is programmed into the communications device. To accomplish this, the end user must supply a router or managed switch to be placed at the carrier's CO (central office) or earth station. A VPN tunnel (virtual private network) is built through the Internet between the corporate network router or switch and the carrier's CO or earth station hub. See Fig. 4. This establishes a secure private link between the corporation and the common carrier. The devices cannot be accessed by anyone on the Internet, without the required credentials, and because of the encryption used in the VPN tunnel. This link is more complicated to setup and is more costly, because of the extra router / managed switch. There is also a charge for the VPN tunnel circuit as well as a shelf fee from the communications carrier to have the user's device located in their CO or hub. The end user normally has complete control of the router / managed switch on site, for programming, testing, updating, etc.

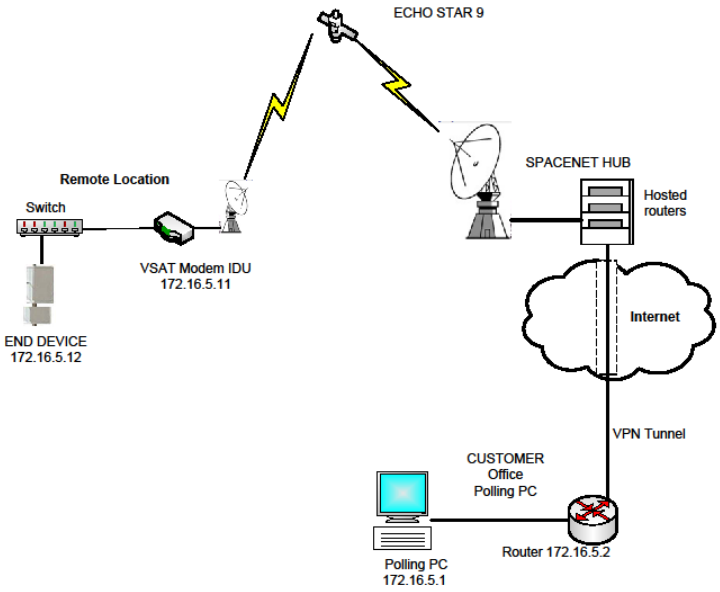

Fig. 4 - Typical VSAT Private IP Network

Benefits For the Corporation

The value of a convergent network that is predicated on IP/Ethernet networking technology is multifaceted, as the various strengths articulated in this document indicate. These include the ability to efficiently reuse existing network infrastructure to create scalable work solutions that grow in tandem with the rprise.

efits for the Field Technician

s important to emphasize, however, that efits accrue to the field technician as well. se benefits fall into two broad categories:

ormation: The amount of information that be made available for diagnosis and repair n IP network is considerably more than t is available in a serial network. More , greater accuracy, and higher relevance to minimize wasted time and out of service utes when problems occur.

ivenience: In an IP network, field nicians are not necessarily required to travel ite to diagnose and/or repair a faulty unit. The vast array of IP-based tools outlined above, combined with the remote management capabilities afforded by an IP network enable field technicians to diagnose problems remotely, saving time, money, and outage minutes