BASIC IP NETWORKING FOR FIELD TECHNICIANS

Burke P. Miller
4RF USA, Inc.
Houston, TX 77041

Introduction

Today's oil & gas industry is facing major technology changes in the field automation and control of devices. In the past nearly all SCADA and EFM devices only had a serial port to gather the data. These devices now have Ethernet ports along with serial ports, to communicate, control, program and transmit the data back to a company central data gathering/polling host. This change from mostly serial to mostly Ethernet communications has made the job of a field automation / measurement technician more complex. Setting up the Ethernet port in a meter involves knowing a number of parameters to ensure reliable communications of the data being polled. This article will cover some of the basic things a technician will have to know to connect to your company WAN (Wide Area Network).

Serial Interface Review

1. Typical interface is asynchronous RS-232
2. Connector types can be DB25, DB9, RJ45, etc.
3. Typical pinout is RXD, TXD, RTS, CTS, GRD.
4. Data speeds typically 4800, 9600 bps.
5. Typical byte configuration is 8N1, 8 data bits, no parity bit, 1 stop bit.
6. A terminal server is a device that interfaces with serial on one end and Ethernet on the other.

Networking Fundamentals

OSI Reference Model

APPLICATION Layer 7		HTTP, FTP, NTP, TFTP, TELNET, SNMP, etc
PRESENTATION Layer 6		PRESENTATION
SESSION Layer 5		SESSION
TRANSPORT Layer 4		End-End Connections & Reachability, Segments (TCP, UDP)
NETWORK Layer 3		IP (the Internet), logical addressing, path routing,
DATALINK Layer 2		Ethernet, physical addressing, MAC, LLC, CSMA/CD, NIC(Ethernet physical & data)
PHYSICAL Layer 1		Media, Signaling, Cat5, fiber, 100BaseT, RJ45, 802.11, 802.15

Physical Layer 1

- Type of media, twisted pair, Cat5, Cat6, 100 BaseT, 1000BaseT, fiber (single or multimode)
- Wireless media, 802.11 WLAN (WiFi), 802.15 Bluetooth
- NIC Network Interface Card, layer 1 and 2 device
- PoE Power over Ethernet, layer 1 and 2 device

Date Link Layer 2

- Physical addressing
- MAC (Media Access Control) every network device has a unique address, 48 bits
- 48 bit hexadecimal value, e.g. 11:22:33:AA:BB:CC
- First 3 octets assigned by IEEE to a manufacturer, 4RF USA, Inc.
- Last 3 octets assigned by vendor, together they form a full MAC
- Devices connected to each other using a shared media is referred to as a LAN
- Hubs -many ports used to connect NICs
- Bridges-two interfaces used to interconnect hubs
- Switches-think of it as a multi-port bridge
- CSMA/CD- Carrier Sense Multiple Access/Collision Detection wait & listen, used in half duplex
- Traffic Types-
    - Unicast- one MAC address sends to one other MAC address
    - Broadcast-one MAC address sends to all MAC addresses
    - Multicast- one MAC address sends to specific group of MAC addresses
- VLAN (Virtual Local Area network) , used to logically partition a single physical switch into multiple virtual switches. Each VLAN is a unique & isolated broadcast domain. These are often used to isolate SCADA traffic from enterprise traffic on a single radio channel.
- Spanning Tree Protocol (STP) Network loops are required for redundancy, unintended loops will cause network to crash. STP is a means to prevent this by injecting special broadcast frames and listening on other ports for them, and blocks interfaces until the loop error is corrected.

Network Layer 3

-IP (the Internet)

-Logical addressing

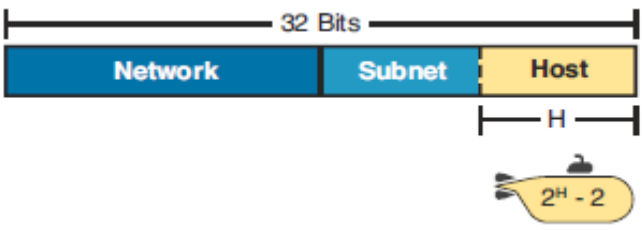
IP Address types-

Unicast- One -one communications, a single IP enabled host

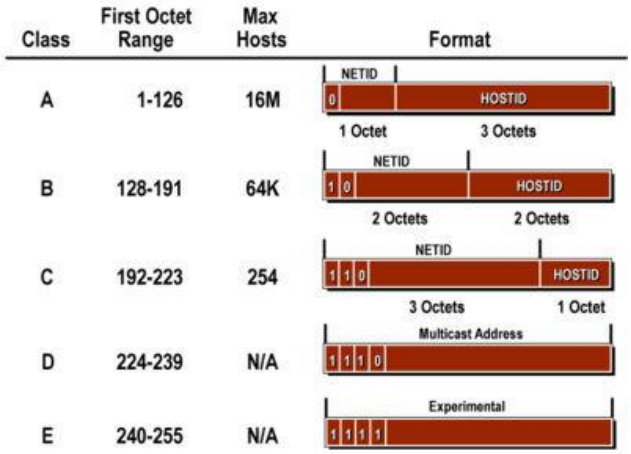
Broadcast – One – All IP addresses communications

Multicast- One- Many IP addresses, specific group of IPs

- IPv4 addressing – 32 bit address
    - IP address format: 169.254.50.10
    - Subnet mask: 255.255.255.0
    - Classless Inter-Domain Routing (CIDR), is displayed as /X, where X is the number of masked bits, 255.255.255.0=/24
    - Defined by the classful network
    - Subnet is a subset of a larger network
    - Host Area – addresses assigned to end devices



- IPv4 Address Classes



- Router- is a layer 3 device that can rout IP addresses between different networks (LANs). Routers are often manageable and can be configured remotely. Many types of radio systems have switching, and routing capabilities built in the radios.
- Time To Live (TTL) a programmed amount of time a packet can remain looping in a network
- Address Resolution Protocol (ARP) a means to dynamically discover the MAC address of a device unknown to the host.
- WAN (Wide Area Network)- circuits used to connect networks geographically separated. These can be leased lines, MPLS, VSAT, cellular, microwave, point-multipoint radio networks.
- FAN (Field Area Network)- typically a field of EFM or SCADA devices connected to a radio network.

Transport Layer 4

-End-End Communications & connectivity protocols

-Transmission Control Protocol (TCP)- is a connection oriented protocol which provides reliable communications between application services. There is a handshaking process (acknowledgement) between the source port and destination port for assured segment delivery, also with explicit connection termination. TCP is often used when a polling host needs to be assured the data is received by the end device, in perfect data packets.

- User Datagram Protocol (UDP) - is a connectionless protocol, with no sequencing of segments, no reliability provided (usually done by host polling software, such as Modbus or BSAP using CRC error checking or retries in polling). It is faster and takes up less bandwidth than TCP.

- Network Address Translation (NAT) - is a method to convert one IP address to another. It was created to deal with the shortage of public IP addresses in IPv4. Often used as a security feature to have a public IP address on the Internet connected to a router that uses NATing to change the IP addressing into a private corporate network block of IP addresses.

-Quality of Service (QoS)- used to differentiate between types of data across the network. Has a queuing mechanism to prioritize data types, assures adequate bandwidth for various types of data. Used in SCADA & EFM networks to assure critical data, such as SCADA gets a higher priority, with enough bandwidth to always get transmitted, with other data types, such as diagnostics and firmware updates having a lower priority level and bandwidth reservation. QoS can be a logical port setting or a physical port on a device, such as a radio.

Application Layer 7

-HTTP, TFTP, FTP, NTP, TELNET, SNMP, Etc

-Network Time protocol (NTP) is a service used to synchronize clocks across many devices. A GPS receiver is often used as the source. This is needed to accurately date and time stamp events or diagnostic results.

-TELNET – this provides remote access to console function in devices, also used to test other port connectivity.

-Simple Network Management Protocol (SNMP) – a protocol standard used in most networks to do troubleshooting and run diagnostics on remote network nodes. Common vendor applications are HP Openview, Solar Winds, Megasys, etc.

Some Advantages of IP Networking for the Field Technician

-it is easy to mix different types of meters in the same radio network

-It is easy to mix a host using a polling protocol with another host using a report by exception (cry out) protocol.

-it is easy for the enterprise to access the field data from meters.

-QoS allows the prioritization of data types and bandwidth allocation.

-Better diagnostics tools combined with remote management capabilities enable field technicians to diagnose problems remotely, saving time, money and outage minutes.