Networking 101

Connectware™

- **What is a Network?**
- **Ethernet**
- **TCP/IP Suite**
- **Address Types**

What is a Network?

A network is defined as a collection of devices connected together. PCs or computers connected at the office with a printer or two using Ethernet. Phones all over the world connected together by giant telephone network infrastructures, otherwise known as the Public Switched Telephone Network (PSTN). The Internet. PLCs, valves and controllers connected to a computer using an RS-485 cable.

They all share the common attribute of connecting a collection of devices together. Networks are commonly categorized according to the size or range within which they connect devices. The four most common categories are:

A ***Local Area Network***, or LAN, is used in an office, a building, or even a campus and is typically a very high speed network (10-1000 Mbps). The technology used most often is Ethernet.

A ***Wide Area Network***, or WAN, describes a network that spans buildings, cities, or continents. WANs often utilize the PSTN, the Internet, or even satellite connections to communicate over large distances.

A ***Metropolitan Area Network***, or MAN, describes a network that spans a metropolitan area. Less common than LANs and WANs, these networks sometimes use wireless technologies (e.g. 900MHz, or 2.4GHz) to provide the network connectivity.

A ***Personal Area Network***, or PAN, describes a relatively new model for networking in which the range is isolated to a small area, commonly the size of a small room, or about 10 meters. This definition is useful in describing a newer technology called Bluetooth®, which provide plug-and-play wireless communications between devices as they move in and out of range of each other.

Ethernet

This is the most common networking technology used today to connect computers together in a LAN environment. Ethernet defines the physical connection used to connect computers. It defines the electrical characteristics, signaling and low-level framing of data. Protocols like TCP/IP, IPX, AppleTalk and NetBEUI can all be transmitted over Ethernet.

Ethernet runs at several speeds; the most common today is 10Mbps and 100Mbps. Just coming on the scene now is 1000Mbps, otherwise known as Gigabit Ethernet. At 10Mbps, Ethernet is 1000 times faster than a 9600bps serial line.

Ethernet is a shared medium. All devices on the network share the bandwidth. It uses a technology called Carrier Sense Multiple Access with Collision Detection (CSMA/CD). What is that? Well, it works something like a very polite crowd of people at a party. Everyone is allowed to speak at any time (that's Multiple Access) except of course when someone else is already speaking (that would be a collision). Not wanting to interrupt another speaker, each person listens carefully to ensure no one else is speaking when beginning to speak (this is Carrier Sense – sensing whether someone is already talking). The speaker continues listening even while speaking to see if somebody else starts speaking at the same time (this would be Collision Detection). Upon detection of a collision, both parties back off, or stop speaking and wait for some random period of time before again attempting to speak.

TCP/IP Suite

TCP/IP – Transmission Control Protocol/Internet Protocol

TCP/IP is a protocol (or language) used for networking. It has become the international language of networking – the language of the Internet. TCP/IP is a more than a protocol because it actually defines a collection of protocols. TCP, UDP, ICMP, ARP and several others are part of the collection.

TCP – Transmission Control Protocol

TCP is the most reliable data transfer protocol. It guarantees that all data being sent is received and is received in the correct order. It does this by requiring all transferred data to be acknowledged using sequence numbers. If the data is not acknowledged within a timeout period, the data is retransmitted.

Another way of describing TCP is the "telephone call protocol." As in a telephone call, one device initiates the connection (effectively dials another device). The receiving device gets the equivalent of a "ring", answers the call, and they begin speaking. All data sent by one device is guaranteed to be received in order on the other end, much like the way you know your spoken words won't be jumbled around at the receiver's end of the call.

UDP – User Datagram Protocol

UDP is the unreliable data transfer protocol. No guarantees, no retransmission, and data packets can arrive out of order. UDP, or User Datagram Protocol, is used to send a packet of information to another device on the network. Because acknowledgements are not required, UDP has much less overhead than TCP and is sometimes thought of as being the more streamlined "faster" cousin of TCP.

UDP operates much like standard mail service. Letters sent don't always make it in the same order sent, and sometimes don't make it at all. But, if you have to contact a very large number of others, it's much more efficient that calling each one on the phone (e.g. initiating a TCP session).

ICMP – Internet Control Message Protocol

ICMP supports packets containing control, error and informational messages. Packet InterNet Groper (PING) is a well known TCP/IP utility that uses ICMP. PING is used to test a network connection and validate that a device is actually present on the network. Often the first test used to determine whether a device is on the network is to attempt to ping it.

Address Types

ARP – Address Resolution Protocol

Another protocol in the TCP/IP suite used to map IP addresses to Ethernet hardware addresses, otherwise known as MAC addresses.

IP Address – Phone numbers of the Internet

IP addresses are designed much like phone numbers. When you see a number like 192.168.1.34, what does that mean?

Before breaking that down, let's take a look at phone numbers, because they are surprisingly similar. In the U.S., 10-digit phone numbers are the norm. The first three digits are called the Area Code. Telephone companies have defined area codes to map to regions. For example, the area code 612 represents Minneapolis, Minnesota, and surrounding areas. The final seven digits of the phone number define the exact phone line within that area code.

IP addresses follow a similar scheme. There is a network portion of the IP address which is functionally equivalent to the Area Code in a phone number, sometimes called the Network ID. There is also another portion that maps nicely to the seven-digit phone number, the Host ID. The Network ID indicates the specific network on which an address resides and the Host ID identifies the specific host or device on that network.

Getting back to that IP address above, 192.168.1.34, how is it broken down? Well, IP addresses are always accompanied by something called the Sub network Mask. This mask identifies which part of the address defines the Network ID and the Host ID. Ones in the mask represent the IP address bits that represent the Network ID. Zeros in the mask indicate which bits represent the Host ID. Assuming the Sub network Mask is 255.255.255.0, the Network ID would be 192.168.1.x. The Host ID would be 34.

MAC Address – Social Security Number for Network Devices

While a MAC address doesn't provide any retirement benefits for networked devices, it does provide a guaranteed unique identifier for every device on a network.

Have you ever looked someone up using their Social Security Number? It is unique to that person and uniquely identifies them. But it doesn't provide any actual routing information to allow you to find that person.

MAC, or Media Access Control, is a layer defined by the Ethernet standard and is independent of a protocol like TCP/IP. Ethernet defines its own addressing scheme, and that scheme is much like the Social Security model in the U.S. Every Ethernet device is assigned a guaranteed unique identifier when it is first built and often that number cannot be changed.