Communications and Protocol Basics

Chris M. Finen, P.E. – Senior Application Engineer
Eaton Corporation - Nashville
(615)333-5479
chrismfinen@eaton.com

Communication Basics - Agenda

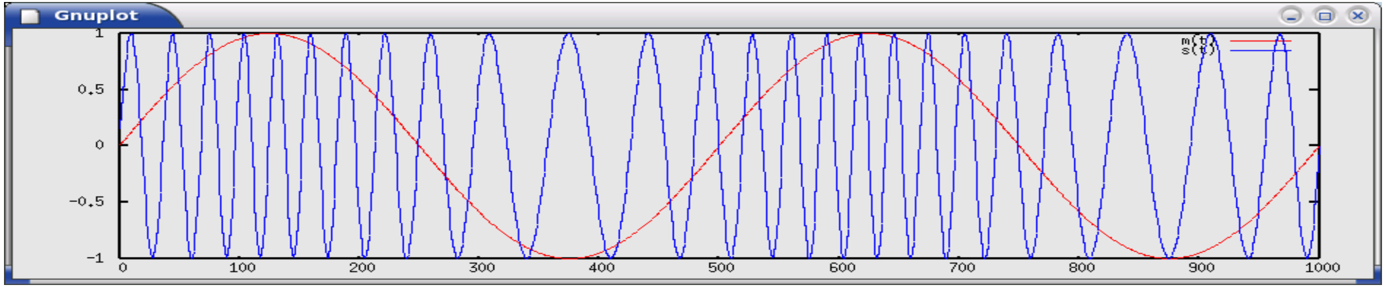
- Transmission Types
- Physical Media
- Communication Networks
- Ethernet Basics
- Protocols
- IoT

Analog Communication

- Analog signals are signals with continuous values in both time and magnitude.
- Any information may be conveyed by an analog signal, often such a signal is a measured response to changes in physical phenomena, such as sound, light, temperature, position or pressure and is achieved using a transducer
- For example, in an analog sound recording, the variation in pressure of a sound striking a microphone creates a corresponding variation in the voltage amplitude of a current passing through it. An increase in the volume of the sound causes the fluctuation of the current's voltage amplitude to increase while keeping the same rhythm.

Analog Communications

- An example of analog signals.

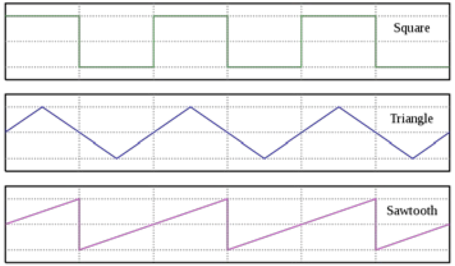


- Analog signals are signals with continuous values in both time and magnitude.
- Any information may be conveyed by an analog signal, often such a signal is a measured response to changes in physical phenomena, such as sound, light, temperature, position or pressure and is achieved using a transducer

Digital Communication

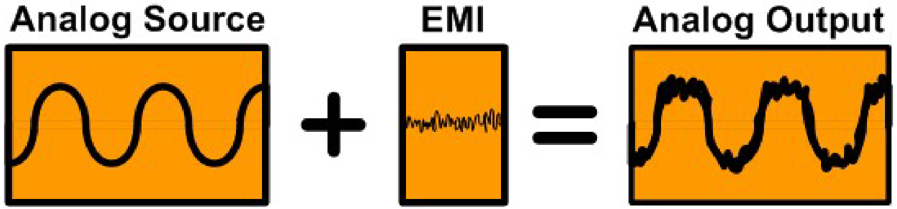
- Digital signals are a series of signals that are in one of two possible states
- Typically represented by binary numbers, "1" or "0".
- Typically the 1 is designated by a higher voltage (ex. 5Vdc) and the 0 as a lower voltage (ex. 0vdc) on a carrier line.

- Example of a digital signals



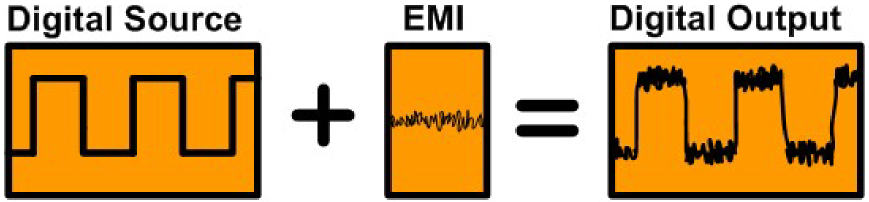
Analog versus Digital Communication

- Analog systems are:
  - less tolerant of noise (interference)
  - make good use of bandwidth
  - are easy to manipulate mathematically
  - require hardware receivers and transmitters that are designed to perfectly fit the particular transmission.
    - If you are working on a new system, and you decide to change your analog signal, you may need to completely change your transmitters and receivers



Analog versus Digital Communication

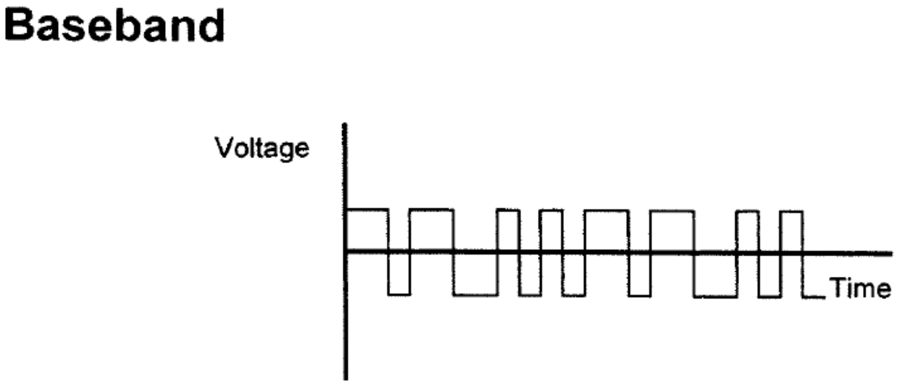
- Digital systems are:
  - more tolerant of noise, but digital signals can be completely corrupted in the presence of excess noise
    - In digital signals, noise could cause a 1 to be interpreted as a 0 and vice versa, which makes the received data different than the original data.
  - more standardized and flexible
    - The primary benefit of digital signals is that they can be handled by simple, standardized receivers and transmitters, and the signal can be then dealt with in firmware / software(which is comparatively cheap to change).



Analog versus Digital Communication – Mobile Phones

- Cellular Communication Generations
  - 1G – Analog
  - 2G – Digital
  - 3G – Mobile Broadband - Digital w/ Security
  - 4G – IP based - Digital w/ Security - 10x faster than 3G
    - 6 GHz frequency band
  - 5G – IP based - Digital w/ Security - 10-20x faster than 4G
    - Much higher frequencies (30-300GHz)
    - Smaller antennas…but more needed

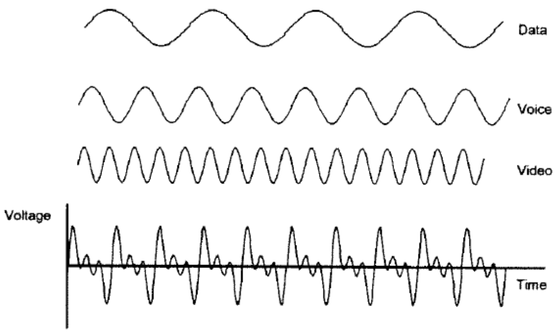
Transmission Types



- Baseband is communication of a single frequency on a dedicated physical media
- Most digital communication is baseband
    - 10Base – T
    - 100Base - T

Transmission Types

Broadband



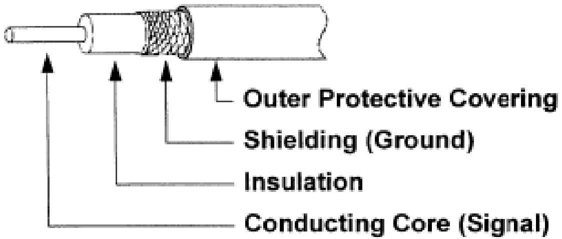
- Broadband is the communication of multiple data streams using a range of frequencies on a shared physical media.
- Multiple data streams are placed in the signal and then decoded on the other end
    - Ex. cable TV, internet, phone, security all on a single coaxial cable connection)

Transmission Types

- Bandwidth
  - a measurement of the bit-rate of available communication resources
  - expressed in bits per second (bps) or multiples of it (bps, kbps, Mbps, Gbps, etc.)
    - Baud = bits per second (bps)
  - Network bandwidth is measure the maximum throughput of a computer network

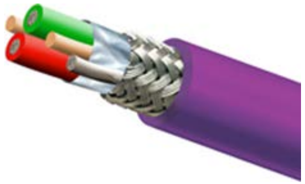
How do you transmit the 1 and 0s?

Coaxial Cable



Advantages	Disadvantages
High Data Rates	Moderately expensive
Long Distances	Easily Tapped (low security)
	Difficult to install (compared with twisted pairs)

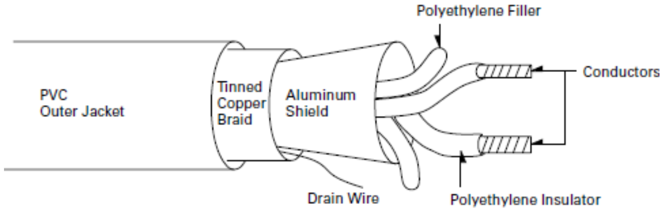
Industrial Communication Network Example: Profibus DP

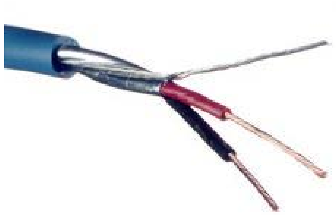


How do you transmit the 1 and 0s?

Twisted Pair Wire

Twisting of the wires make the wire less susceptible to outside interference. Shielded twisted pairs include a grounding shield around the pair that make the cabling go for longer distance at higher data rates.

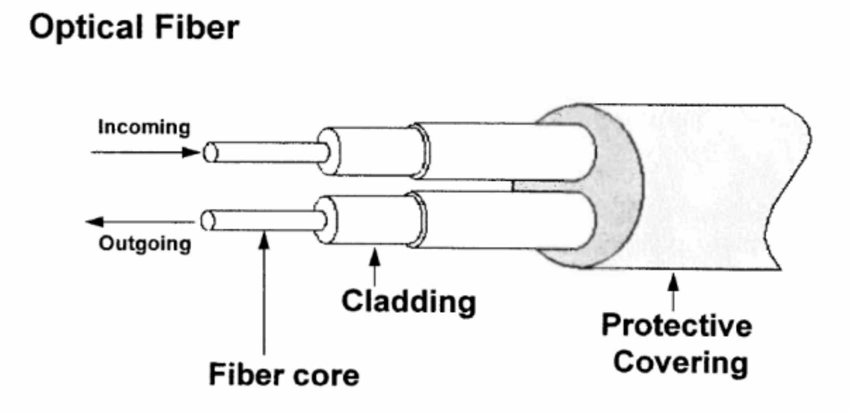




Advantages	Disadvantages
Inexpensive	Limits on distance and data rates
Easy to install	Easily Tapped (low security)

Industrial Communication Network Examples: Modbus RTU, INCOM

How do you transmit the 1 and 0s?



Advantages

Immune to electrical interference

Very high data rates

Difficult to tap without being detected

Disadvantages

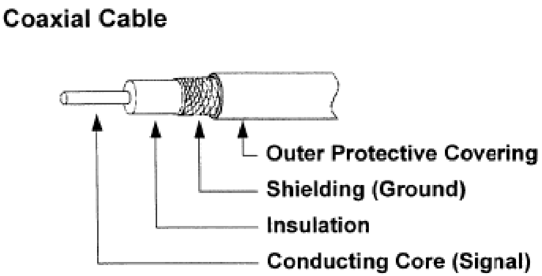
Expensive cabling

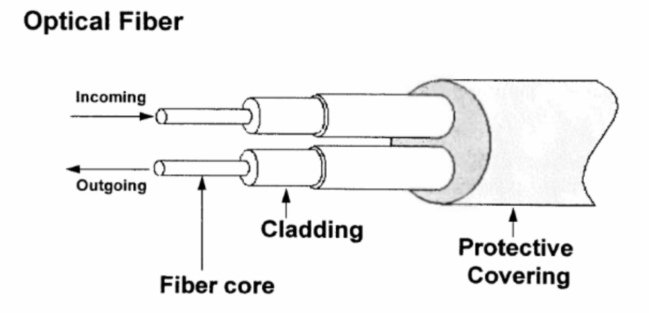
Expensive interface equipment

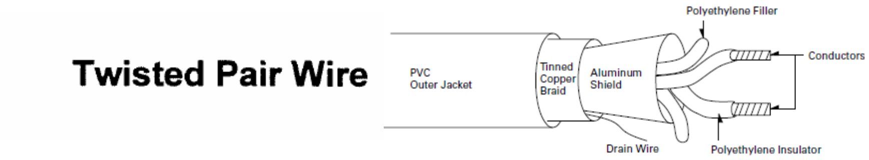
Powering Business Worldwide

How do you transmit the 1 and 0s?

- These items are simply the physical medium for the data to flow.







Communication Networks

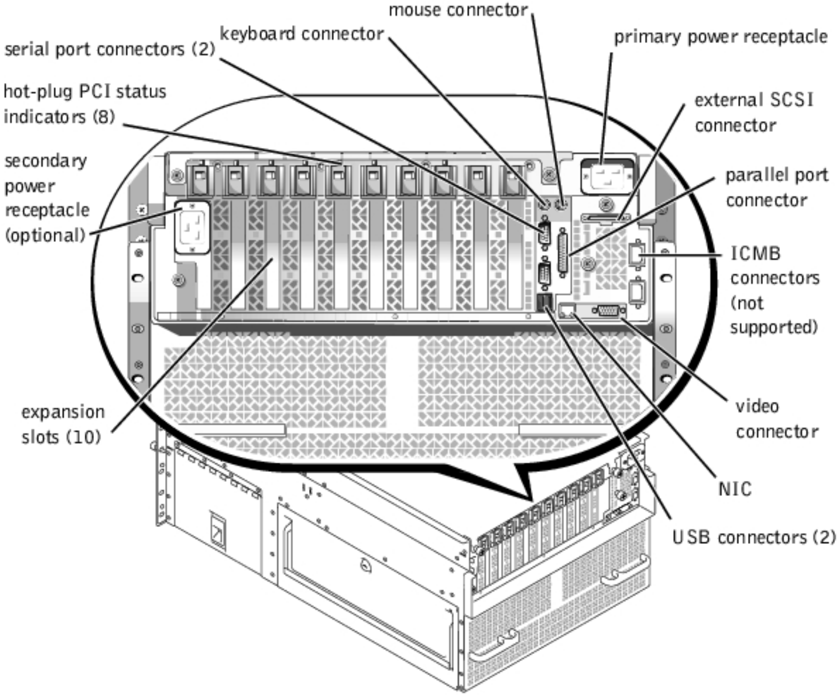
- “Serial Networks”
  - RS-232
  - RS-422
  - RS-485
- Ethernet Networks
  - Copper
  - Fiber
  - Wireless

Communication Networks – RS232

- **RS-232** is a standard for serial binary single-ended data and control signals it is commonly used in computer serial ports.
- This **connects two devices together** at one time. No more. No less.
- The RS-232 standard defines the voltage levels that correspond to logical one and logical zero levels for the data transmission and the control signal lines. Valid signals are plus or minus +/- 3 volts.
- Examples: Hardwired keyboard to computer connection, Protective relay to laptop, etc.
- Network length is limited to about 25 feet max.

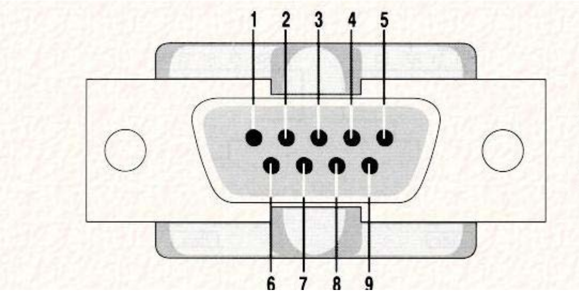
Communication Networks – RS232

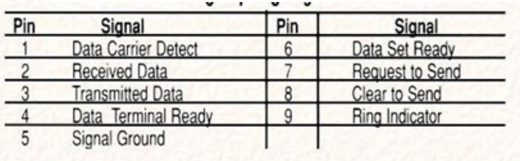
- **Serial connectors on the back of PCs communicate via RS-232**



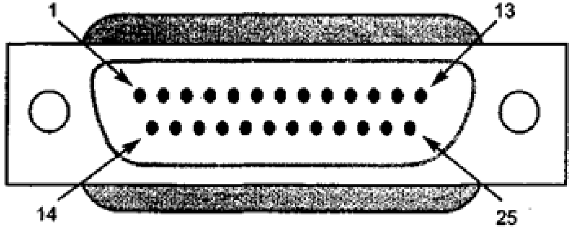
Communication Networks – RS232

- You often hear about a 9 pin (DB9) or 25 pin (DB25) connector in RS232 networks.



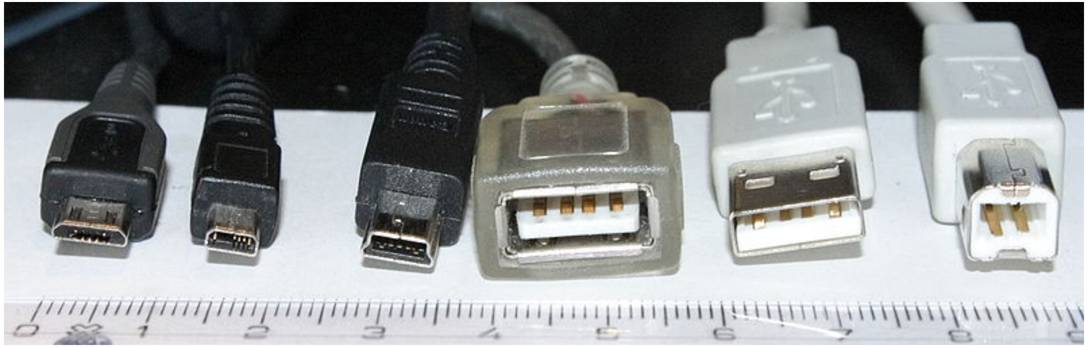


Pin	Signal	Pin	Signal
1	Data Carrier Detect	6	Data Set Ready
2	Received Data	7	Request to Send
3	Transmitted Data	8	Clear to Send
4	Data Terminal Ready	9	Ring Indicator
5	Signal Ground		



Communication Wiring – RS232->USB

- A USB connector has replaced the traditional pin out connectors serial ports on computers.
- Compared with RS-232, USB is faster, uses lower voltages, and has connectors that are simpler to connect and use. Both standards have software support in popular operating systems. USB is more complex than the RS-232 standard because it includes a protocol for transferring data to devices. This requires more software to support the protocol used. RS-232 only standardizes the voltage of signals and the functions of the physical interface pins.
- Still only connects two devices together. (Unless a multi-port USB adapter is used.)
- Network length is limited to about 25 feet max.

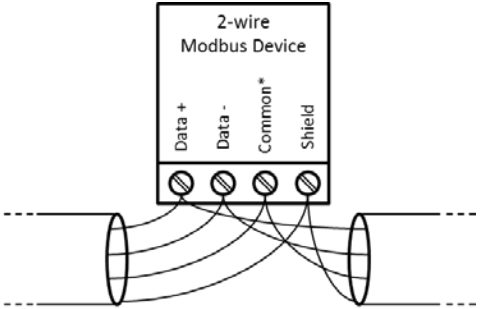


Communication Networks – RS485

- EIA-485 (also known as RS485) only specifies electrical characteristics of the driver and the receiver. It does not specify or recommend any data protocol.
- There is typically one master device and several "slaves" devices in this topology. Up to 32 devices max.
- Network speed (baud rate) is typically 9.8k – 57.4kbps
- Networks length can be up to 4000ft (1200m)

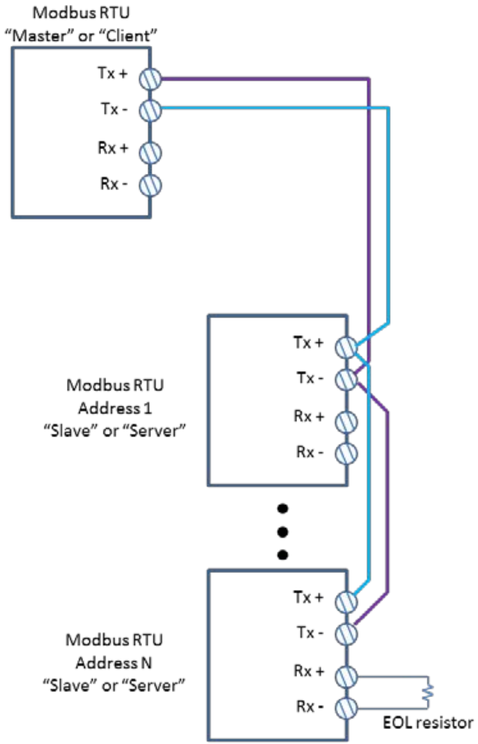
Communication Networks - RS-485

- Multiple receivers may be connected to such a network in a linear, multi-drop configuration. These characteristics make such networks useful in industrial environments and similar applications. This is also known as daisy chain communications



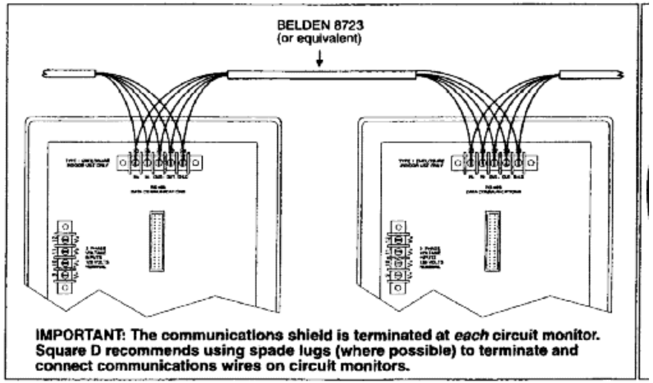
* Required per RS-485 spec, but frequently not provided or the Common and Shield are combined

2-Wire RS-485 (With Devices that support 2 or 4W



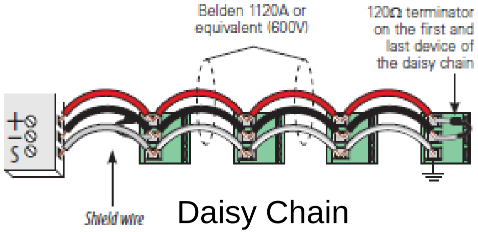
Communication Networks – RS485

Can ONLY use simple daisy-chain topology



IMPORTANT: The communications shield is terminated at *each* circuit monitor. Square D recommends using spade lugs (where possible) to terminate and connect communications wires on circuit monitors.

Figure 5-11: CORRECT circuit monitor communications wiring



Daisy Chain

Other wiring topologies are not allowed

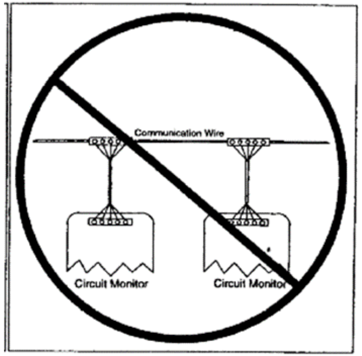
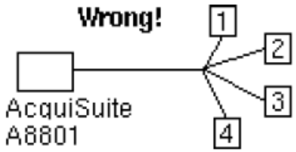


Figure 5-12: INCORRECT circuit monitor communications wiring

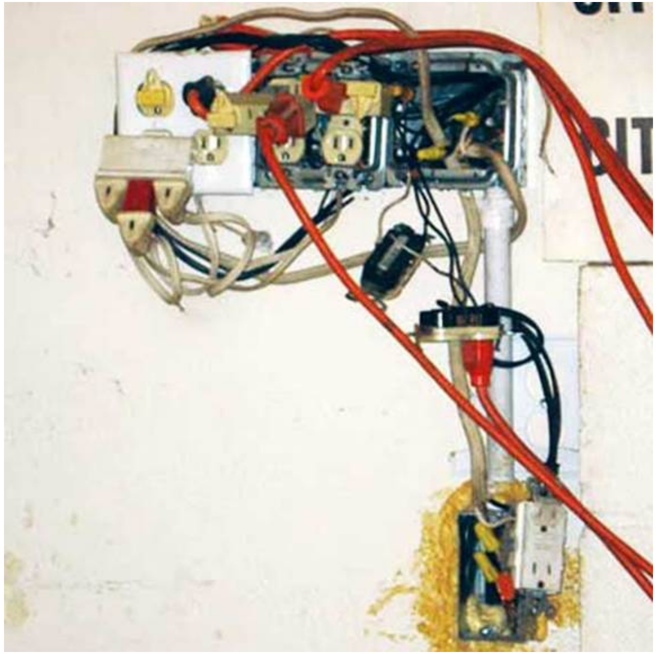
Trunk and Drop Topology



Simple Star Topology

Networking “Rules”

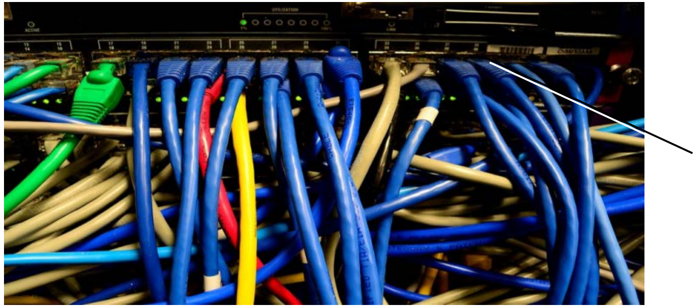
- It is imperative that you follow the strict network rules associated with the given communication network



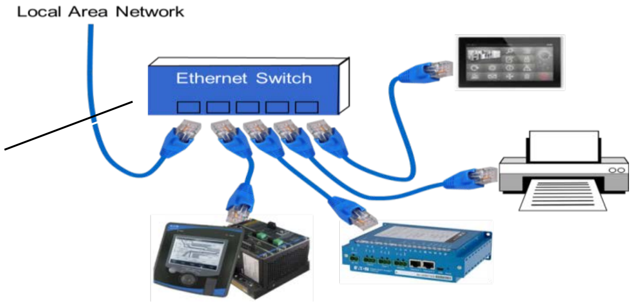
Networking “Rules”

- Improvising is not the answer

Communication Networks - Ethernet

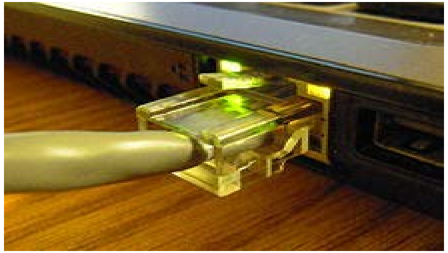


Ethernet Switch



- Invented at Xerox in 1970s. 1983 IEEE 802.3 released
- Allows devices to talk to each other rather than just master<->slave (peer-to-peer) (multiple “masters”)
- 10Mbps (10BASE-T), 100 Mbps (100BASE-TX), and 1000 Mbps (1 Gbps) (1000BASE-T)
- T = “twisted pair”
- “T” systems are point-to-point. No daisy-chaining of Ethernet.
- Multipoint connections supported with “switches”

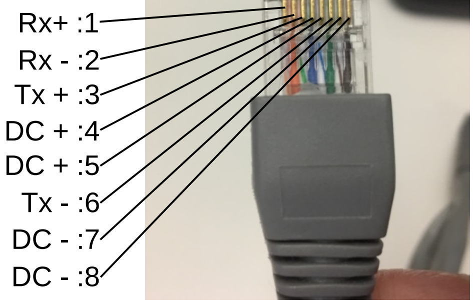
Ethernet - What is important to know?



RJ45 connector on CAT 5 cable

RJ-45 Pinout

10/100 PoE mode B



Rx+ :1

Rx - :2

Tx + :3

DC + :4

DC + :5

Tx - :6

DC - :7

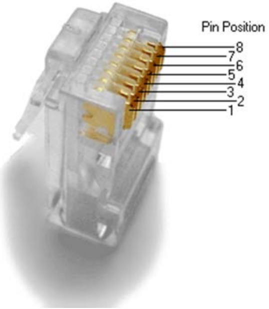
DC - :8

- 8-conductor (4 twisted pairs)
  - 10/100BASE-T(X) (2 pair)
  - 1000BASE-T (all 4 pair)
- 300V rated

- Copper can have maximum effective length of 100 meters (328 feet), regardless of speed
  - CAT 5, 5e good for up to 1000BASE-T, 6 → 10 Gig
  - 5 → 5e: tighter twist, 5e → 6: barrier between T & R
  - Keep away from power (Standard - 300V insulated Ethernet cable)
    - Ethernet uses no more than +/- 2.5 vdc to communicate

Copper – Ethernet

- Ethernet Cable Types

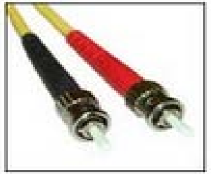


RJ45 connector

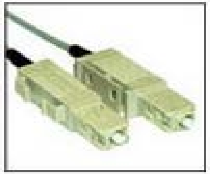
	Cable Type	Maximum Data Transmission Speed	Maximum Bandwidth
Category 3	UTP	10 Mbps	16 MHz
Category 5	UTP	10/100 Mbps	100 MHz
Category 5 e	UTP	1000 Mbps	100 MHz
Category 6	UTP or STP	1000 Mbps	250 MHz
Category 6 a	STP	10,000 Mbps	500 MHz
Category 7	SSTP	10,000 Mbps	600 MHz

Fiber Optic - Ethernet

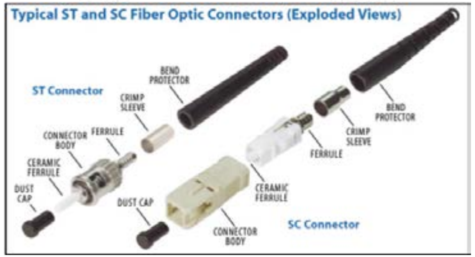
- Fiber Optic (noise immunity, longer distance)
  - **Multi-mode** to 2000 meters (6560 feet) plastic fiber (cheaper)
  - **Single-mode** to ~20-30 km (12.4 – 18.6 miles)

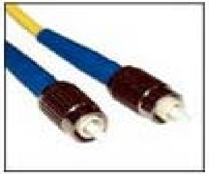


ST

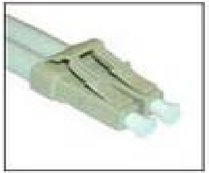


SC





FC

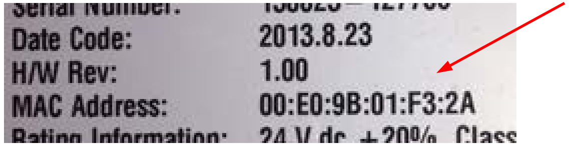


LC

NOTE: Pay attention to connector, switch, and fiber – they must be compatible

Ethernet - What is important to know?

- Ethernet devices all have a *unique* 48-bit address called a **Media Access Control** (MAC) address

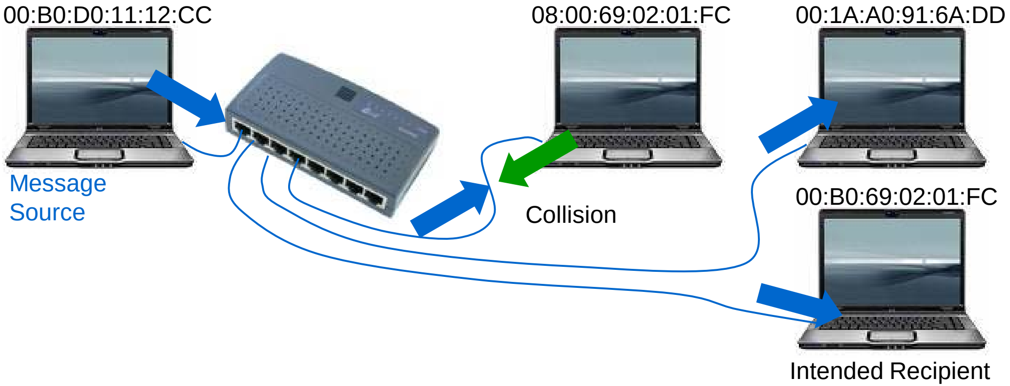


Serial Number:	[illegible]
Date Code:	2013.8.23
H/W Rev:	1.00
MAC Address:	00:E0:9B:01:F3:2A
Rating Information:	24 V dc ±20% Class

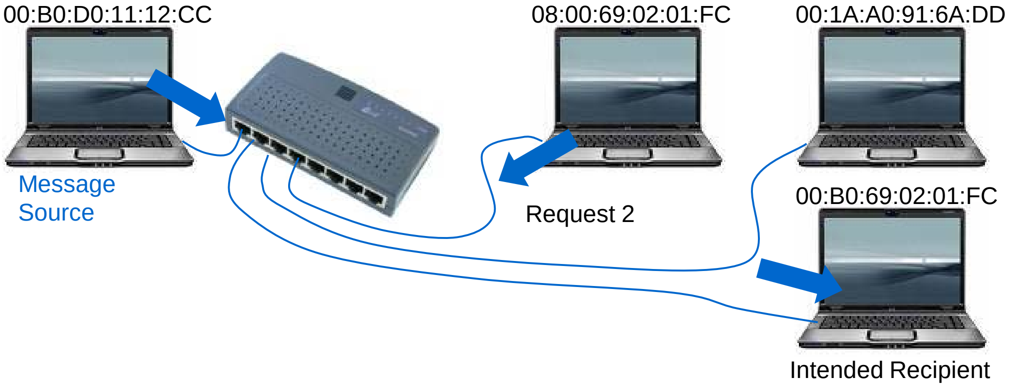
- 48-bits supports 281 474 976 710 656 unique addresses!
  - Blocks of addresses assigned to Ethernet hardware ***vendors*** by the IEEE
- This is like the specific communication chip’s DNA
  - NOTE: This is different than an “IP” address

Ethernet Networks

- Hub
  - Message heard by all nodes
  - Collisions possible. Requires retransmission



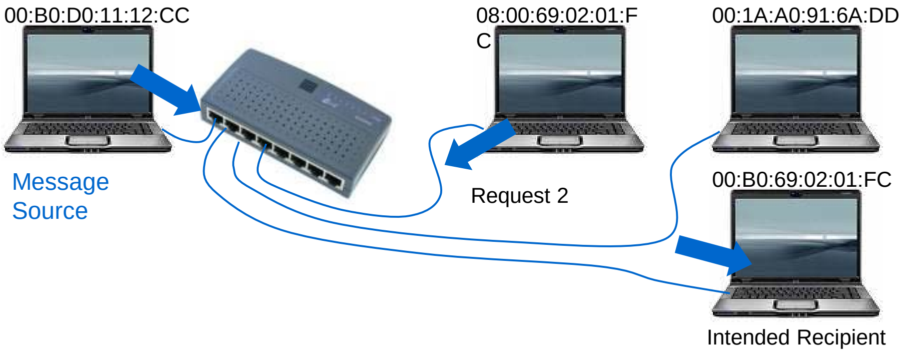
- Switch (Unmanaged)
  - Message heard by all nodes
  - Eliminate collisions
  - Store and forward messages
  - Allows mixing of different bit rates and data formats



© 2019 Eaton, All Rights Reserved

Ethernet Networks

- Managed Switch
  - Messages can be examined to do different things based on what is seen
  - Can prioritize messages
  - Messages can be sent to specific recipients
  - Can segment or reroute messages for redundant loop topologies
  - Managed switches have their own unique address on the network



00:B0:D0:11:12:CC

Message Source

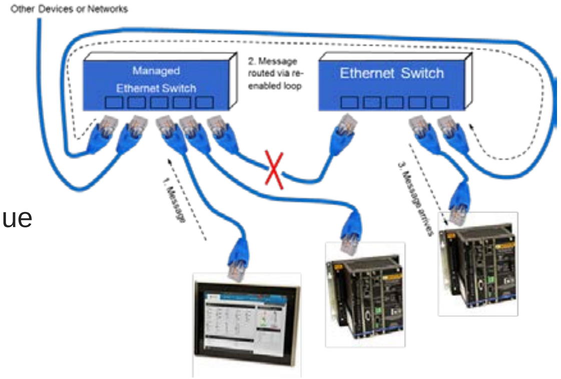
08:00:69:02:01:FC

Request 2

00:1A:A0:91:6A:DD

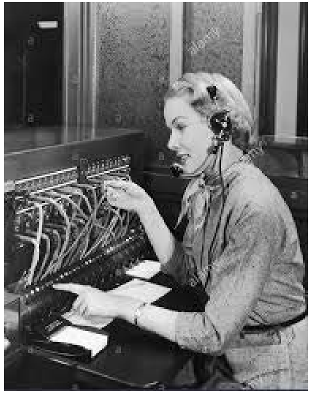
00:B0:69:02:01:FC

Intended Recipient



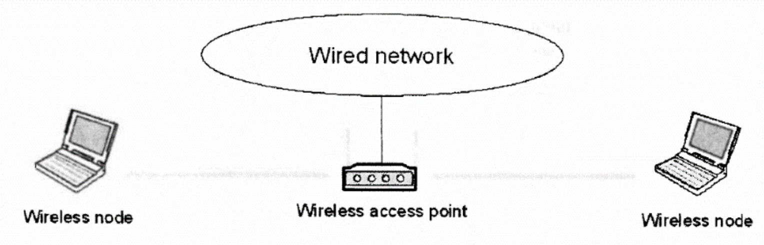
Looped Ethernet network

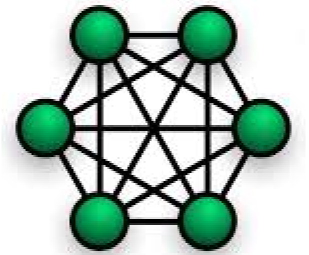
=



Communication Methods - Wireless

- IEEE 802.11 is a set of standards for wireless communication between devices.
- Wireless devices can communicate directly with each other without a physical connection.





Wireless Mesh Network

IEEE 802.1	Local Area Network (LAN) Bridging
IEEE 802.3	Ethernet standards
IEEE 802.11	Wireless LAN (Wi-Fi, including meshed networks)
IEEE 802.15	Wireless Personal Area Network (PAN)(includes Bluetooth, ZigBee, etc.)

Communication Network Methods

- Remember that RS-232, RS-485, Ethernet, and Wireless are network methods and standards for how the devices connect and communicate 1’s and 0’s only.
- They do not define the communication protocol or “language” that is “spoken”.

Communication Protocols

- INCOM
- Modbus RTU
- DNP3
- DeviceNet
- Profibus
- BacNet
- Lonworks

Shielded Twisted Pair Networks

- Modbus TCP
- ProfiNet
- BacNet IP
- Ethernet/IP
- EtherCAT
- TCP/IP

Ethernet-Based Networks

Powering Business Worldwide

Communication Protocols

- Protocol is the specific “language” that is being communicated over the wiring method.
- Examples:

Wiring Method	Protocol
RS-485	Modbus RTU
Ethernet	Modbus TCP
Wireless	TCP/IP

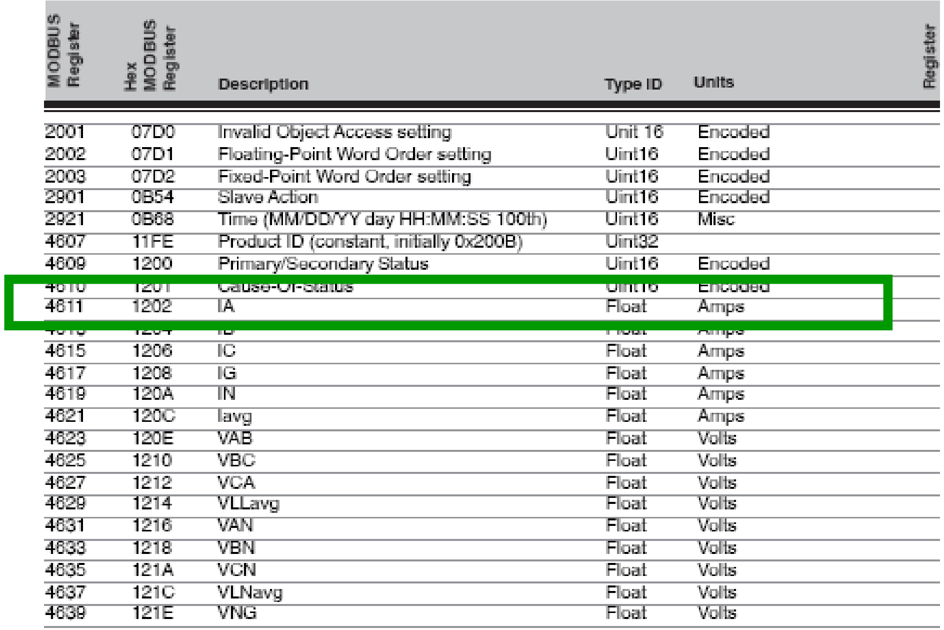
“Ethernet is not a protocol!”

Communication Protocols - Modbus

- **Modbus** is a serial communications protocol published by Modicon in 1979 for use with its programmable logic controllers (PLCs).
- It has become a standard communications protocol in industry, and is now the most commonly available means of connecting industrial electronic devices.
- Suppliers large and small, system integrators, end users, open source developers, educators and other interested parties can become Modbus members.
- Most widely used industrial communication protocol in the world
- The main reasons for the extensive use of Modbus over other communications protocols are:
  - It is openly published and royalty-free
  - Relatively easy industrial network to deploy
  - It moves raw bits or words without placing many restrictions on vendors
  - However, flexibility means lack of standardization

Communication Protocols - Modbus

- Each piece of data in a device is set up as a “packet”
- A modbus master (PC, PLC, etc.) can be set up to reach out to the device on it’s network and grab a certain packet of data.
- A **modbus map** is required to know how to interpret the data that is returned



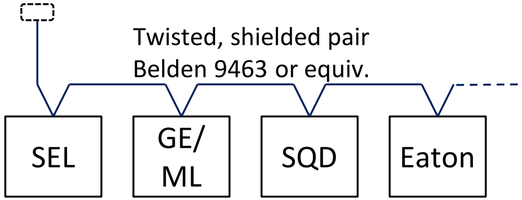
MODBUS Register	Hex MODBUS Register	Description	Type ID	Units	Register
2001	07D0	Invalid Object Access setting	Unit 16	Encoded	
2002	07D1	Floating-Point Word Order setting	Uint16	Encoded	
2003	07D2	Fixed-Point Word Order setting	Uint16	Encoded	
2901	0B54	Slave Action	Uint16	Encoded	
2921	0B68	Time (MM/DD/YY day HH:MM:SS 100th)	Uint16	Misc	
4607	11FE	Product ID (constant, initially 0x200B)	Uint32		
4609	1200	Primary/Secondary Status	Uint16	Encoded	
4610	1201	Cause-Of-Status	Uint16	Encoded	
4611	1202	IA	Float	Amps	
4613	1204	IB	Float	Amps	
4615	1206	IC	Float	Amps	
4617	1208	IG	Float	Amps	
4619	120A	IN	Float	Amps	
4621	120C	Iavg	Float	Amps	
4623	120E	VAB	Float	Volts	
4625	1210	VBC	Float	Volts	
4627	1212	VCA	Float	Volts	
4629	1214	VLLavg	Float	Volts	
4631	1216	VAN	Float	Volts	
4633	1218	VBN	Float	Volts	
4635	121A	VCN	Float	Volts	
4637	121C	VLNavg	Float	Volts	
4639	121E	VNG	Float	Volts	

In this case, a computer can ask for Modbus register 4611 which is the data packet that contains current in phase A.

Communication Protocols – Modbus

Devices and External **Serial** Protocols **The Same**

Connection to External Network or Device (ex. PLC, SCADA, BMS, Operator Interface)



Example Protocol:

- Modbus RTU
- DNP3 serial

Devices and External **Serial** Protocols **Do Not Match**

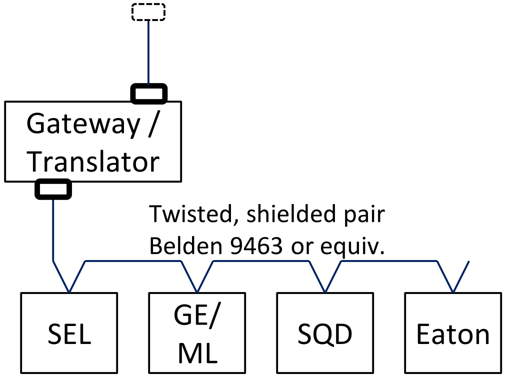
Example Protocol:

- Modbus TCP
- BACnet/IP
- EtherNet/IP
- IEC 61850

Ethernet-based Connection to External Network

Example:

- PXG900



Example Protocol:

- Modbus RTU
- DNP3 serial

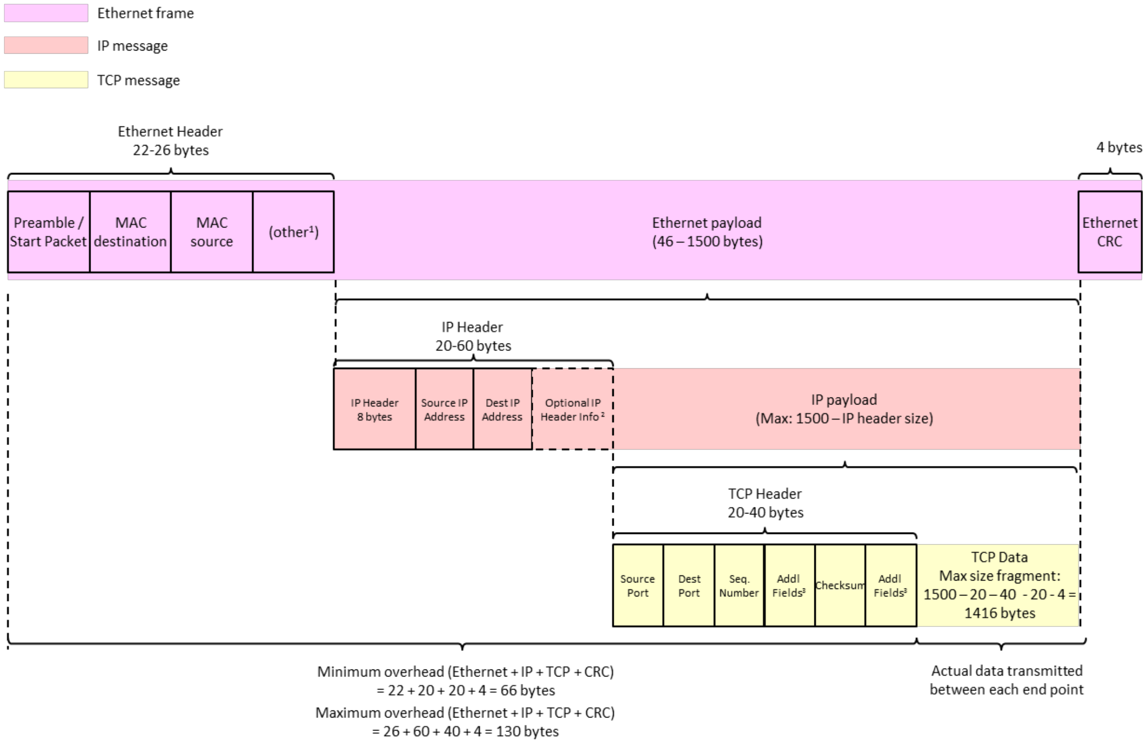
Communication Protocols – TCP/IP

- The **Internet Protocol Suite** (commonly known as **TCP/IP**) is the set of Ethernet/Wireless-based communication protocols used for the Internet and other similar networks.
- It is named from two of the most important protocols in it: the Transmission Control (TCP) and the Internet Protocol (IP), which were the first two networking protocols defined in this standard.
  - **TCP (Transmission Control Protocol):** A protocol designed to increase the reliability of the messages sent.
  - **IP (Internet Protocol):** The Internet Protocol is an agreed upon format for packaging data and sending over the Internet infrastructure.

Communication Protocols - TCP/IP

- TCP/IP protocols are transmitted over Ethernet cabling.
- You may have heard of some of the suites within TCP/IP
  - User Datagram Protocol (UDP)
  - 20/21: File Transport Protocol (FTP)
  - 25: Simple Mail Transport Protocol (SMTP)
  - 53: Domain Name System (DNS)
  - 80: Hypertext Transport Protocol (HTTP)
  - 110: Post Office Protocol 3 (POP3)
  - 123: Network Time Protocol (NTP)
  - 143: Internet Messaging Access Protocol (IMAP)
  - 161: Simple Network Management Protocol (SNMP)
  - 443: HTTP Secure (HTTPS)
  - 502: Modbus TCP

TCP/IP Message Packet



Ethernet frame

IP message

TCP message

Ethernet Header
22-26 bytes

4 bytes

Preamble / Start Packet

MAC destination

MAC source

(other[1])

Ethernet payload
(46 – 1500 bytes)

Ethernet CRC

IP Header
20-60 bytes

IP Header 8 bytes

Source IP Address

Dest IP Address

Optional IP Header Info[2]

IP payload
(Max: 1500 – IP header size)

TCP Header
20-40 bytes

Source Port

Dest Port

Seq. Number

Addl Fields[3]

Checksum

Addl Fields[3]

TCP Data
Max size fragment:
1500 – 20 – 40 - 20 - 4 =
1416 bytes

Minimum overhead (Ethernet + IP + TCP + CRC)
= 22 + 20 + 20 + 4 = 66 bytes

Maximum overhead (Ethernet + IP + TCP + CRC)
= 26 + 60 + 40 + 4 = 130 bytes

Actual data transmitted
between each end point

[1] Optional 802.1q (Quality of Service [QoS] routing information, Ethernet type or length

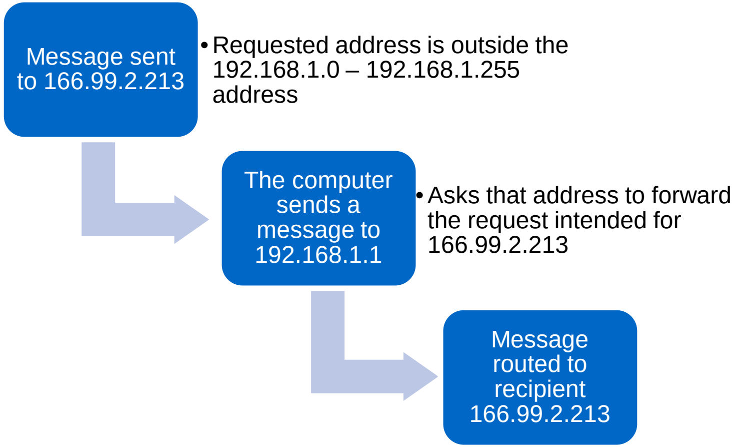
[2] Refer to https://en.wikipedia.org/wiki/IPv4#Header for more information on these infrequently used options

[3] Refer to https://en.wikipedia.org/wiki/Transmission_Control_Protocol#TCP_segment_structure for more information

Powering Business Worldwide

Communications Protocols – TCP/IP

- **IP Addresses** – Every device on any network is assigned a unique address
  - In Ethernet world, they look something like 198.168.111.255
- **Subnet Mask** – Defines what other addresses are contained within the same subnet as this device
  - 255.255.255.0
- **Gateway Address** – If a message is sent to an address outside the defined subnet, it is sent to the Gateway device to be forwarded
- Example:
  - Local computer IP address: 192.168.1.10
  - Local computer subnet mask: 255.255.255.0
  - Local computer gateway address: 192.168.1.1



Message sent to 166.99.2.213

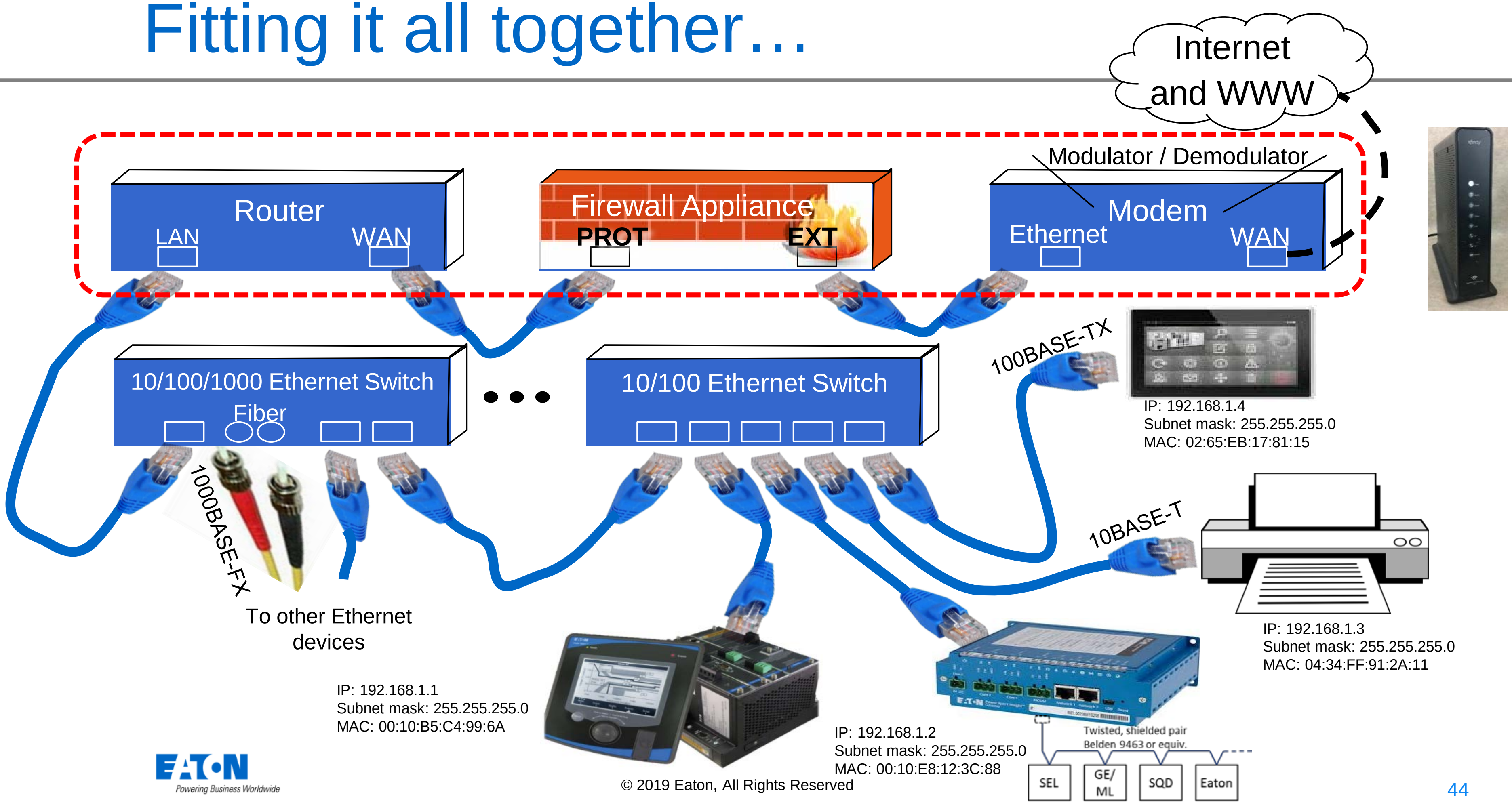
- Requested address is outside the 192.168.1.0 – 192.168.1.255 address

The computer sends a message to 192.168.1.1

- Asks that address to forward the request intended for 166.99.2.213

Message routed to recipient 166.99.2.213

Fitting it all together…



Internet and WWW

Modulator / Demodulator

Router

LAN

WAN

Firewall Appliance

PROT

EXT

Modem

Ethernet

WAN

10/100/1000 Ethernet Switch

Fiber

10/100 Ethernet Switch

100BASE-TX

10BASE-T

1000BASE-FX

To other Ethernet devices

IP: 192.168.1.4
Subnet mask: 255.255.255.0
MAC: 02:65:EB:17:81:15

IP: 192.168.1.3
Subnet mask: 255.255.255.0
MAC: 04:34:FF:91:2A:11

IP: 192.168.1.1
Subnet mask: 255.255.255.0
MAC: 00:10:B5:C4:99:6A

IP: 192.168.1.2
Subnet mask: 255.255.255.0
MAC: 00:10:E8:12:3C:88

Twisted, shielded pair
Belden 9463 or equiv.

SEL

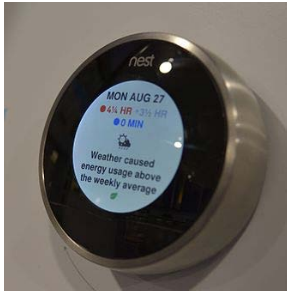
GE/ ML

SQD

Eaton

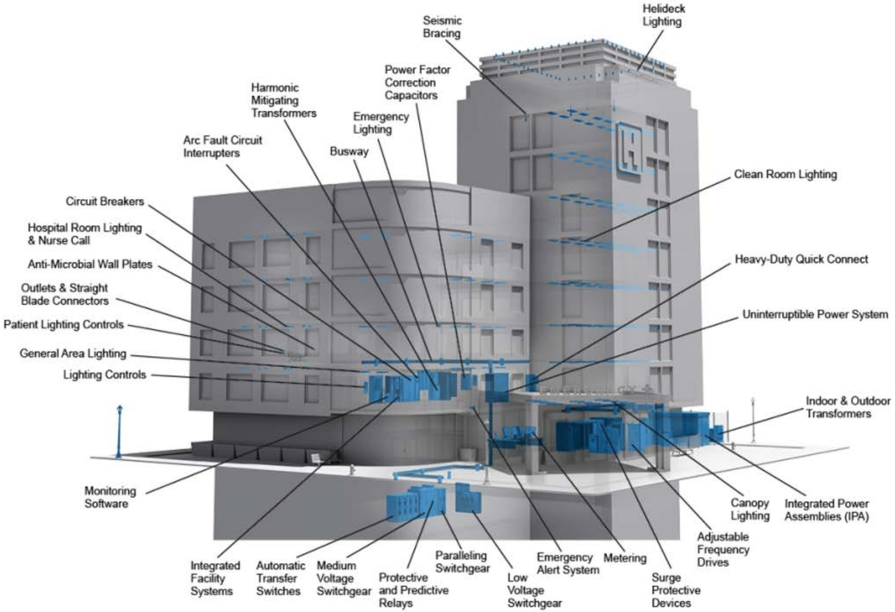
IoT (Internet of Things)

- Broadly it is the interconnection of “things” (devices) to the Internet as opposed to people connecting to the Internet.
- This IoT connectivity has now extended beyond traditional computers, smartphones, etc. to cover a vast array of
  - Sensors
  - Actuators
  - Cameras
  - Lights
  - Etc.
- Interconnectivity of devices allows data exchange and interaction to accomplish tasks, improve productivity, etc.

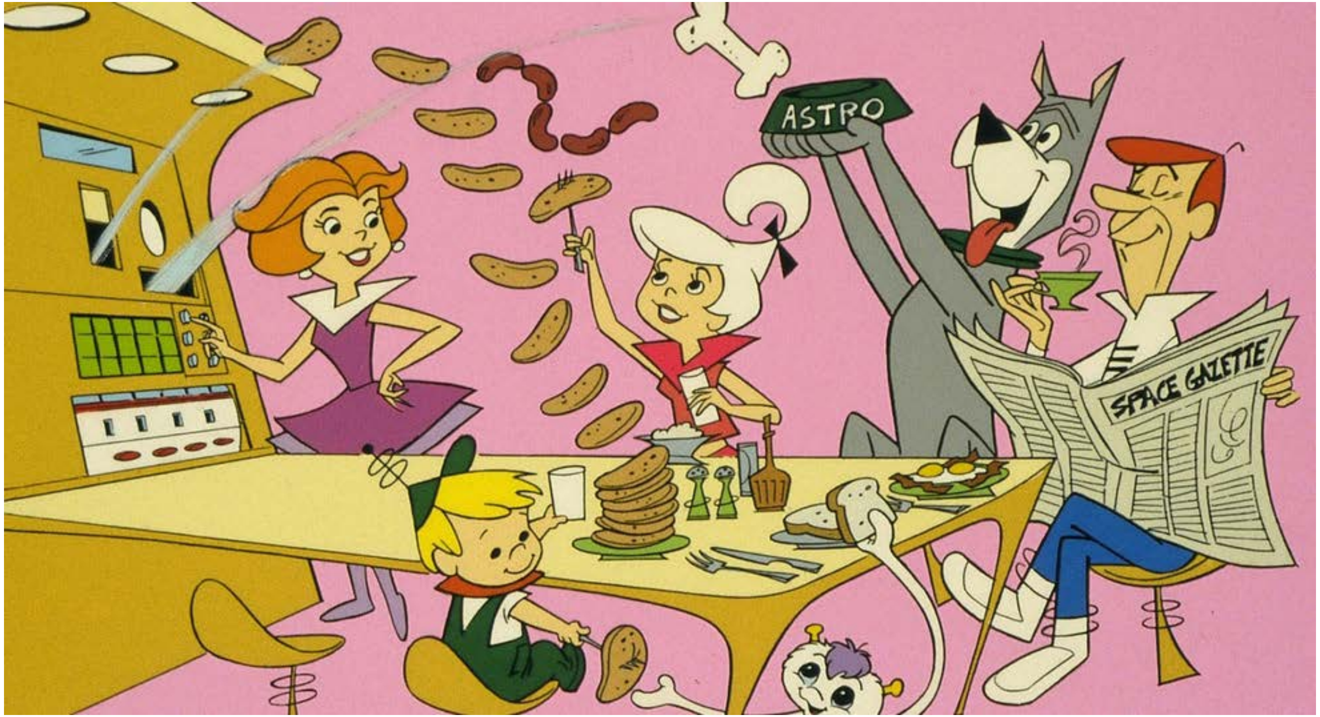


IoT (Internet of Things)

- IoT connectivity is now finding industrial application
- Industrial and Commercial facilities, such as Hospitals, are made up of numerous individual communication and control systems and sub-systems
- The interconnectivity of the devices in these systems allows data and information exchange that is being used to increase productivity, reduce cost, optimize operation, etc. in ways previously not possible


Helideck Lighting
Seismic Bracing
Power Factor Correction Capacitors
Harmonic Mitigating Transformers
Emergency Lighting
Arc Fault Circuit Interrupters
Busway
Clean Room Lighting
Circuit Breakers
Hospital Room Lighting & Nurse Call
Anti-Microbial Wall Plates
Heavy-Duty Quick Connect
Outlets & Straight Blade Connectors
Uninterruptible Power System
Patient Lighting Controls
General Area Lighting
Lighting Controls
Indoor & Outdoor Transformers
Monitoring Software
Canopy Lighting
Integrated Power Assemblies (IPA)
Adjustable Frequency Drives
Integrated Facility Systems
Automatic Transfer Switches
Medium Voltage Switchgear
Protective and Predictive Relays
Paralleling Switchgear
Low Voltage Switchgear
Emergency Alert System
Metering
Surge Protective Devices

Questions?



EATON

Powering Business Worldwide