Fundamentals of EtherNet/IP Networking

Allen-Bradley • Rockwell Software

Rockwell Automation

What you will learn

- Trends in Industrial Network Convergence
  - Technology enablers and business drivers
- Fundamentals of EtherNet/IP
  - What it is, capabilities and features
  - Networking basics
    - breaking down the lingo and acronyms
    - models and standards
  - Multidiscipline control applications
  - Representative plantwide network architecture
  - Advantages which enables and drives convergence of control and information

Agenda

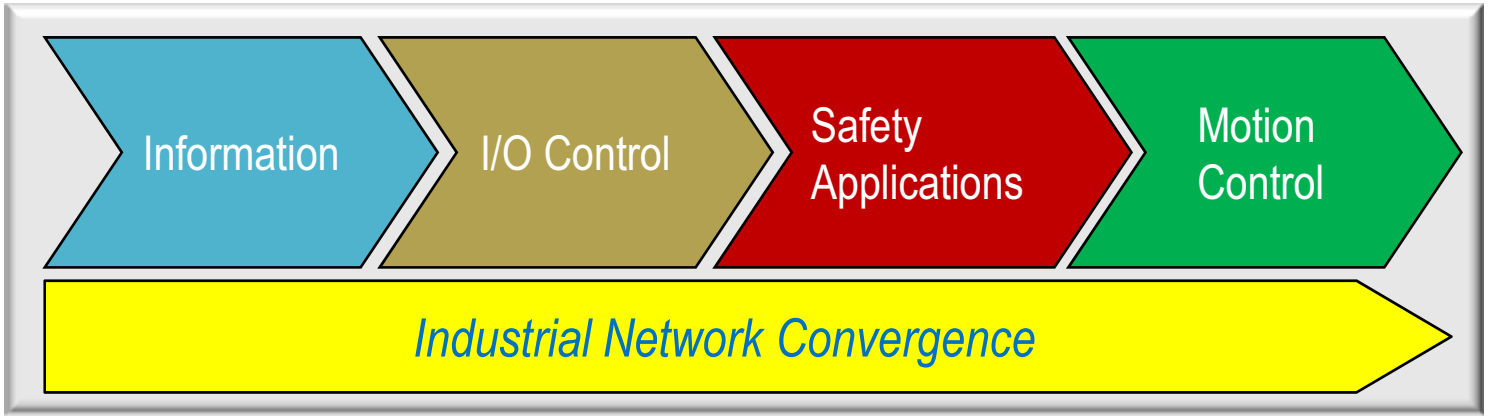
1. Industrial Network Trends
2. OSI Reference Model
3. Layers 1 - 7
4. Plantwide Network Architecture
5. EtherNet/IP Advantage Summary

Industrial Networks
Continuing Trends

- Open Networks Are In Demand
  - Broad availability of products, applications and vendor support for Industrial Automation and Control System (IACS)
  - Network standards for coexistence and interoperability
- Convergence of Network Technologies
  - Reduce the number of different networks in an operation and create a seamless information sharing from the plant floor to the enterprise
  - Use common network design and troubleshooting tools across the plant and enterprise, and avoid special tools for each application
- Better Asset Utilization to Support Lean Initiatives
  - Reduce training, support, and inventory for different networking technologies
  - Common network infrastructure assets, while accounting for environmental requirements
- Future Proof – Maximizing Investments
  - Support new technologies and features without a network forklift upgrade

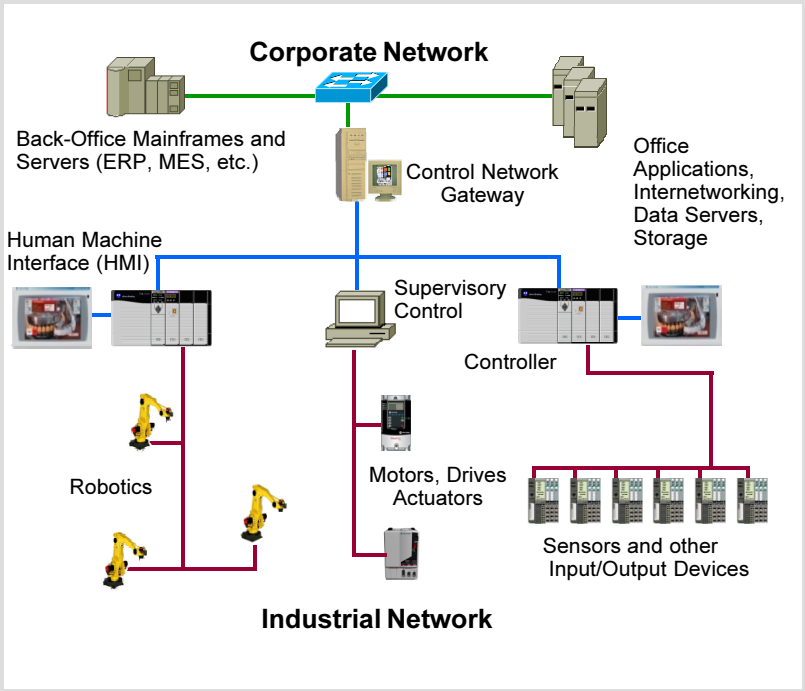
Industrial Network Convergence
Continuing Trend

Evolution of industrial Ethernet applications

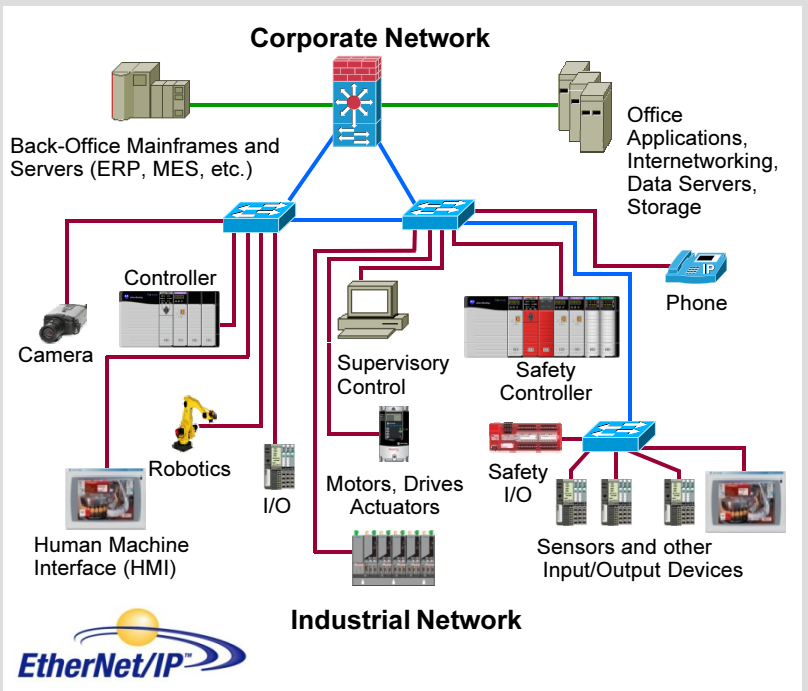


EtherNet/IP - Enabling/Driving Convergence of Control and Information

Industrial Network Convergence
Continuing Trend



Traditional – 3 Tier Industrial Network Model

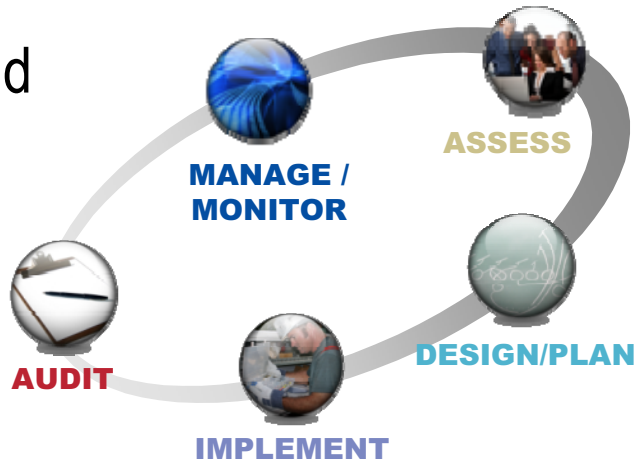


Converged Plantwide Ethernet Industrial Network Model

EtherNet/IP - Enabling/Driving Convergence of Control and Information

Industrial Network Design Methodology

- Understand application and functional requirements
  - What devices are to be connected – industrial and non-industrial
  - Determine data requirements for availability, integrity and confidentiality
  - Communication patterns, topology and resiliency requirements
  - Types of traffic – information, control, safety, time synchronization, motion control, voice, video
- Develop a logical framework (roadmap)
  - Define zones and segmentation
  - Place applications and devices in the logical framework based on requirements
- Develop a physical framework to align with and support the logical framework
- Determine security requirements, take into consideration IT requirements and establish early dialogue with IT
- Use technology and industry standards, reference models and reference architectures

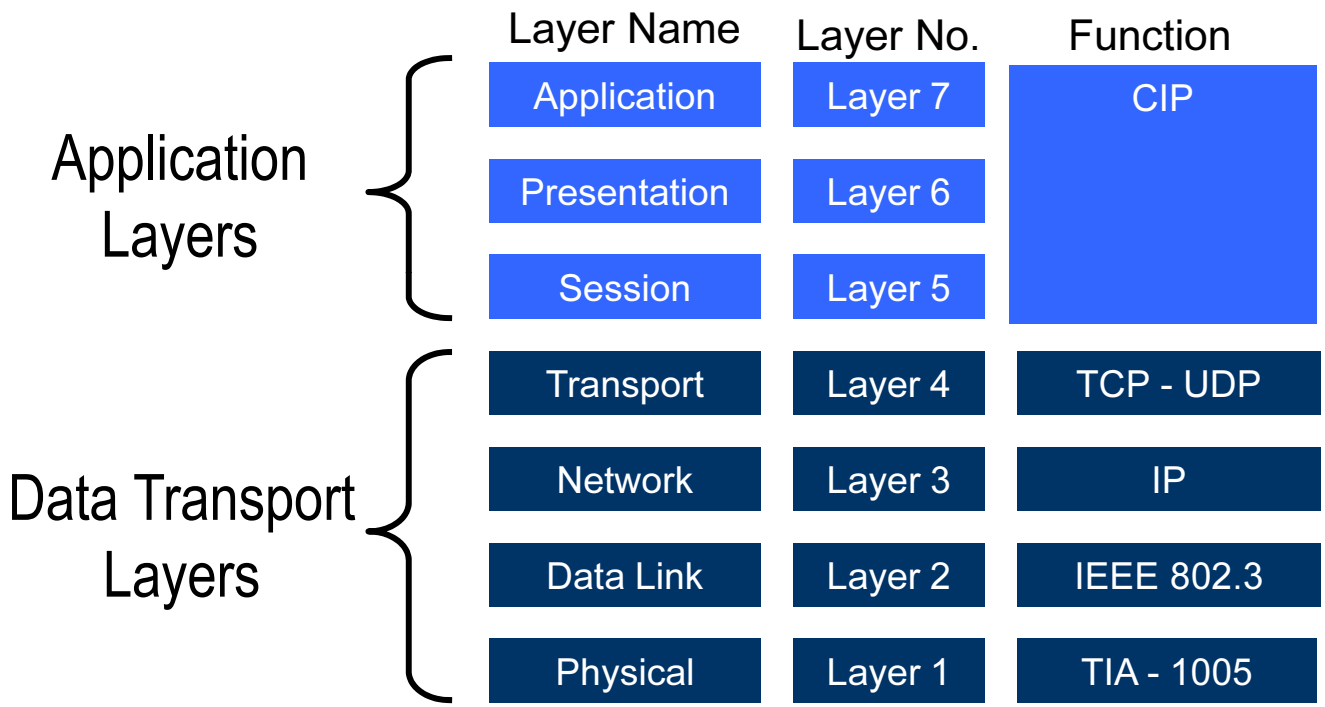


OSI Reference Model
Open Systems Interconnection

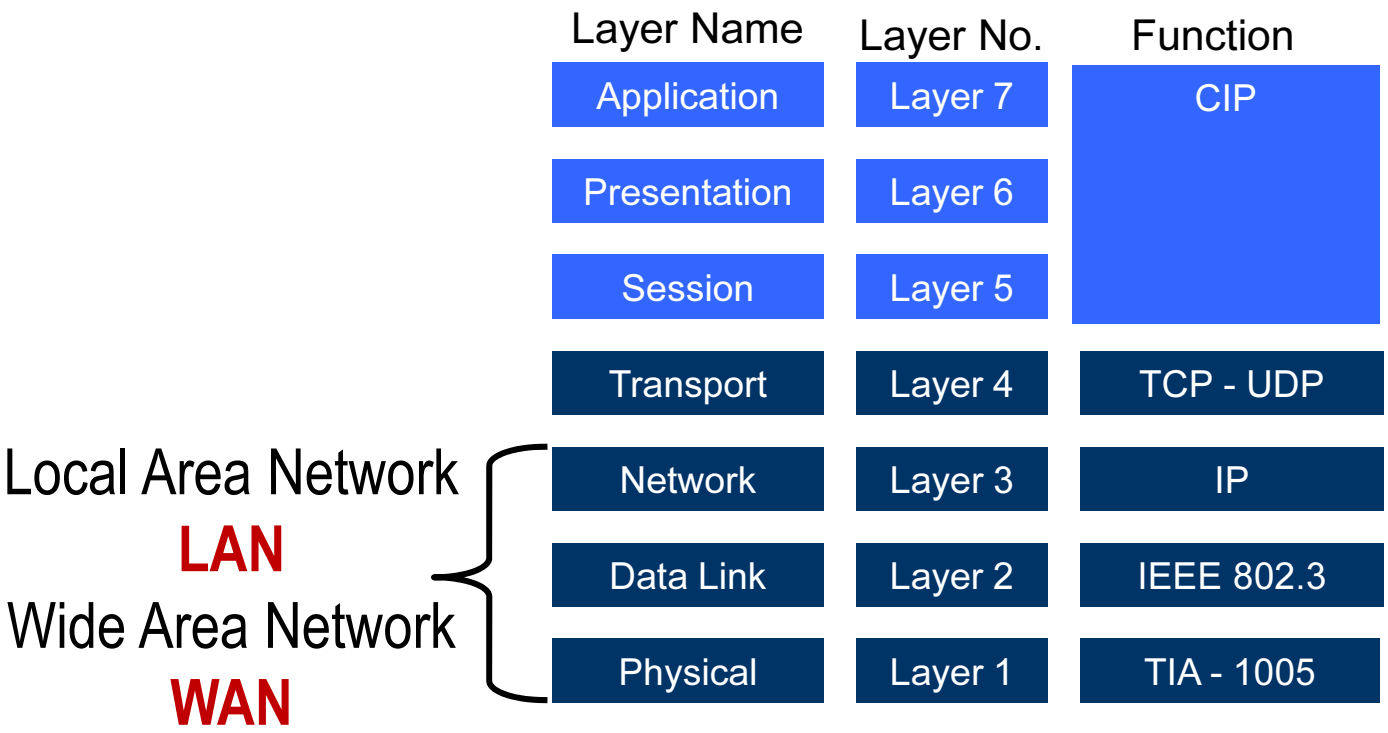
Layer Name		Layer No.	Function	Examples
Application		Layer 7	Network Services to User App	CIP
Presentation		Layer 6	Encryption/Other processing	
Session		Layer 5	Manage Multiple Applications	
Transport		Layer 4	Reliable delivery/Error correction	TCP - UDP
Network	Routers 	Layer 3	Logical addressing - Routing	IP
Data Link	Switches 	Layer 2	Media Access Control	IEEE 802.3
Physical	Cabling	Layer 1	Specifies voltage, pin-outs, cable	TIA - 1005

5-Layer TCP/IP Model

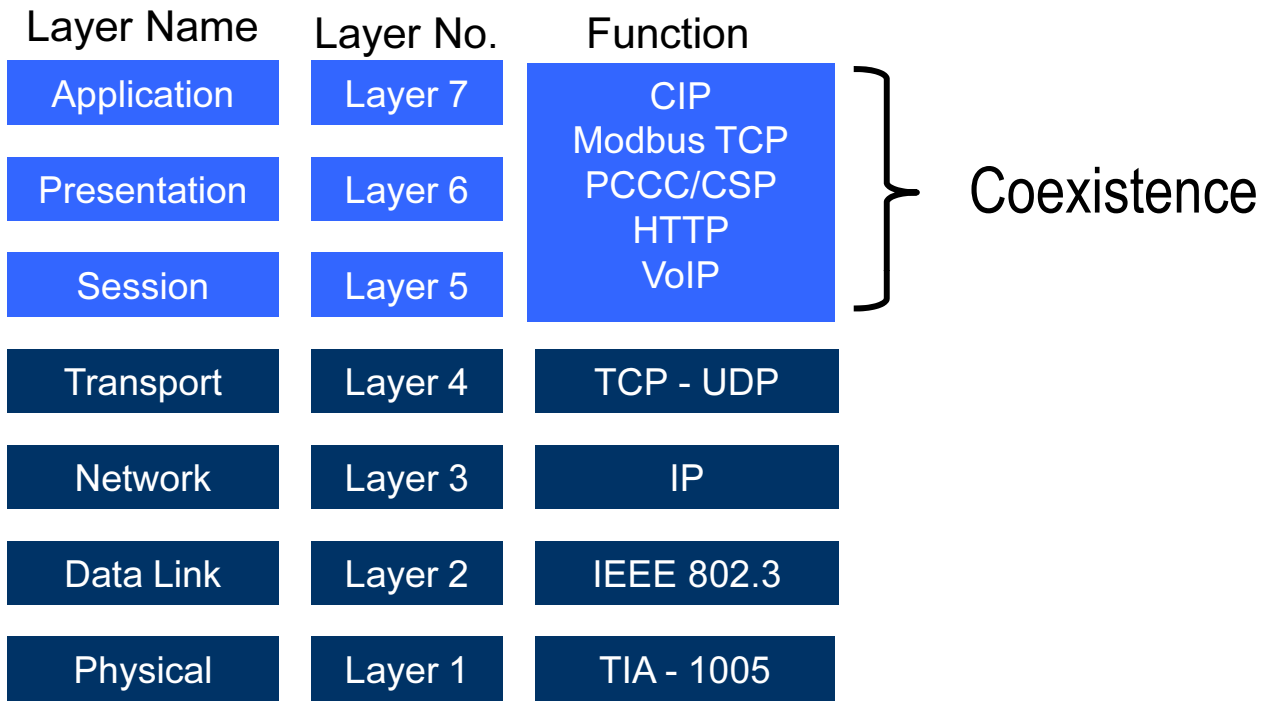
OSI Reference Model
Protocol Stack



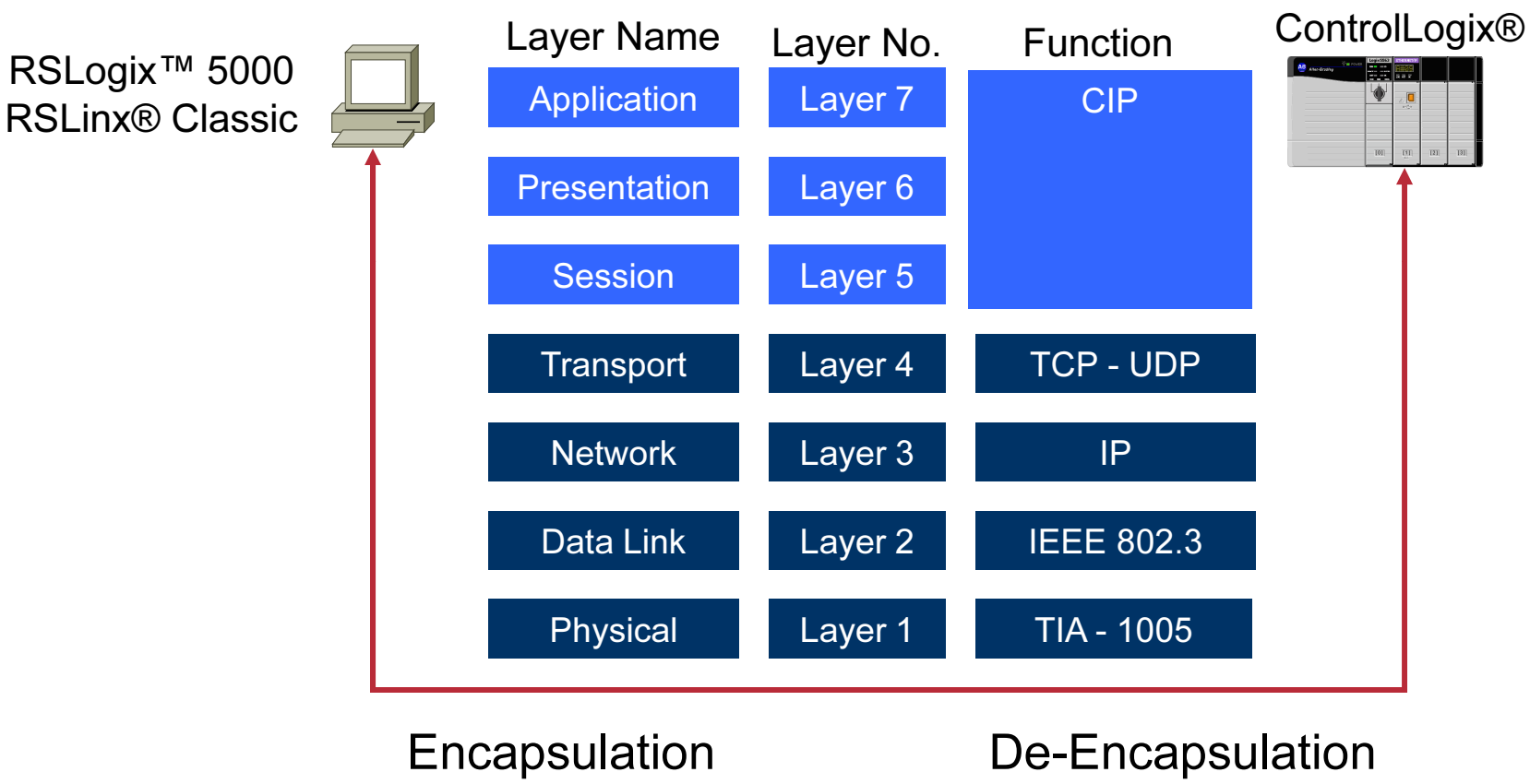
OSI Reference Model
Protocol Stack



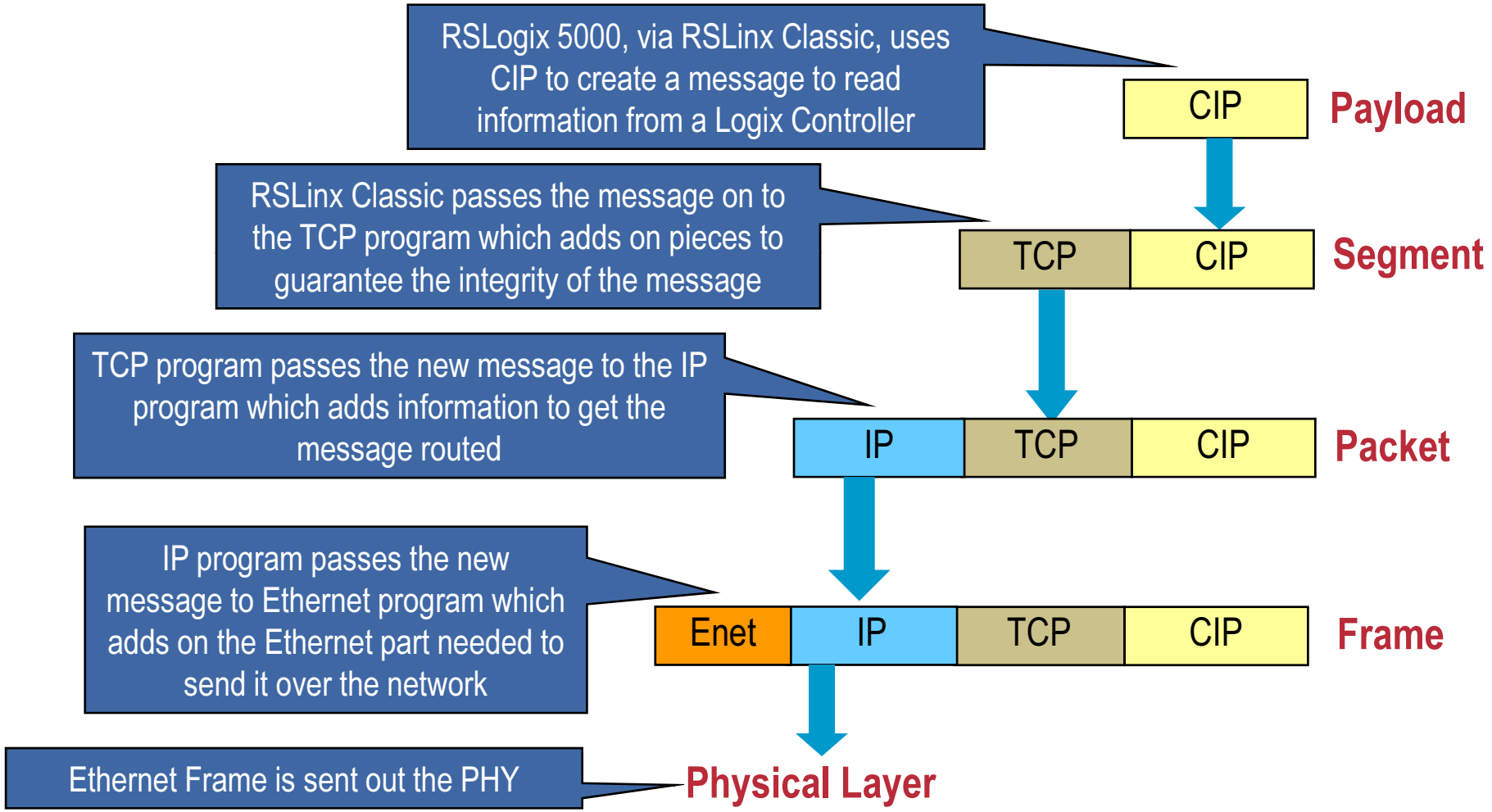
OSI Reference Model
Protocol Stack



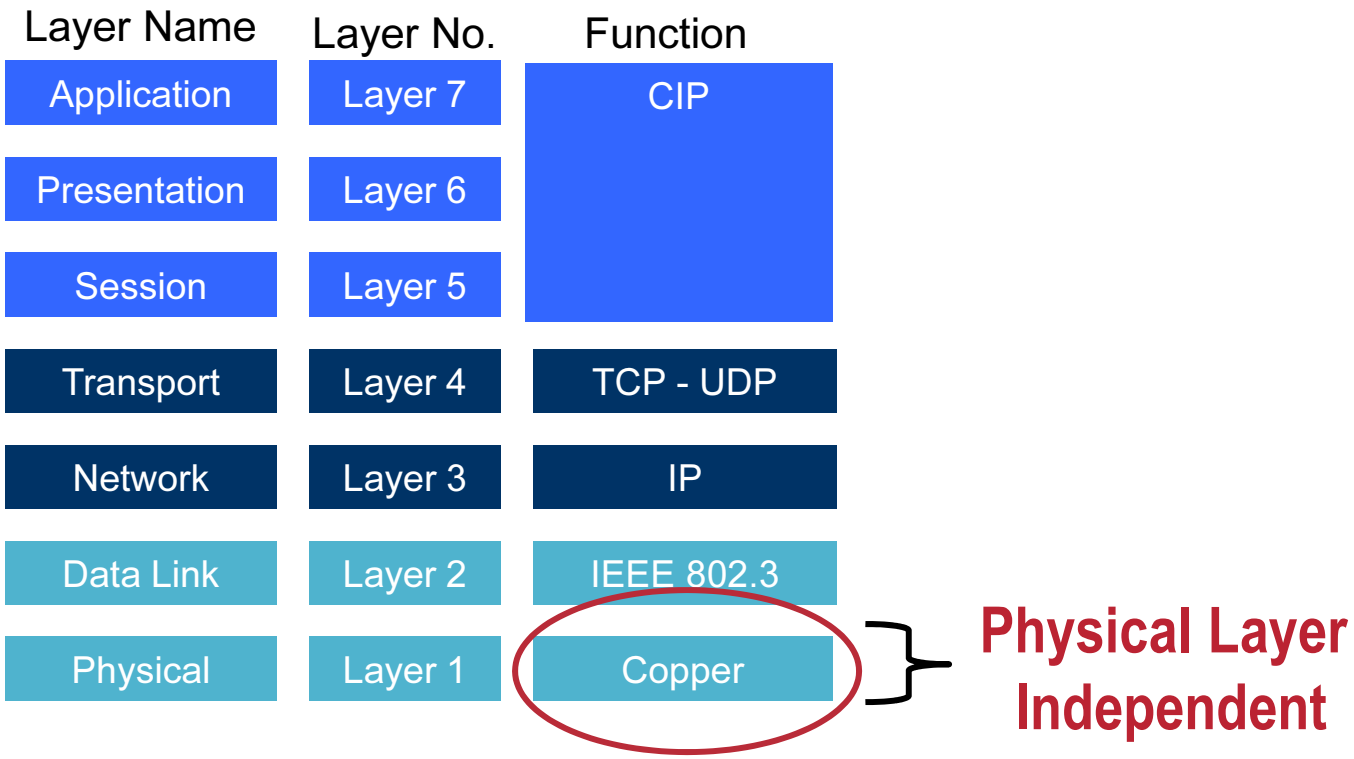
OSI Reference Model
Protocol Stack



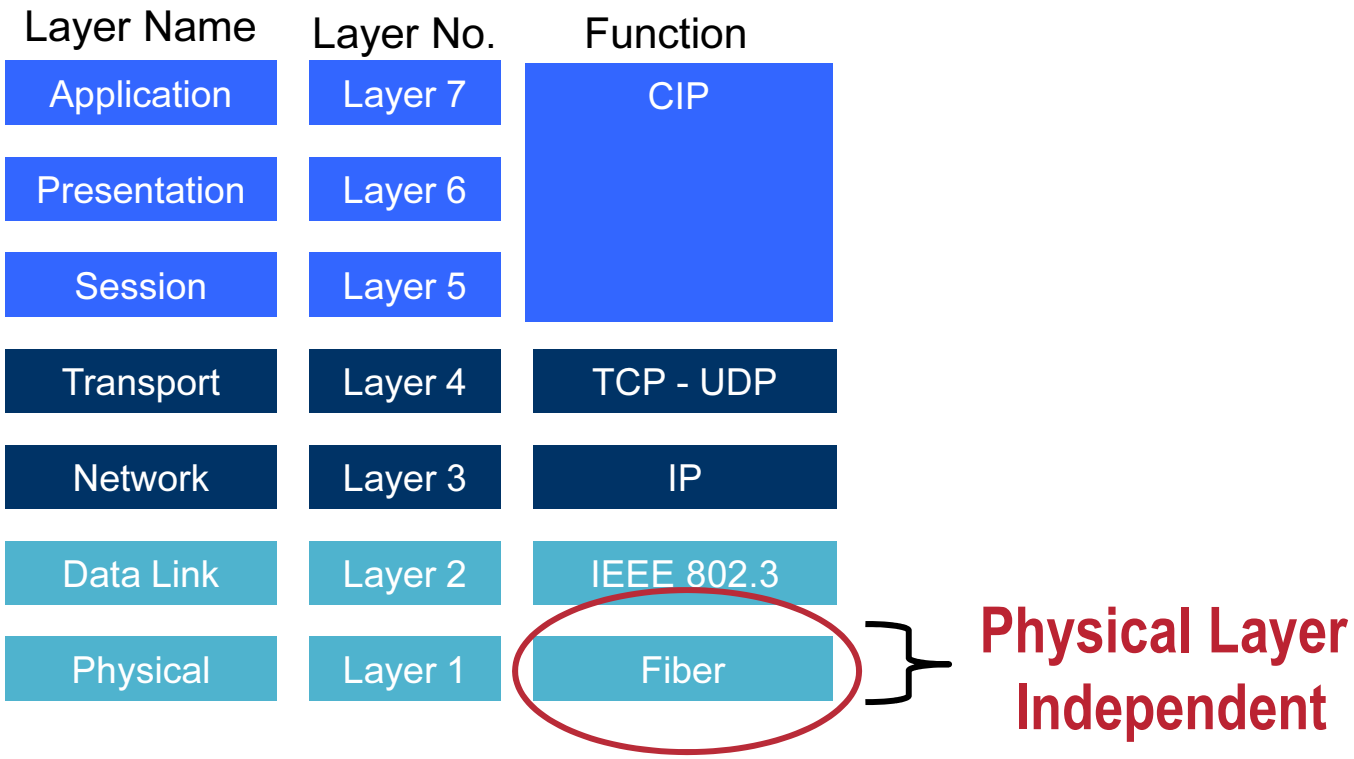
OSI Reference Model
Protocol Stack Example - Encapsulation



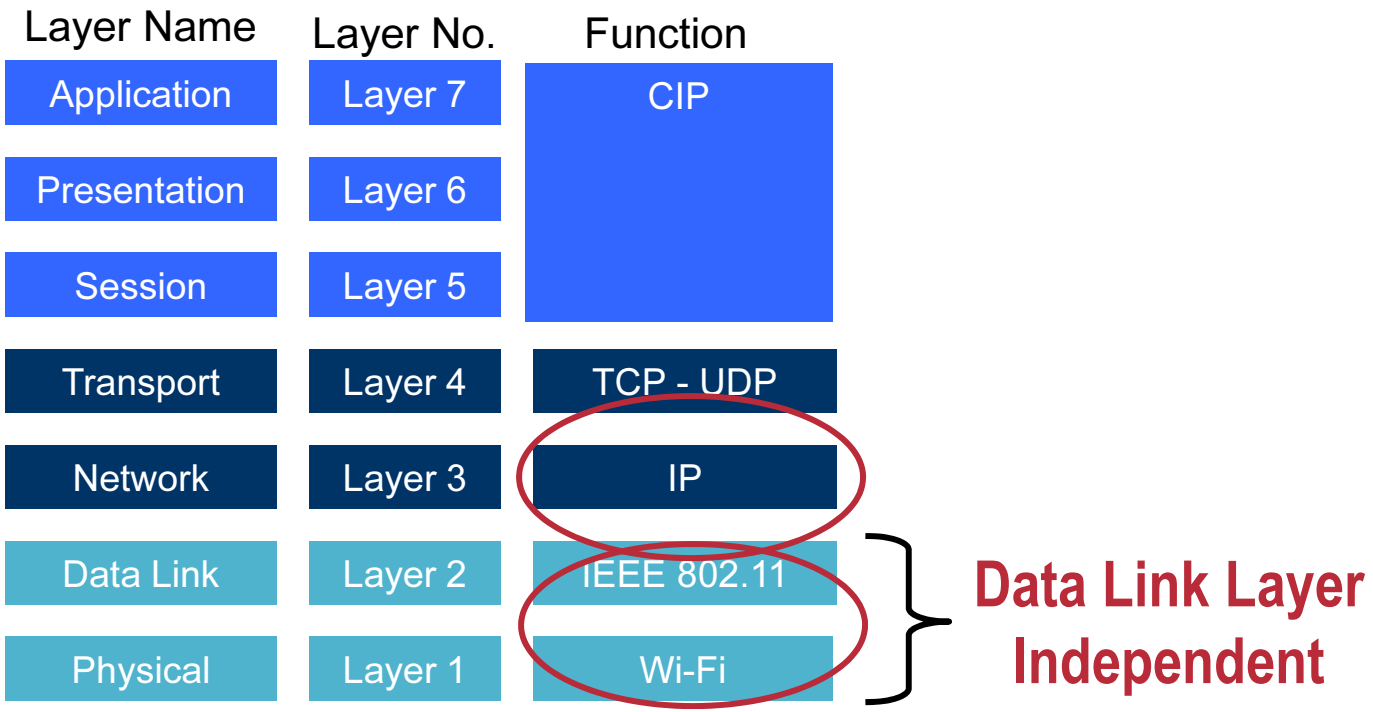
OSI Reference Model
Physical Layer Independent



OSI Reference Model
Physical Layer Independent

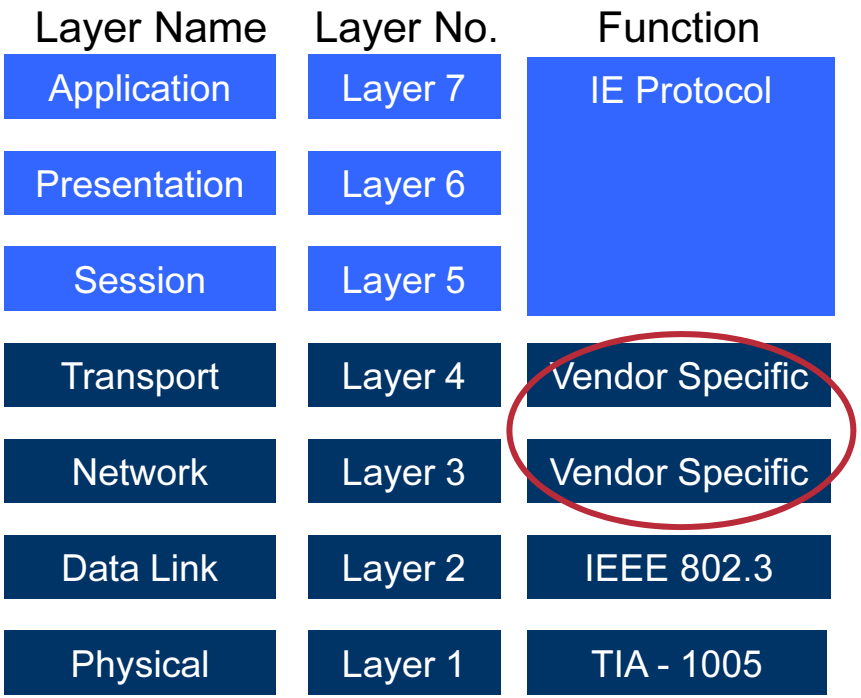


OSI Reference Model
Data Link Layer Independent

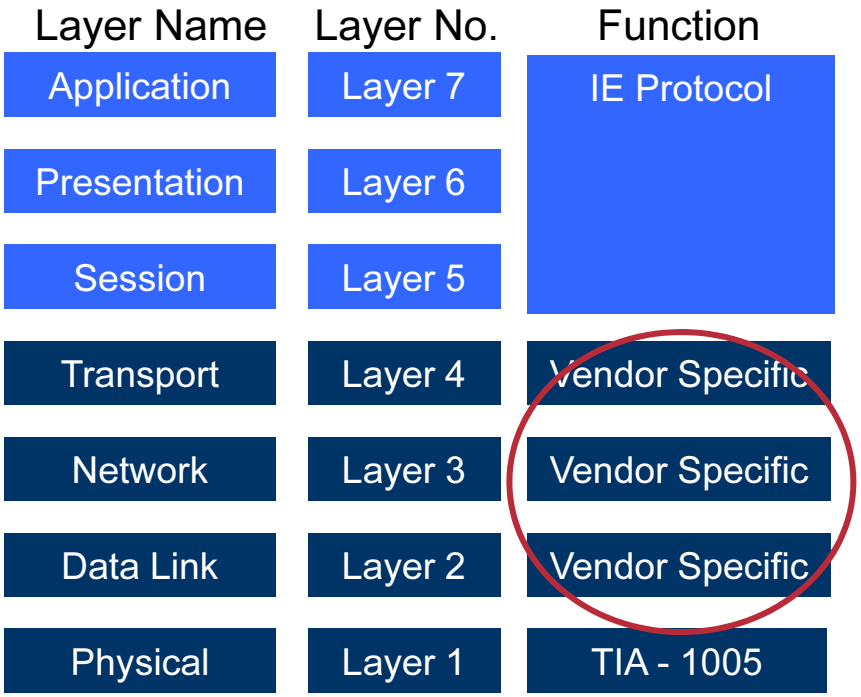


Standard IP provides Routing and Data Link Independence

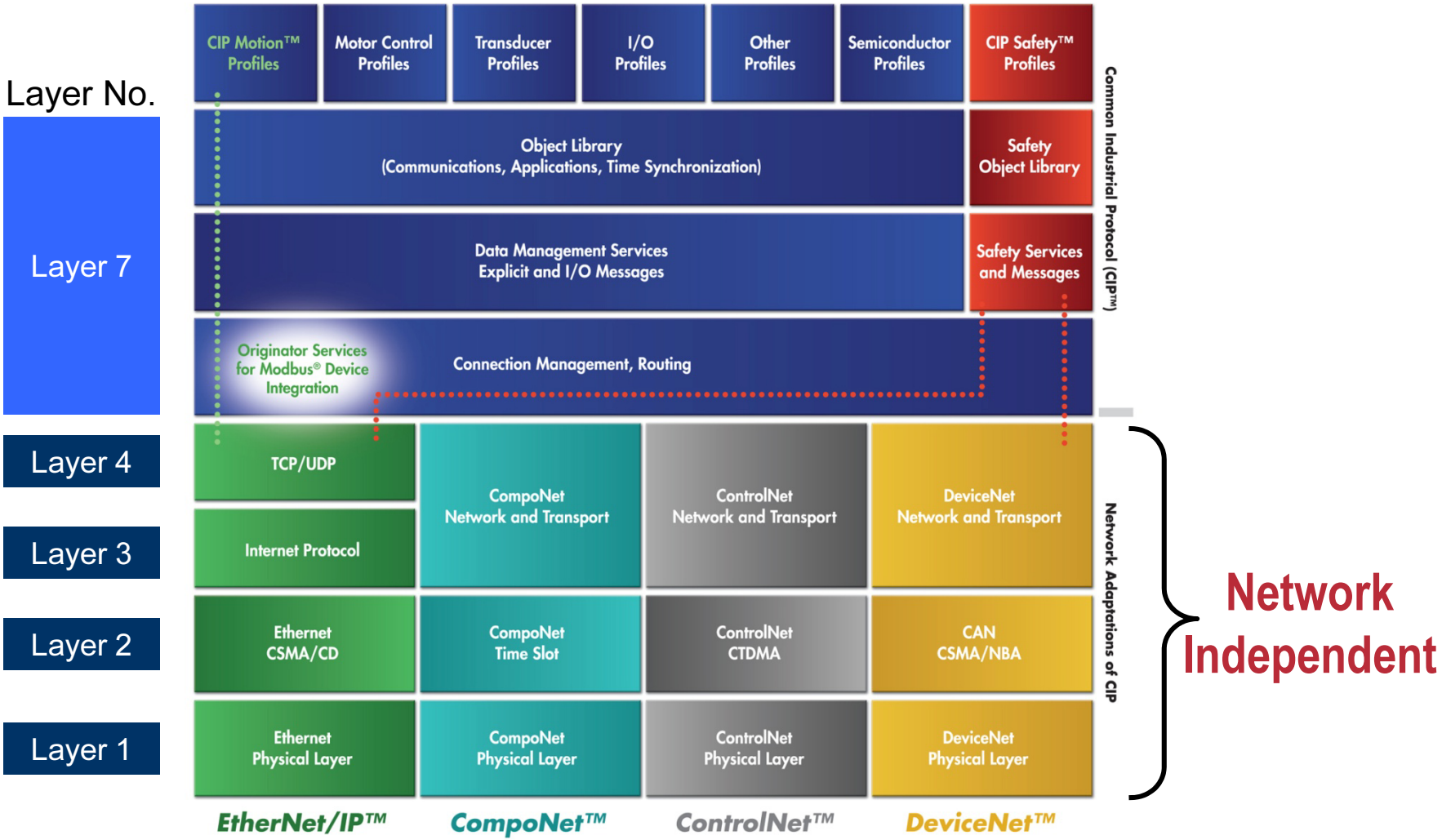
OSI Reference Model
Open Systems Interconnection



OSI Reference Model
Open Systems Interconnection



OSI Reference Model
Network Independent



OSI Reference Model
Open System Interconnection

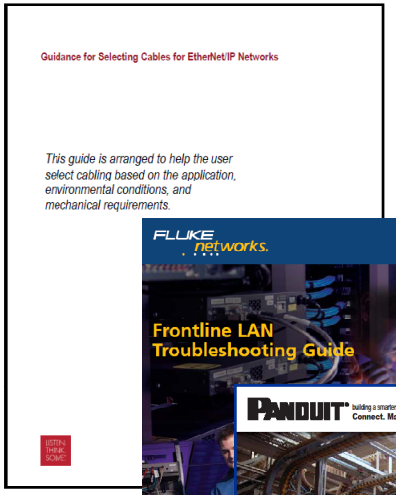
EtherNet/IP™

Layer Name		Layer No.	Function	Examples
Application		Layer 7	Network Services to User App	CIP
Presentation		Layer 6	Encryption/Other processing	
Session		Layer 5	Manage Multiple Applications	
Transport		Layer 4	Reliable delivery/Error correction	TCP - UDP
Network	Routers 	Layer 3	Logical addressing - Routers	IP
Data Link	Switches 	Layer 2	Media Access Control	IEEE 802.3
Physical	Cabling	Layer 1	Specifies voltage, pin-outs, cable	TIA - 1005

Similar sounding network devices and services exist at Layer 2 (L2) and Layer 3 (L3) – e.g. QoS, Resiliency, Security

Layer 1 - Physical Layer

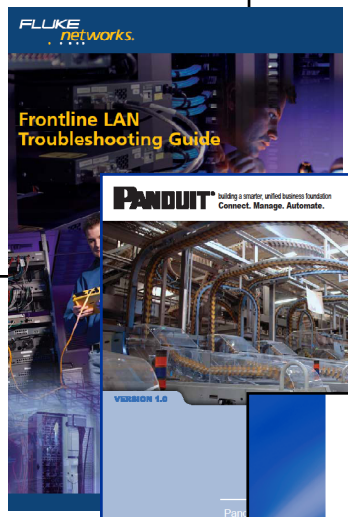
- Design and implement a robust physical layer
- Environment Classification - MICE
- More than cable
  - Connectors
  - Patch panels
  - Cable management
  - Grounding, Bonding and Shielding (noise mitigation)
- Physical Media
  - Wired vs. Wireless
  - Copper vs. Fiber
  - UTP vs. STP
  - Singlemode vs. Multimode
  - SFP – LC vs. SC
- Topology



Cable Selection ENET-WP007

FLUKE networks.

LAN Troubleshooting Guide



PANDUIT

Industrial Ethernet Physical Infrastructure Reference Architecture Design Guide

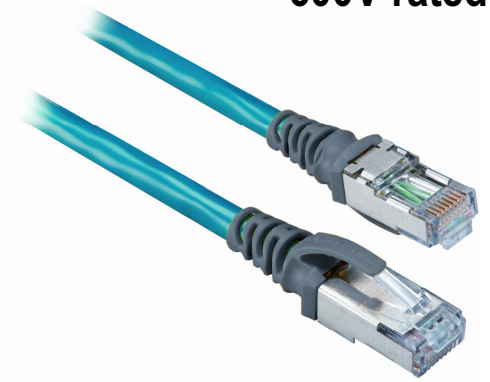
ODVA

ODVA Guide

Layer 1 – Physical Layer
Industrial Connectivity for MICE RISKS

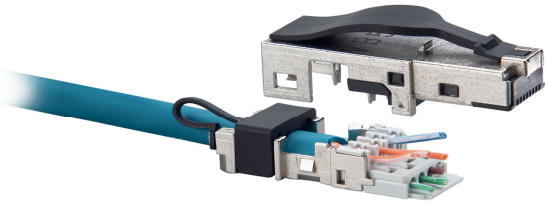
M12 Connectivity

600V rated cable



RJ45 Connectivity

Accessories



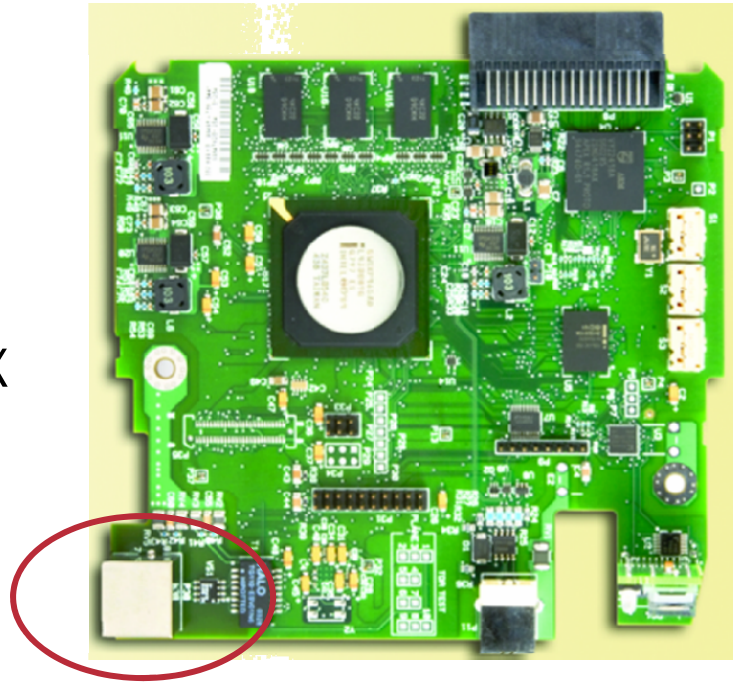
http://www.ab.com/networks/media/ethernet/

Baseband vs. Broadband

- Baseband
  - Single signal/frequency/channel over the cable
  - Example – Ethernet
- Broadband
  - Multiple signals/frequencies/channels over the cable simultaneously
  - Traditional Definition
    - Classic Broadband has a “carrier” for each channel
    - Example - Cable TV, Wi-Fi, Power-Line Communications
  - Current Definition
    - Broadband Internet access – high speed Internet access

Layer 1 – Physical Layer

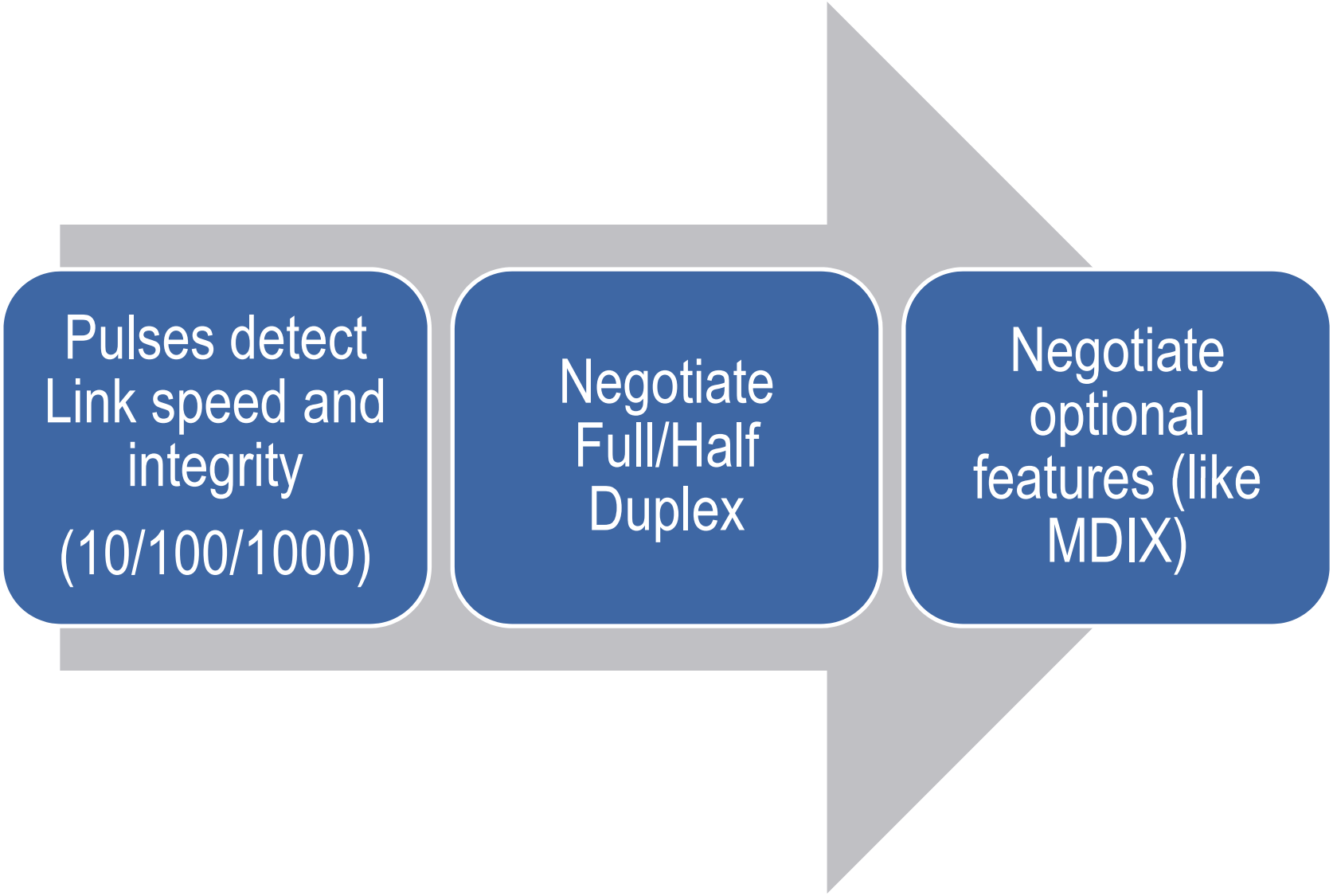
- Responsible for converting a frame, Layer 2 output, into electrical signals to be transmitted over the physical network.
  - LAN or WAN - voltage levels, physical data rates, maximum transmission distances, physical connectors
- It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects
- Ethernet examples:
  - 10Base-2, 10Base-5, 10Base-T, 100Base-TX 100Base-SX
- PHY examples:
  - RS-232
  - T1, E1
  - ISDN
  - 802.11



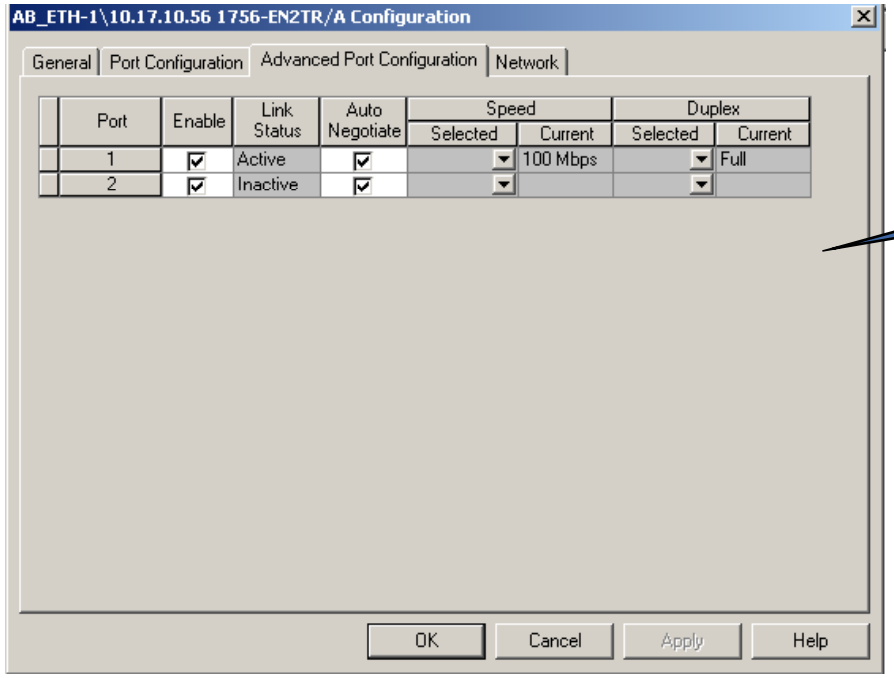
Layer 1 – Physical Layer
Half versus Full Duplex transmission

- Half Duplex
  - One station transmits, other listens.
  - While transmitting, you do not receive, as no one else is transmitting.
  - If someone else transmits while you are transmitting, then a collision occurs
  - Any “Receive-while-Transmit” condition is considered a collision
  - **NON-DETERMINISTIC**
- Full Duplex (standardized in 802.3x)
  - Transmit and receive at the same time.
  - Transmit on the transmit pair, and receive on the receive pairs.
  - No collision detection, backoff, retry, etc.
  - Collision Free. No CS, no MA, no CD. Only relationship to Half Duplex is frame format & encoding/signaling method
  - **DETERMINISTIC**

Layer 1 – Physical Layer
Auto-Negotiation vs. Fixed Settings



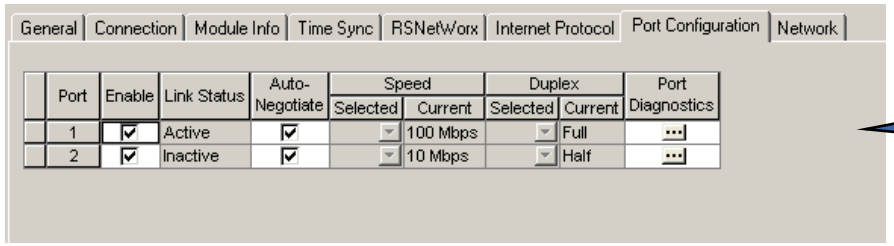
Layer 1 - Physical Layer
EN2TR Example



RSLinx Classic Module Configuration

EN2TR Webpage Network Settings

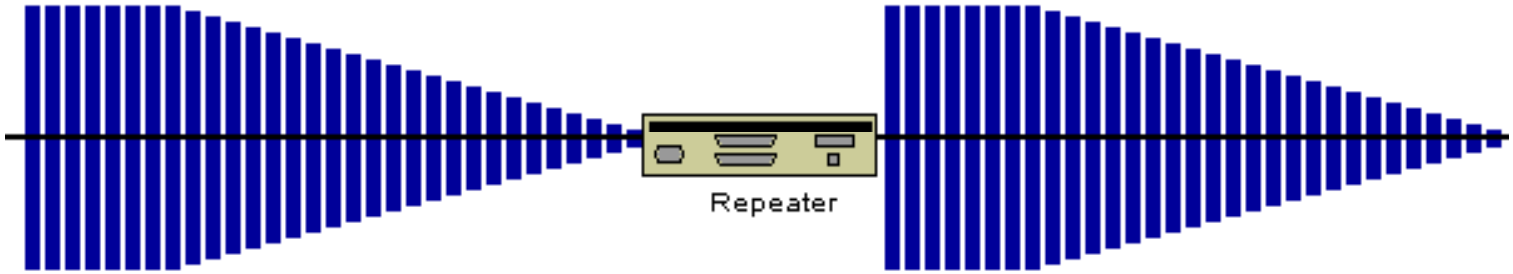
Ethernet Port 1	
Interface State	Enabled
Link Status	Active
Speed	100 Mbps
Duplex	Full Duplex
Autonegotiate Status	Autonegotiate Speed and Duplex



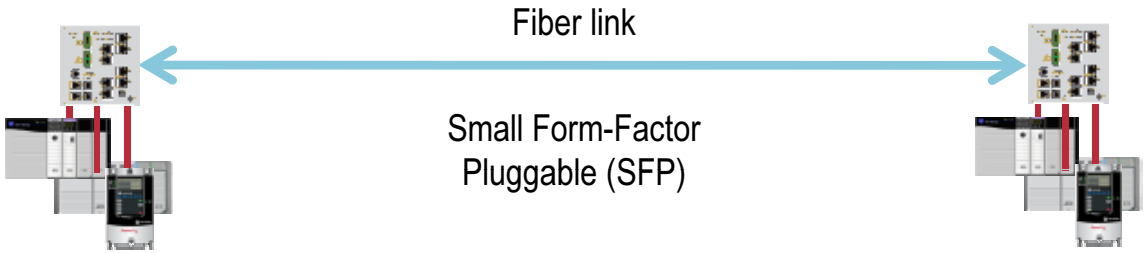
RSLogix 5000 EN2TR Properties

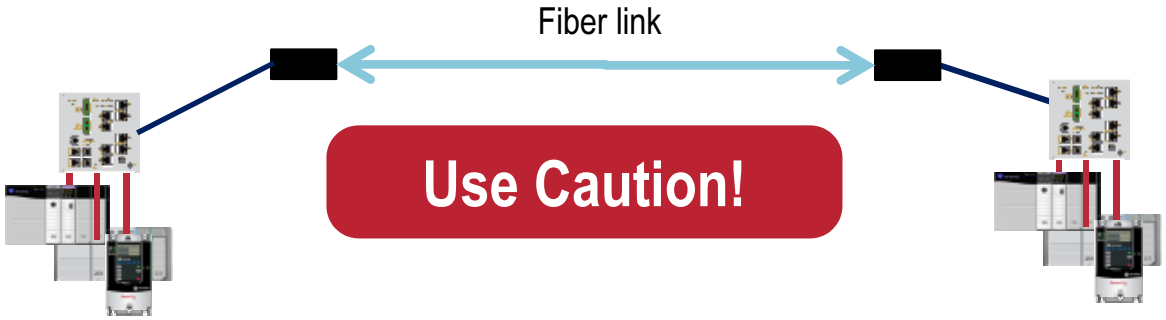
Layer 1 – Physical Layer
Infrastructure – Active Devices

- A repeater recreates the incoming signal and re-transmits it without noise or distortion that may have effected the signal as it was transmitted down the cable.
- Repeaters were available on legacy Ethernet to increase the overall length of the network and allow additional nodes to be added.



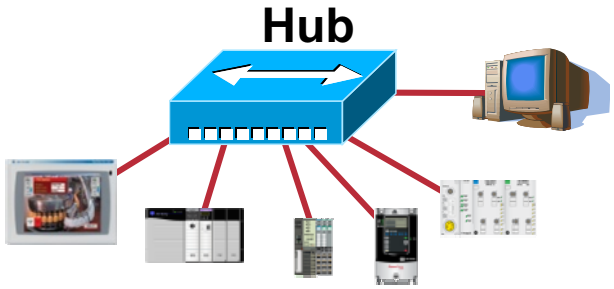
Layer 1 - Physical Layer
Infrastructure - Active Devices - Media Converters



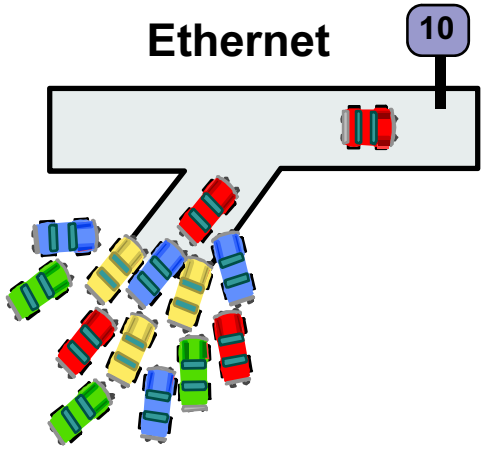


Layer 1 – Physical Layer
Infrastructure – Active Devices

- Hub – Multiport Repeater
- A hub is at the center of a star topology and utilizes twisted pair or fiber cable to connect to devices. Hubs may be connected together using a variety of media as a backbone between hubs.
- A hub **broadcasts** everything it receives on any channel out all other channels Non-Deterministic



All nodes share 10 Mbps



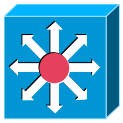
One device sending at a time

Layer 1 Domain

Layer 1 – Physical Layer
Topology - Linear

Layer 2 Access Switch
Stratix 8000

Layer 2 Bridge



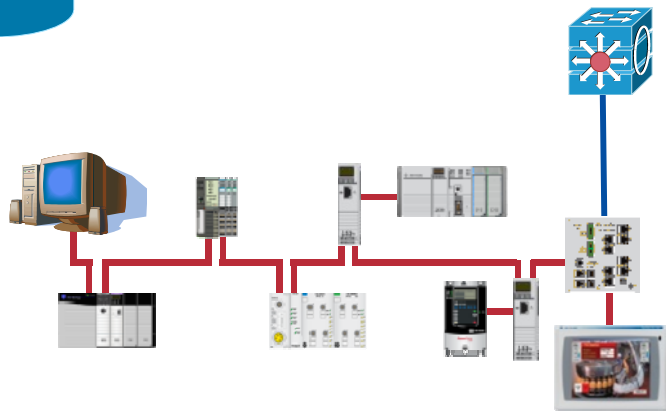
Multi-Layer Switch
Layer 2 and Layer 3
Stratix 8300

Layer 3 Router

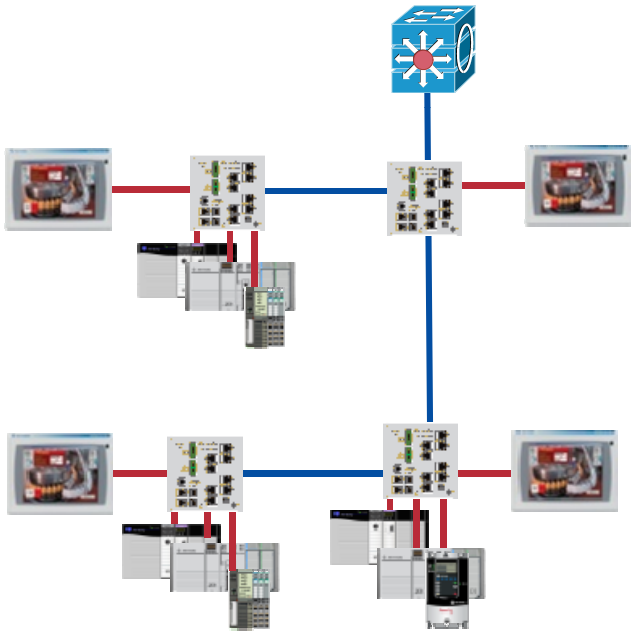
Layer 2 Access Link

Layer 2 Interswitch Link

Layer 3 Link

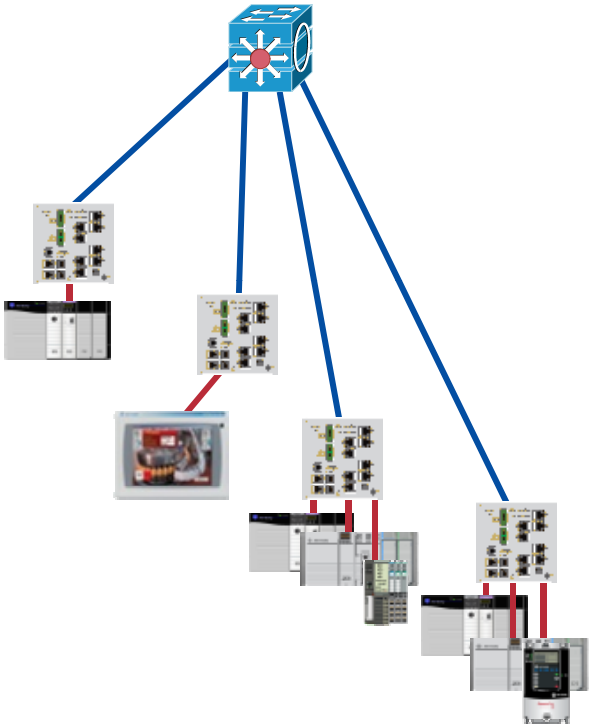


Linear - Device



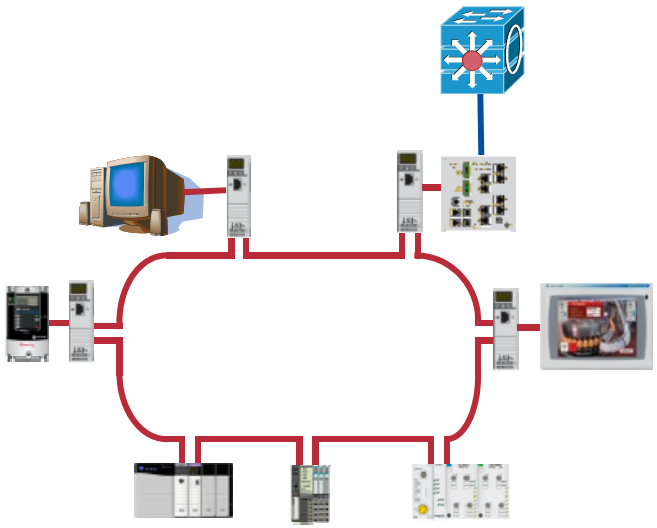
Linear - Switch

Layer 1 – Physical Layer
Topology - Star

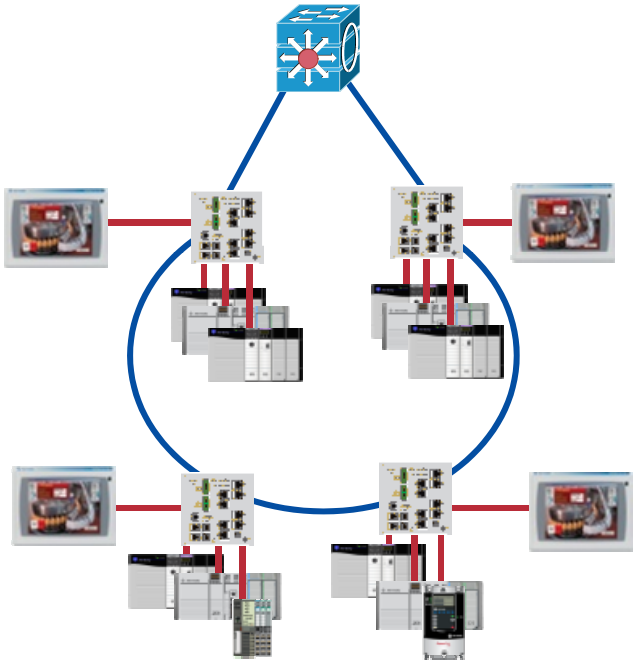


Star

Layer 1 – Physical Layer
Topology - Ring

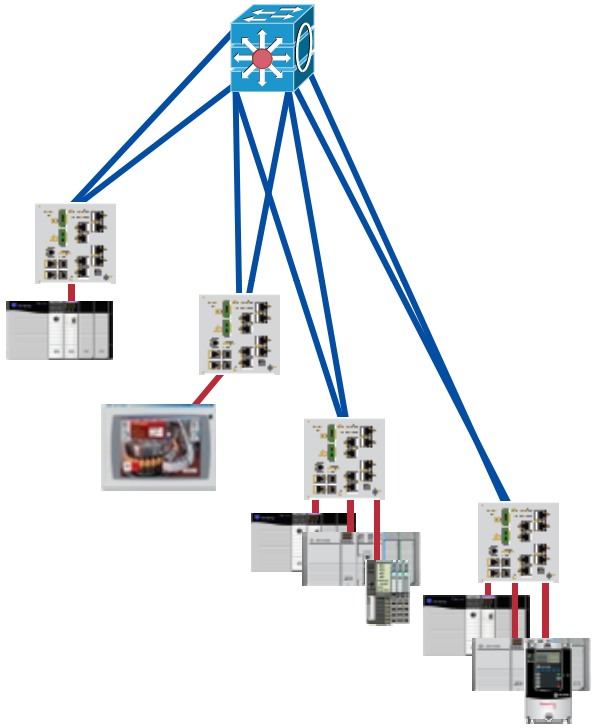


Ring - Device



Ring - Switch

Layer 1 – Physical Layer
Topology – Redundant Star



Redundant Star

Layer 2 – Data Link
802.3 – Ethernet – Local Area Network (LAN)

- The Data Link layer is divided into two sub layers: The **Media Access Control** (MAC) layer and the **Logical Link Control** (LLC) layer.
- The MAC sub layer controls how a device on the network gains access to the data and permission to transmit it.
- The LLC layer controls frame synchronization, flow control and error checking.
- LAN Media Access:
  - CSMA/CD
- Layer 2 LAN and WAN Examples:
  - 802.3, 802.5, Frame Relay, ATM, ISDN, MPLS (service providers)
- Layer 2 Protocol Examples:
  - ARP – Address Resolution Protocol
- Layer 2 Services Examples
  - QoS – Quality of Service, VLAN – Virtual Local Area Network , Resiliency and Security

Layer 2 – Data Link
Hardware Addressing

- All devices on Ethernet communicate using the Ethernet address for the device. This address is sometimes referred to as the "hardware address" or "MAC address" (MAC stands for **Media Access Controller**).
- The hardware address is a unique (in the world) 6-byte address that is embedded in the circuitry of every device that sits on an Ethernet network.
- Every vendor of Ethernet products obtains their own unique address range (Allen-Bradley's is 00:00:BC:XX:XX:XX).

00:00:BC:03:52:A9

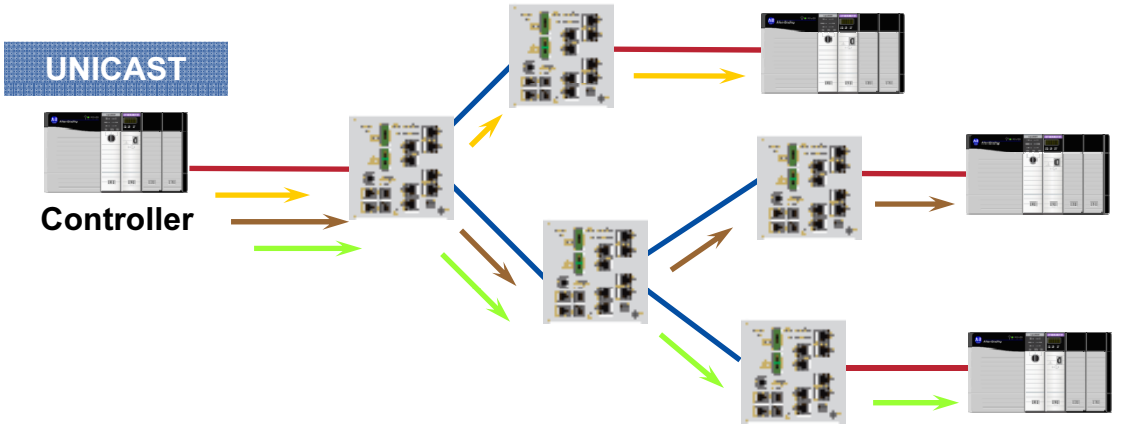
Note that each digit of the MAC address is a hex number (range 0-F)

Layer 2 – Data Link
LAN Transmission Methods

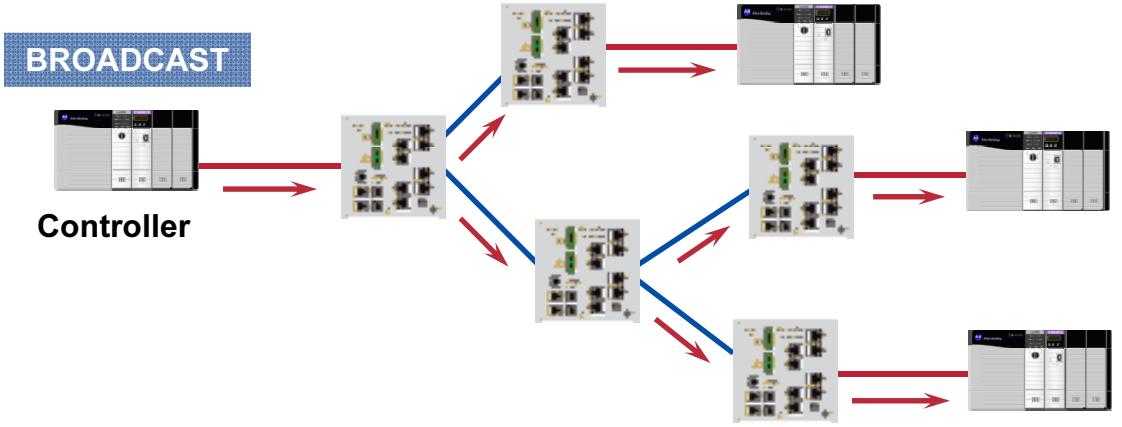
- Unicast
  - A method by which a frame is sent to a single destination.
- Multicast
  - A technique that allows copies of a single frame to be passed to a selected subset of possible destinations.
  - Example: 01-00-0C-CC-CC-CC (Cisco Discovery Protocol – CDP)
- Broadcast
  - A frame delivery system that delivers a given frame to all hosts on the LAN.
  - FF:FF:FF:FF:FF:FF

Layer 2 - Data Link
LAN Transmission Method - Examples

One-to-one, individual transactions:
Example – Logix Message Instruction, Logix P/C Connection

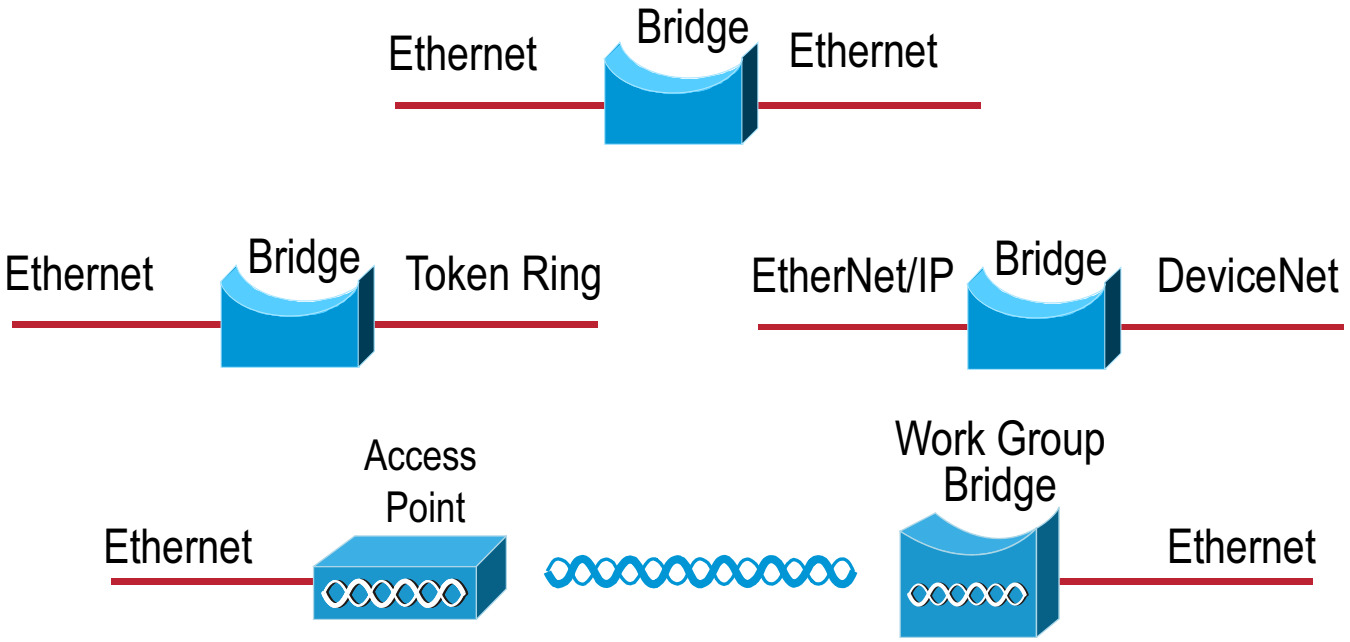


One-to-all, single transaction:
Examples – ARP, RSLinx Classic RSWho Browse



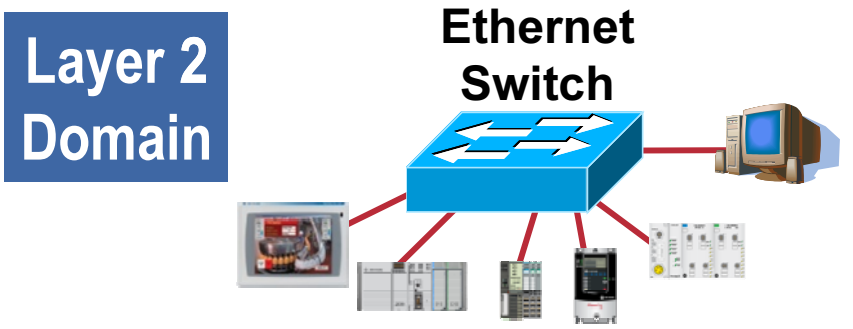
Layer 2 - Data Link
Bridging

- A bridge is a device that isolates traffic between segments by selectively forwarding frames to their proper destination. It is transparent to the network and protocol independent.
- Similar to the repeater, the bridge isn't used much any more, but more advanced devices which perform the bridging function are commonly used.

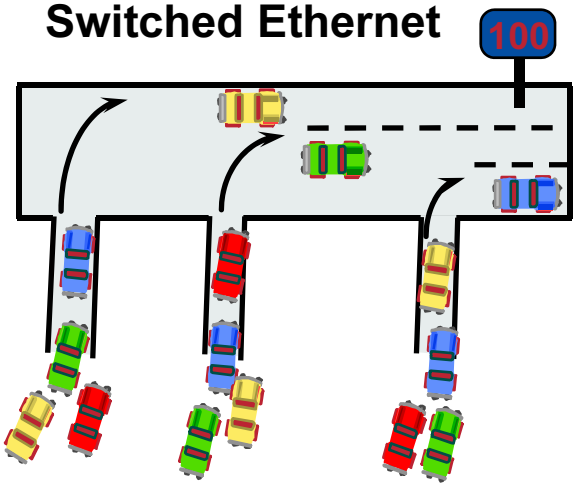


Layer 2 - Data Link
Switching

- Multi-port Bridge
- Ethernet has progressed exponentially since it was first introduced
  - Cost
  - Performance
  - Shared Media vs. Switches
  - Collisions vs. Determinism
- Multiple devices sending at the same time
- Requirements for an scalable industrial networking solution go even farther

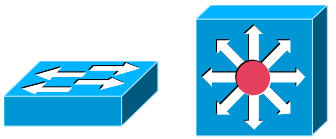


Each node has 100 Mbps

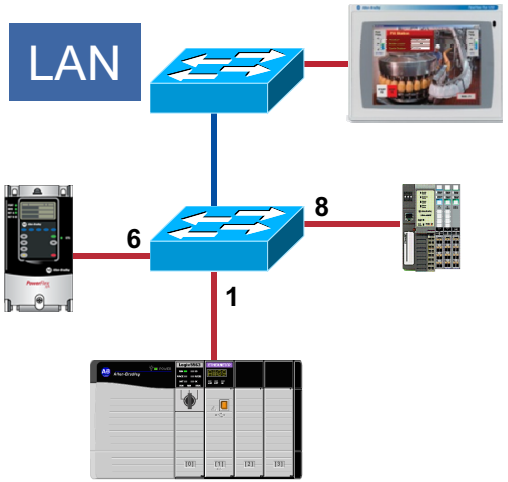


Each node has 100 Mbps

Layer 2 - Data Link
Switching



- Stratix 8000 and 6000
- All ports are in the same broadcast domain
- Forwards frames based on the MAC address and a forwarding table
- CAM Table – content addressable memory
  - Learns a station's location by examining source address
  - Sends out all ports when destination address is broadcast, multicast, or unknown address
  - Forwards when destination is located on different interface
- Managed switches provide Layer 2 features, such as segmentation (VLAN tag), security, QoS, resiliency, etc.

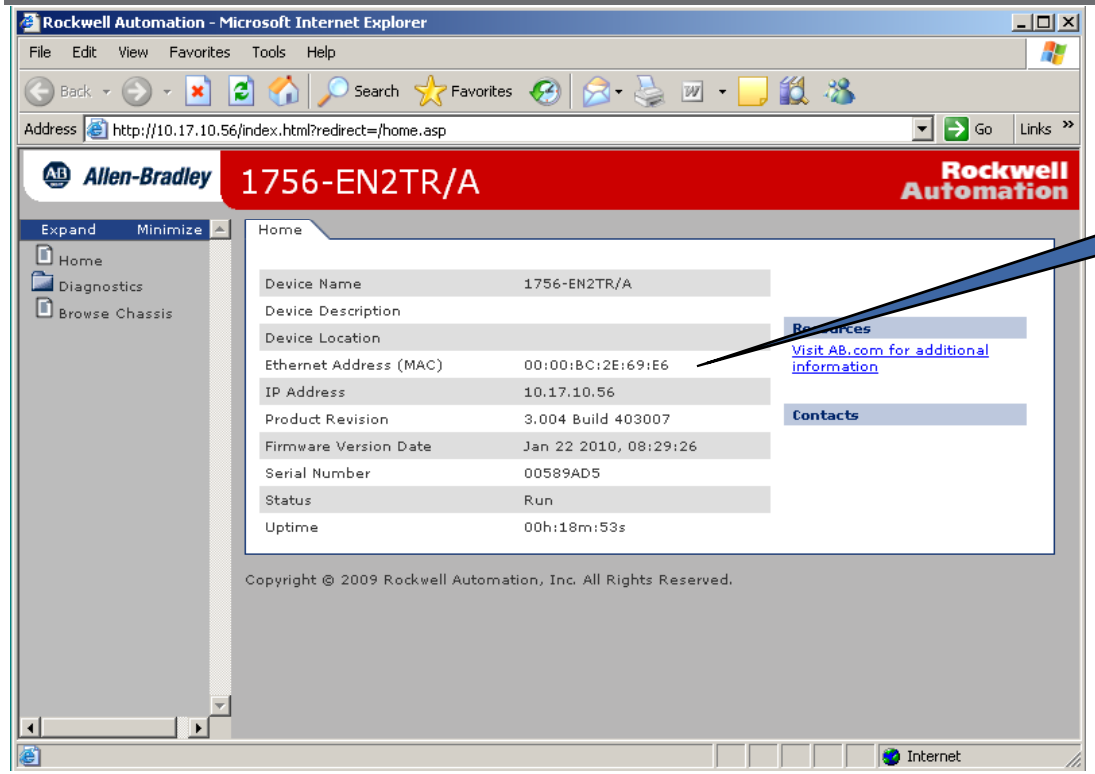


Layer 2 – Data Link
Switching Options

- Industrial versus Commercial
  - Panel & DIN Rail Mounting vs. Rack (e.g. 1RU)
- Managed versus Unmanaged

	Advantages	Disadvantages
Managed Switches	• Segmentation services (VLANs) • Diagnostic information • Security services • Prioritization services (QoS) • Multicast management services • Network resiliency • **Loop prevention**	• More expensive • Requires some level of support and configuration to start up
Unmanaged Switches	• Inexpensive • Simple to set up	• No management capabilities • No security • No diagnostic information • Difficult to troubleshoot • No resiliency support • No loop prevention

Layer 2 - Data Link
EN2TR Example



EN2TR Webpage
MAC Address

Media Counters Port 1	
Alignment Errors	0
FCS Errors	0
Single Collisions	0
Multiple Collisions	0
SQE Test Errors	0
Deferred Transmissions	0
Late Collisions	0
Excessive Collisions	0
MAC Transmit Errors	0
Carrier Sense Errors	0
Frame Too Long	0
MAC Receive Errors	0

Media Counters:

Current Port: 1

Counter Name	Value	Counter Name	Value
Alignment Errors	0	Late Collisions	0
FCS Errors	0	Excessive Collisions	0
Single Collisions	0	MAC Transmit Errors	0
Multiple Collisions	0	Carrier Sense Errors	0
SQE Test Errors	0	Frame Too Long	0
Deferred Transmissi	0	MAC Receive Errors	0

RSLinx Classic
EN2TR Diagnostics
Ethernet Statistics

EN2TR Webpage
Ethernet Statistics

Layer 3 - Network
Internet Protocol (IP) Packet

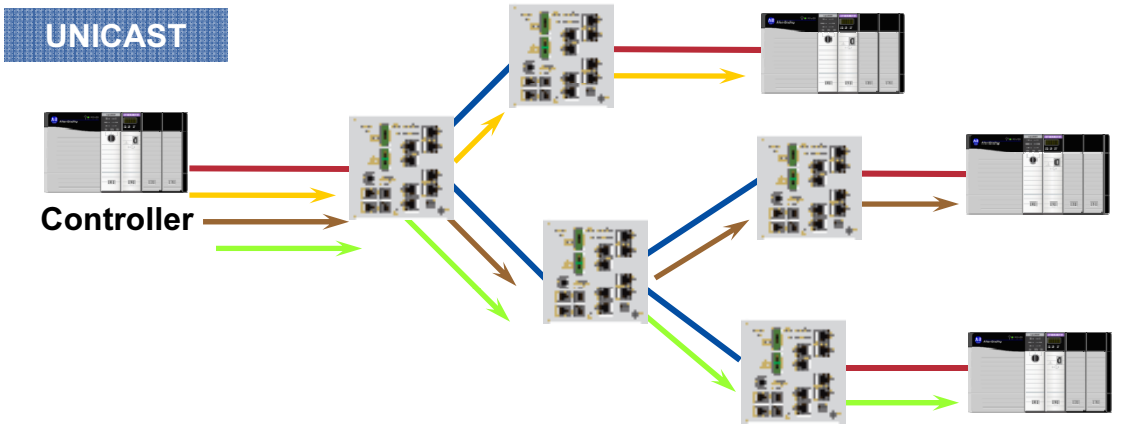
- This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node.
- Routing and forwarding are functions of this Layer, as well as addressing, and internetworking.
- IP Address, Subnet Mask, Default Gateway
- Layer 3 Protocol Examples:
  - ICMP – Internet Control Message Protocol
  - IPsec – Internet Protocol Security
  - IGMP – Internet Group Management Protocol
- Routed protocol vs. Routing Protocol vs. Router Redundancy
- Layer 3 Services Examples
  - QoS – Quality of Service, Resiliency, Security

Layer 3 - Network
LAN Transmission Methods

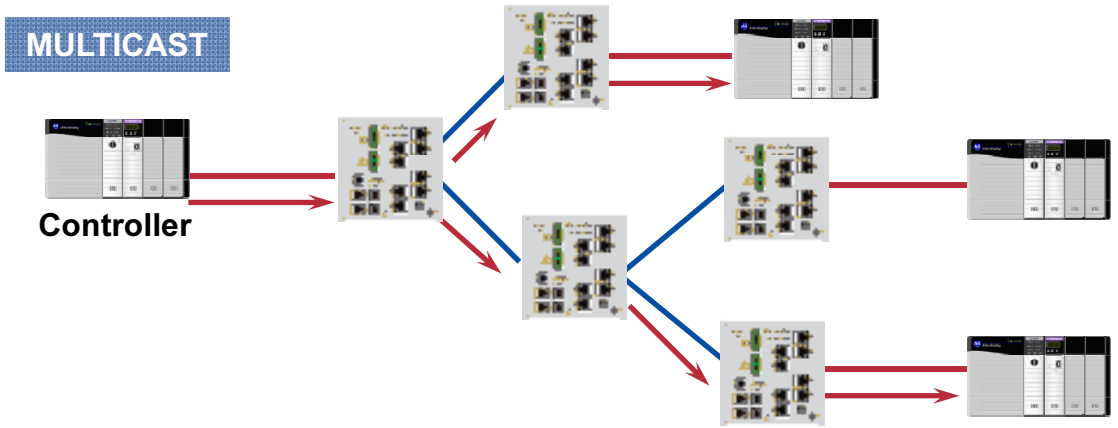
- Unicast
  - A method by which a packet is sent to a single destination.
- Multicast
  - A technique that allows copies of a single packet to be passed to a selected subset of possible destinations
  - 224.0.0.0 - 239.255.255.255
  - EtherNet/IP IP Multicast Address Range:
    - 239.192.0.0 - 239.195.255.255
- Broadcast
  - A packet delivery system that delivers a given packet to all hosts on the LAN.
  - 255.255.255.255

Layer 3 - Network
LAN Transmission Method - Examples

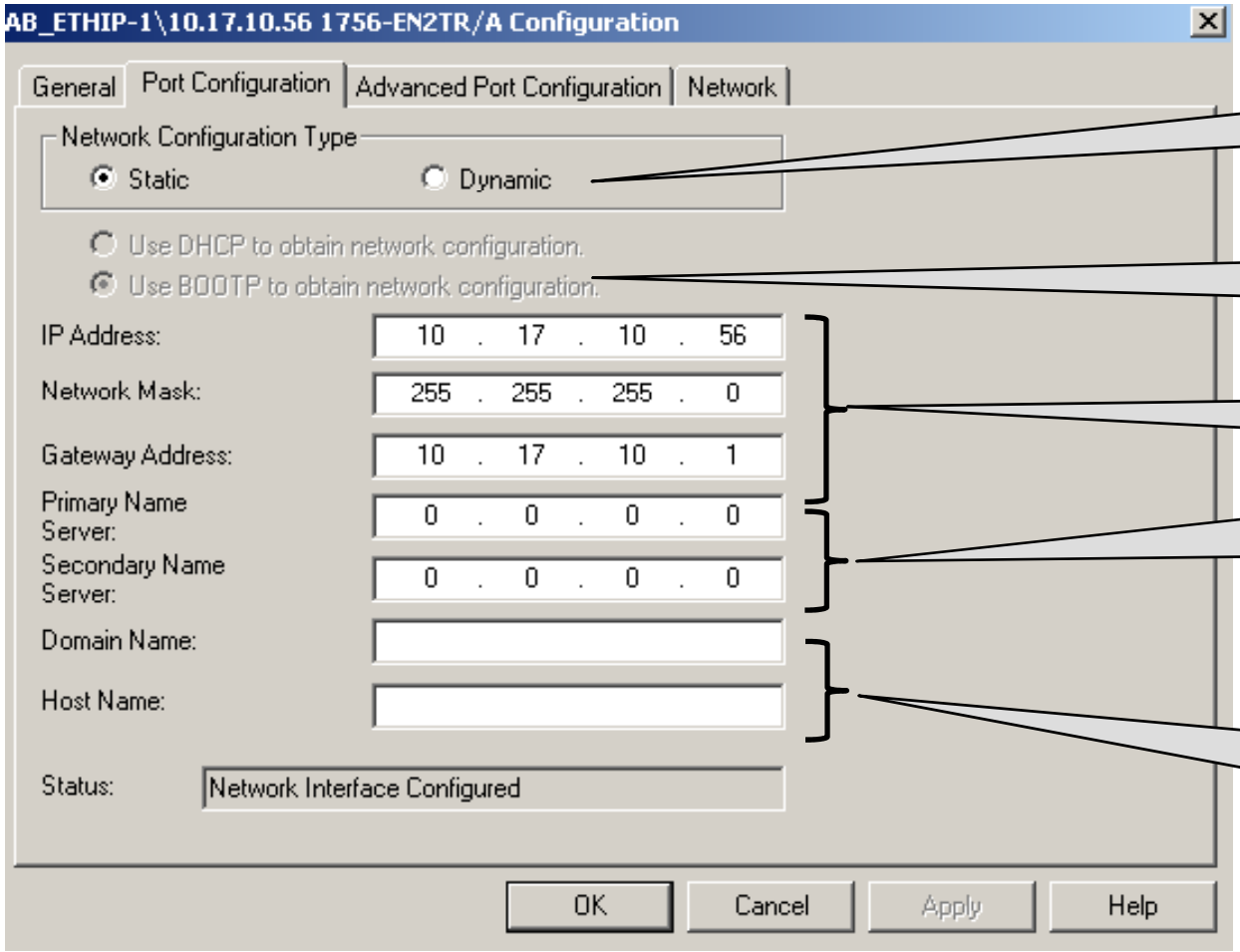
One-to-one, individual transactions:
Example – Logix Message Instruction, Logix P/C Connection



One-to-many, single transaction:
Examples – IP Multicast, IP Surveillance, Webcast Streaming



Layer 3 - Network
Internet Protocol Address



Fixed or assigned from a pool?

What type of server? If assigning from a pool

Unique Network Identity

Resolves Hostnames to IP addresses on the network

"User-Friendly" Name to identify a node on the network

Layer 3 – Network
IP Addressing Schema

Option	Description	Advantages	Disadvantages
Static Hardware	Devices hard coded with an IP Address	Simple to commission and replace	In large environments, can be burdensome to maintain Limited ranged of IP addresses and subnet Not all devices support
Static via BOOTP Configuration	Server assigns devices IP addresses Precursor to DHCP	Supported by every device	Requires technician to configure IP address/MAC address when a device is replaced Adds complexity and point of failure
DHCP	Server assigns IP addresses from a pool (NOT RECOMMENDED for industrial devices)	Efficient use of IP address range Can reduce administration work load	More complex to implement and adds a point of failure Devices get different IP addresses when they reboot
DHCP Option 82	Server assigns consistent IP addresses from a pool (NOT RECOMMENDED)	Efficient use of IP Address range Can reduce administration work load	More complex to implement and adds a point of failure Mixed environments may not work
DHCP port-based allocation	Automatically assign IP address per physical switch port	Efficient use of IP Address range Eases commissioning and maintenance in large environments	Requires some maintenance and upkeep, on a per switch basis

Layer 3 – Network
IP - Addressing

- Internet Protocol Version 4 – IPv4
- IP addresses are unique in the internet. This allows devices on networks throughout the world to be interconnected
- IP addresses are actually 32 bit address that are normally grouped into 4 bytes to make them easier to read. For example, an IP address of:

  129 . 8 . 128 . 31

- Is actually:

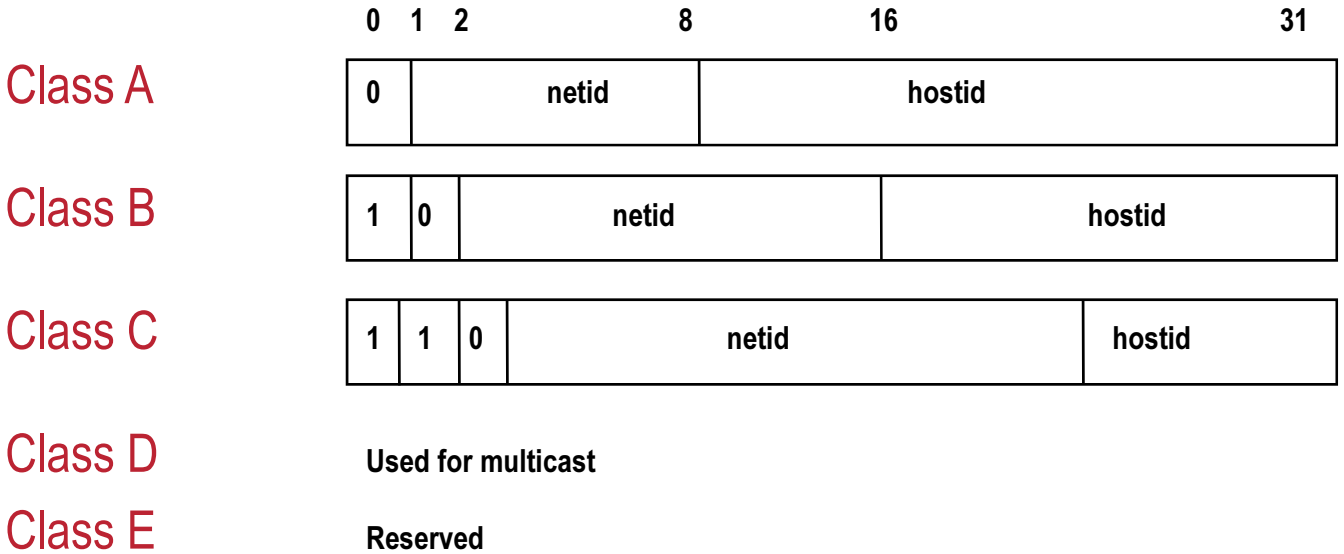
  10000001 00001000 10000000 00011111

  (binary 129) (binary 8) (binary 128) (binary 31)

- IP addresses are also broken down into classes. Each class of IP address identifies what part of the total IP address is used to identify the network it is on, and what part of the IP address is used to identify the end device on that network.

Layer 3 - Network
IP - Addressing

- The 4 classes of addresses are shown below:



- Range of first byte values for the 4 classes:

Class A	1 – 127	ex: 127.100.4.56
Class B	128 – 191	ex: 130.151.195.9
Class C	192 – 223	ex: 192.120.2.6
Class D	224 – 248	ex: 233.5.11.56

Layer 3 – Network
IP – Subnet Mask

- Subnet Mask: Used to determine if a message is for a node on the local network, or it must be routed to a remote network. All nodes on the local network must have the same subnet mask.

255.255.0.0

- Subnet masks are also really 32 bit numbers that are represented as 4 bytes to make them easier to read. This subnet mask is actually:

11111111	**11111111**	**00000000**	**00000000**
(binary 255)	(binary 255)	(binary 0)	(binary 0)

- Wherever a “1” appears in the subnet mask, it is identifying that the corresponding bit in the IP address is part of the network address. The subnet mask is used to compare 2 IP addresses together to determine if they are on the same network.

Layer 3 - Network
Private IP Addresses

- Private addresses are special IP addresses that can be used by anyone. Information from devices with private addresses does not get routed on the Internet, so there is not a conflict with multiple enterprises using the same private addresses.
- Private addresses:
  - Do not require registration or approval from an Internet registry.
  - Greatly expand the number of available IP addresses to an enterprise
  - Help address the problem of a lack of available IP addresses
- Private address ranges:

  10 .0 . 0 .0 – 10.255.255.255

  172.16.0.0 – 172.31.255.255

  192.168.0.0 – 192.168.255.255

Layer 3 - Network
IPv4 vs. IPv6 Packet

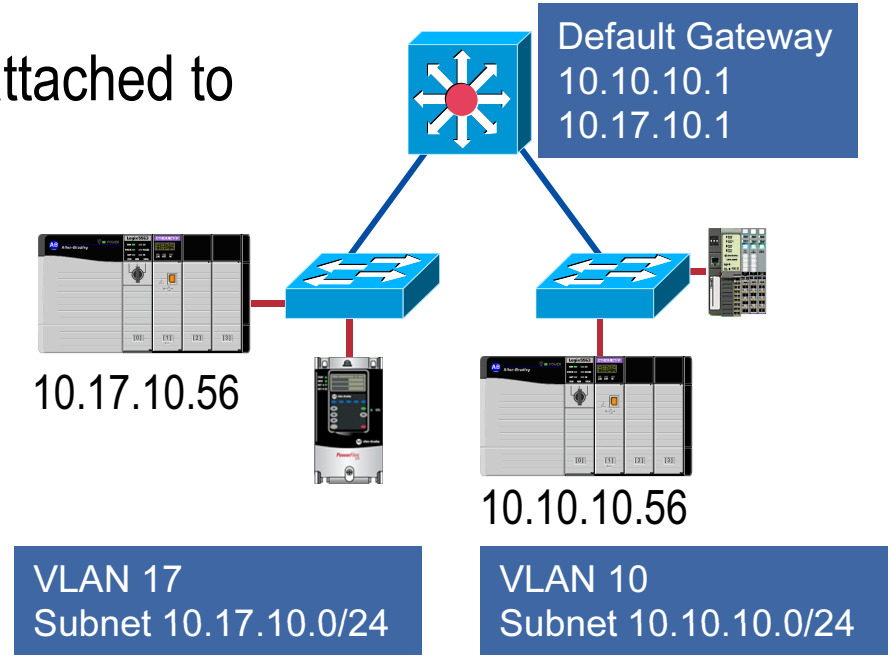
- Internet Engineering Task Force (IETF)
- IPv4
  - 10.10.10.10, 32-bit address, 4 bytes, 2^{32} addresses
  - IPsec is optional
  - Unicast, Multicast, and Broadcast
  - QoS – Differentiated Services Code Point
- IPv6
  - 1080:0:0:0:8:800:200C:417A, 128-bit address, 16 bytes, 2^{128} addresses
  - IPsec is not optional
  - Unicast, Multicast, and Anycast
  - QoS - Flow classes and flow labels
  - Address Scoping (reachability)
    - Node-local …. example – loopback address
    - Link-local …. local link only, automatically configured (based on MAC with IPv6 prefix)
    - Global …. globally routable

Layer 3 - Network
IP - Default Gateway

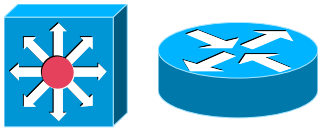
- Gateways and Routers use the network portion of IP addresses to identify where networks are
- Stratix 8300 – Layer 2 and Layer 3 switching
- A table is kept that tells the device which port a message should be transmitted out in order to get the message to the proper network.
- If the particular network is not directly attached to that device, it will simply forward the message to the next gateway or router in the path for further routing.
- Time-to-live (TTL)
  - RA EtherNet/IP implementation for multicast – TTL=1
  - RA EtherNet/IP implementation for unicast – TTL=64

Routing Table

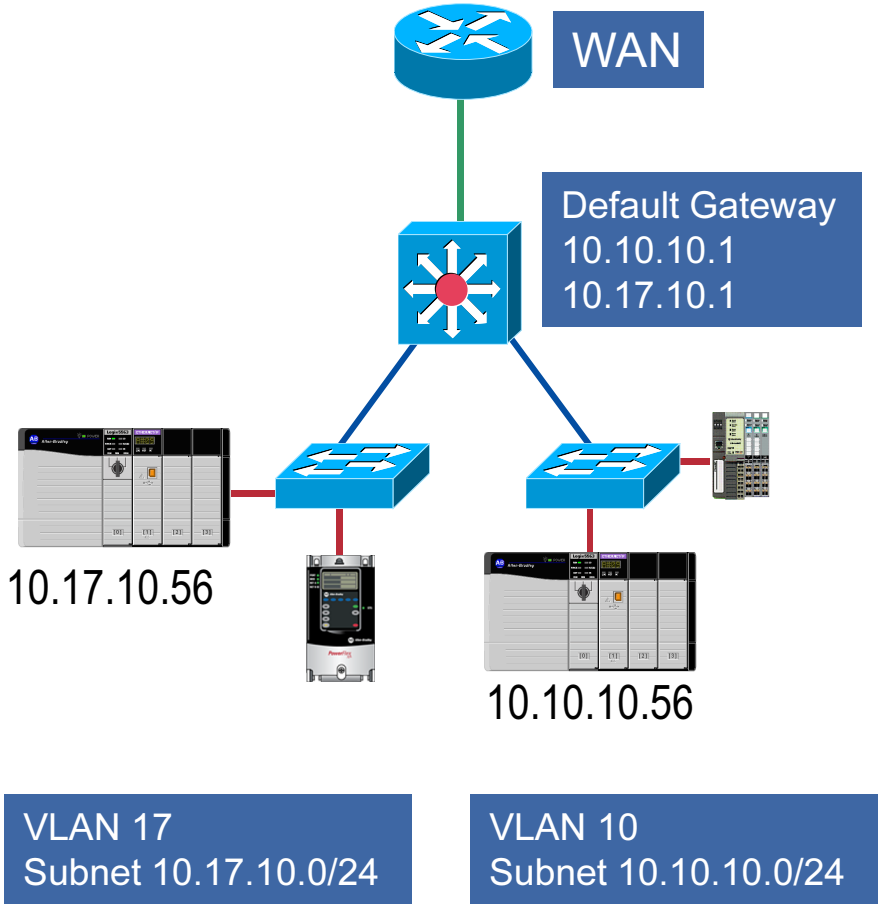
Network	Port
10.17.10.0	1
10.10.10.0	2



Layer 3 - Network
Routing

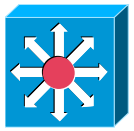


- Switch/route packets by IP Address
- Extend network distance
  - LAN, MAN, WAN
- Connect different LANs
  - Broadcast control
  - Multicast control, EtherNet/IP multicast not routable - TTL=1
- Layer 3 features such as security, QoS, resiliency, etc.
- Make sure IT understands required protocols
  - Is there a need to route to other subnets?
  - Multicast traffic?
  - Security or segmentation?



Layer 3 – Network
Switching vs. Routing

WANs



LANs

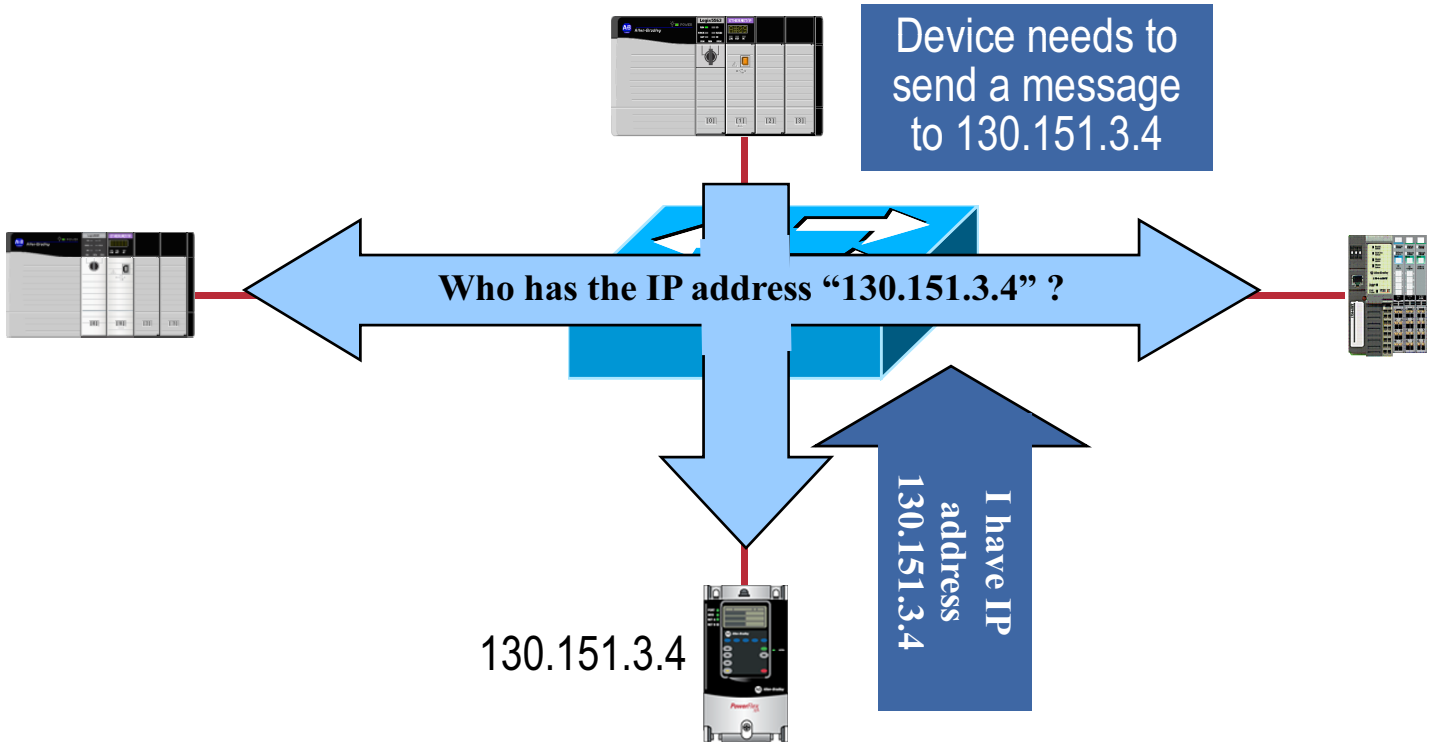
- Layer 3 - Router
  - Connects WANs
  - Scalable
  - Pro: Rich set of routing protocols, applications and functionality: VPN, security, and multi-service capabilities
  - Con: Path determination calculations slow down the router
  - Building maps and giving direction based on Layer 3 characteristics
- Layer 3 - Switch
  - Connects LANs, inter-VLAN routing
  - Fixed
  - Pro: Faster path determination
  - Con: Limited set of protocols and applications supported
  - Forwarding frames based on Layer 2 characteristics

Layer 3 - Network
Router and Routing

- Routed protocols
  - Examples:
    - Internet Protocol (IP)
    - Novel Netware Internetwork Packet Exchange (IPX)
- Routing Protocols
  - Routers talking to routers
  - Maintaining optimal network topology/path to subnets, and forwarding packets along those paths – static and dynamic routes
  - Examples:
    - OSPF – Open Shortest Path First, IETF Standard (Link-State Routing)
    - EIGRP – Enhanced Interior Gateway Routing Protocol, Cisco innovation (Distance Vector Routing)
- Router Redundancy Protocols
  - Fault tolerance for default gateways
  - Examples:
    - VRRP – Virtual Router Redundancy Protocol, IETF Standards
    - HSRP – Hot Standby Router Protocol , Cisco innovation
    - GLBP – Gateway Load Balancing Protocol , Cisco innovation

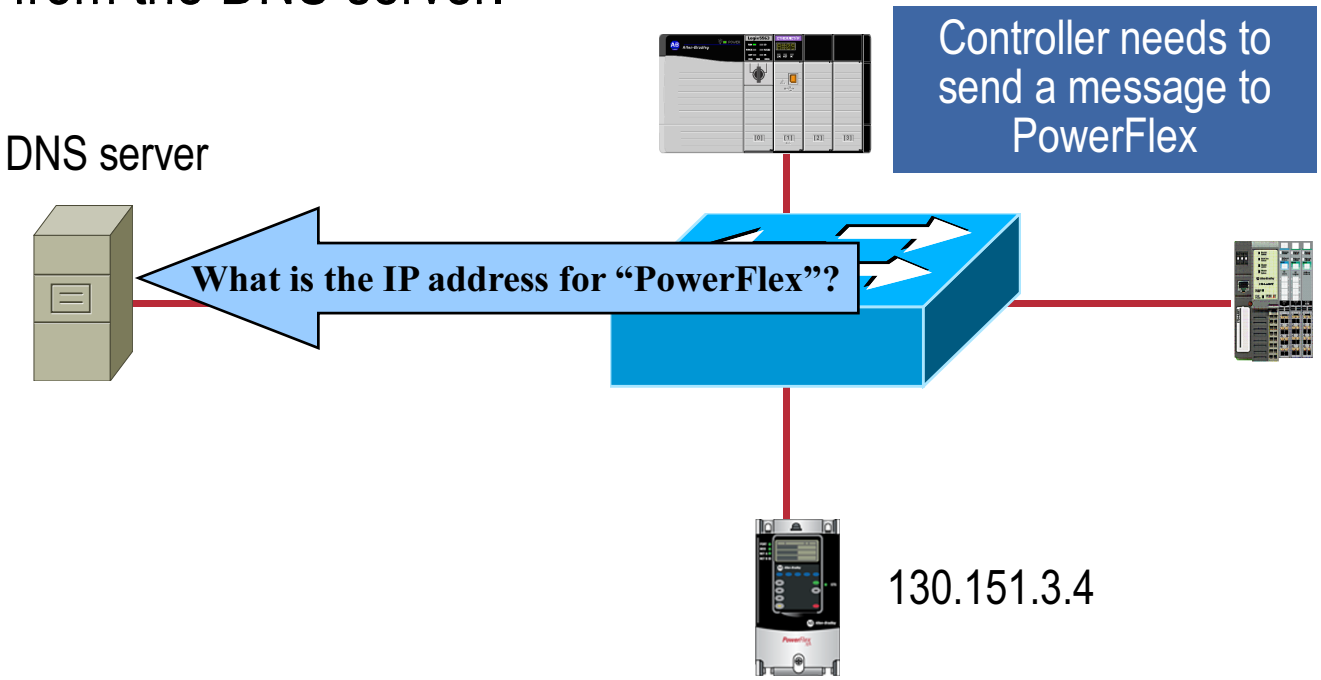
Layer 3 - Network
Address Resolution Protocol - ARP

- An ARP request is a broadcast message that asks “who has this IP address?”. The device which has that IP address will respond and the requestor will then add the IP address / hardware address pair to its ARP cache. The original device can now send the message.



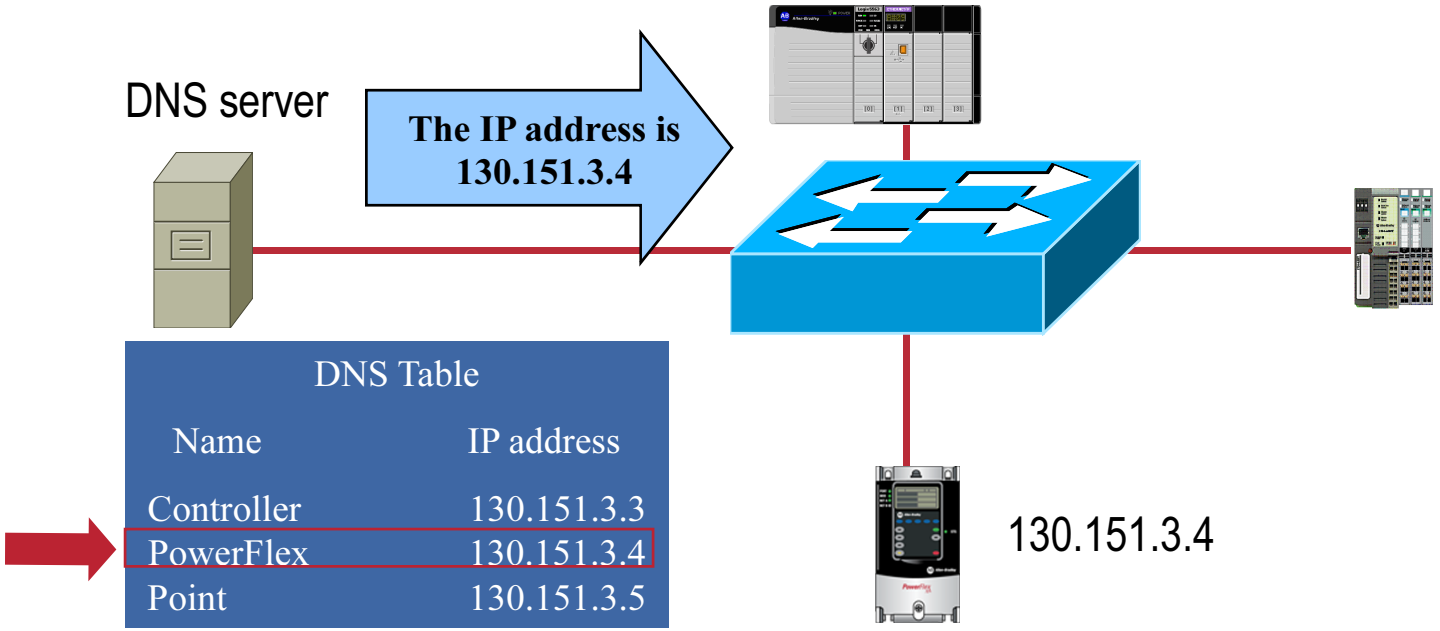
Layer 3 - Network
Domain Name System - DNS

- DNS is a name resolution protocol that allows users to identify devices by names rather than IP addresses. In order for DNS to work, a DNS server is configured to hold a table of names and the associated IP addresses. When a device attempts to send a message to a device with an unknown name, it will request the IP address of the named device from the DNS server.



Layer 3 - Network
Domain Name System - DNS

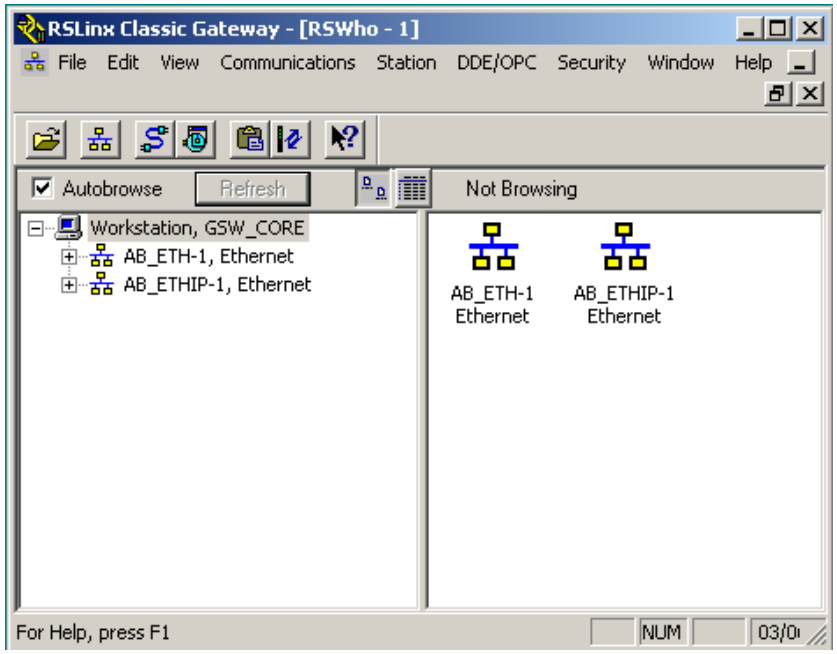
- The DNS server will refer to it's table and send back an IP address for the requested name. Once the client device receives the IP address for a name, it will store it in it's own table so it does not have to ask for the IP address every time. The device may still have to do an ARP request, since it must ultimately decode the IP address into a hardware address.



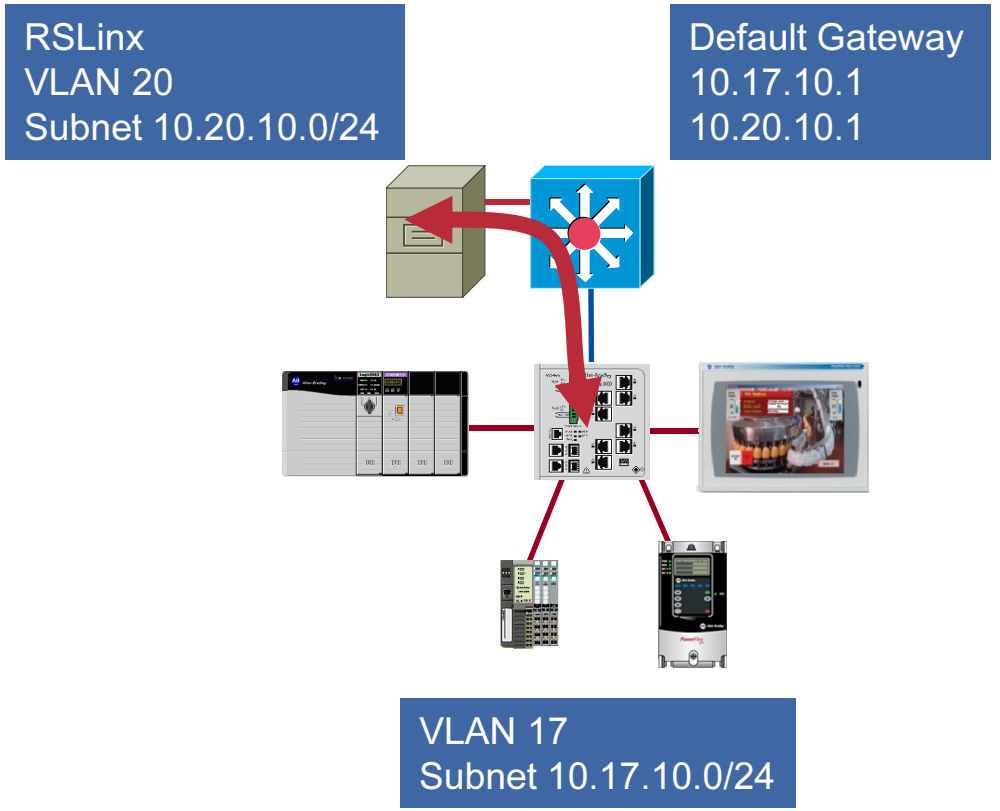
Layer 3 – Network
Network Address Translation (NAT)

- NAT allows a single device, commonly a router, to act as an agent between the Internet (public network) and the private network. This means that only a single, unique IP address is required to represent an entire group of computers.
- RFC 1631 and RFC 1918 describe NAT
- Can take a number of different forms and work in several different ways, but mapping and lookup tables are the basic tools behind NAT.
- NAT operates at the Network Layer (Layer 3) of the OSI model

Layer 3 - Network
RSLinx and Layer 3 Devices

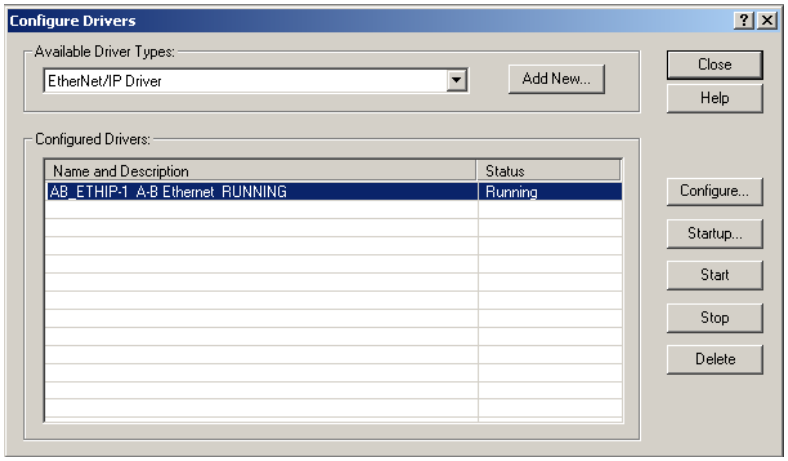


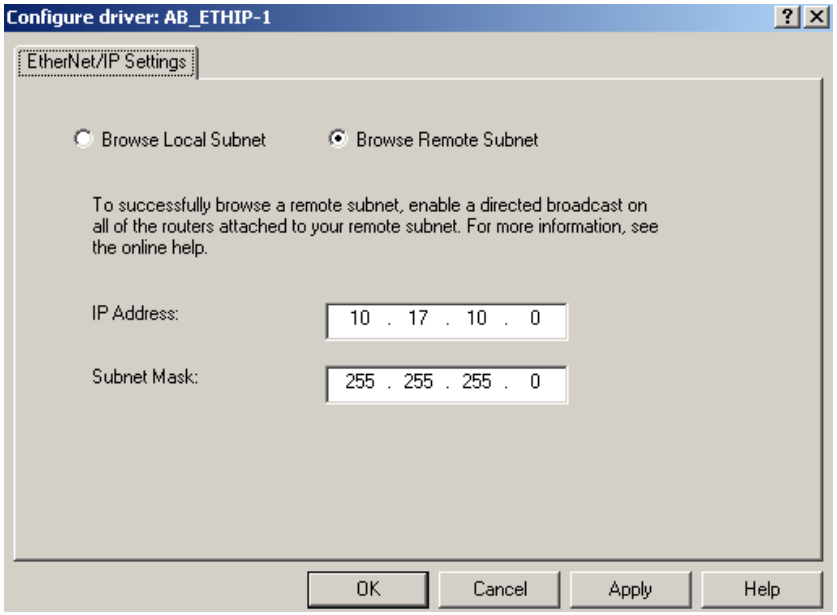
- RSLinx Classic
  - Ethernet Devices Driver
    - Manual entering of IP addresses
  - EtherNet/IP Driver
    - Autobrowse (broadcast)

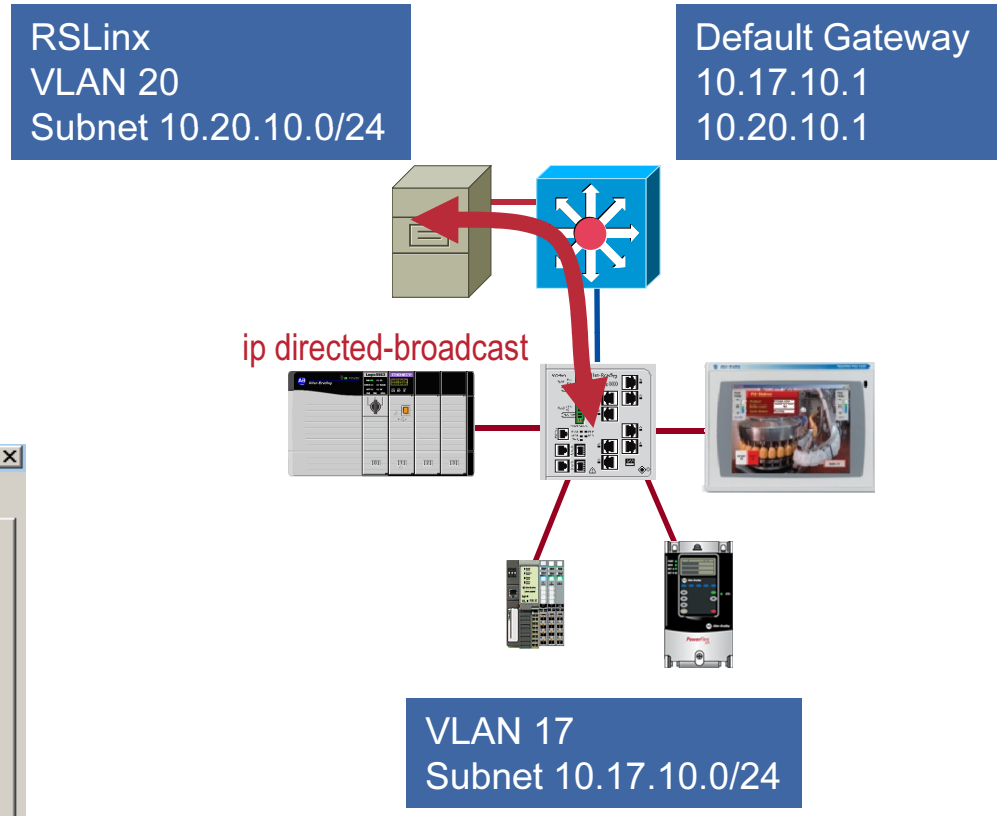


- For either driver, specify Default Gateway within the EtherNet/IP devices and the RSLinx platform

Layer 3 - Network
RSLinx and Layer 3 Devices





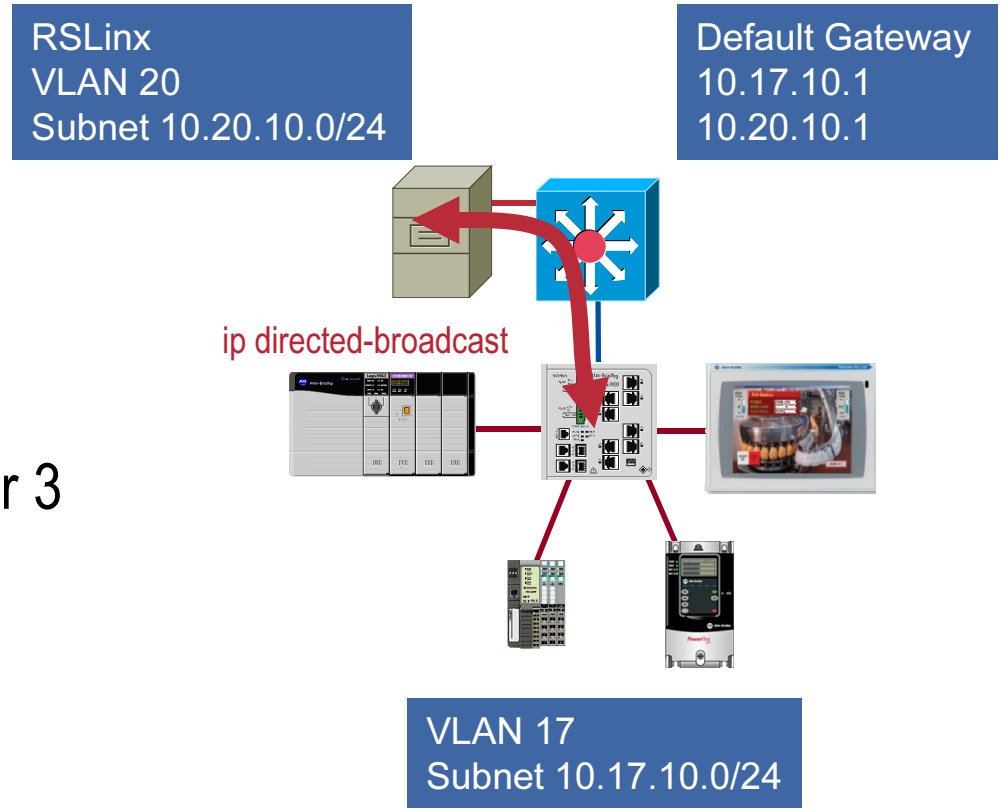


- For EtherNet/IP driver, configure Browse Remote Subnet

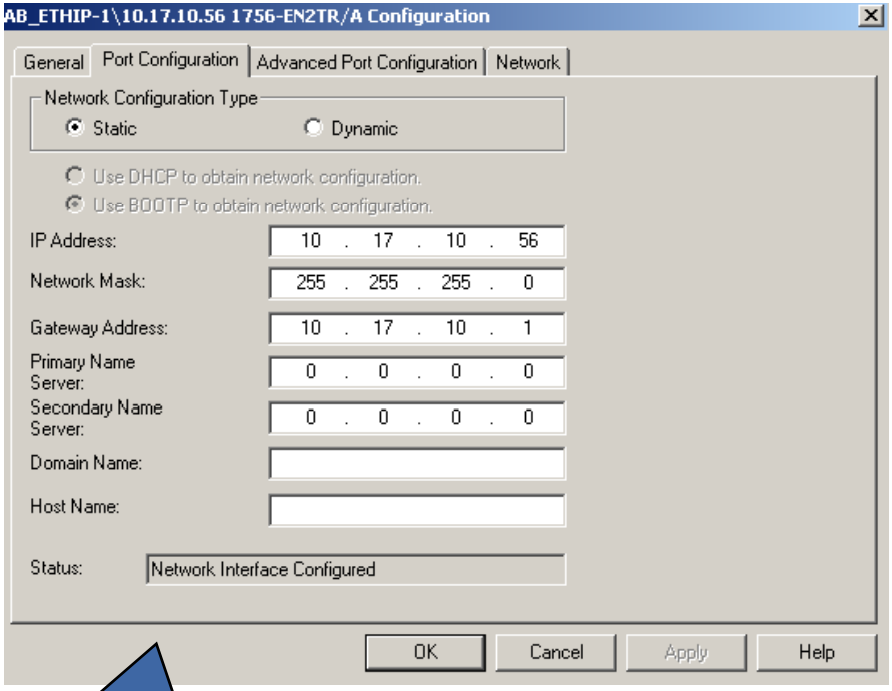
Layer 3 - Network
RSLinx and Layer 3 Devices

&

- For EtherNet/IP driver, enable IP Directed Broadcast on Cisco Layer 3 Device (disabled by default)
  - ip directed-broadcast [access-list-number] … CLI command
- RSLinx Enterprise
  - No support for IP Directed Broadcast, must manually enter IP addresses

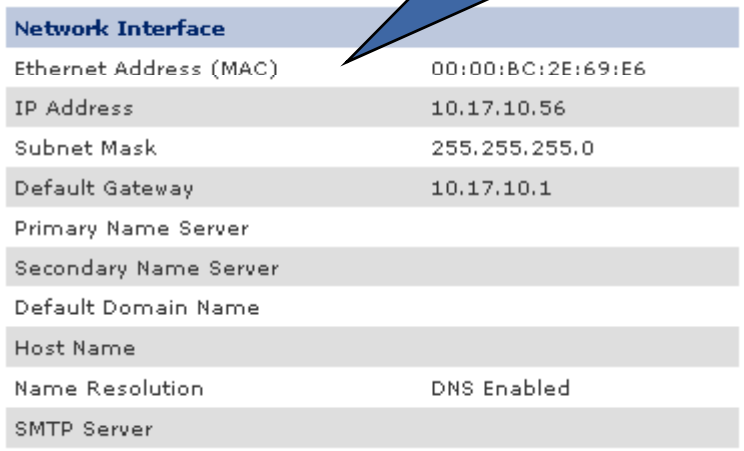


Layer 3 - Network
EN2TR Example

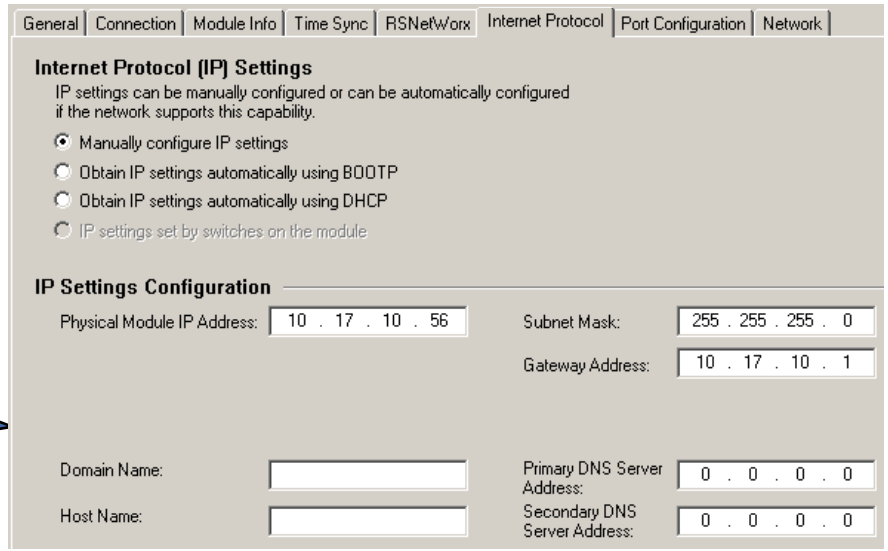


RSLinx Classic Module Configuration

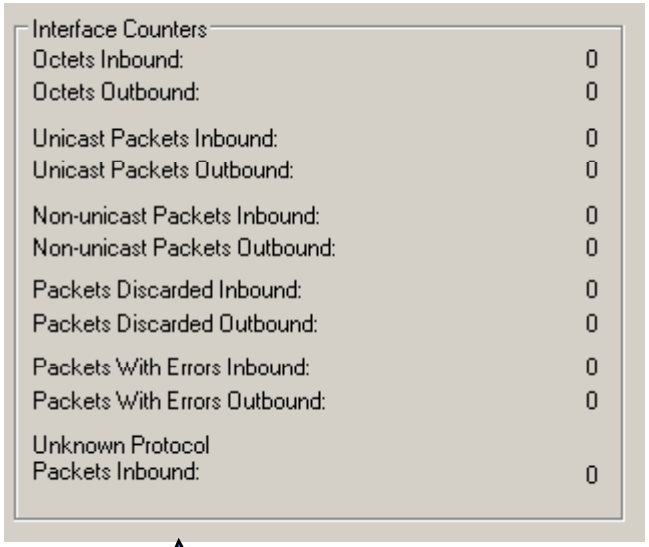
EN2TR Webpage Network Settings



RSLogix 5000 EN2TR Properties



Layer 3 - Network
EN2TR Example



RSLogix 5000
EN2TR Properties
Port Diagnostics

EN2TR Webpage
ARP Table

ARP Table

Physical Address	Net Address
00:00:00:00:00:00	10.17.10.50
00:00:00:00:00:00	10.17.10.51
00:00:00:00:00:00	10.17.10.52
00:00:00:00:00:00	10.17.10.54
00:00:00:00:00:00	10.17.10.57
00:00:00:00:00:00	10.17.10.58
00:00:00:00:00:00	10.17.10.60
00:00:00:00:00:00	10.17.10.62
00:00:00:00:00:00	10.17.10.64
00:00:00:00:00:00	10.17.10.66
00:00:00:00:00:00	10.17.10.68
00:00:00:00:00:00	10.17.10.70
00:00:00:00:00:00	10.17.10.72
00:24:E8:B3:8A:81	10.17.10.100
00:00:00:00:00:00	10.17.10.104

IP Statistics

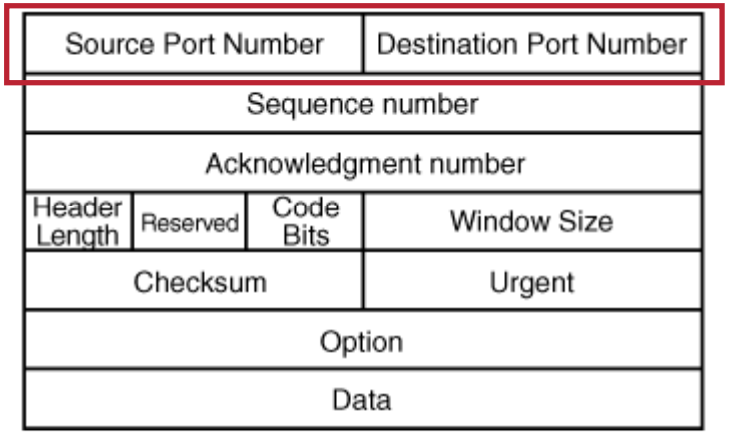
Forwarding	1
Default TTL	64
In receives	59092
In header errors	0
In address errors	280
Forwarded datagrams	0
Unknown protocols	0
In discards	0
In delivers	57553
Out requests	56226
Out discards	0
Out no routes	0
Reassembly timeout	20
Reassemblies requested	0
Reassemblies OK	0
Reassemblies failed	0
Reassemblies fragment OKs	0
Reassemblies fragment fails	0
Reassemblies fragment creates	0
Reassemblies routing discards	0

EN2TR Webpage
IP Statistics

Layer 4 - Transport
Segment

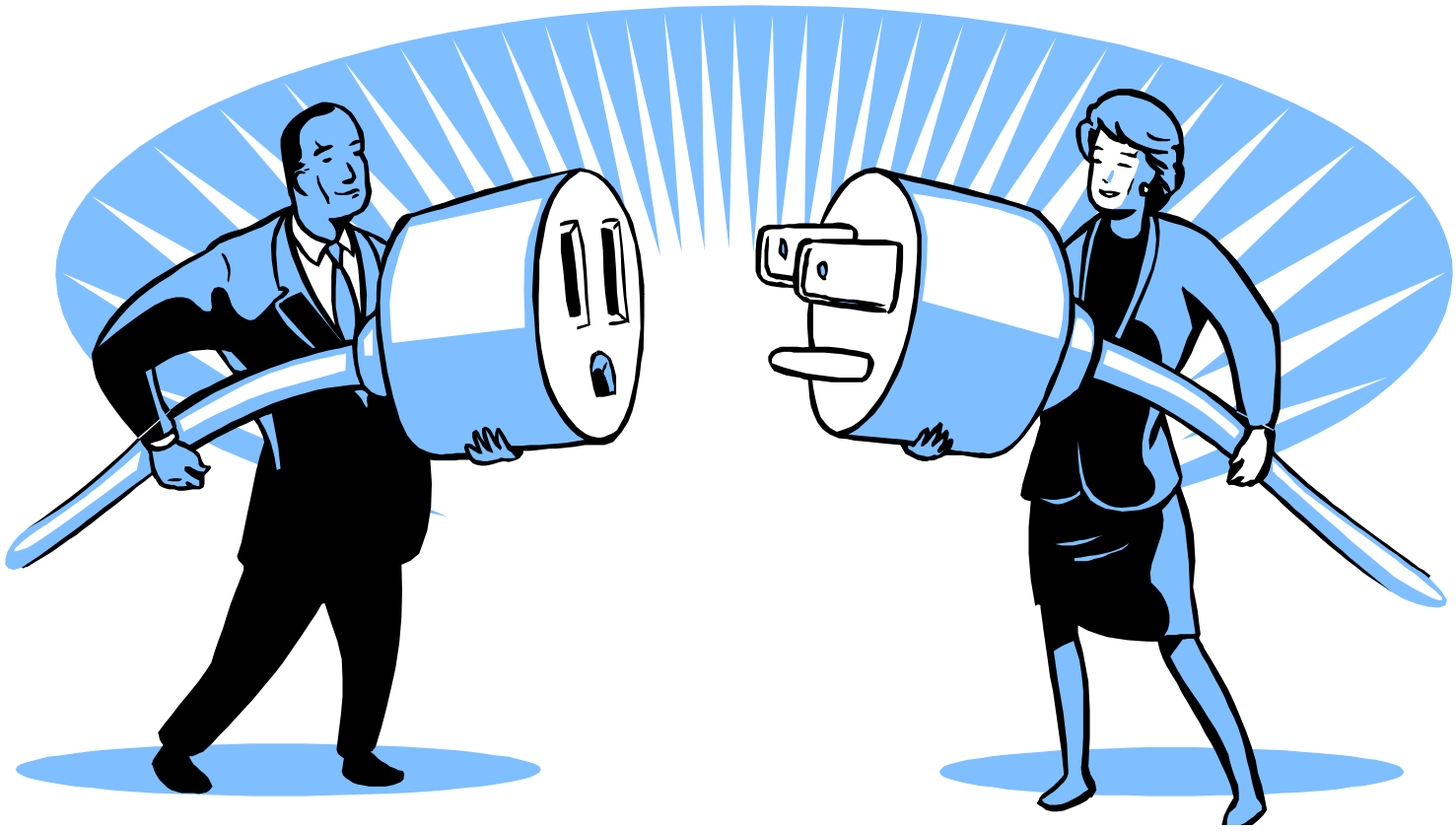
- This layer provides transparent transfer of data between end systems, or devices, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.
- User Datagram Protocol - UDP
  - Connectionless/best effort
  - Does not use acknowledgements
  - IP - Unicast and Multicast
  - CIP – used for Class 1 (Implicit) I/O and P/C connections – port 2222
- Transmission Control Protocol - TCP
  - Connection-oriented, end-to-end reliable transmission
  - Utilizes acknowledgements (ACK) to ensure reliable delivery
  - IP - Unicast
  - CIP – used for Class 3 (Explicit) messaging such as Operator Interface – port 44818

UDP Header



TCP Header

Layer 4 - Transport
Ports and Sockets



KnowledgeBase Answer# 29402

Layer 4 - Transport
ControlLogix Module connection support (partial list)

Communications Module	TCP connections	CIP Connections
1756-ENBT	64	128
1756-EN2T	128	256
1756-EN2TR	128	256
1756-EN3TR	128	256
1756-EN2F	128	256

ENET-UM001G-EN-P EtherNet/IP Modules in Logix5000 Control Systems
…. provides connection and packet rate specs for modules

Layer 4 - Transport
EN2TR Example

TCP Connections (EtherNet/IP Port)	
Active	12
Maximum Observed	16
Maximum Supported	128

EN2TR Webpage
Diagnostic Overview

EN2TR Webpage
UDP Statistics

UDP Statistics	
In datagrams	3
No ports	1
In errors	0
Out datagrams	4

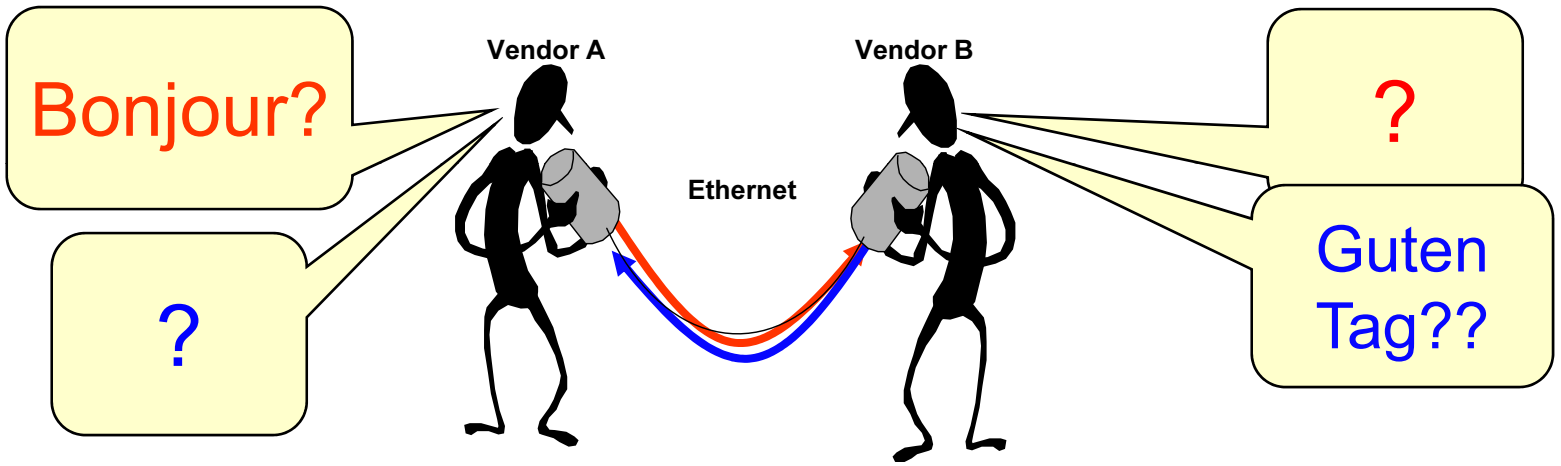
TCP Connection Table

State	Local Address	Local Port	Remote Address	Remote Port
TIME_WAIT	10.17.10.56	80	10.17.10.100	2807
TIME_WAIT	10.17.10.56	80	10.17.10.100	2808
TIME_WAIT	10.17.10.56	80	10.17.10.100	2809
TIME_WAIT	10.17.10.56	80	10.17.10.100	2810
TIME_WAIT	10.17.10.56	80	10.17.10.100	2811
TIME_WAIT	10.17.10.56	80	10.17.10.100	2812
TIME_WAIT	10.17.10.56	80	10.17.10.100	2813
TIME_WAIT	10.17.10.56	80	10.17.10.100	2814
TIME_WAIT	10.17.10.56	80	10.17.10.100	2815
ESTABLISHED	10.17.10.56	80	10.17.10.100	2816
ESTABLISHED	10.17.10.56	44818	10.17.10.100	2004
SYN_SENT	10.17.10.56	53612	10.17.10.72	44818
SYN_SENT	10.17.10.56	53613	10.17.10.104	44818
SYN_SENT	10.17.10.56	53614	10.17.10.68	44818
SYN_SENT	10.17.10.56	53615	10.17.10.60	44818
SYN_SENT	10.17.10.56	53616	10.17.10.62	44818
SYN_SENT	10.17.10.56	53617	10.17.10.50	44818
SYN_SENT	10.17.10.56	53618	10.17.10.54	44818
SYN_SENT	10.17.10.56	53619	10.17.10.58	44818
SYN_SENT	10.17.10.56	53620	10.17.10.66	44818
SYN_SENT	10.17.10.56	53621	10.17.10.64	44818
SYN_SENT	10.17.10.56	53622	10.17.10.70	44818

EN2TR Webpage
TCP Connection

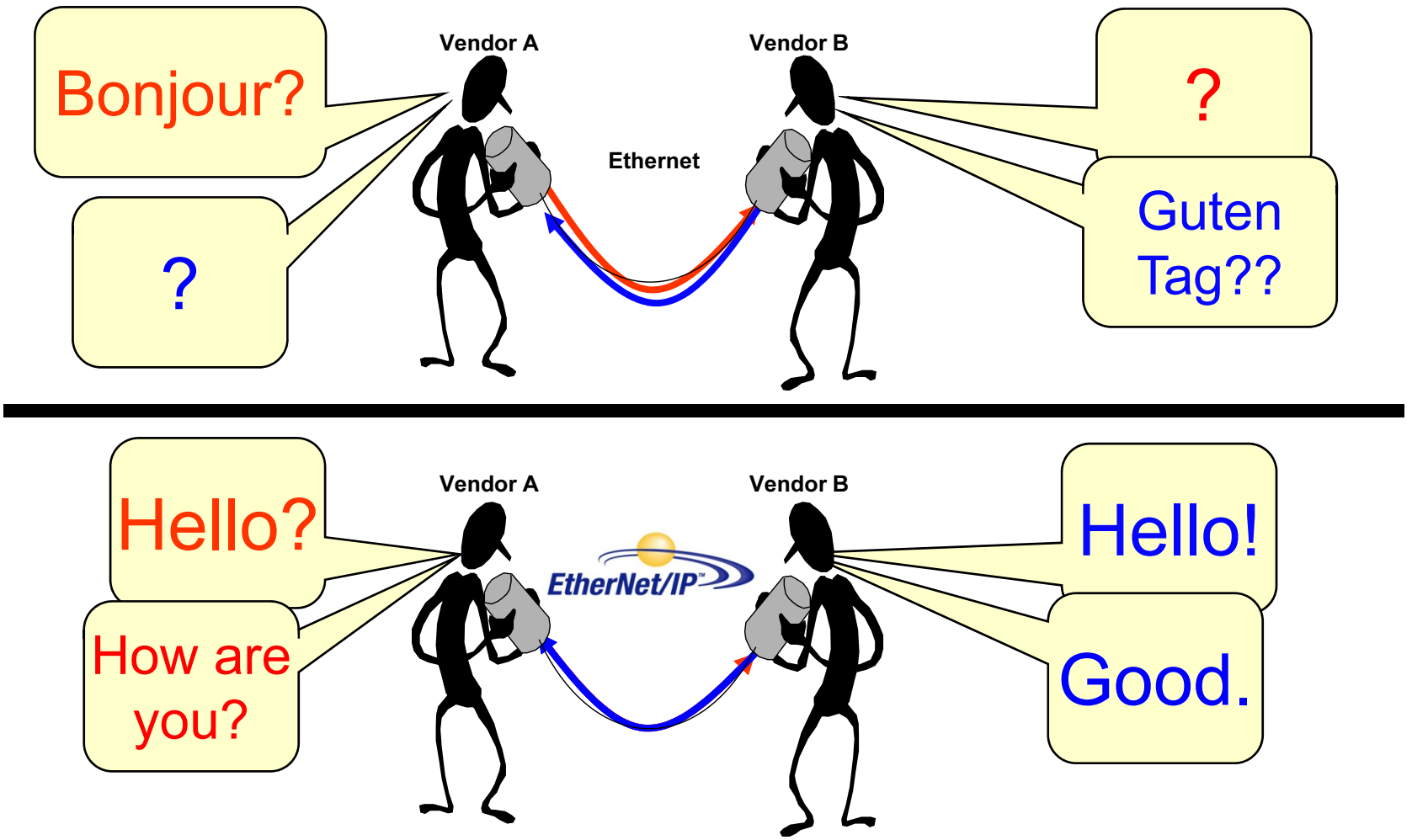
Layer 7 - Application
Common Industrial Protocol

Is Ethernet and TCP/IP Enough?



Ethernet just defines Layers 1 and 2 of Protocol Stack
TCP/IP corresponds to Layers 3 and 4 of Protocol Stack

Layer 7 - Application
Common Industrial Protocol

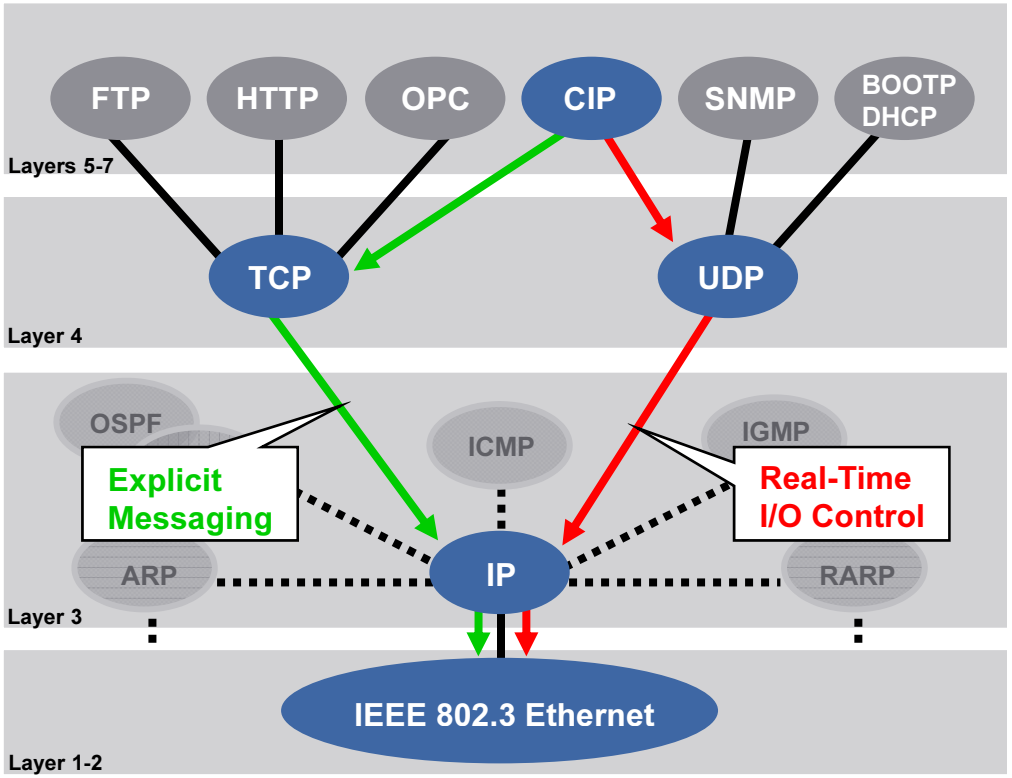


An open, common, standard, and proven language is everything!!

Layer 7 - Application
Common Industrial Protocol

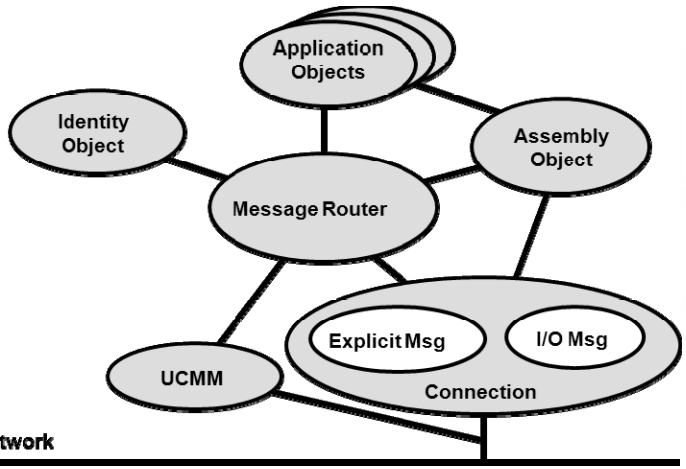
- CIP: Implicit traffic
  - I/O control, drive control, Produced/Consumed tags
  - Uses UDP protocol (unicast and multicast)
- CIP: Explicit traffic
  - HMI, Message Instructions, Program upload/download
  - Uses TCP protocol
- Other common traffic
  - HTTP, Email, SNMP, etc.
- Advantages of EtherNet/IP
  - Standard Ethernet and IP Protocol suite
  - Future proof
  - Established – 280+ registered vendors
  - Supported – All EIP products require conformance testing

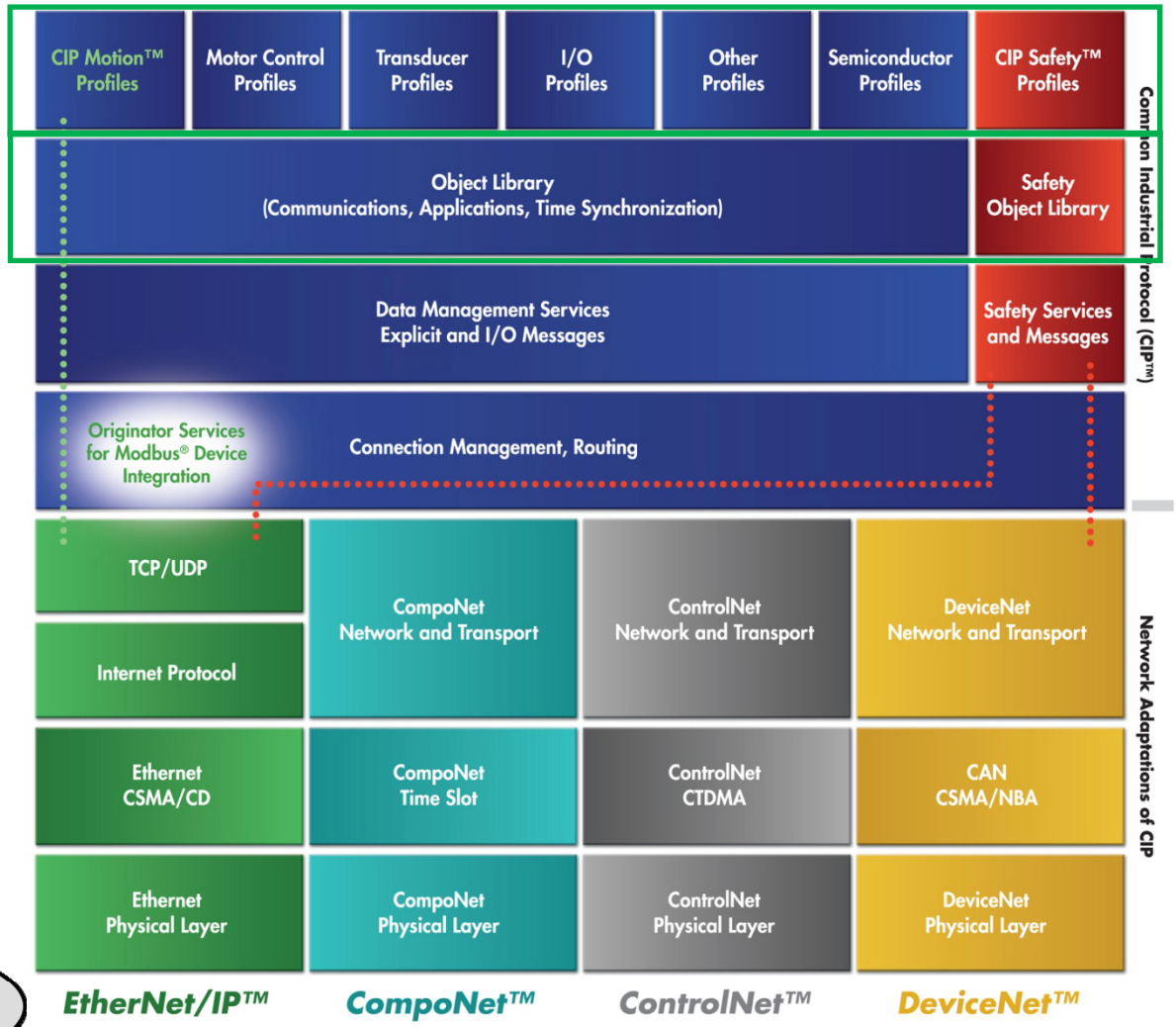
Ethernet/Industrial Protocol or EtherNet/IP specifies how CIP communication packets can be transported over standard Ethernet and TCP/IP technology.



Layer 7 - Application
Common Industrial Protocol

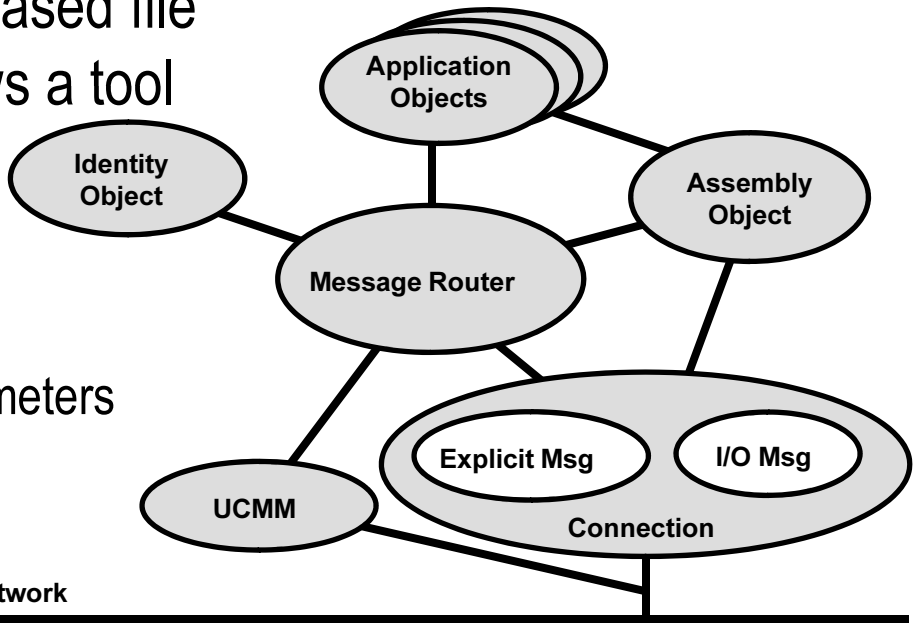
- CIP uses object modeling to describe devices
- Device Profiles define the communication view of a device
- Electronic Data Sheets (EDS)





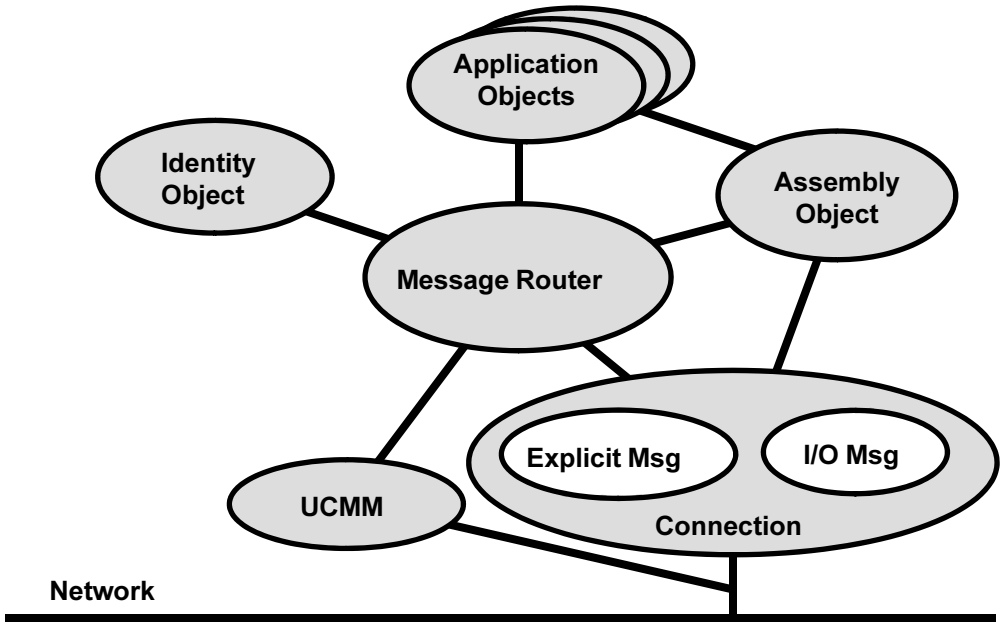
Layer 7 - Application
CIP - Object Modeling

- CIP uses object modeling to describe devices
  - A device is described as a collection of objects
  - Objects divide the functionality of a device into logically related subsets
- Device Profiles define the communication view of a device
  - Purpose is to provide interoperability and interchangeability
  - By using these Device Profiles, devices have a consistent behavior
- Electronic Data Sheets (EDS) - A text based file provided by the manufacturer that allows a tool to learn about the device's:
  - Structure and meaning of I/O data
  - What I/O data transfer types are available
  - Network accessible application config parameters



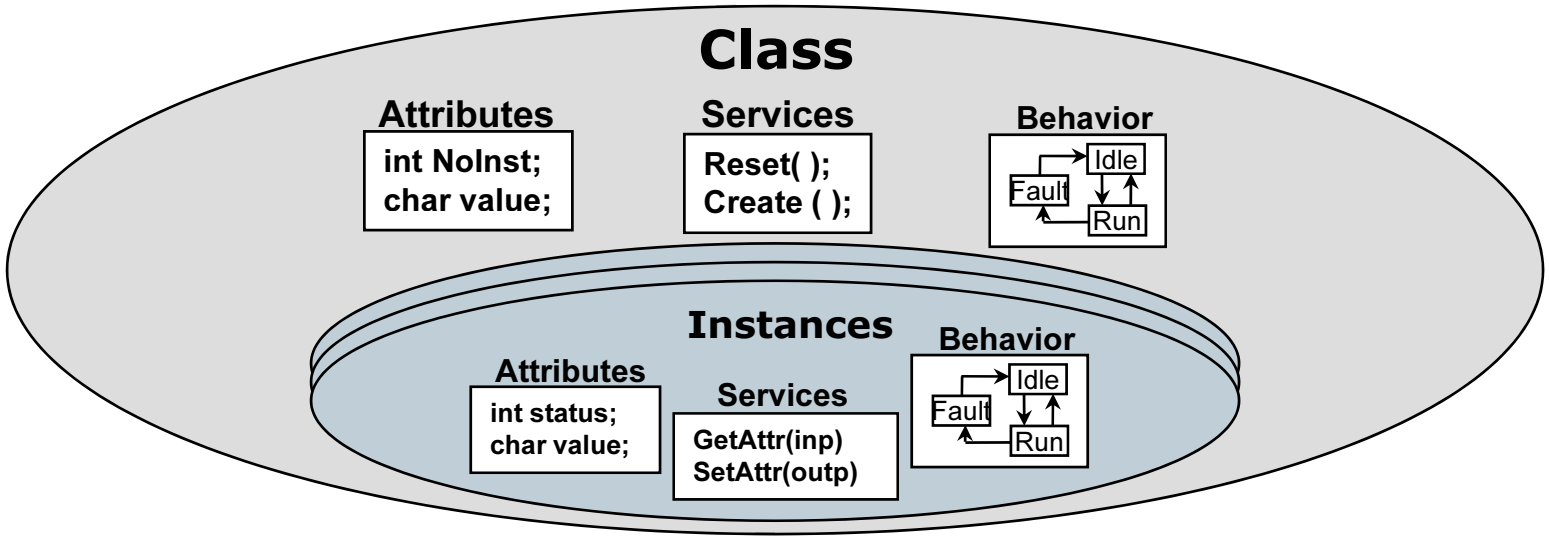
Layer 7 - Application
CIP - Object Modeling

- CIP uses object modeling to describe devices
  - A device is described as a collection of objects
  - Objects divide the functionality of a device into logically related subsets
    - Each with well defined behavior



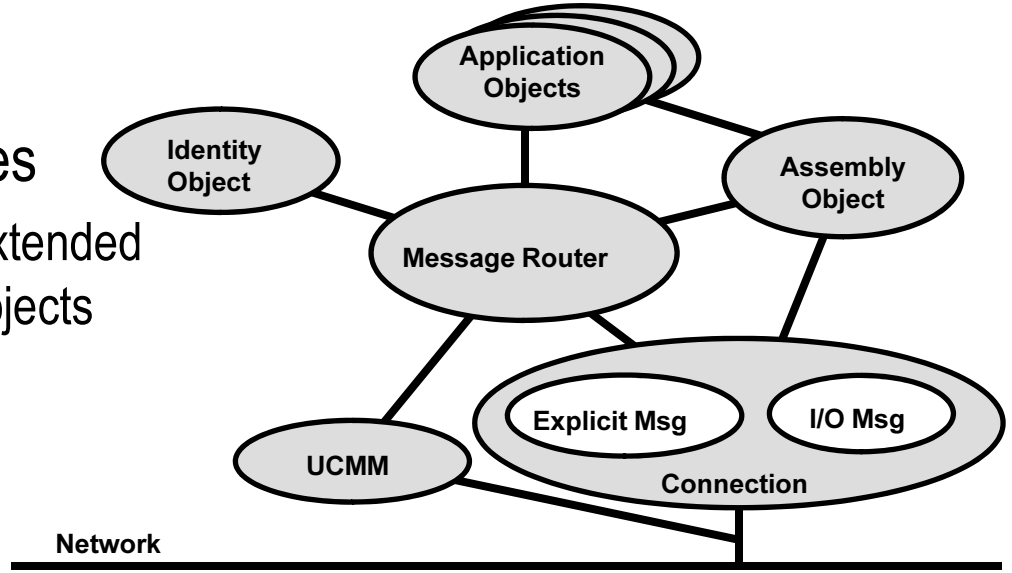
Layer 7 - Application
CIP - Object Class

- Each distinct type of object belongs to a specific *Class*
- Objects that belong to the same class are called *Instances* of that class
- Data items within an object are called *Attributes*
- All attributes can be addressed with Class:Instance:Attribute IDs
- *Services* are explicit tasks that an object performs
  - These may be directed at a specific instance or at the class, which affect all instances of the class



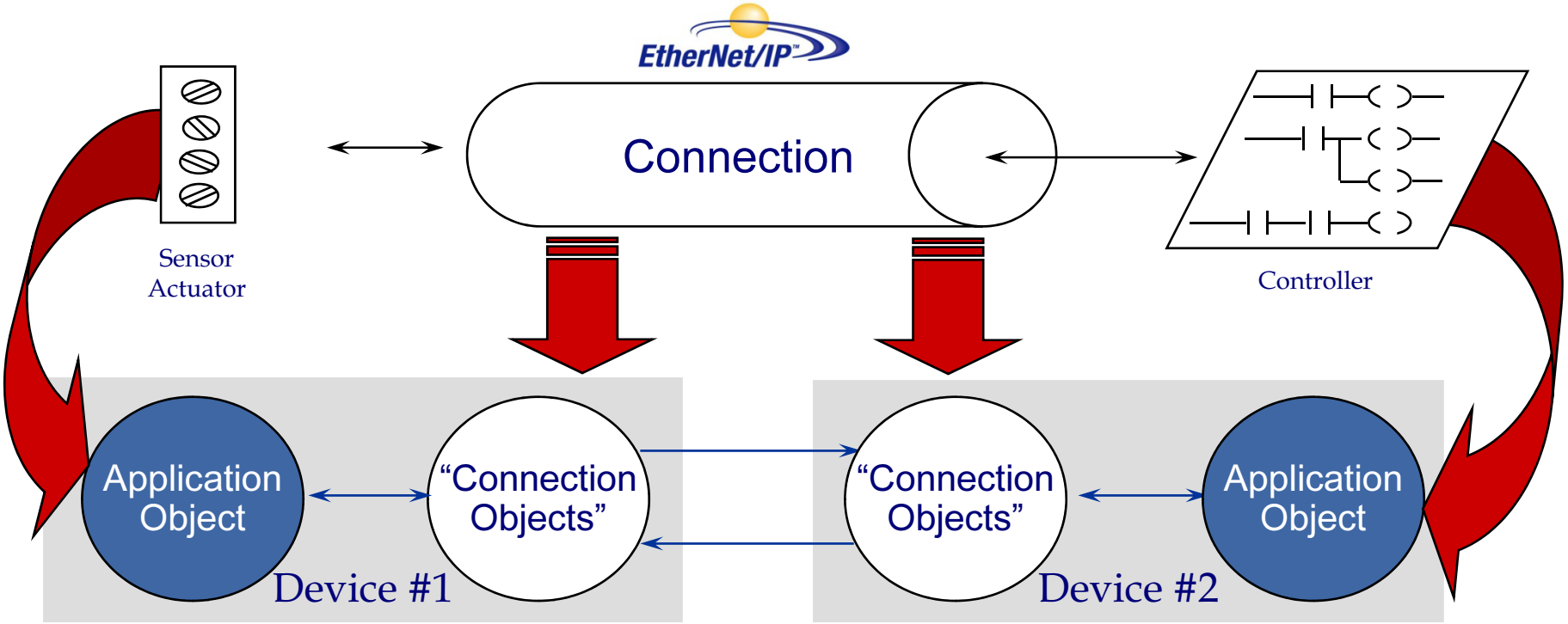
Layer 7 - Application
CIP - Device Profiles

- Device Profiles define the communication view of a device
  - Purpose is to provide interoperability and interchangeability
  - By using these Device Profiles, devices have a consistent behavior
    - Among vendors
    - Among networks
  - The structure of the input/output data that the device exchanges
  - The device's configuration data
- CIP defines profiles for many standard industrial control devices
  - Standard Device Profiles may be extended by vendor-specific attributes and objects
  - There is a generic profile and a vendor specific profile



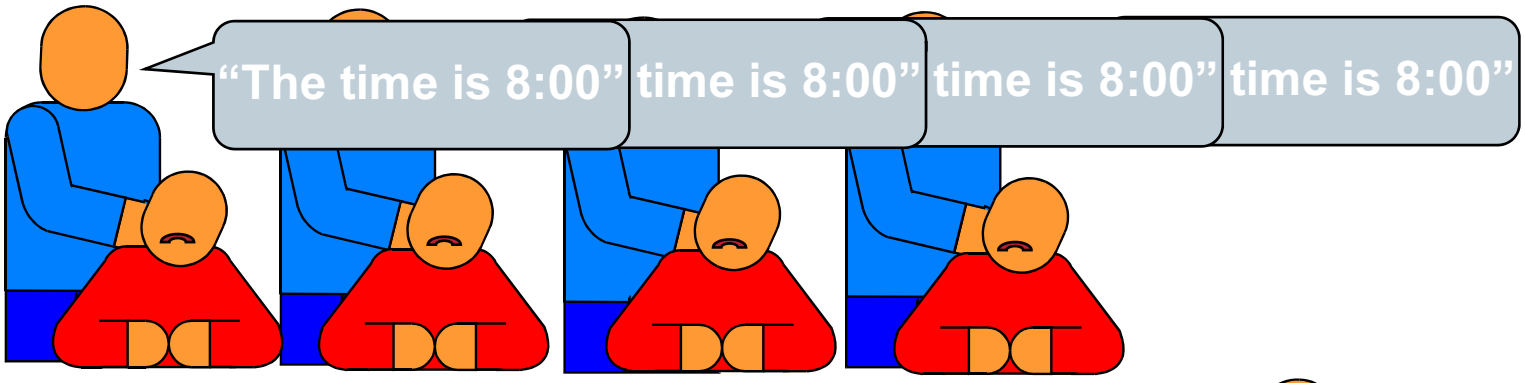
Layer 7 - Application
CIP Objects

- Connection Objects model the communication characteristics of a particular application to application(s) relationship
  - In EtherNet/IP these are actually several objects

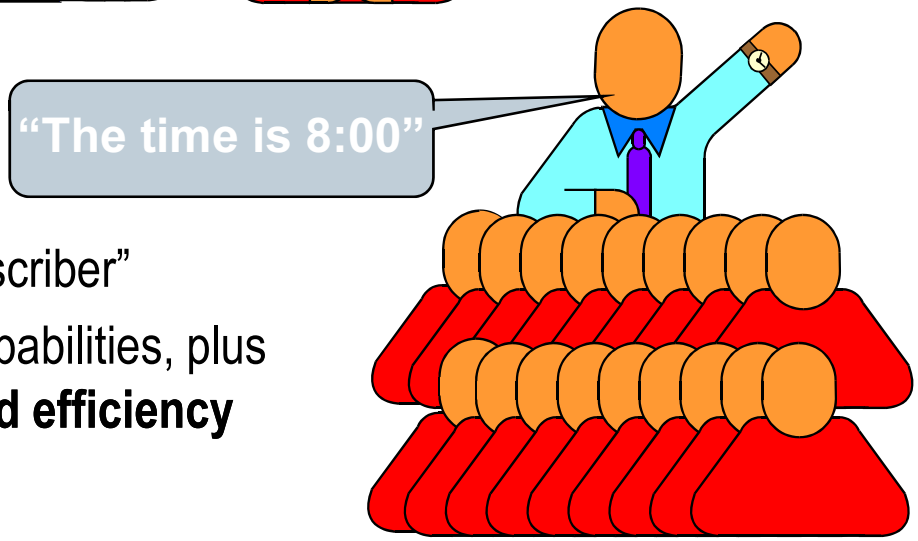


Layer 7 – Application
CIP – Producer/Consumer vs. Source/Destination

- Source/Destination
  - often referred to as “Polling” or “Request/Response”

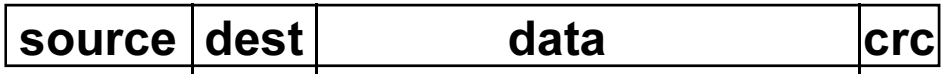


- Producer/Consumer
  - also referred to as “Publisher/Subscriber”
  - contains all Source/Destination capabilities, plus additional capabilities for **improved efficiency**



Layer 7 – Application
CIP – Producer/Consumer vs. Source/Destination

- Source/Destination (point to point)

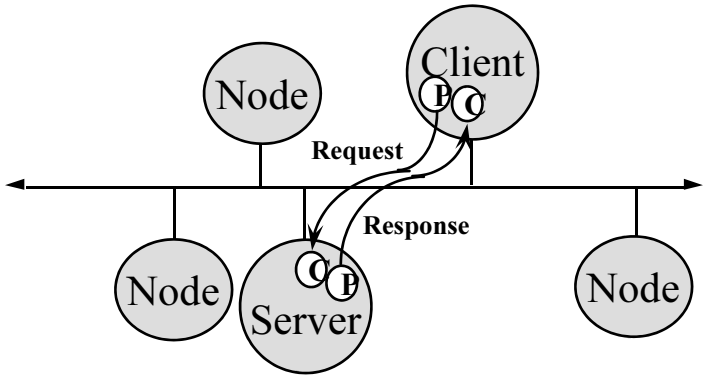


  - Synchronized action between nodes is very difficult as data arrives at a different time to each node
  - Wastes bandwidth as data must be sent multiple times when only the destination is different
  - Results in the need for multiple networks
- Producer/Consumer (the data is identified)

  - Multiple nodes can consume the same data at the same time from a single producer so nodes can be synchronized
  - More efficient bandwidth usage
  - Results in higher degree of determinism and repeatability

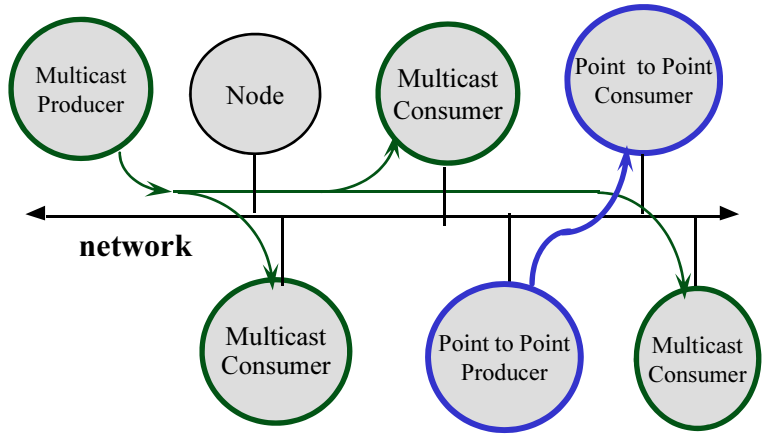
Layer 7 - Application
CIP - Unconnected Messaging

- Most basic means of communicating
  - All nodes must support (on EtherNet/IP)
- Unconnected Message Manager (UCMM) is always available
  - No reservation mechanism means it may get busy
- No maintenance or setup required
  - Use only when needed
  - No need to 'keep it alive' with periodic messages
- Supports all explicit services defined by CIP
- It is possible to build a node that only communicates in this manner
  - Such a device would have limited usefulness



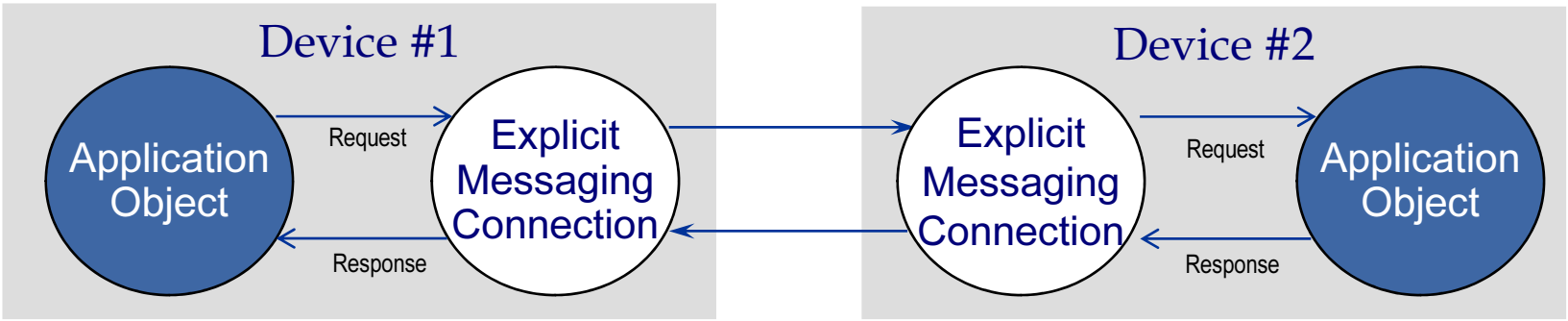
Layer 7 - Application
CIP - Connected Messaging

- A relationship between two or more applications on different nodes
- Explicit or Implicit connections are available
- Supports the Producer-Consumer model
  - Efficient transfer mechanism
- Provides timeout indication
  - Applications aware if relationship breaks down
- Resources for a particular application are reserved in advance
- A limited resource
  - a node can run out of connections



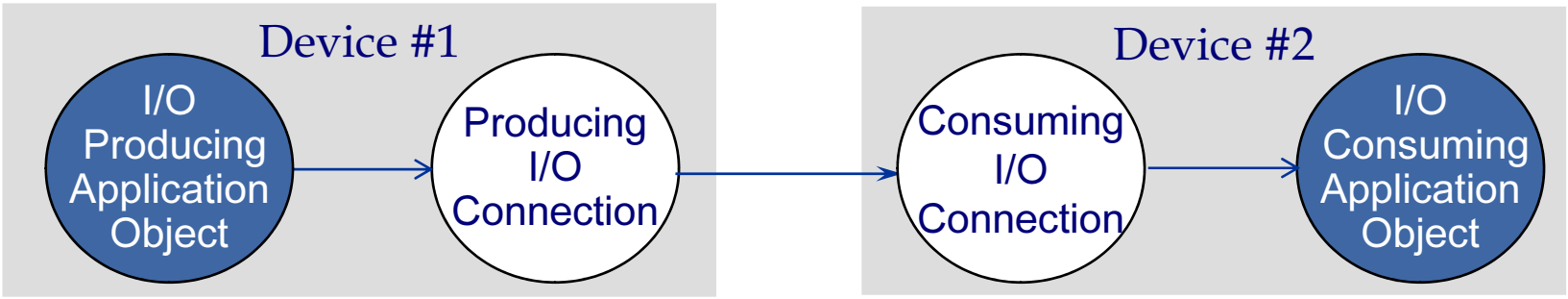
Layer 7 - Application
CIP - Explicit Messages

- **Explicit Messages** are used for point to point, client-server type transactions – transport class 3 (Class 3)
  - The Server side is bound to the Message Router object
    - Has access to all internal resources
  - The Client side is bound to a client application object
    - Has a need to generate requests to the server
  - Uses an explicit messaging protocol in the data portion of the message packet
  - Connected or Unconnected
  - Application Examples: Configuration, Diagnostics, and Data collection
    - RSLinx, Message instructions



Layer 7 - Application
CIP - Implicit Messages

- **Implicit Messages** transfer application specific **I/O** data – transport class 0/1 (Class 1)
  - The data source/destination is an application object (e.g. Assembly object)
  - There is no protocol in the message data - it's all I/O data
  - Data transfer is more efficient because the meaning of the data is known ahead of time
  - Transfer is initiated on a time basis (Cyclic Trigger) or Requested Packet Interval (RPI)
  - Connection timing mechanism to alert application that the other side has stopped communicating – heartbeat
  - Only connected - there is no unconnected implicit messaging
  - Application Examples: Real-time I/O data, Functional safety data, Motion control data

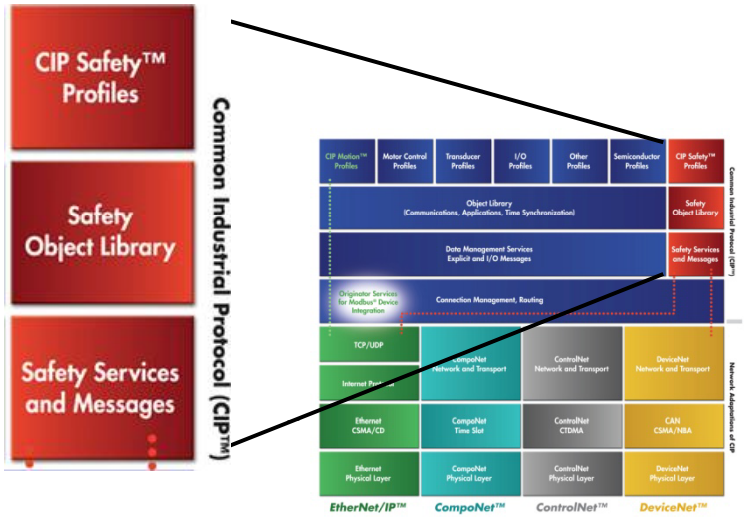


Layer 7 - Application
CIP - Electronic Data Sheet (EDS)

- A text based file provided by the manufacturer that allows a tool to learn about the device's:
  - Structure and meaning of I/O data
  - What I/O data transfer types are available
  - Network accessible application config parameters
  - Supports modular products for complex devices
    - Constructs describe a rack system: Chassis, modules & communication adapters
- EDS file format linked to the product's identity
  - Tailored to individual product features

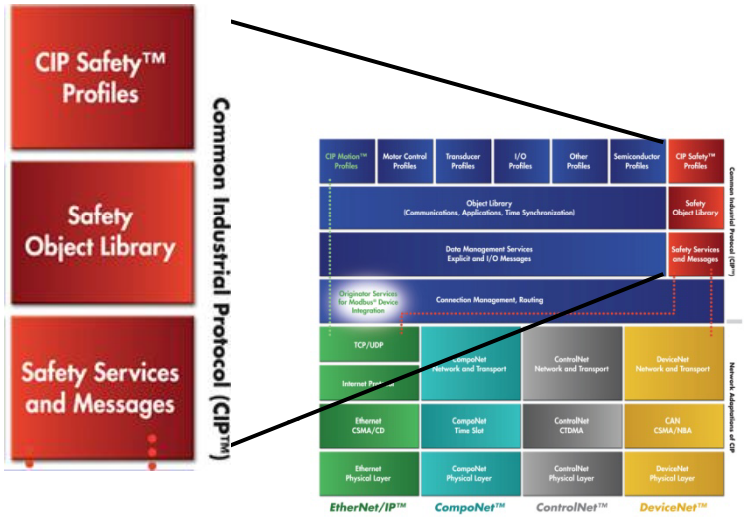
CIP Safety
Layer 7 - Application

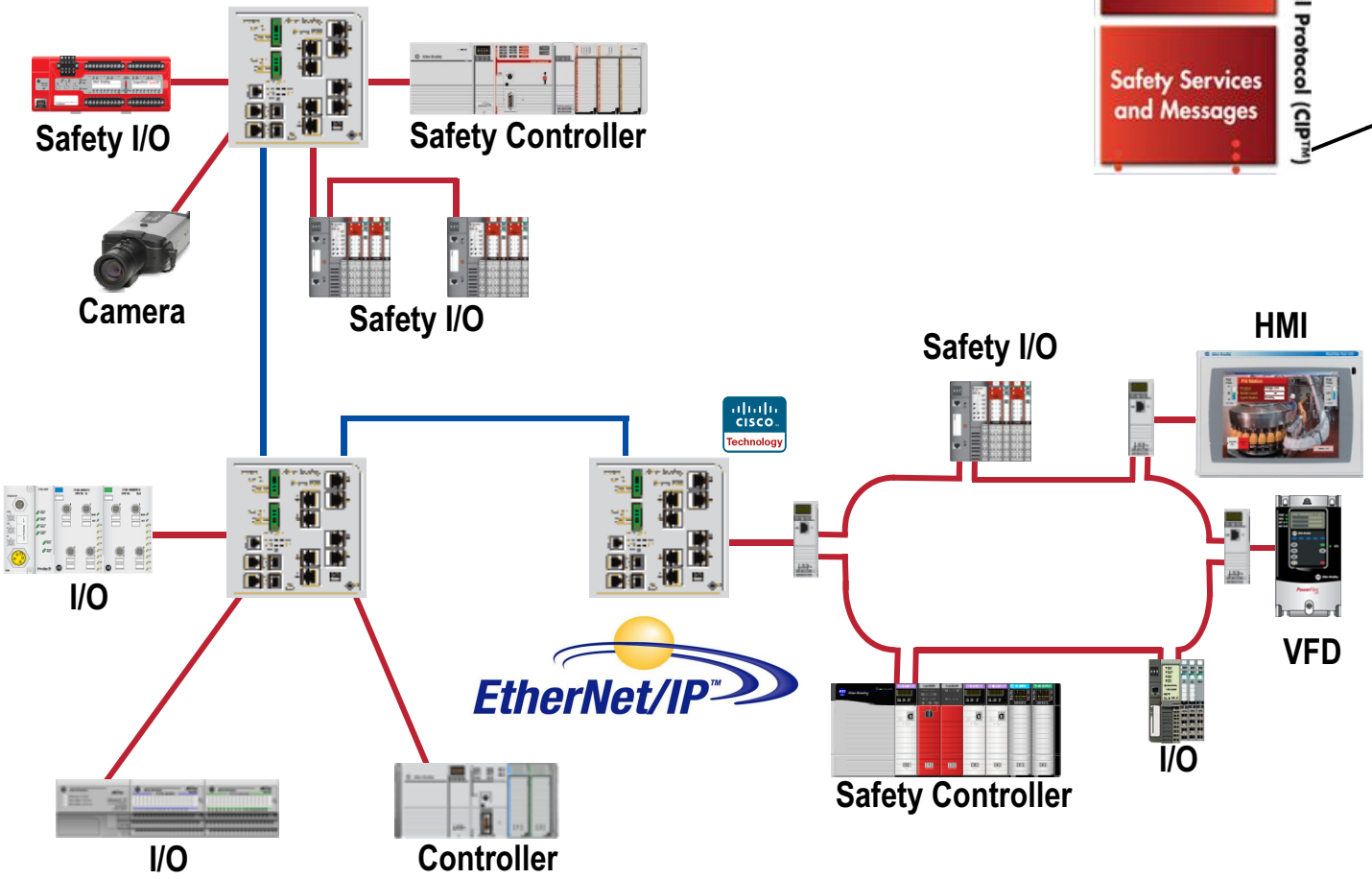
- High-integrity Safety Services and Messages for CIP
- IEC 61508 – SIL3 and EN 954-1 - Cat 4



CIP Safety
Layer 7 - Application

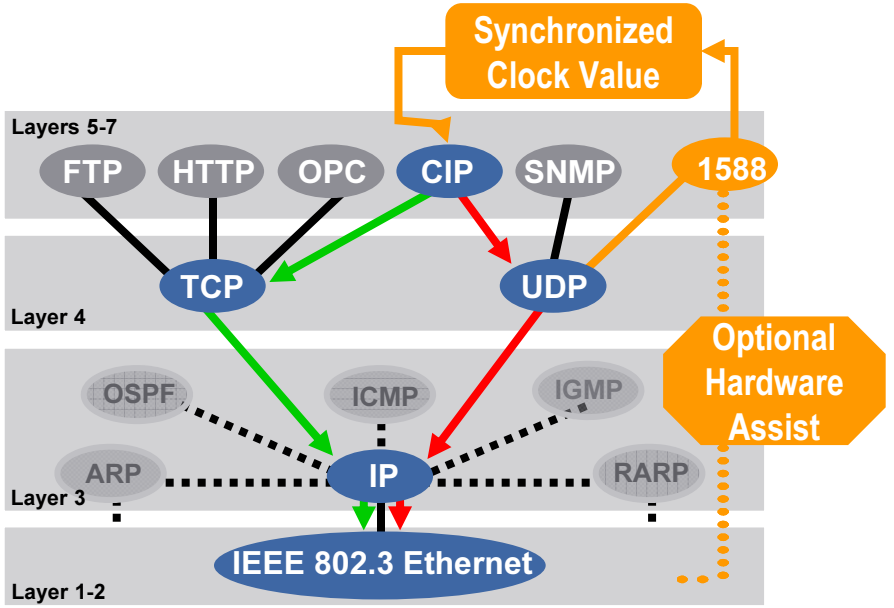
- High-integrity Safety Services and Messages for CIP
- IEC 61508 – SIL3 and EN 954-1 - Cat 4



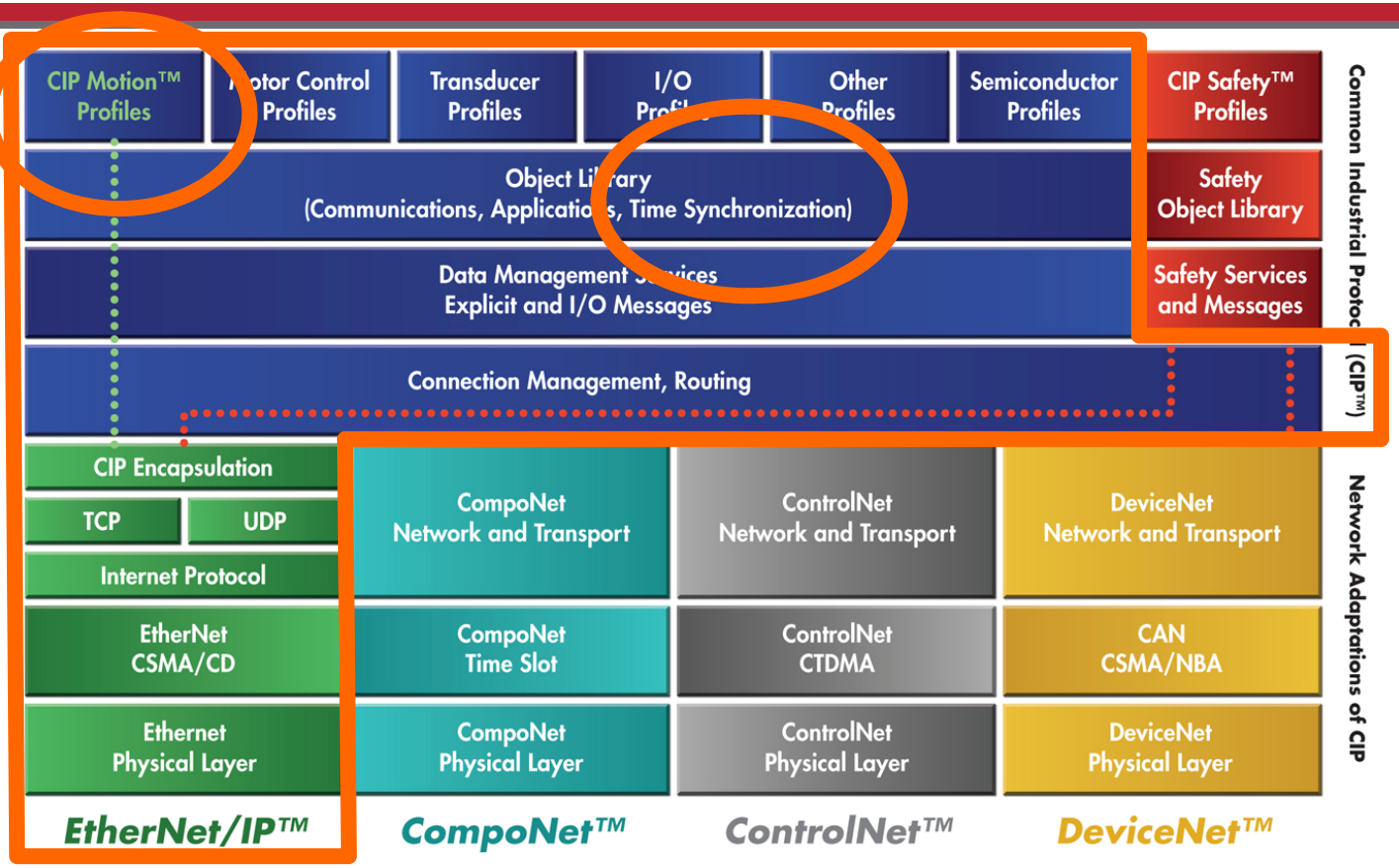


CIP Sync
Layer 7 - Application

- Defines time synchronization services for CIP Networks
- Allows distributed control components to share a common notion of time
- Implements IEEE-1588 precision clock synchronization protocol
  - Referred to as precision time protocol (PTP)
  - Provides +/- 100 ns synchronization (hardware-assisted clock)
  - Provides +/- 100 µs synchronization (software clock)
- Time Synchronized Applications such as:
  - Input time stamping
    - Alarms and Events
    - Sequence of Events recording
    - First fault detection
  - Time scheduled outputs
  - Coordinated Motion



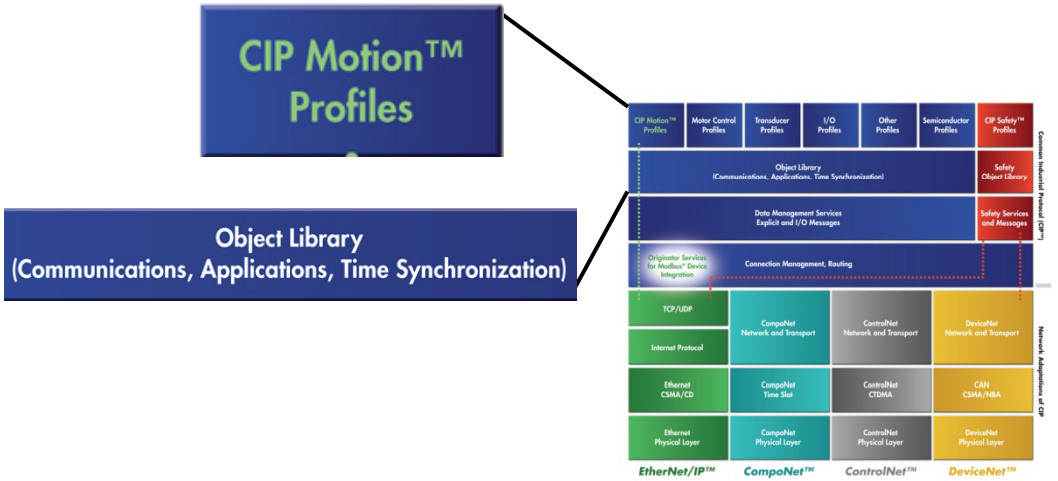
CIP Motion
Layer 7 - Application

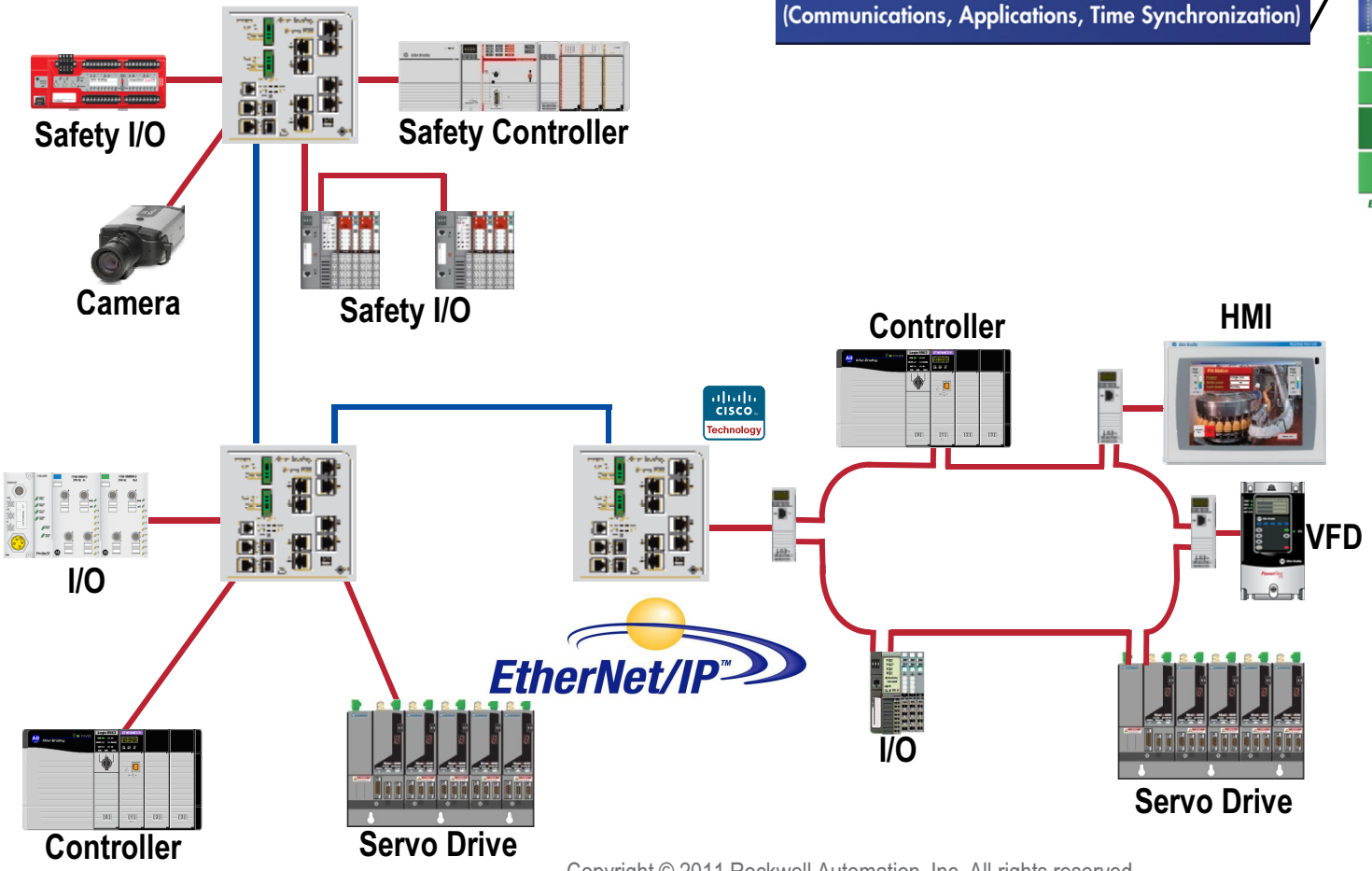


- Traditional approach to motion control - Network Scheduling (time-slot)
- CIP Motion approach - Pre-determined Execution Plan, positioning path, based on a common understanding of time between the motion controller and drives …… where to be and at what time

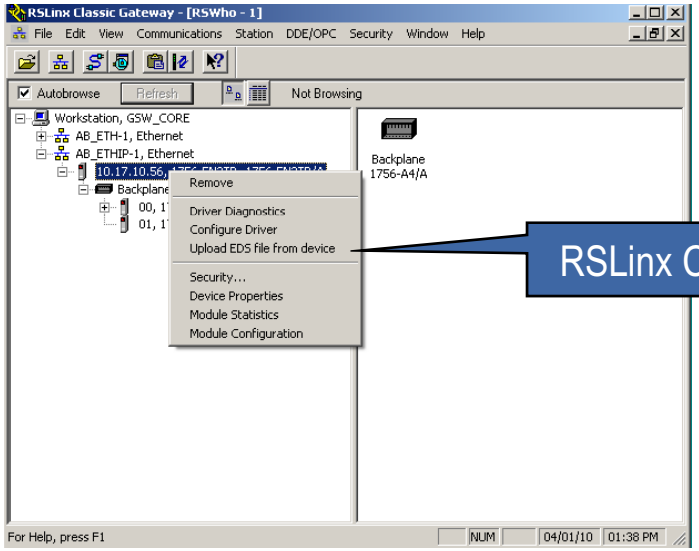
CIP Motion
Layer 7 - Application

- Controller and Drive Profiles
- Motion Axis Object





Layer 7 - Application
EN2TR Example



RSLinx Classic - EDS

Connection Manager

	Requests	Format Rejects	Resource Rejects	Other Rejects	Connection Timeouts
Open	0	0	0	0	0
Close	0	0		0	

RSLinx Classic EN2TR Diagnostics Connection Manager

EN2TR Webpage Diagnostic Overview

CIP Connection Statistics (All Ports)	
Active Total	0
Active Messaging	0
Active I/O	0
Maximum Total Observed	5
Maximum Total Supported	259

HMI/MSG (EtherNet/IP Port - Class 3)	
Sent Packets Per Second	0
Received Packets Per Second	0
Sent Bytes Per Second	0
Received Bytes Per Second	0
Sent Packet Count	17297
Received Packet Count	17297

I/O and Prod/Cons Packets Per Second (EtherNet/IP Port - Class 1)	
Total	0
Sent	0
Received	0

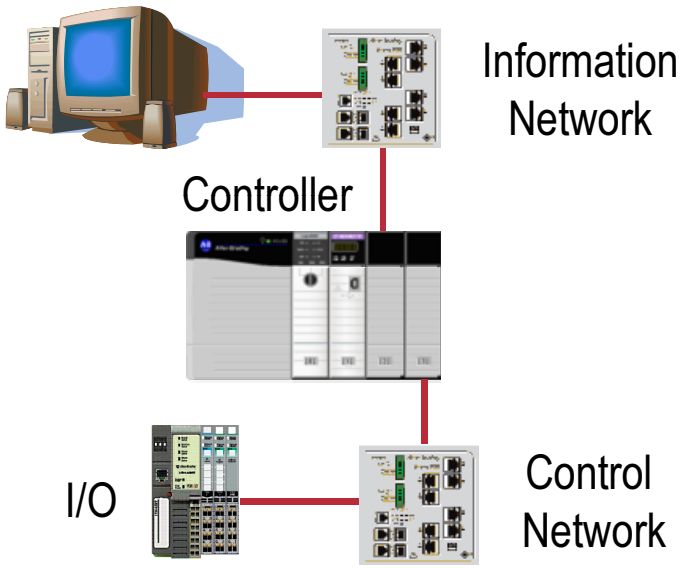
I/O and Prod/Cons Packet Counts (EtherNet/IP Port - Class 1)	
Total	0
Sent	0
Received	0
Rejected	0
Missed	0

Multicast Producers (EtherNet/IP Port - Class 1)	
Active	0
Maximum Observed	0
Maximum Supported	32
Base Address	239.192.71.224

EN2TR Webpage Diagnostic Overview

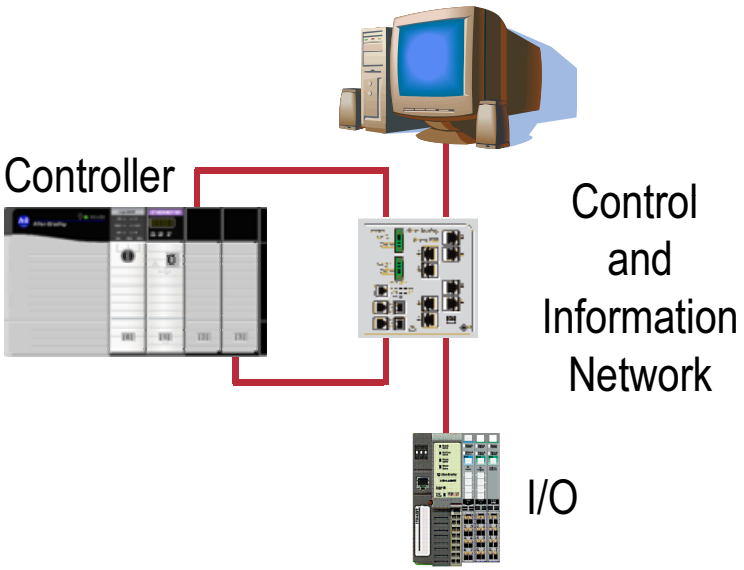
Network Architectures
Physical Segmentation

- Two NICs for Network Segmentation



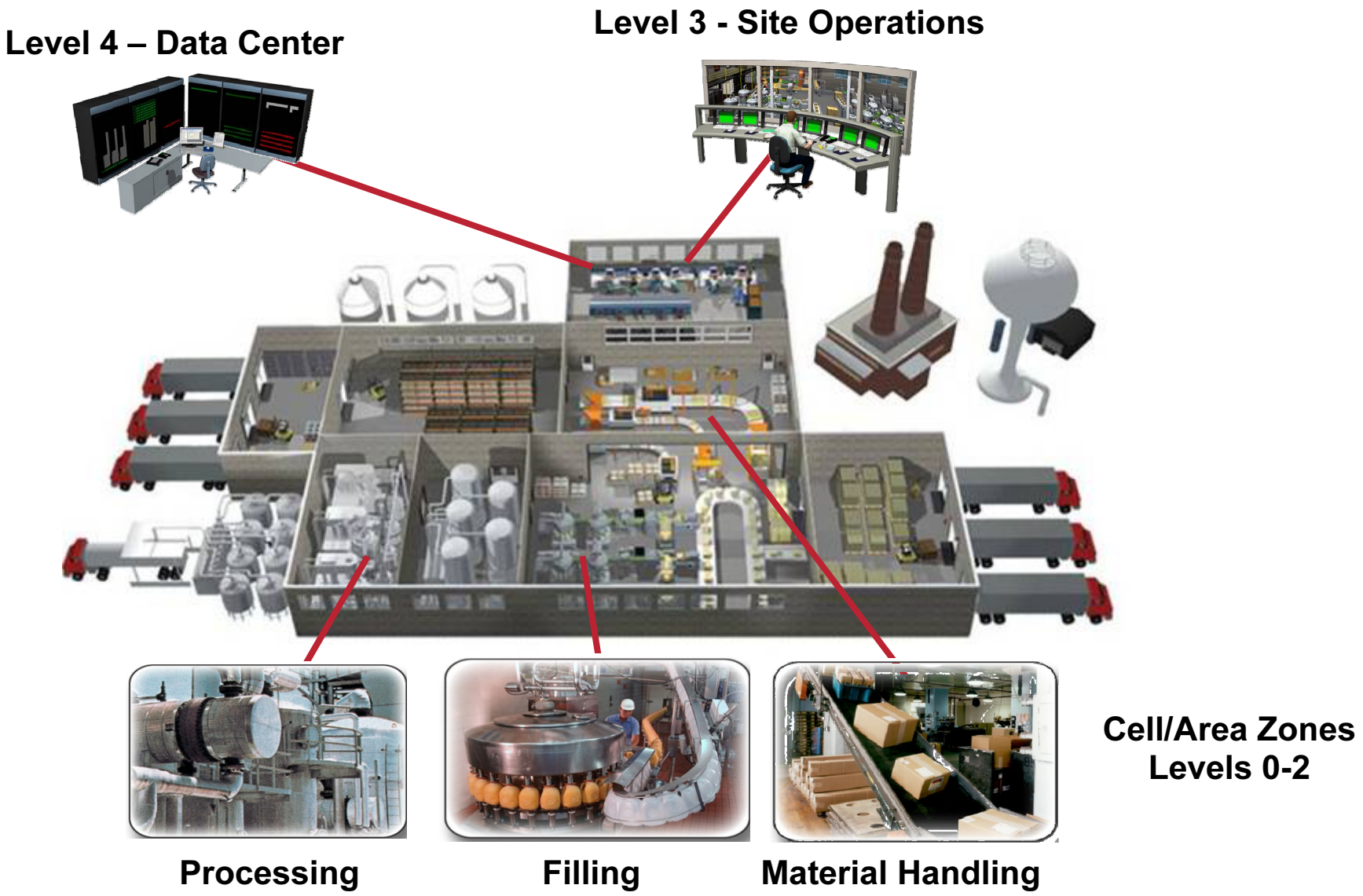
- Benefits
  - Clear network ownership demarcation line
- Challenges
  - Limited visibility to control network devices for asset management
  - Limited future-proof capability

- Two NICs for Scalability - performance and capacity

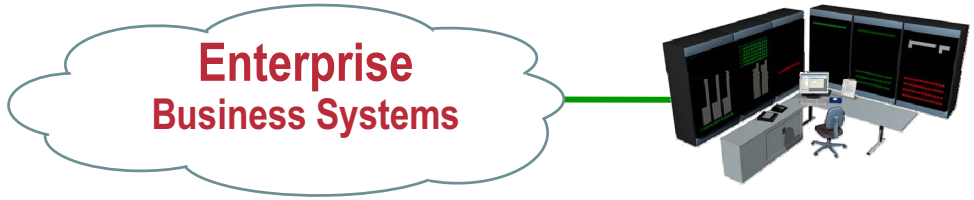


- Benefits
  - Plantwide information sharing for data collection and asset management
  - Future-proof
- Challenges
  - Blurred network ownership demarcation line

Plantwide Network Architectures



Plantwide Architectures
Industrial Network – Isolated LANs

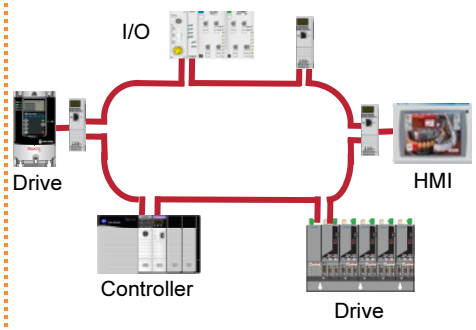


Level 4 – Data Center

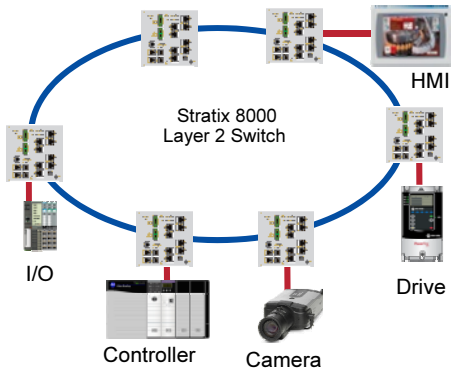
IT Network

Industrial Network

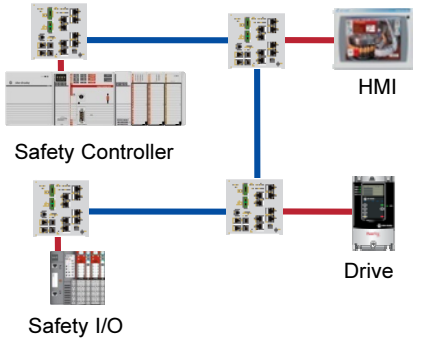
Level 3 - Site Operations
- FactoryTalk Application Servers
- FactoryTalk Services Platform
- Data Servers



Filling Cell/Area Zone
Levels 0-2
Ring Topology
Device Level Ring



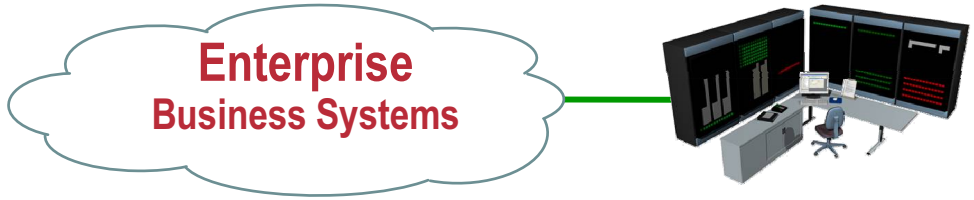
Processing Cell/Area Zone
Levels 0-2
Ring Topology
Resilient Ethernet Protocol (REP)



Material Handling Cell/Area Zone
Levels 0-2
Bus/Star Topology

Islands of Automation Systems

Plantwide Architectures
Industrial Network - Plantwide LAN

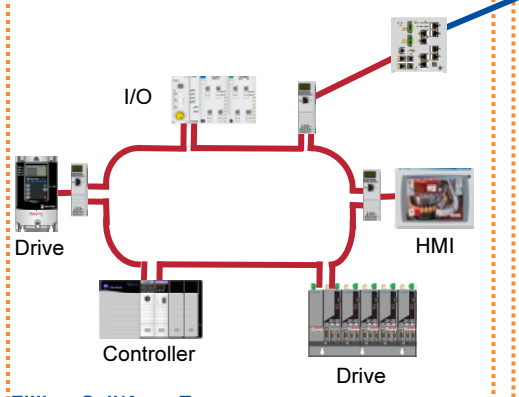


Level 4 – Data Center

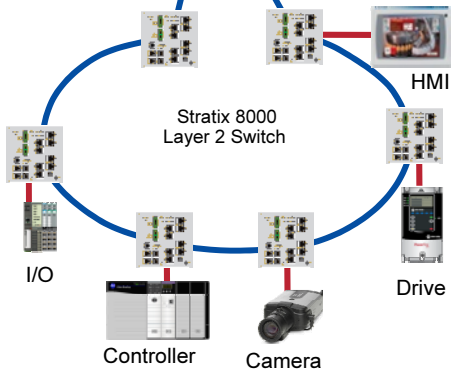
IT Network

Industrial Network

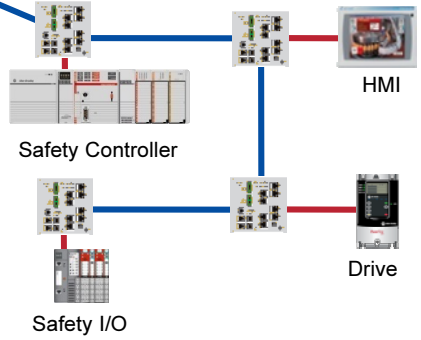
Level 3 - Site Operations
- FactoryTalk Application Servers
- FactoryTalk Services Platform
- Data Servers



Filling Cell/Area Zone
Levels 0-2
Ring Topology
Device Level Ring



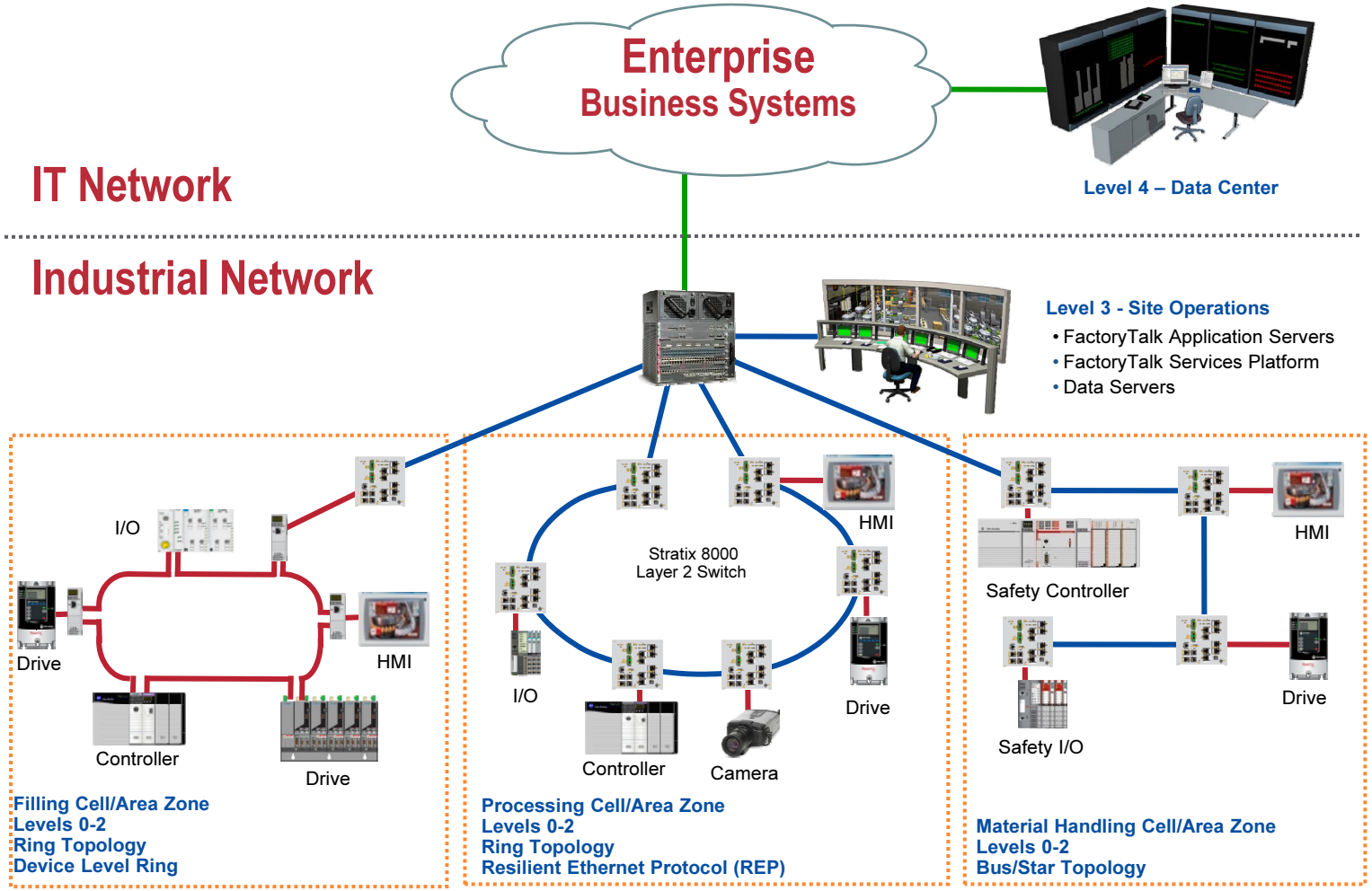
Processing Cell/Area Zone
Levels 0-2
Ring Topology
Resilient Ethernet Protocol (REP)



Material Handling Cell/Area Zone
Levels 0-2
Bus/Star Topology

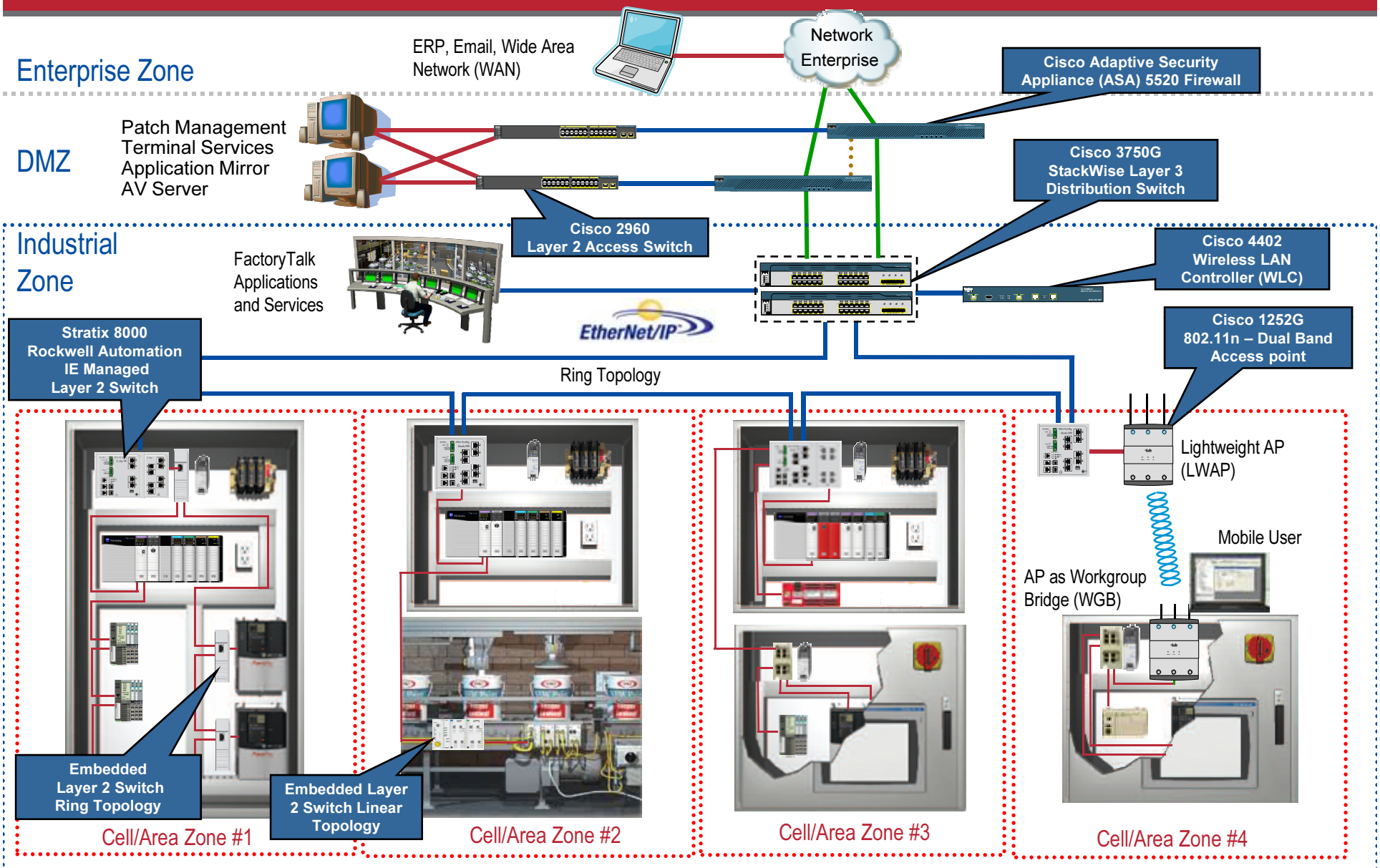
Islands of Plantwide Systems

Plantwide Architectures
Converged Industrial and IT Network



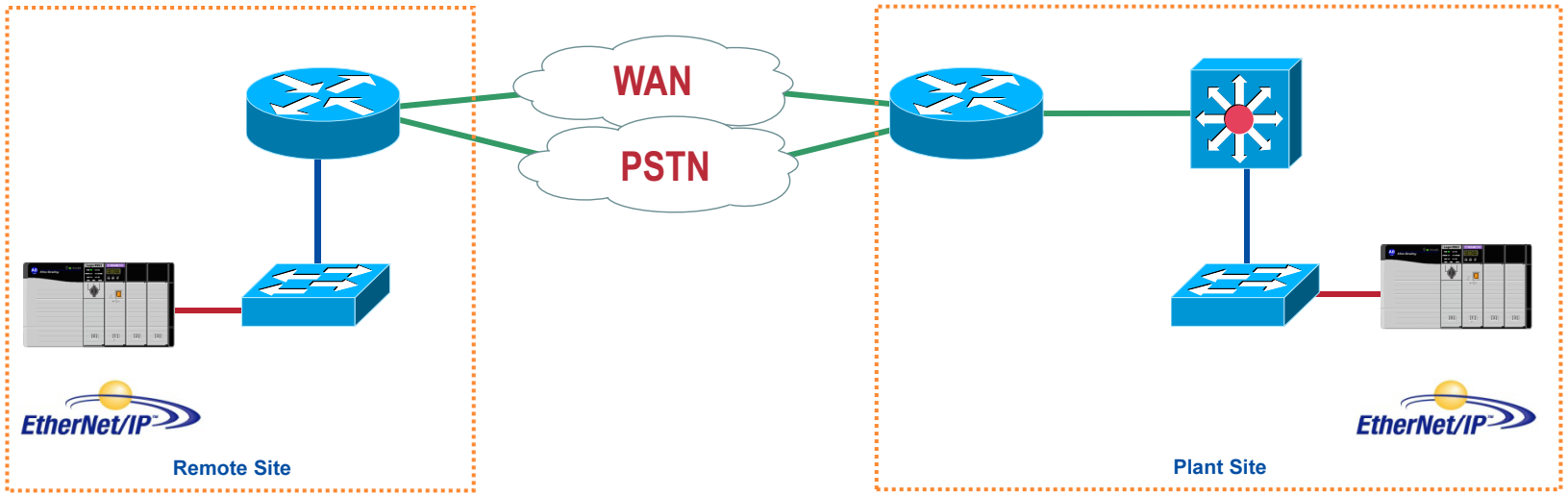
Business and Plantwide System Convergence

Industrial and IT Network Convergence
Representative Configurations



Network Architectures
Wide Area Network (WAN)

- Broad geographic area
  - WAN Examples:
    - Point-to-Point Link – PSTN Leased Lines – T1, E1
    - Circuit Switching - ISDN
    - Packet Switching - Frame Relay, Broadband DSL, Broadband Cable
  - Higher Latency
    - Use case examples – HMI and Data Collection



EtherNet/IP Advantage Summary

- ODVA - Cisco Systems and Rockwell Automation are principal members
- IT friendly - Standard Ethernet and TCP/IP Protocol Suite
- Future proof – Sustainable
  - Industry Standards such as IEEE and IETF
- Portability and Routability
  - Physical layer and data link layer independence
- Established – 280+ Registered Vendors, over 3,000,000 nodes
- Supported – All EtherNet/IP products require conformance testing
- Multidiscipline Support
  - Information, Diagnostics, Configuration, Time Synchronization, Energy Management and Control - Discrete, Continuous Process, Batch, Safety, Drive, and Motion
- Common industrial application protocol
  - DeviceNet, ControlNet and EtherNet/IP
  - Seamless bridging throughout CIP networks

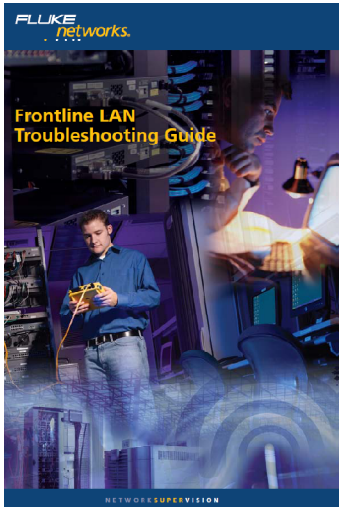
Additional Material
ODVA

- Website:
  - http://www.odva.org/
- Media Planning and Installation Manual
  - http://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00148R0_EtherNetIP_Media_Planning_and_Installation_Manual.pdf
- Network Infrastructure for EtherNet/IP: Introduction and Considerations
  - http://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00035R0_Infrastructure_Guide.pdf
- Device Level Ring
  - http://www.odva.org/Portals/0/Library/CIPConf_AGM2009/2009_CIP_Networks_Conference_Technical_Track_Intro_to_DLR_PPT.pdf
- The CIP Advantage
  - http://www.odva.org/default.aspx?tabid=54

Additional Material
Rockwell Automation

- Networks Website: http://www.ab.com/networks/
- EtherNet/IP Website: http://www.ab.com/networks/ethernet/
- Media Website: http://www.ab.com/networks/media/ethernet/
- Embedded Switch Technology Website: http://www.ab.com/networks/switches/embedded.html
- Publications:
  - ENET-AP005-EN-P Embedded Switch Technology Manual
  - ENET-UM001G-EN-P EtherNet/IP Modules in Logix5000 Control Systems …. provides connection and packet rate specs for modules
  - 1783-UM003 Stratix 8000 and Stratix 8300 Ethernet Managed Switches User Manual
- Network and Security Services Website:
  - http://www.rockwellautomation.com/services/networks/

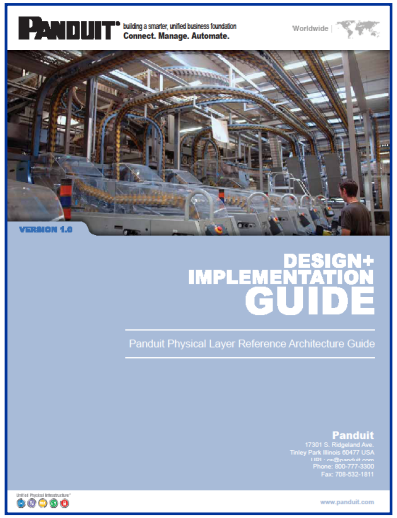
Additional Material
Fluke Networks



- Fluke Networks Websites
  - www.flukenetworks.com
  - www.flukenetworks.com\industrial
  - www.flukenetworks.com\knowledgebase
- Frontline troubleshooting best practices
  - http://www.flukenetworks.com/FNet/en-us/findit?Document=9822807
- Frontline LAN Troubleshooting Guide
  - http://networking.flukenetworks.com/?elqpurlpage=258&document=3331616
- Industrial Ethernet Resource Portal
  - https://admin.acrobat.com/IEPortal

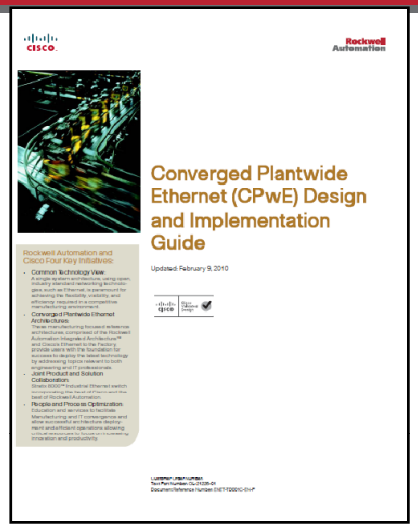
Additional Material
Panduit Corp

- Panduit Corp. Website:
  - http://www.panduit.com/
- Industrial Automation Solutions:
  - http://www.panduit.com/Solutions/IndustrialAutomation/index.htm
  - Industrial Automation Product Systems Brochure
  - Industrial Communication Solutions – Interactive Roadmap



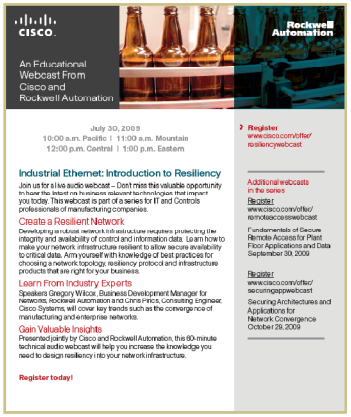
Additional Material
Cisco and Rockwell Automation Alliance

- Website
  - http://www.ab.com/networks/architectures.html
- Design Guides
  - CPwE DIG 2.0
- Education Series
- Whitepapers
  - Securing Manufacturing Computer and Controller Assets
  - Production Software within Manufacturing Reference Architectures
  - Achieving Secure Remote Access to Plant Floor Applications and Data



Additional Material
Cisco and Rockwell Automation Alliance

- Education Series Webcasts
  - The Trend - Network Technology and Cultural Convergence
  - What every IT professional should know about Plant Floor Networking
  - What every Plant Floor Controls Engineer should know about working with IT
  - Industrial Ethernet: Introduction to Resiliency
  - Fundamentals of Secure Remote Access for Plant Floor Applications and Data
  - Securing Architectures and Applications for Network Convergence
  - Available Online
    - http://www.ab.com/networks/architectures.html



LISTEN.
THINK.
SOLVE.®

Fundamentals of EtherNet/IP Networking

Thank you for participating!

Please tidy up your area
before leaving.