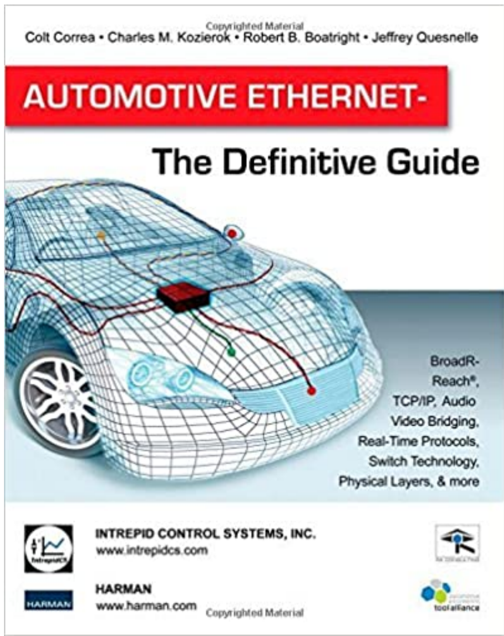
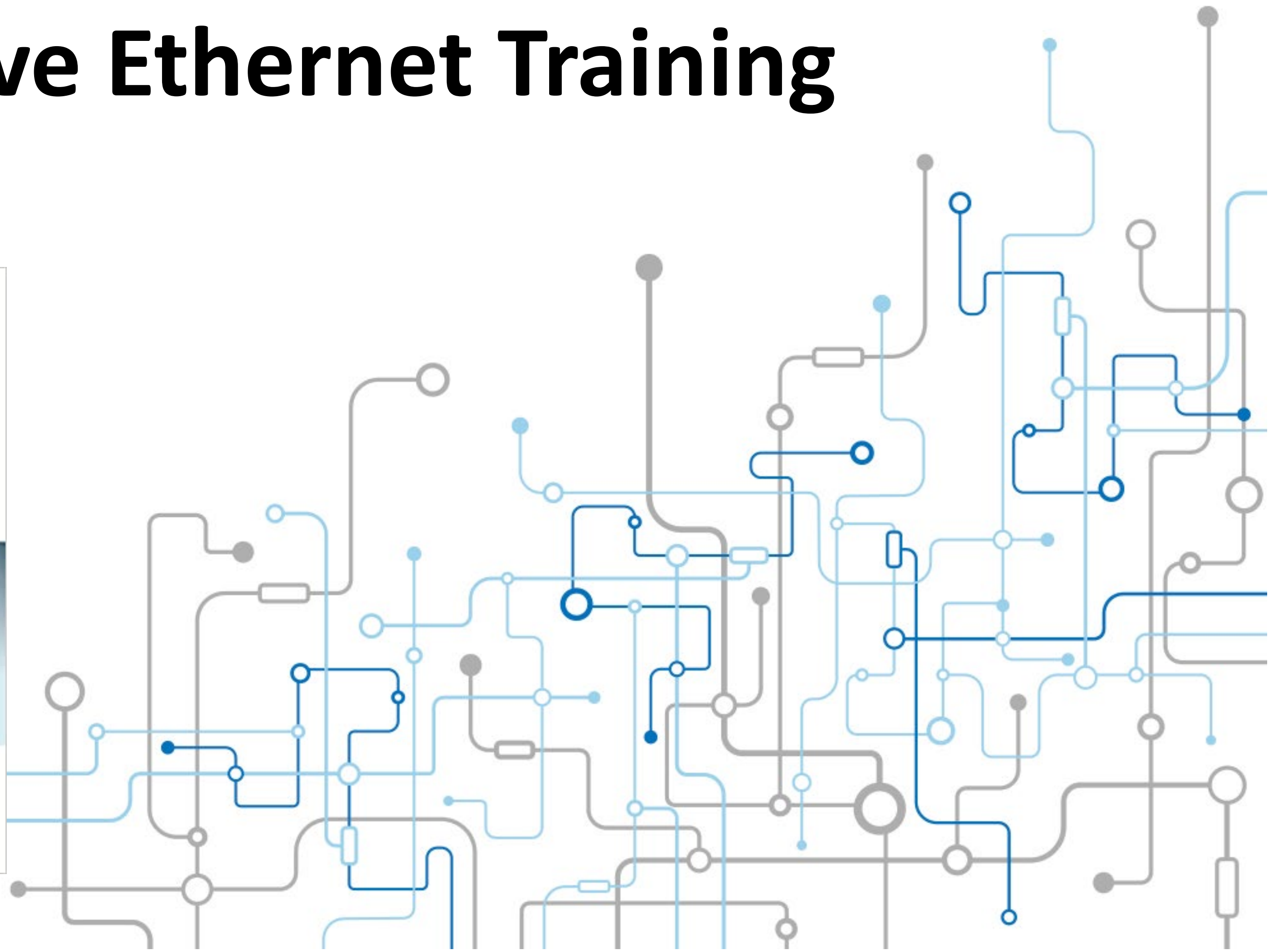
Automotive Ethernet Training





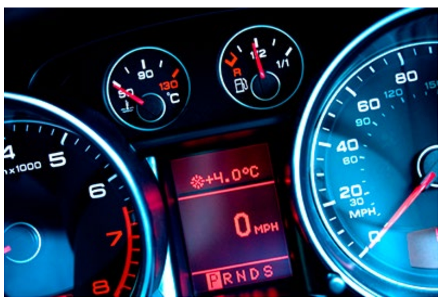
Colt Correa
Author – Automotive Ethernet - The Definitive Guide

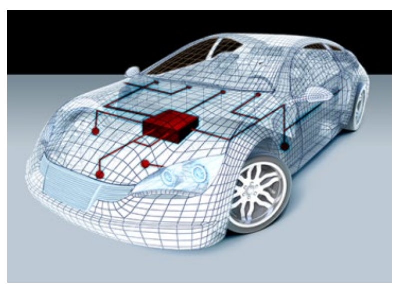
INTREPID CONTROL SYSTEMS
www.intrepidcs.com

automotive engineering tool alliance

INTREPID CONTROL SYSTEMS, INC.

- Supplier of Automotive Network and Data Logging systems for 25+ years
- Product focused company
- Private company and virtually debt free



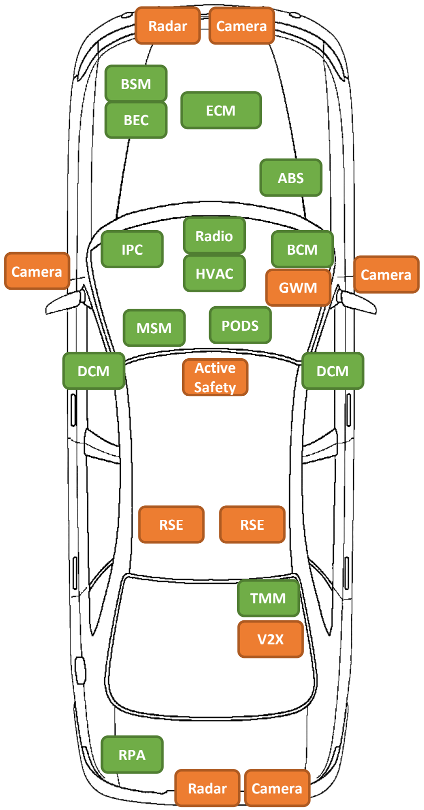


- Global support network to react to customer needs quickly
- Investing in new technology
- Automotive Ethernet, CAN FD, Cybersecurity


Software compatible with all hardware
Remote Wireless Data Logging
Standalone Data Logger Support
Vehicle Network Interfaces
Education
BIG Data
Software for Network Analysis Simulation Data Logger Setup Automated QA
Versatile Product Family
Automotive Ethernet Tools
Analog I/O & Digital I/O
Gateway / Node SIM
Calibration Tools
Accessories

CAN CANnot Any Longer

- Rising demands for bandwidth, QoS, and determinism:
  - Decentralization of functions
  - Integration of consumer products and services
  - Streaming media
  - V2X / Autonomous vehicles
- CAN's evolution to CAN FD addresses bandwidth, but not growing gaps in other areas



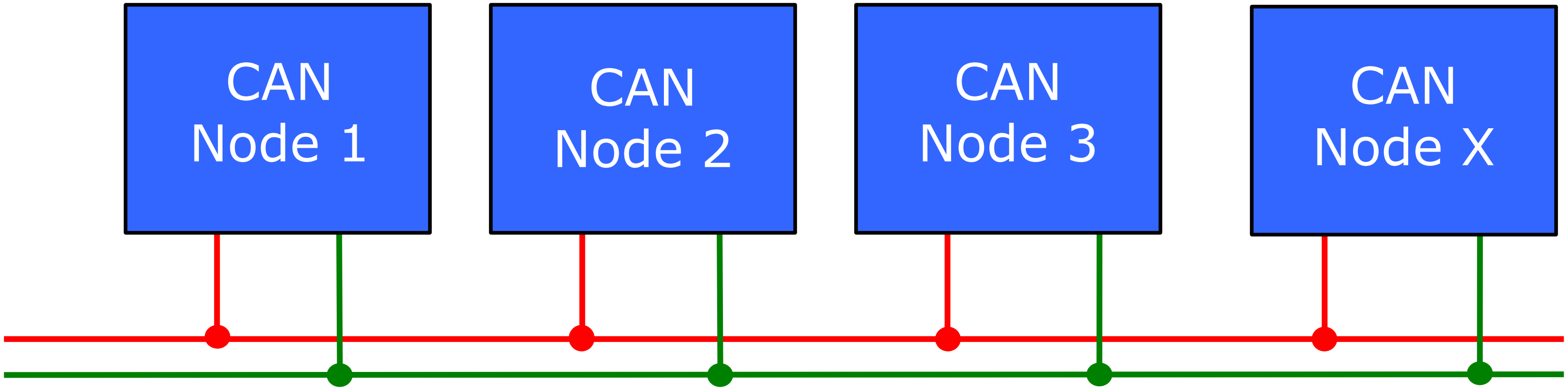
Why Ethernet?

- For one…..Bandwidth!
- Long history of adapting to meet evolving applications and requirements
- Successful efforts to adapt to automotive environment
- Reuse, Reuse, Reuse!!!

Will there be one network to rule them all?

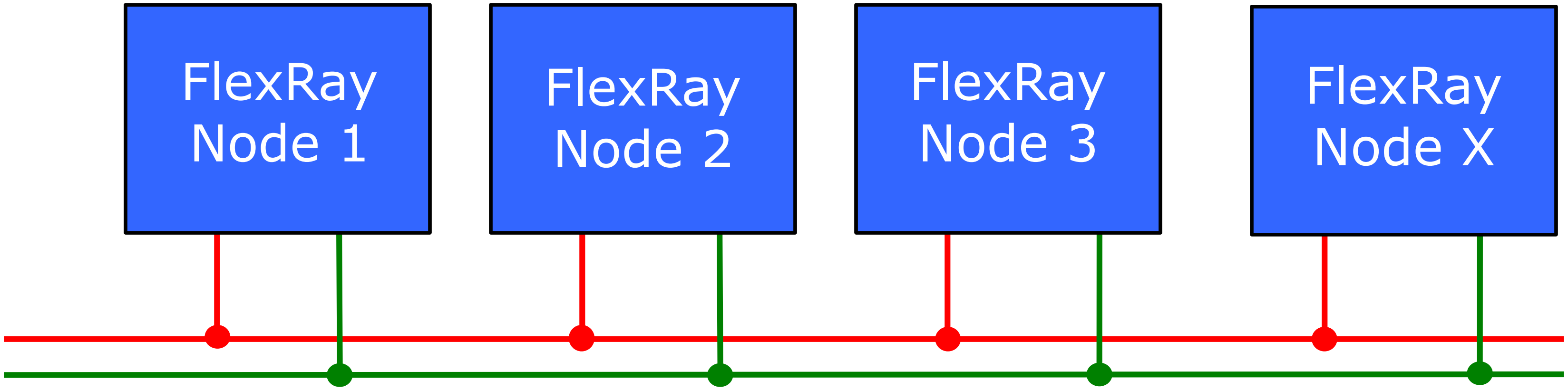
Comparing Ethernet to CAN and FlexRay

CAN



- Multidrop topology with the ability to add and remove nodes without major effects on other nodes
- Up to 1Mb/s for standard CAN.
- Single twisted pair copper wire
- Easy environment for tool manufacturers: plug and play
- Message or packet-based communication
- Arbitration based method to handle collisions

FlexRay

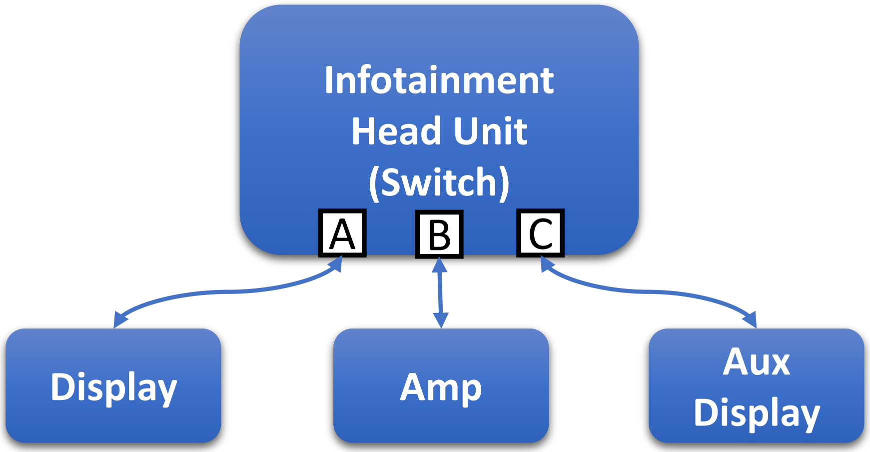


- Multidrop topology but all nodes must be pre-programmed with a fixed configuration
- Up to 10Mb/s on each twisted pair
- Single twisted pair copper wire
- Easy environment for tool manufacturers: plug and play
- Message or packet-based communication
- Collision avoidance based on time slots for each node

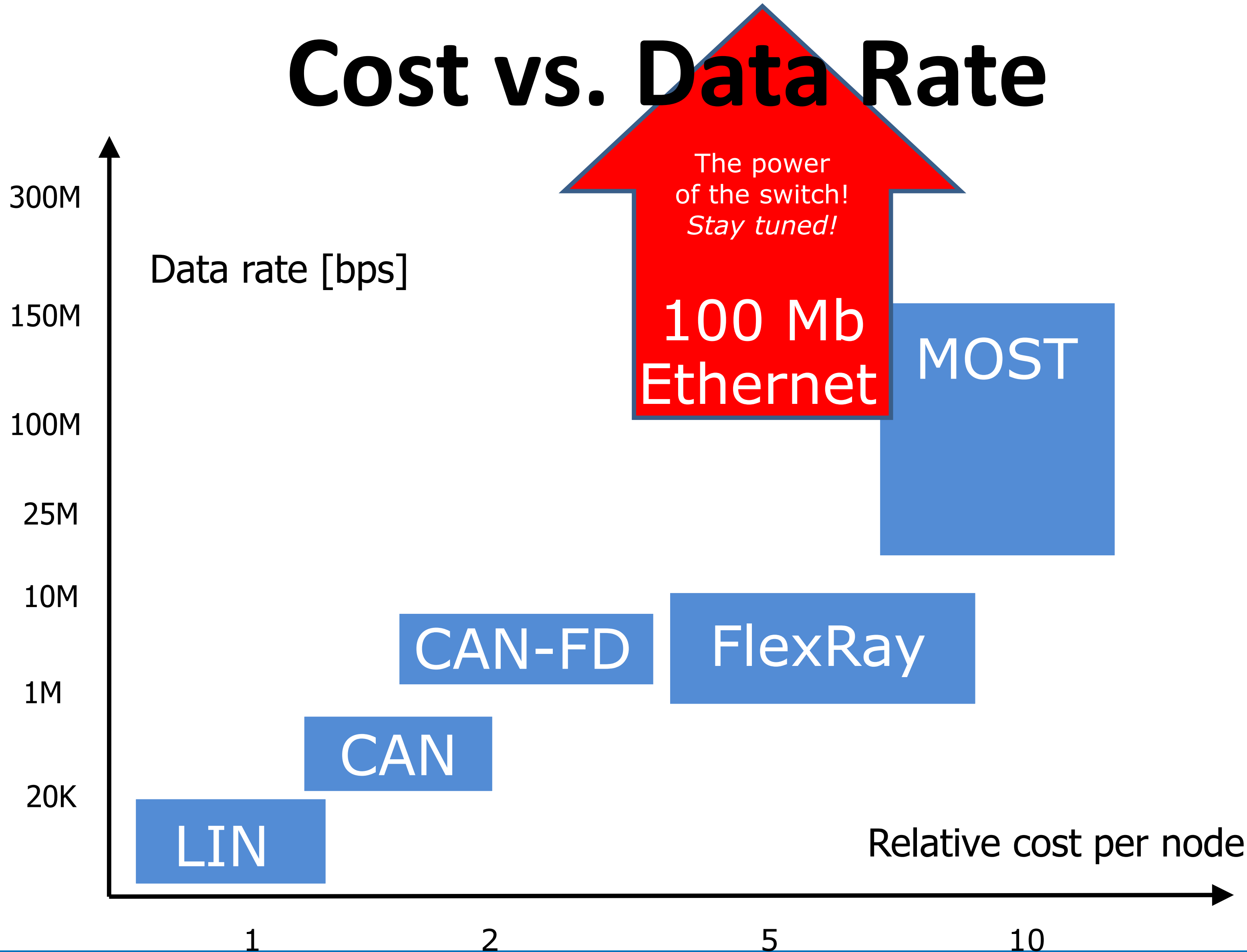
Automotive Ethernet

(100BASE-T1 / 1000BASE-T1)

- Pros
  - Up to 1000 Mb/s
    (each direction and each leg)
  - Widely used technology
    (much support)
  - Good clock synchronization technology available (based on IEEE 1588)
  - History of adaptation to solve new problems.
- Cons
  - Requires a switch
  - Not possible to add or remove nodes unless the switch has spare ports
  - Tools cannot just connect and sniff the bus

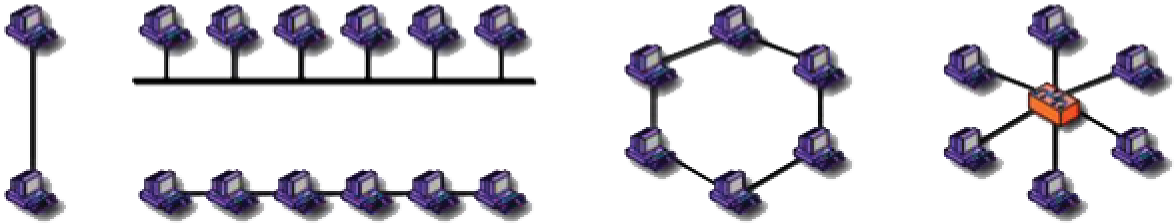


Cost vs. Data Rate



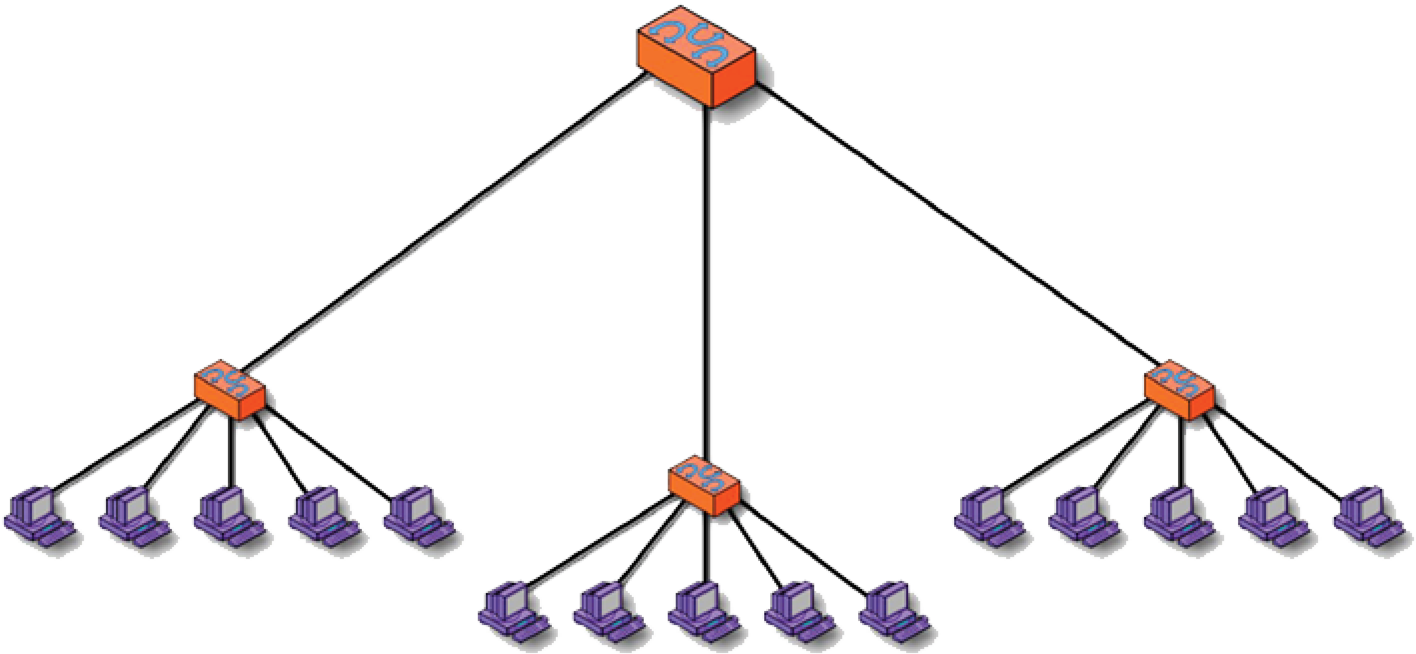
Networking Topologies

- Define how devices are connected together
- Determine network characteristics
- Simple topologies:
  - Point-to-point (or port)
  - Bus (chained or attached) - like CAN and LIN
  - Ring
  - Star
- Complex topologies combine these



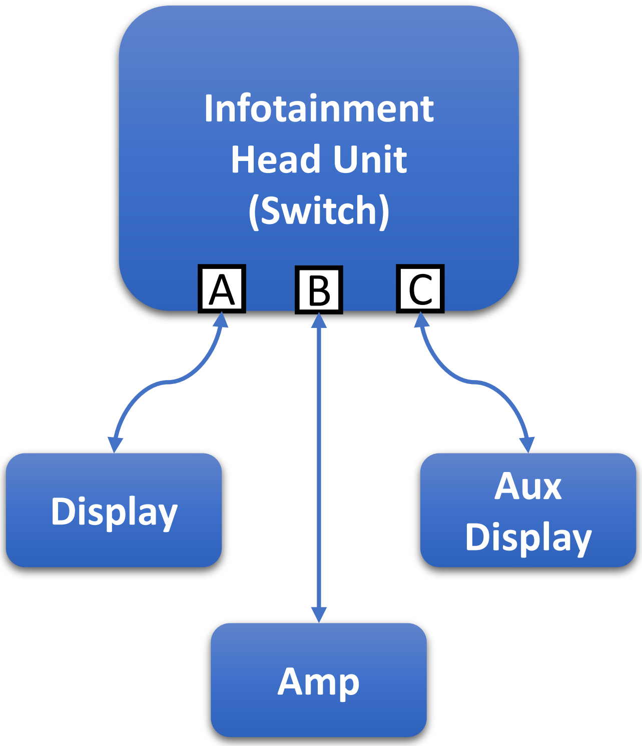
Hierarchical Star Topology

- Also “tree topology” or “star of stars”
- Multiple levels can be created



Today's Ethernet Network

- Original Ethernet (Like CAN)
  - Bus architecture
  - Multiple Nodes / Single Medium
  - Collisions + Arbitration = Inefficient
- Most modern networks are a switched network
  - Devices connected through switches
  - Optimized traffic flow
  - Buffering eliminates collisions
- Each leg (A,B,C) acts as its own network.
- Impossible for Ethernet frames to "collide" using modern full-duplex communication.



Physical Layer

7 **Application Layer**

6 **Presentation Layer**

5 **Session Layer**
Interhost Communication

4 **Transport Layer**
TCP / UDP

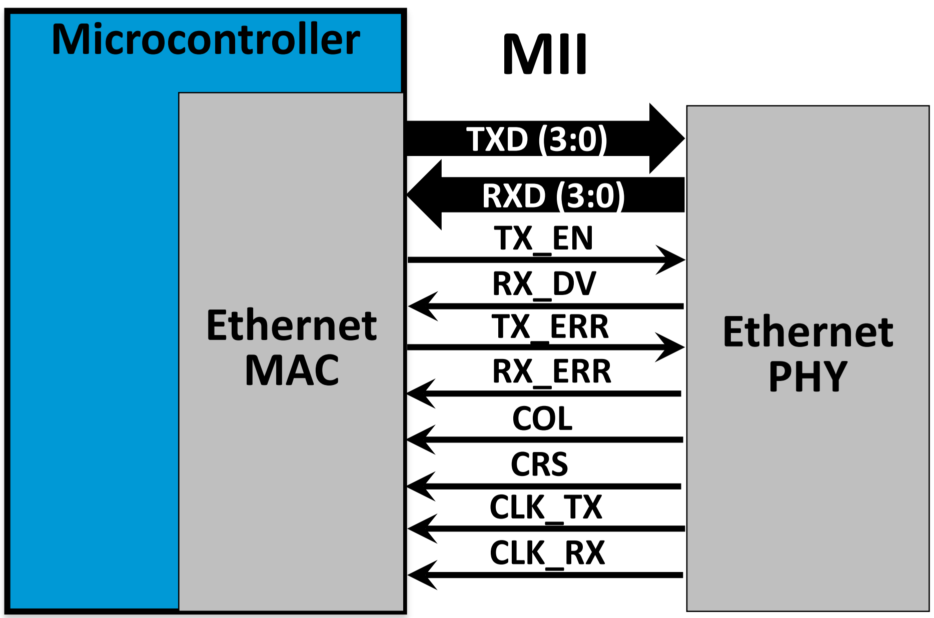
3 **Network Layer**
IP Addressing, Routing

2 **Data Link Layer**
The Ethernet Frame, MAC Addresses

1 **Physical Layer**
Bit Stream, Physical Medium, Methods of Transferring Data

The Power of MII

- Ethernet Node
  - Microcontroller
  - Ethernet MAC controller
  - Ethernet physical layer (PHY).

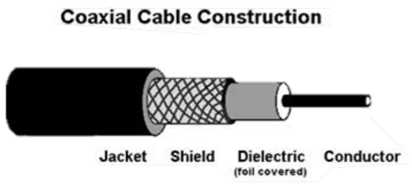


- MII
  - Media Independent Interface
  - Industry standard digital interface
  - enables different PHYs to be used with any MAC.
  - Evolved into a few variations
    - RMII: Reduced
    - GMII: Gigabit
    - RGMII: Reduced Gigabit
    - SGMII: Serial Gigabit

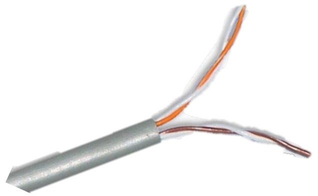
Swap out any Ethernet physical layer and reuse everything above

Consumer Ethernet Media

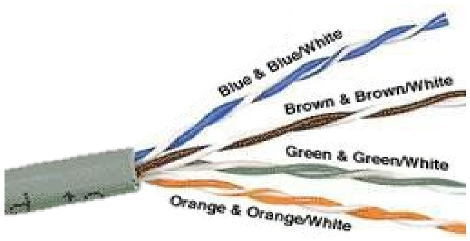
- Coax: 10BASE2 (old days)
  - One conductor
  - Half-duplex
- 10/100 Ethernet 100 Mb/s
  - 2 twisted pairs
  - 4 wires
  - Full-duplex
- Gigabit Ethernet
  - 4 twisted pairs
  - 8 wires
  - Full-duplex



10BASE-2

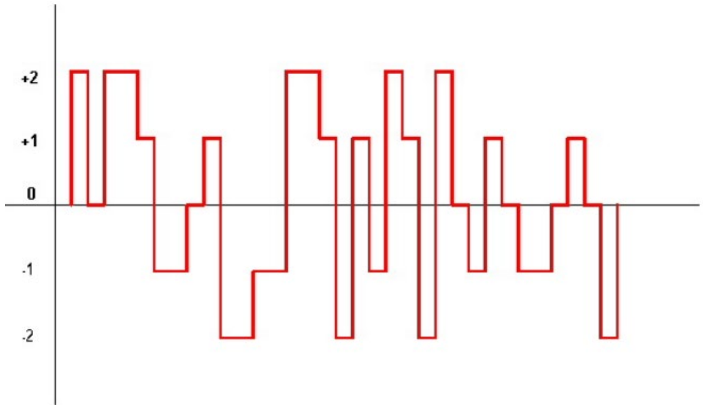


10/100BASE-TX

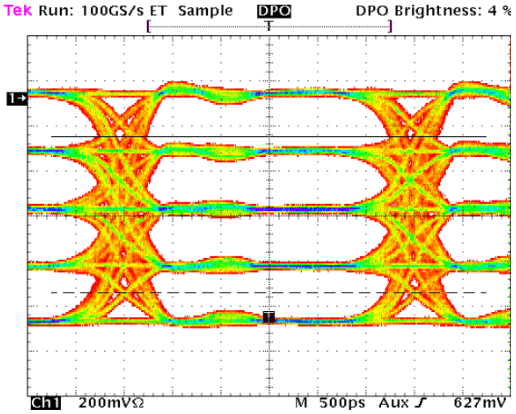


1000BASE-T

1000BASE-T Physical Layer



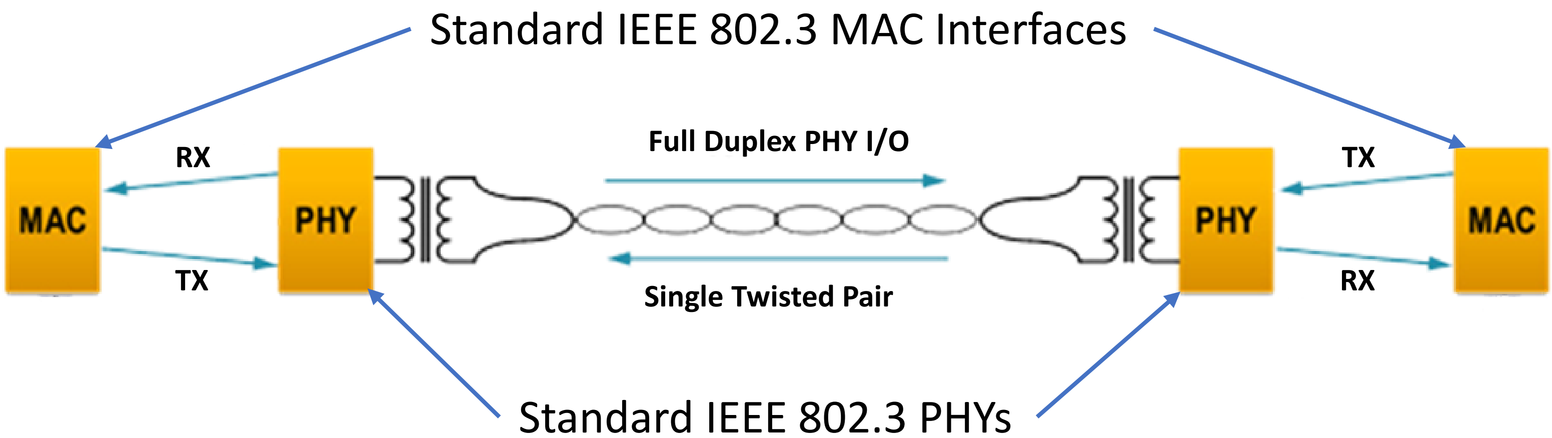
- PAM-5 (5 logical “states”)
- 2 bits encoded in 5 levels
- 500 mV max span signal
- 100 ms span = 1 logic level



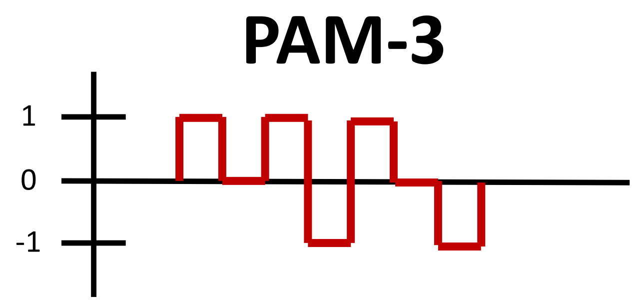
- 4 Twisted Pair
- 250 Mbits/s per twisted pair
- 62.5 MHz frequency
- 125 Mbaud (each direction)
- Uses PAM5 + FEC

Taken from the IEEE tutorial on 802

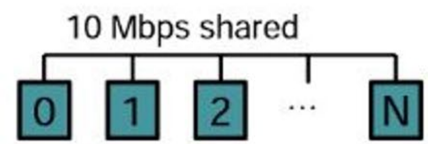
Automotive Physical Layer
100/1000 Mbps



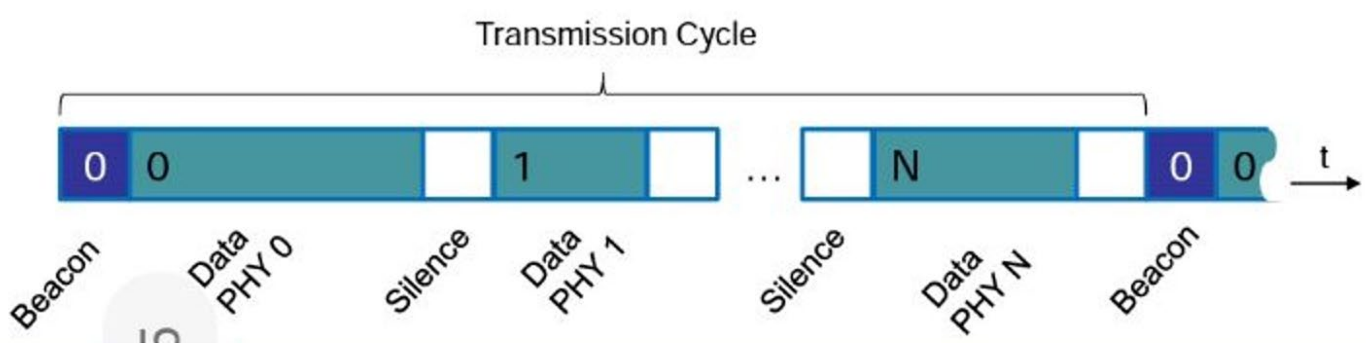
- IEEE 802.3bw: 100BASE-T1
  - 66.6 Mbaud
  - 33.3 MHz Clock
  - Max length 25 meters
  - 2 symbols provide 3 bits of info: 66.6M x 3/2 = 100 Mb/s
- IEEE Std 802.3bp: 1000BASE-T1
  - 750 MBaud
  - 125 MHz Clock
  - Max length 15 meters



10BASE-T1S
Differentiating Features

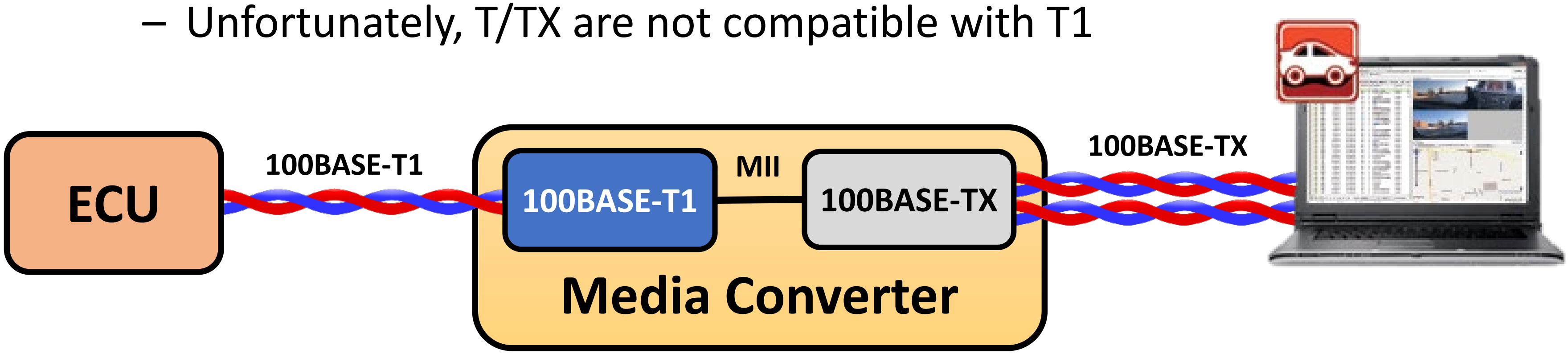


- **Goals**
  - Full bandwidth utilization
  - Reduce latency
  - Quality of Service (QoS)
- **Principle**
  - Avoid physical collisions on the medium by organizing the media access
    - Called Physical Layer Collision Avoidance (PLCA)
- **How it is done**
  - Only the PHY that owns a transmit opportunity is allowed to send data
  - Transmit opportunities are given in a round robin manner
  - A new cycle of transmit opportunities is started when the master node sends a BEACON
  - Works on top of Carrier Sense Multiple Access/Collision Detection (CSMA/CD)



Mixing Physical Medium

- Plugging together 1000BASE-T and 100BASE-TX works
  - “T” implies 8-wire and backward compatible with 4-wire media (TX)
  - Auto negotiation resolves speed
- Does not work for all media
  - Cannot plug an optical fiber to an electrical connector
  - Unfortunately, T/TX are not compatible with T1



A Media Converter connects 2 dissimilar media

Media Converters

- Convert between different Physical Layer implementations of same network
- Commonly used in AE to connect 100/1000BASE-T1 to conventional Ethernet
- Intrepid's RAD-Moon:
  - 100BASE-T1 to 100BASE-TX
  - 4-wire to 2-wire
  - Essentially two different PHYs connected back-to-back
- RAD-MoonDuo:
  - 2x RAD-Moons in same form factor
  - PHY register access
  - 100BASE-T1/USB Bridge
- RAD-Moon2/SuperMoon:
  - 1000BASE-T1 to 1000BASE-T
  - 8-wire to 2-wire
  - Combine RAD-SuperMoon with RAD-Moon2 to implement an active tap (more on that later)

Data Link Layer

7 **Application Layer**

6 **Presentation Layer**

5 **Session Layer**
Interhost Communication

4 **Transport Layer**
TCP / UDP

3 **Network Layer**
IP Addressing, Routing

2 **Data Link Layer**
The Ethernet Frame, MAC Addresses

1 **Physical Layer**
Bit Stream, Physical Medium

The Ethernet Frame

- Lowest level structure to carry all data the data on Ethernet to meet the needs of Layer 2.
  - Device addressing
  - Message formatting,
  - Error detection
  - QoS
- Frames can carry 46 to 1,500 bytes of data
- 12,336 bits at 100 Mb/s takes 123.4 µs

  (compare to a 1 Mb/s 8-byte data frame)
- Gigabit = 12.34 µS Max Frame Transmission Time

802.3 Ethernet frame structure								
Preamble	Start of frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interframe gap
7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	46-1500 octets	4 octets	12 octets
		← 64-1518 octets (16-1522 octets for 802.1Q tagged frames) →						
← 84-1538 octets (88-1542 octets for 802.1Q tagged frames) →								

MAC Address

- Low-level / physical network address:
  - Programmed into hardware devices
  - 6 bytes long, each node globally unique *(usually)*
  - First 3 bytes is registered to an organization (OUI)
  - In AE, MAC address = Ethernet address
- Used to direct data on an Ethernet network:
  - Used in all 802 protocols (such as Wi-Fi)
  - Source / destination
  - Certain bit patterns in the address imply the type of ***addressing***.

802.3 Ethernet frame structure								
Preamble	Start of frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interframe gap
7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	46-1500 octets	4 octets	12 octets
		← 64-1518 octets (16-1522 octets for 802.1Q tagged frames) →						
← 84-1538 octets (88-1542 octets for 802.1Q tagged frames) →								

Unicast Addresses

- "Point-to-point"
- Used to send data to a specific node
- Universally Administered Address (UAA)
  - 2nd LSb of first octet of MAC address is "0"
  - Assigned by manufacturer using OUI
  - Most commonly **00**:XX:XX:XX:XX:XX
  - Globally unique
- Locally Administered Address (LAA)
  - 2nd LSb of first octet of MAC address is "1"
  - Designates the address is probably not unique outside an ***engineered network.*** *(Like say…., **parts** of an automotive network)*
  - E.g **02**:XX:XX:XX:XX:XX

Multicast Addresses

- “One-to-many”
- Specific MAC address that certain NICs are programmed to accept
- Used for protocol, process or vendor specific messaging
- LSb of the first octet of the Address = “1”
- Most commonly **01**:XX:XX:XX:XX:XX
- Broadcast
  - Special case where all NICs are intended to receive
  - MAC address is all 1’s (FF:FF:FF:FF:FF:FF hex)

Length/Ethertype/VLAN

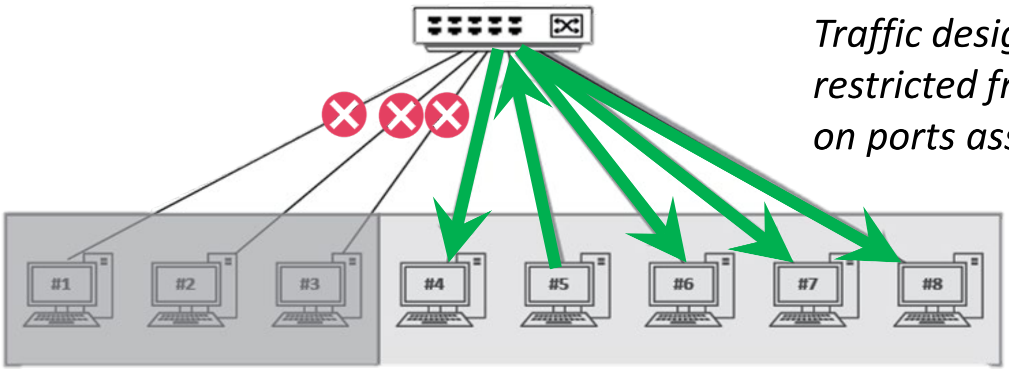
- Originally, the 16-bit Value following the SA indicated the length of the frame in bytes.
- As Ethernet evolved, this 16-bit value was repurposed*.
  - Needed a way to specify different information in the same space
  - Values < 1536 indicate length (legacy support)
  - Ethertype:
    - 2 Bytes indicating how information is organized in the Layer 2 header.
    - A value of 0x8100 or 0x9100 indicates the presence of a VLAN information followed by an Ethertype
    - Any other value is just an Ethertype

802.3 Ethernet frame structure								
Preamble	Start of frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interframe gap
7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	46-1500 octets	4 octets	12 octets
		← 64-1518 octets (16-1522 octets for 802.1Q tagged frames) →						
← 84-1538 octets (88-1542 octets for 802.1Q tagged frames) →								

*An example of Ethernet evolving to solve future problems as needs arise; key factor in automotive adoption.

Virtual LANs (VLANs)

- QoS at Layer 2 in hardware
- Ports assigned to "Virtual LANs"
  - Switch enforces forwarding restrictions based on VLAN configuration
  - VLAN traffic is blocked on ports not "a member" of that VLAN
- Used to optimize bandwidth use with least resources



Traffic designated on VLAN #2 is restricted from being forwarded on ports assigned to VLAN #1

How is this done? More on this when we talk about switches in detail…..

Common Automotive Ethertypes

General Use	0x0800	IPv4
	0x86DD	IPv6
	0x0806	Address Resolution Protocol
	0X8100	VLAN - Single Tag
	0x9100	VLAN - Double Tag
	0x88F5	Multiple VLAN Reservation Protocol

AVB	0x22F0	IEEE 1722
	0x88F7	generalized Precision Time Protocol
	0x22EA	Multiple Stream Reservation Protocol

V2X	0x88DC	Wave Short Message Protocol

Payload

- Where the actual Ethernet data is
- Ethertype defines the organization of the payload
- For example in IPv4, the beginning of the IP header starts here.

802.3 Ethernet frame structure								
Preamble	Start of frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interframe gap
7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	46-1500 octets	4 octets	12 octets
		← 64-1518 octets (16-1522 octets for 802.1Q tagged frames) →						
← 84-1538 octets (88-1542 octets for 802.1Q tagged frames) →								

Frame Check Sequence (CRC)

- Cyclical redundancy check for data integrity
- If the CRC fails, the frame is usually discarded by the switch or Ethernet MAC
- No built-in error recovery like CAN

(this is implemented at higher layers; hint: TCP)

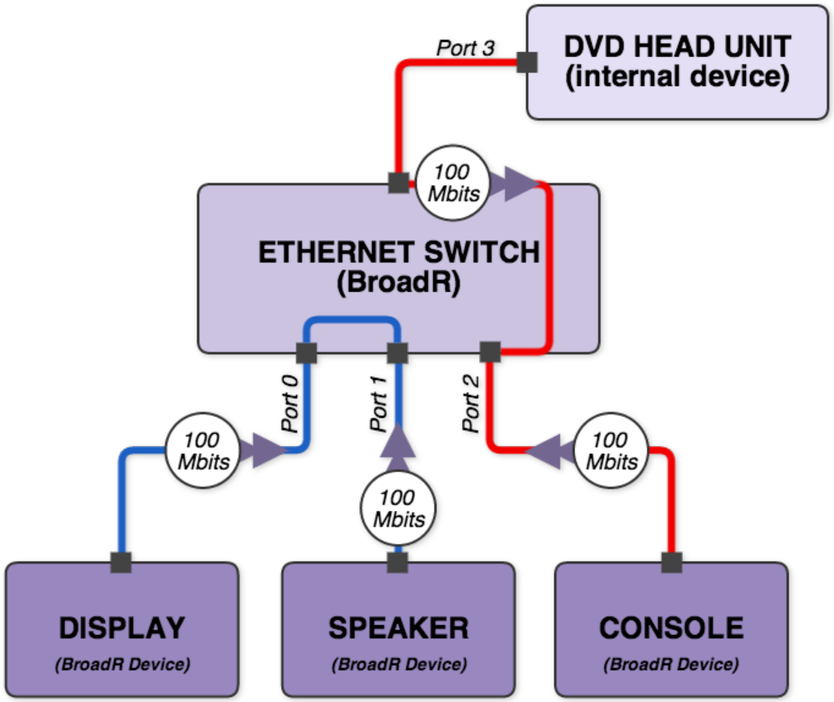
802.3 Ethernet frame structure								
Preamble	Start of frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interframe gap
7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	46-1500 octets	4 octets	12 octets
		← 64-1518 octets (16-1522 octets for 802.1Q tagged frames) →						
← 84-1538 octets (88-1542 octets for 802.1Q tagged frames) →								

Ethernet Switches

"The Why and the How"

Why Use A Switch?

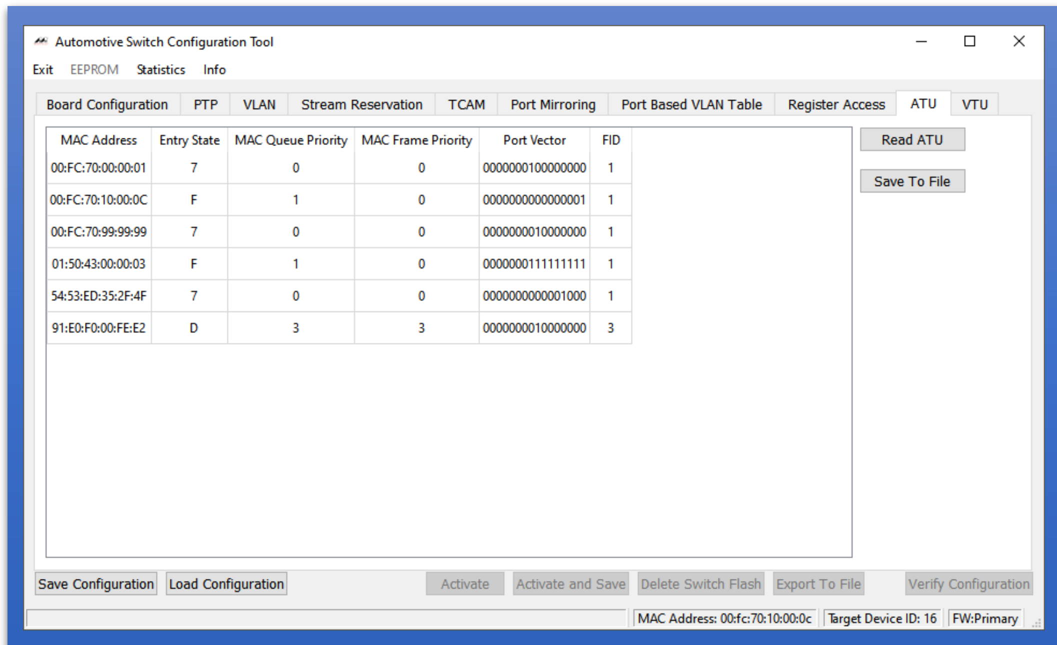
- Conserve bandwidth by intelligent forwarding based on MAC Address
  - Each physical port connection independent
  - No collisions
- Enables L2 QoS
  - Drops bad frames
  - VLAN Enforcement/Management
  - Traffic Prioritization
  - Ingress Limiting
  - AVB/TSN Protocols
- Switches have evolved to deliver additional features and functionality



400 Mbits of bandwidth!

Intelligent Frame Forwarding

- L2 Address Table
  - Used by *Address Translation Unit*
  - Table of Address/Port (physical) associations
- Information Stored
  - MAC Address
  - Destination Port Vector (DPV)
    (bit array of ports for the MAC)
  - VLAN Information
    (FID / Filtering Information Database)
  - Static or Learned
  - Priorities



MAC Address	Entry State	MAC Queue Priority	MAC Frame Priority	Port Vector	FID
00:FC:70:00:00:01	7	0	0	0000000100000000	1
00:FC:70:10:00:0C	F	1	0	0000000000000001	1
00:FC:70:99:99:99	7	0	0	0000000010000000	1
01:50:43:00:00:03	F	1	0	0000000111111111	1
54:53:ED:35:2F:4F	7	0	0	0000000000001000	1
91:E0:F0:00:FE:E2	D	3	3	0000000010000000	3

Unmanaged and Smart Switches

- No official delineation
- Unmanaged Switch
  - Little or no configuration
  - MAC Based Routing
  - Learns L2 Address Table
  - Floods unknown DAs
  - Possibly static L2 Address table configuration
- Smart Switch
  - Basic VLAN Support (Static Config, Enforcing Tag/Priority, tag/un-tag, etc.)
  - Port Mirroring

Managed Switches

Managed Switch enhances QoS and Security

- Addition of host processors or embedded cores
- Firmware executes protocols
  - Dynamic VLAN management (MVRP)
  - Manage Redundant Paths (Spanning Tree Protocol, etc.)
  - AVB/TSN Protocols
- Other advanced features
  - Deep Packet Inspection
  - Ingress Policing and Limiting

Smart Switch Example: RAD-Pluto

5-Ports - Based on NXP SJA1105

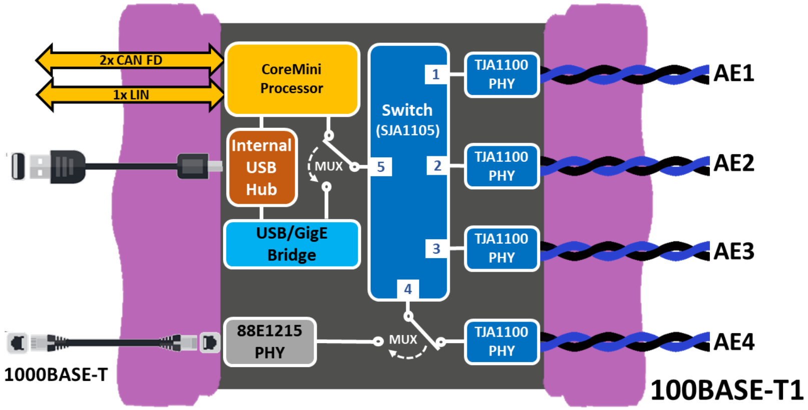
- 3x 100BASE-T1
- 1x 100BASE-T1 or 1x 1000BASE-T
- 1x USB3/GIGE Bridge

Integral CAN/LIN Interfaces

- 2x CAN-FD
- 1x LIN
- Embedded Function Block Execution

Use Cases

- VLAN Tagging/Untagging (Static)
- Port Forwarding
- Gateway applications
- Media Conversion
- Frame Mirroring and VLAN tagging for advanced debug and monitoring.



Managed Switch Example: RAD-Jupiter

Based on Marvell 88Q5050

7-Port Managed Switch
- 5x 100BASE-T1
- 1x 1000BASE-T1 or 1000BASE-T
- USB3/GIGE Bridge or 1x 1000BASE-T
- **AVB/TSN Protocol Support**
- **Packet Inspection (TCAM)**
- **Per-port address whitelisting/blacklisting**

Advanced Features
- **AVB/TSN Protocols**
- **TCAM**
- **Ingress Rate Limiting**
- **“Cut-Through” Forwarding**

Integral CAN/LIN Interfaces
- 2x CAN-FD
- 1x LIN
- Embedded Function Block Execution

Use Cases
- **AVB/TSN Development & Testing**
- Gateway applications
- Media Conversion
- Frame Mirroring and VLAN tagging for advanced debug and monitoring.

Network Layer

7	**Application Layer**
6	**Presentation Layer**
5	**Session Layer** Interhost Communication
4	**Transport Layer** TCP / UDP
3	**Network Layer** IP Addressing, Routing
2	**Data Link Layer** The Ethernet Frame, MAC Addresses
1	**Physical Layer** Bit Stream, Physical Medium

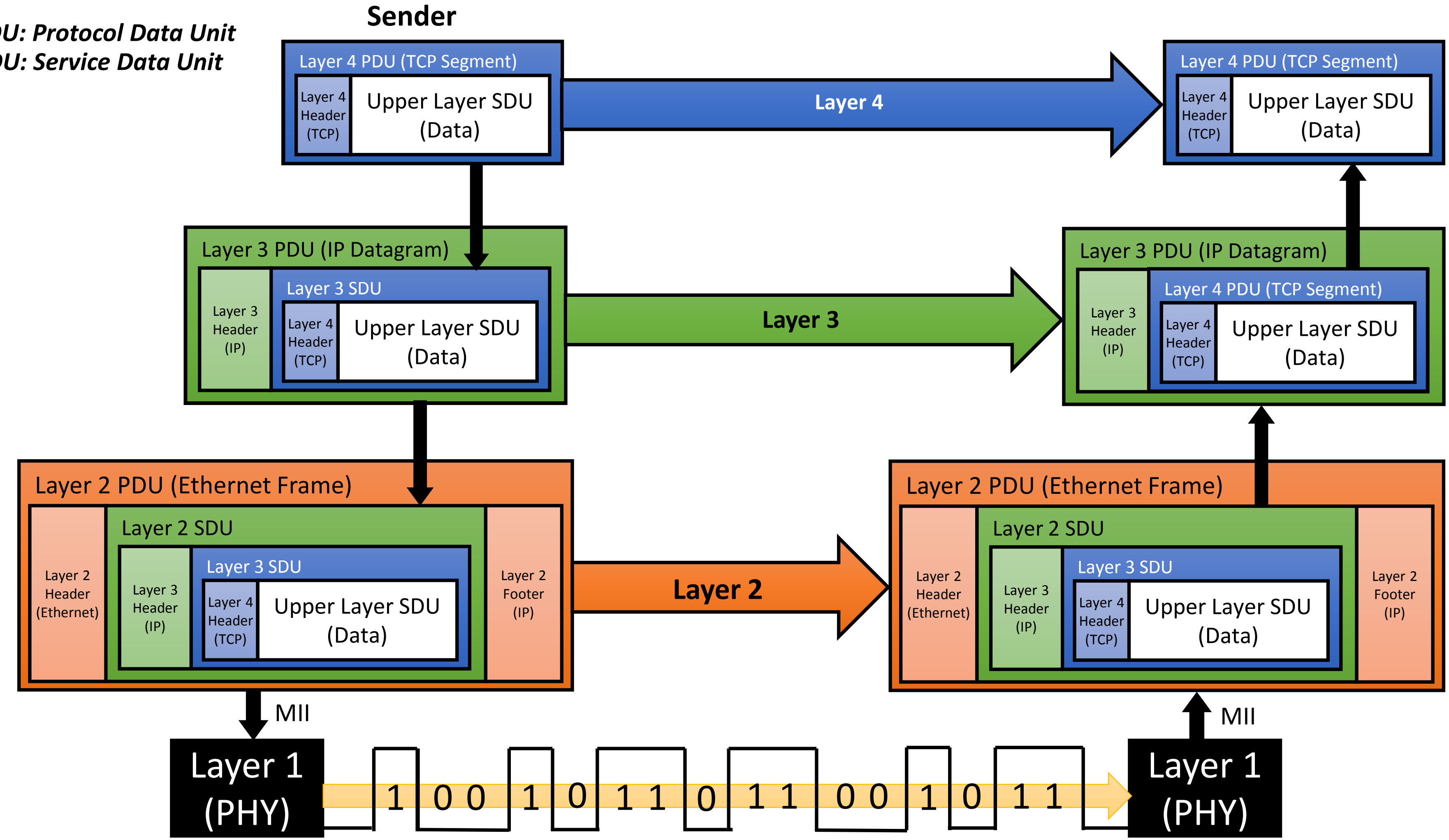
Why do we need higher layer protocols?

Inherent problems with Ethernet….

- MAC Addresses tied to hardware (physical address)
  - Much like CAN frames
  - Physical Addressing
    - What if you move a server to new hardware with a new MAC Address?
  - Connectionless
    - What if the receiver is not ready or has a limited buffer size?
    - What if the same physical address is running multiple logical programs?
- An Ethernet frame is 1500 bytes.
- Ethernet is lossy
  - No guarantee frames arrive in order
  - No guarantee frames arrive at all…..

Message Encapsulation

PDU: Protocol Data Unit
SDU: Service Data Unit



IP Header

(Slide 1/4)

IPv4 has the EtherType 0x0800

4 for IPv4

Internet Header Length (# of 32-bit words)

Differentiated Service (Traffic Management)

Offsets	**Octet**	**0**								**1**								**2**								**3**							
Octet	**Bit**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**
0	**0**	Version				IHL				DSCP						ECN		Total Length															
4	**32**	Identification																Flags			Fragment Offset												
8	**64**	Time to Live								Protocol								Header Checksum															
12	**96**	Source IP Address																															
16	**128**	Destination IP Address																															
20	**160**	Options (if IHL > 5)																															

A number used to identify fragments of the same datagram

Explicit Congestion Notification

(extension to detect dropped packets)

Total length of header and data

IP Header

(Slide 2/4)

For large packets being fragmented, the position of this fragment

<table>
<tr><th>Offsets</th><th>Octet</th><th colspan="8">0</th><th colspan="8">1</th><th colspan="8">2</th><th colspan="8">3</th></tr>
<tr><th>Octet</th><th>Bit</th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td>0</td><td>0</td><td colspan="4">Version</td><td colspan="4">IHL</td><td colspan="6">DSCP</td><td colspan="2">ECN</td><td colspan="16">Total Length</td></tr>
<tr><td>4</td><td>32</td><td colspan="16">Identification</td><td colspan="3">Flags</td><td colspan="13">Fragment Offset</td></tr>
<tr><td>8</td><td>64</td><td colspan="8">Time to Live</td><td colspan="8">Protocol</td><td colspan="16">Header Checksum</td></tr>
<tr><td>12</td><td>96</td><td colspan="32">Source IP Address</td></tr>
<tr><td>16</td><td>128</td><td colspan="32">Destination IP Address</td></tr>
<tr><td>20</td><td>160</td><td colspan="32">Options (if IHL > 5)</td></tr>
</table>

Each router decrements by one;
if zero is reached, packet is discarded

Flags:
bit 0: Reserved; must be zero
bit 1: Don't Fragment (DF)
bit 2: More Fragments (MF)

IP Header

(Slide 3/4)

<table>
<tr><th>Offsets</th><th>Octet</th><th colspan="8">0</th><th colspan="8">1</th><th colspan="8">2</th><th colspan="8">3</th></tr>
<tr><th>Octet</th><th>Bit</th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td>0</td><td>0</td><td colspan="4">Version</td><td colspan="4">IHL</td><td colspan="6">DSCP</td><td colspan="2">ECN</td><td colspan="16">Total Length</td></tr>
<tr><td>4</td><td>32</td><td colspan="16">Identification</td><td colspan="3">Flags</td><td colspan="13">Fragment Offset</td></tr>
<tr><td>8</td><td>64</td><td colspan="8">Time to Live</td><td colspan="8">Protocol</td><td colspan="16">Header Checksum</td></tr>
<tr><td>12</td><td>96</td><td colspan="32">Source IP Address</td></tr>
<tr><td>16</td><td>128</td><td colspan="32">Destination IP Address</td></tr>
<tr><td>20</td><td>160</td><td colspan="32">Options (if IHL > 5)</td></tr>
</table>

The protocol of the payload – the “layer 4” protocol

Source IP address

Checksum of the header (only)

Protocol Number	Protocol
1	ICMP - Internet Control Message Protocol
2	IGMP - Internet Group Management Protocol
6	TCP - Transmission Control Protocol
17	UDP - User Datagram Protocol

IP Header

(Slide 4/4)

<table>
<tr><th>Offsets</th><th>Octet</th><th colspan="8">0</th><th colspan="8">1</th><th colspan="8">2</th><th colspan="8">3</th></tr>
<tr><th>Octet</th><th>Bit</th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td>0</td><td>0</td><td colspan="4">Version</td><td colspan="4">IHL</td><td colspan="6">DSCP</td><td colspan="2">ECN</td><td colspan="16">Total Length</td></tr>
<tr><td>4</td><td>32</td><td colspan="16">Identification</td><td colspan="3">Flags</td><td colspan="13">Fragment Offset</td></tr>
<tr><td>8</td><td>64</td><td colspan="8">Time to Live</td><td colspan="8">Protocol</td><td colspan="16">Header Checksum</td></tr>
<tr><td>12</td><td>96</td><td colspan="32">Source IP Address</td></tr>
<tr><td>16</td><td>128</td><td colspan="32">Destination IP Address</td></tr>
<tr><td>20</td><td>160</td><td colspan="32">Options (if IHL > 5)</td></tr>
</table>

Destination IP address

Extra options; in practice almost always empty

Transport Layer

7 **Application Layer**

6 **Presentation Layer**

5 **Session Layer**
Interhost Communication

4 **Transport Layer**
UDP / TCP

3 **Network Layer**
IP Addressing, Routing

2 **Data Link Layer**
The Ethernet Frame, MAC Addresses

1 **Physical Layer**
Bit Stream, Physical Medium

The Departure from Signal-Based Messaging

- CAN was always meant to be a sensor network
  - "Implicit availability" – periodic messages with latest values
  - Works well for simpler systems to just get signal values from point A to point B
- Consequently CAN is not well suited for
  - Two nodes need to ***negotiate parameters***
  - ***Stateful connections*** between many functional units (think of the communication between a hands-free phone and the head unit)
- Ethernet Protocols introduce the concept of a logical connection
  - Exclusive between 2 software processes
  - Negotiation on connection, flow control, and disconnection
  - In some cases reliability (at the expense of high availability)

Process-Level Addressing: Ports

- IP address identifies a device (ECU or NIC on a PC)
- TCP and UDP use *Ports* to identify software processes
  - Application or Function
  - Virtual ECU within the module
- IP address + port = ***socket***
  - Sockets uniquely identify an Internet connection between specific processes on two different IP Addresses
- TCP and UDP messages include 16-bit source and destination port addresses (0 to 65,535)
- Well-known ports solve the problem of how to know where to send particular types of requests on a device (e.g., 80 for Web servers)

A word about “ports”

- Logical Ports
  - Layer 4 concept to differentiate logical connections
  - Port + IP Address = Socket
- Physical Ports
  - Connection between Physical Layer (PHY) and the Physical Media
  - “Port” on a switch
  - “Port” on a computer

It’s all about the context...

For example, are these referring to a physical or logical port

The switch needs to be configured to forward between the desired ports for your application. *Switch = Layer 2, must be physical*

The router is setup for port forwarding. *Router = Layer 3, must be logical*

The server is connected to the wrong port. *Need more info….*

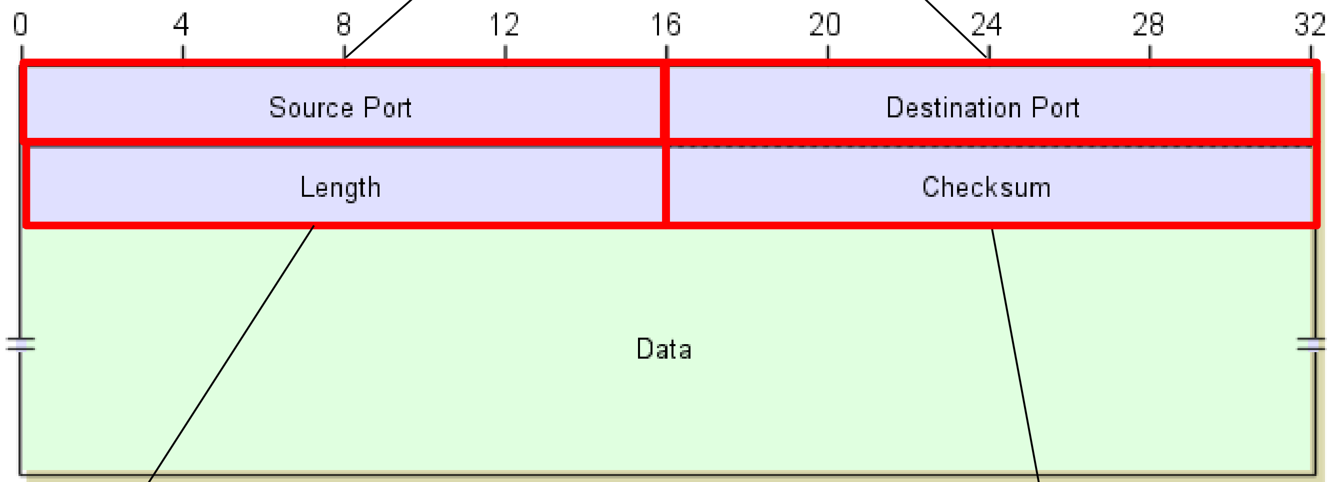
UDP (User Datagram Protocol)

User Datagram Protocol (UDP)

- Lighter transfer protocol than TCP
  - Unreliable by design
    - Does not guarantee delivery and packet order
    - Used where timely delivery is more important than service guarantees
- Analogous to a CAN frame
  - No acknowledgement from recipient ("Fire and Forget")
  - Usually no specific recipient (multi or broadcast)
  - Easy to "map" CAN messaging over to Ethernet with UDP
  - Unlike CAN, UDP has no U-Code
    - Flag set when expected information is not received
    - UDP intended to be lightweight. Need something more? Use another protocol (like TCP).

UDP Header

Source and Destination Ports –
Assigned to specific processes



Length of UDP (up to 64K bytes)

Optional checksum, 0 = no checksum,
All 1's = 0 checksum

TCP (Transmission Control Protocol)

Transmission Control Protocol (TCP)

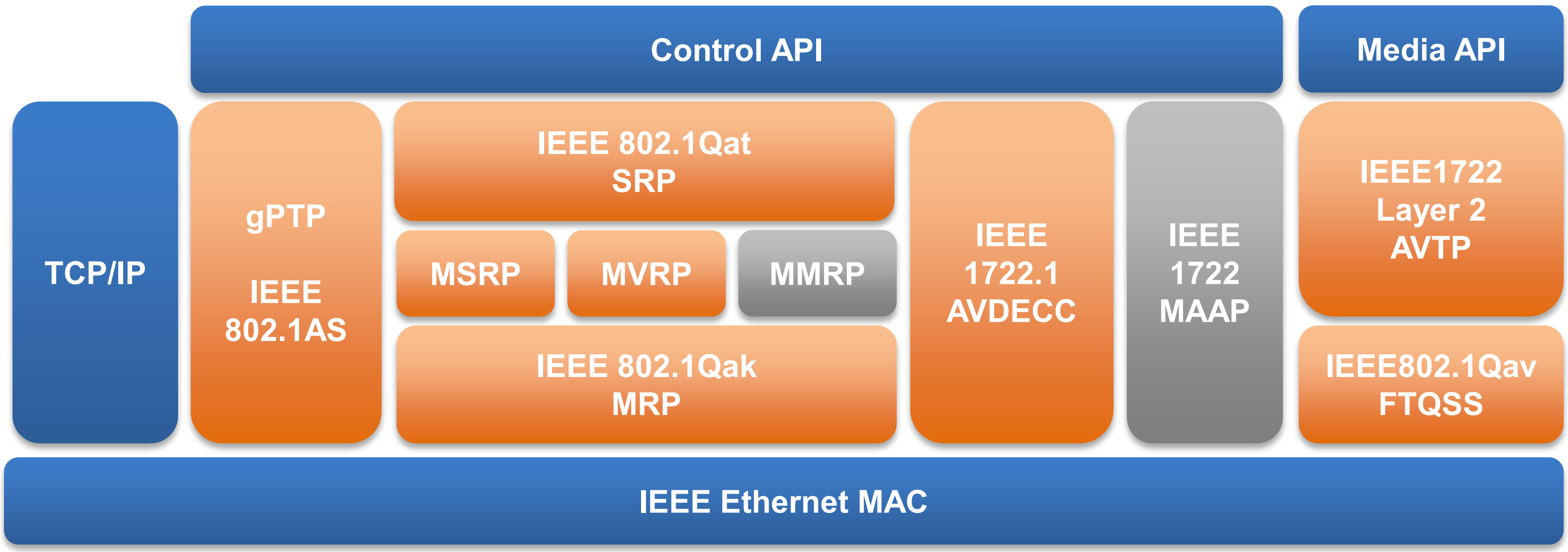
- TCP is a full-featured transfer protocol
  - TCP turns Ethernet into a ***reliable, connection-oriented*** stream
  - Analog in CAN is ISO 15765-2
- Unlike other protocols, TCP has the native concept of a connection
  - For two nodes to talk, one must initiate a connection to another, and it must be accepted
  - Creates an implicit ***client/server*** model
  - Web browsers talk to websites over TCP

Transmission Control Protocol (TCP)

- TCP guarantees that all packets will
  - Arrive at the client
  - Be seen by the receiving application in the same order they were sent
- The second point is one often overlooked by other protocols
- Since Ethernet is switched, each packet could take different paths and arrive out-of-order

AVB Stack Components

(A 3-hour class in itself)



AVB vs. TSN Protocols

Time Synchronization

- IEEE802.1AS gPTP
- IEEE802.1AS-Rev

Resource Management

- IEEE802.1Qat SRP
- IEEE802.1Qcc
  SRP enhancement and performance improvement

Transport Stream and Control

- IEEE1722
  AVTP
- IEEE 1722.1
  AVDECC

Scheduling

- IEEE802.1Qav
  FQTSS (CBS)
- IEEE802.1Qch
  Cyclic queuing and forwarding
- IEEE802.1Qbv
  Enhancements for Scheduled Traffic (TAS)
- IEEE802.1Qcr
  Asynchronous Traffic Shaping

Preemption

- IEEE802.1Qbu
  Frame Preemption
- IEEE802.3br
  Interspersing Express Traffic

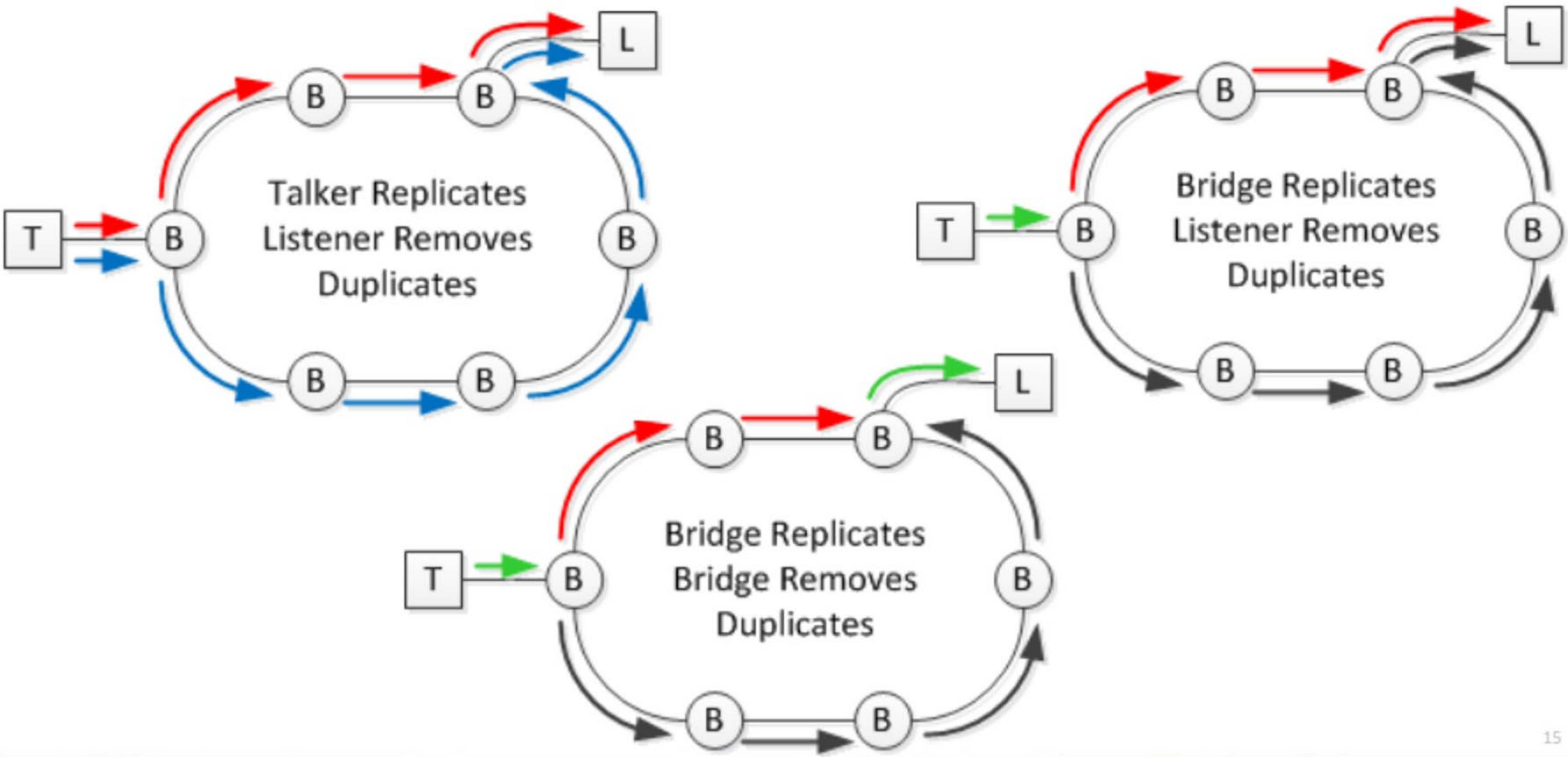
Fault Tolerance

- IEEE802.1CB
  Frame Replication and Elimination for Reliability
- IEEE802.1Qca
  Path Control and reservation for redundancy
- IEEE802.1Qci
  Per-Stream Filtering and Policing

AVB Protocol

Newly Developed for TSN

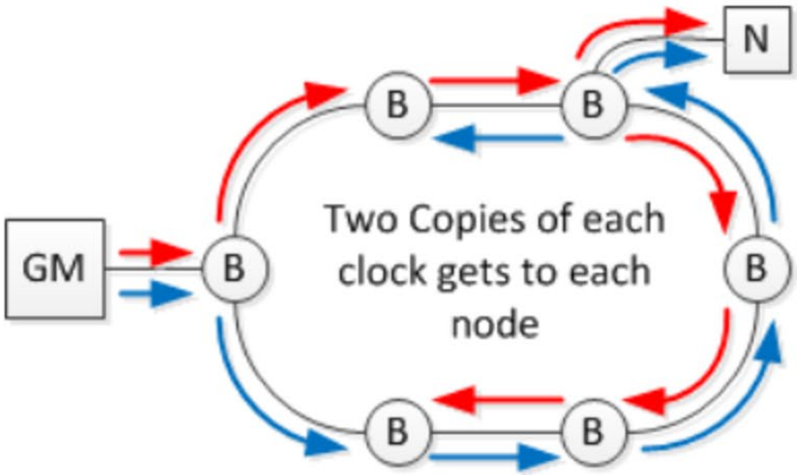
Frame Replication and Elimination (802.1CB)



INTREPID CONTROL SYSTEMS www.intrepidcs.com

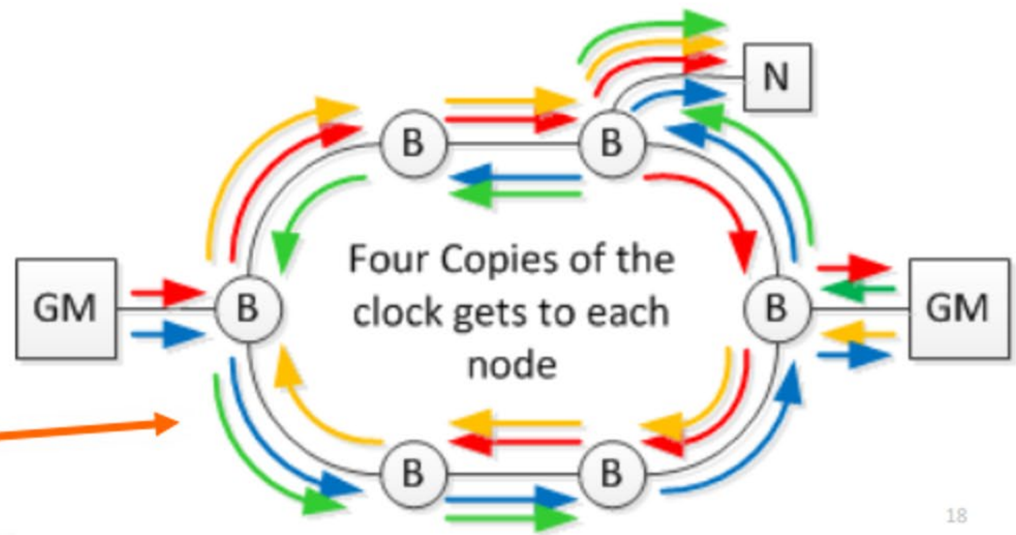
automotive engineering tool alliance

Enhanced gPTP (802.1AS-Rev)



- Single Grand Master transmitting 2 copies of its clock using separate paths

- Dual Active Grand Masters each transmitting 2 copies of their clock using separate paths



Questions?

Discover more at www.intrepidcs.com

Or contact us:

Sales:
icssales@intrepidcs.com
+1 (586) 731-7950 x 2

Technical Support:
icssupport@intrepidcs.com
www.intrepidcs.com/support
+1 (586) 731-7950 x 1

John Simon,
Product & Applications Manager
jsimon@intrepidcs.com