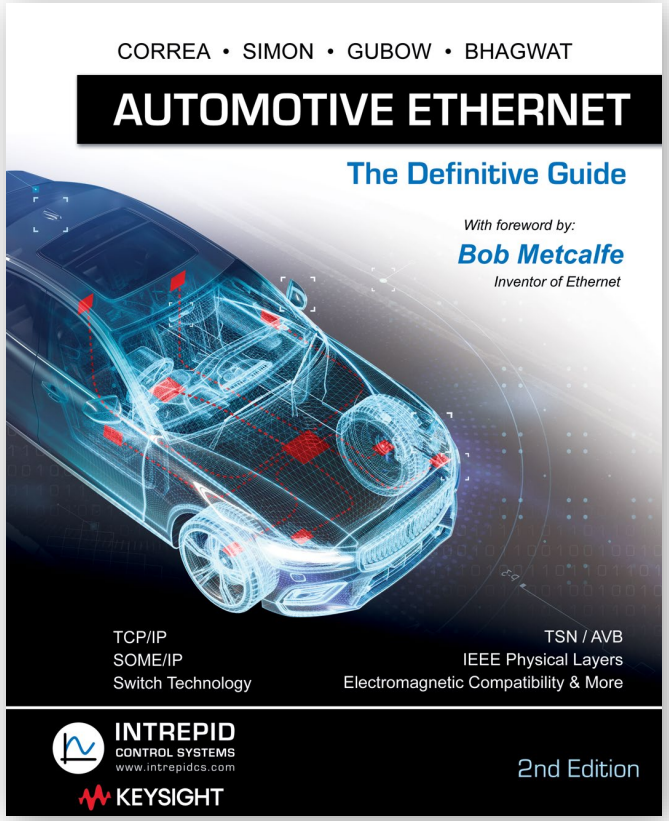
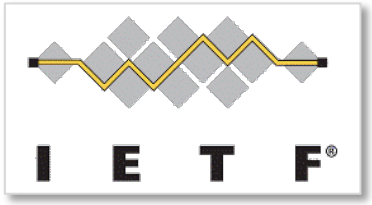
Introduction to Automotive Ethernet



Relevant Organizations



Internet Engineering Task Force (IETF)

RFCs (793, 768, 791)

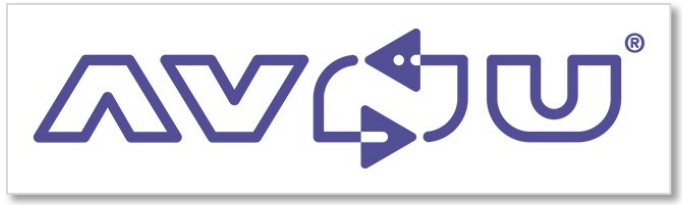
Institute of Electrical and Electronics Engineers
(802.3, 802.11, 802.1AS, 802.bla.bla)

Automotive Ethernet SIG
(IEEE 100BASE-T1, 1000BASE-T2, 1000BASE-RH)

International Organization for Standardization
(ISO14229, ISO15765-2, ISO7498-1)

Relevant Organizations…

Association for Standardization of Automation and Measuring Systems



AVB / TSN Certification

AUTomotive Open System ARchitecture

Society of Automotive Engineers (J1962, J1939, J2534)

Networking Fundamentals

Networking Fundamentals

Automotive Networking is simply any method of enabling ECU / Computers / Nodes / Device Hosts to exchange data.

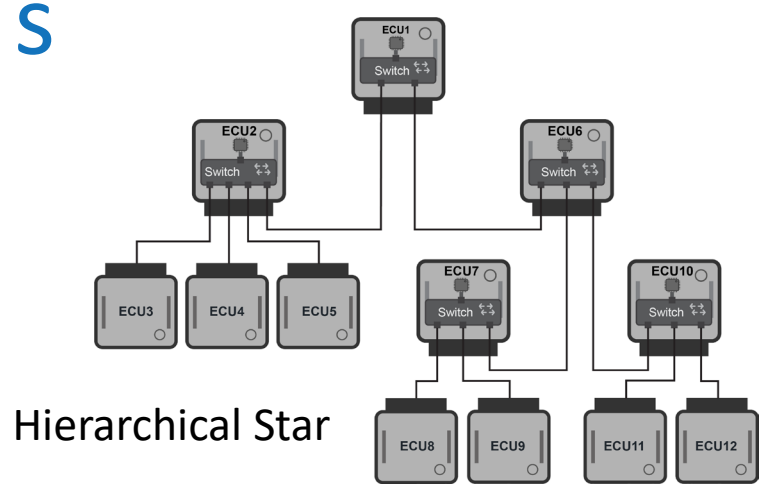
Note: We will use ECU / Computer / Node / Host / Device interchangeably

Practical concepts to consider in networking:

- How to prevent, control or handle possible message / frame collisions?
- How will topology affect wiring costs, length and weight?
- How robust communication will be if there is a physical failure?
- What type of data must be carried on the network? (Stream, packet, etc.)

Basic Networking Topologies

- A topology defines how devices are physically connected
- Tradeoffs in network characteristics
  - Cost
  - Redundancy
  - Latency
  - Etc.

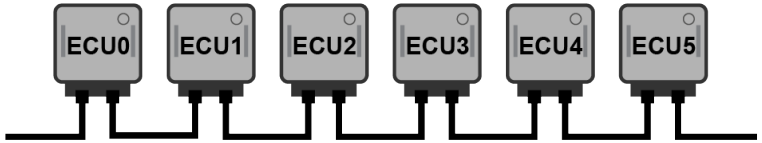


Hierarchical Star

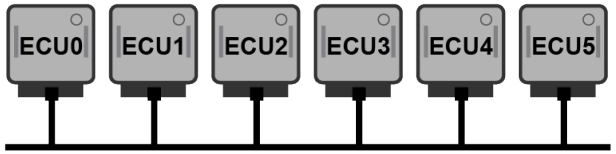
SerDes Ethernet

Point to point

A2B / FireWire



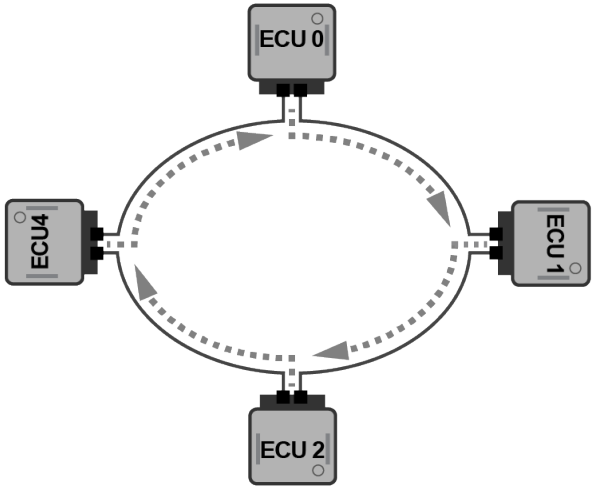
Daisy Chain



BUS

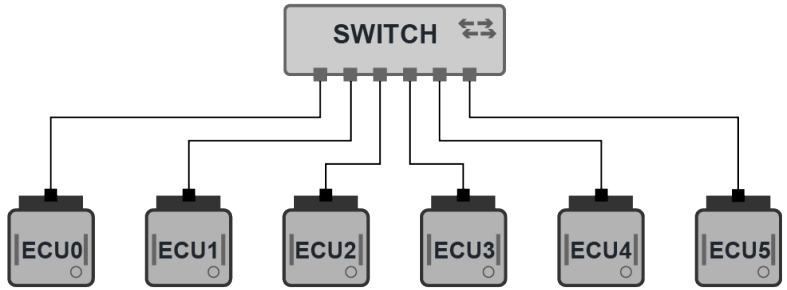
CAN FD / LIN / FlexRay / 10BASE-T1S

MOST Ethernet



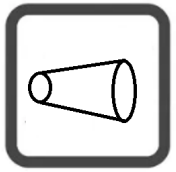
Ring

Ethernet



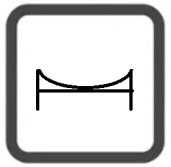
Star

Common Ethernet Device Types

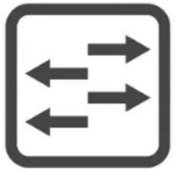


Repeater – Has 2 ports. Transmits all network traffic received on one port out the other port.

Hub – Almost the same as a Repeater but has more than 2 ports. Transmits all traffic received on one port out all others.



Bridge – Smart device with 2 ports. Forwards traffic received based on strict rules. Primarily operates on Layer 2 of OSI.

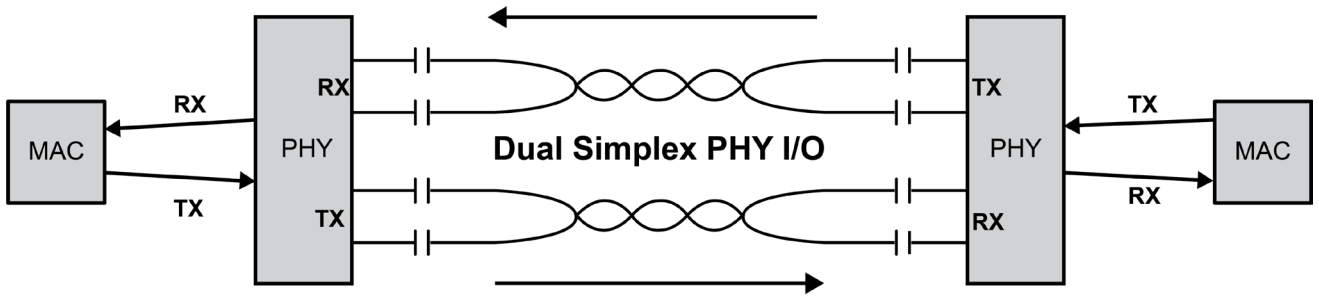


Switch – Bridge with more than 2 ports. Fundamental part in Automotive Networking. Primarily operates on Layer 2 of OSI.

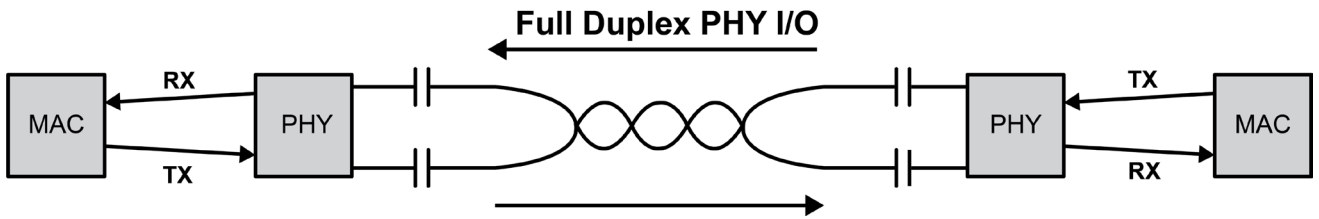
Router – Primarily responsible for directing IP traffic at Layer 3. Used as a device to interact with the internet.

Network Transmission Modes

- Simplex: one-way street (P.A. System)
- Half-Duplex: one at a time Transmit, Multi-Rx (CAN / LIN, 10BASE-T1S)
- Full-Duplex: two devices at the same time (Telephony)



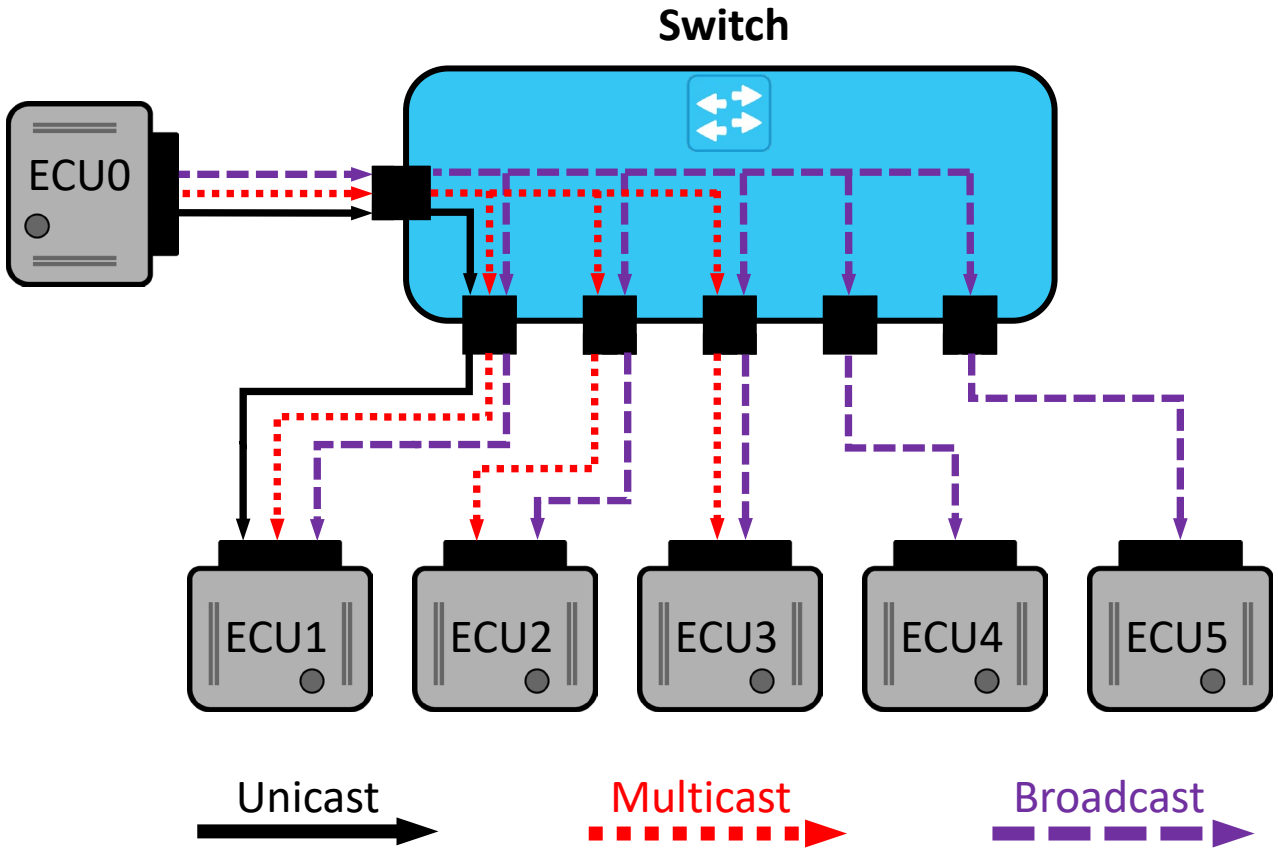
"Dual simplex" ➔ two one-way streets ➔ 100BASE-**TX used in DoIP**



"True full-duplex" ➔ uses one physical link ➔ 100/1000/MultiGBASE-**T1**

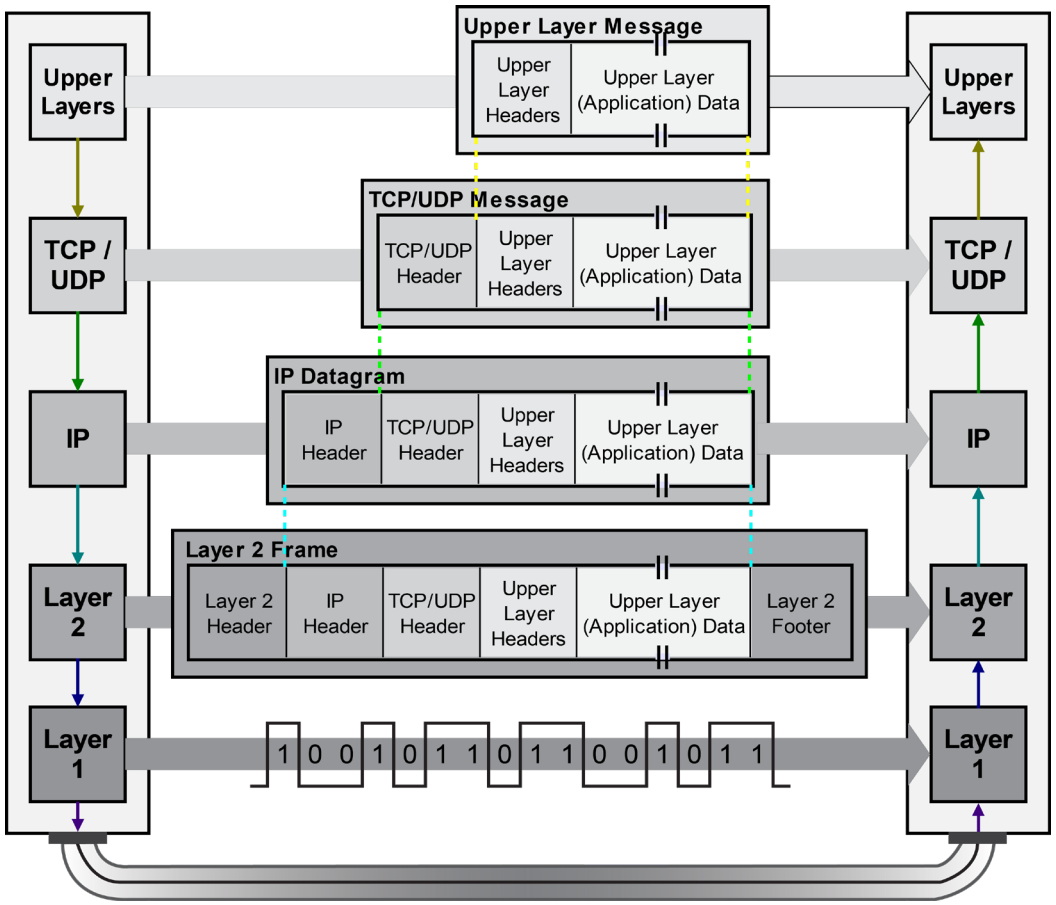
Network Addressing Methods

- Unicast: one to one
  - Client/Server
- Broadcast: one to all
  - Management and discovery protocols
- Multicast: one to many
  - Streams



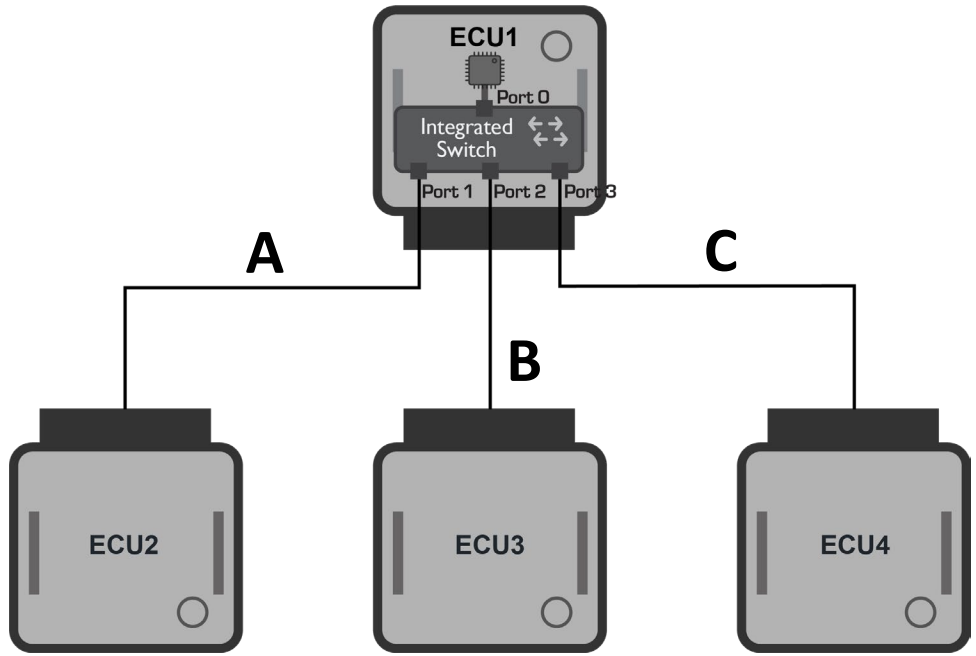
Data Encapsulation

- Protocol Data Unit (PDU)
  - Header + Payload
  - A PDU created at one layer becomes the payload of the service at the next lower level
- Transmitted Data
  - Passed down the stack
  - Each layer adds its own header
  - Messages are nested like “Russian dolls”
- Received Data
  - Nested message passed back up the stack
  - Each header is used to control that layer’s operation and is then removed



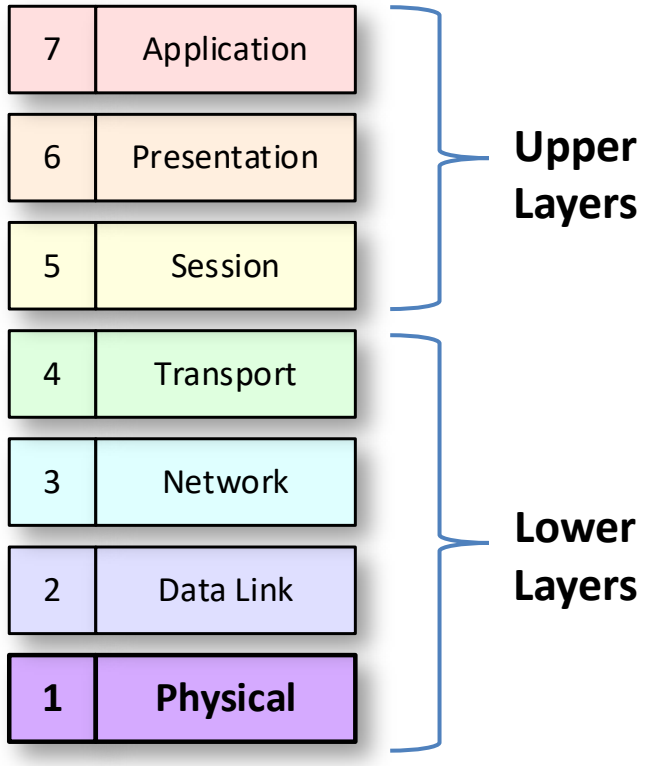
Today's Ethernet Network

- 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.

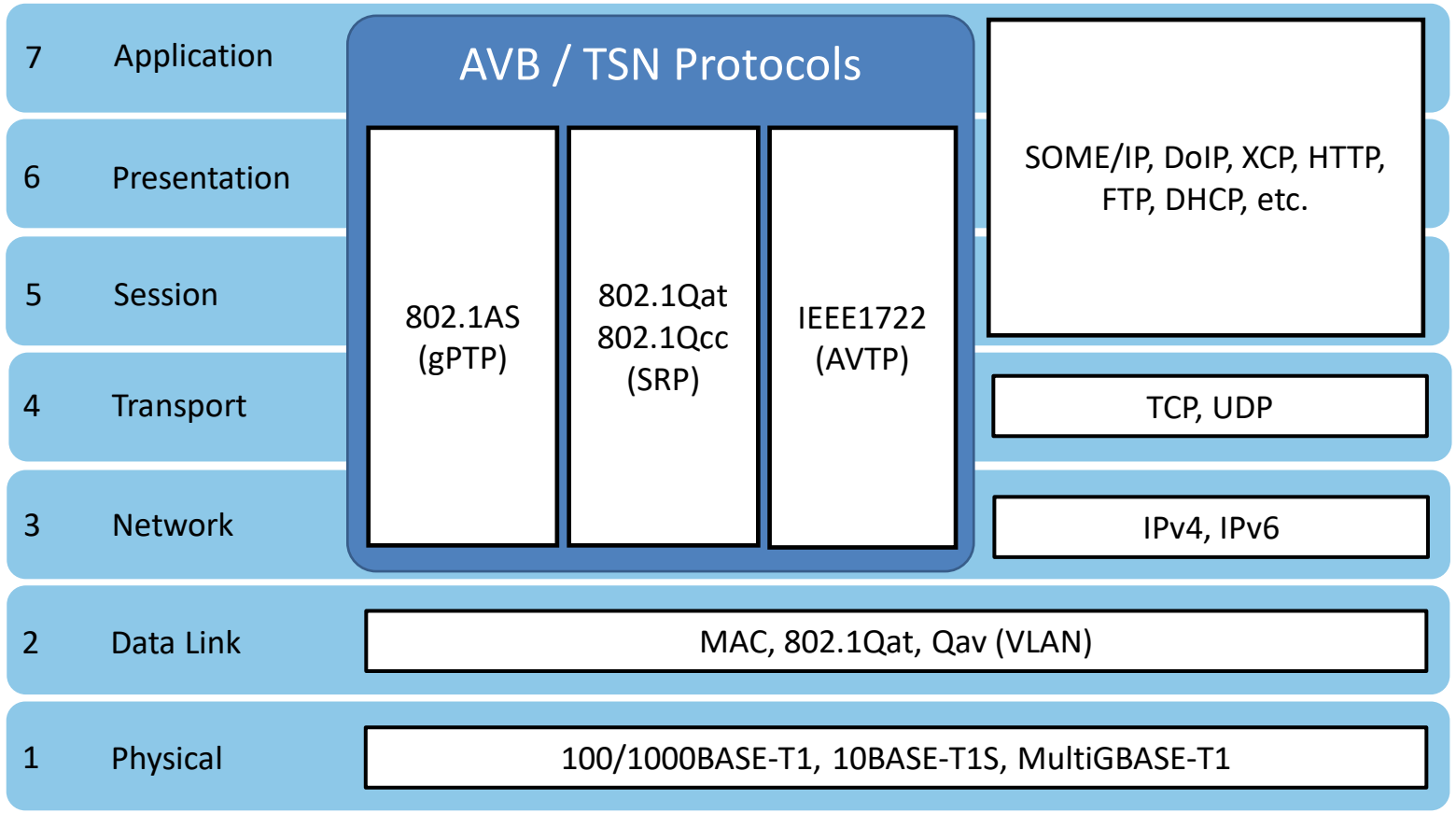


Layers and Layer Groupings

- Layers numbered in increasing order from most concrete to most abstract
- Lower layers: 1 to 4
- Upper layers: 5 to 7
- Layer 4 can go in either place
- Some technologies don't fit the paradigm strictly (TCP/IP)
- Some ignore this aspects of this model (AVB/TSN)



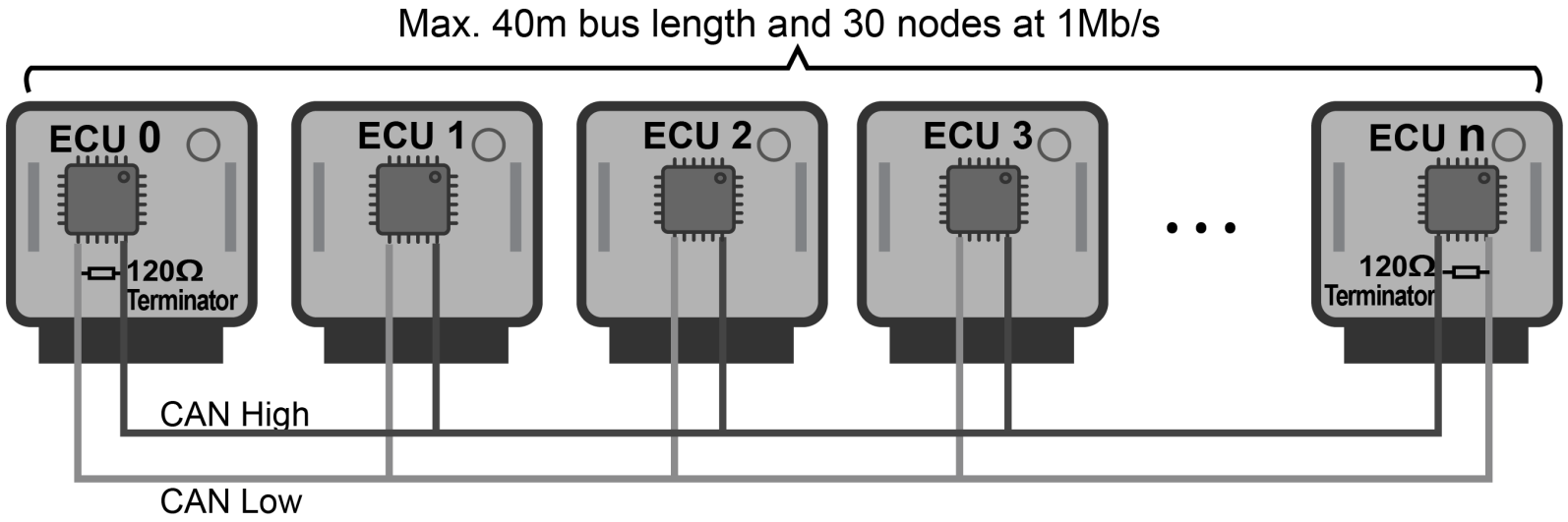
OSI applied to Protocol Suites



Automotive Networking Technologies Compared

CAN

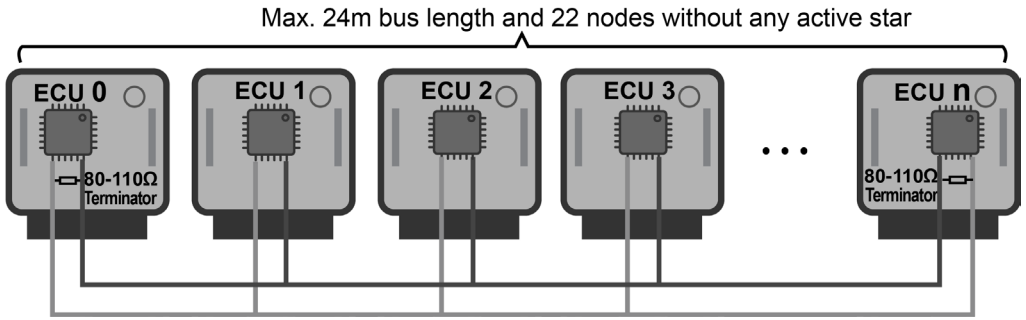
- Basics
  - Multi-drop
  - UTP
  - Up to 10 Mbit/s
  - Most widely used Automotive Technology

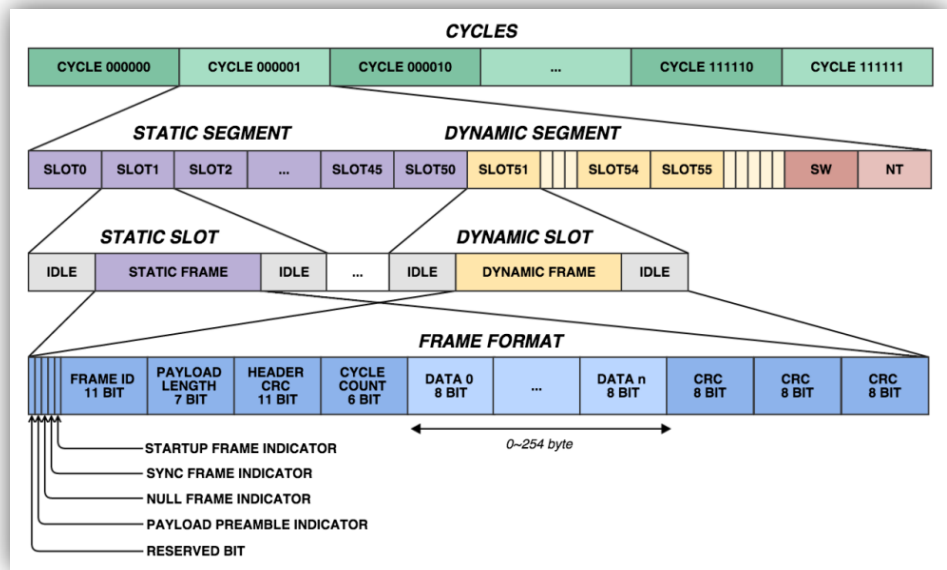


- Pros
  - Add and remove nodes without major effects on other nodes
  - Easy environment for tool manufacturers: plug and play
- Cons
  - Limited Bandwidth up to 8-10 Mbs
  - Relatively Small Payload CAN FD at 64

FlexRay

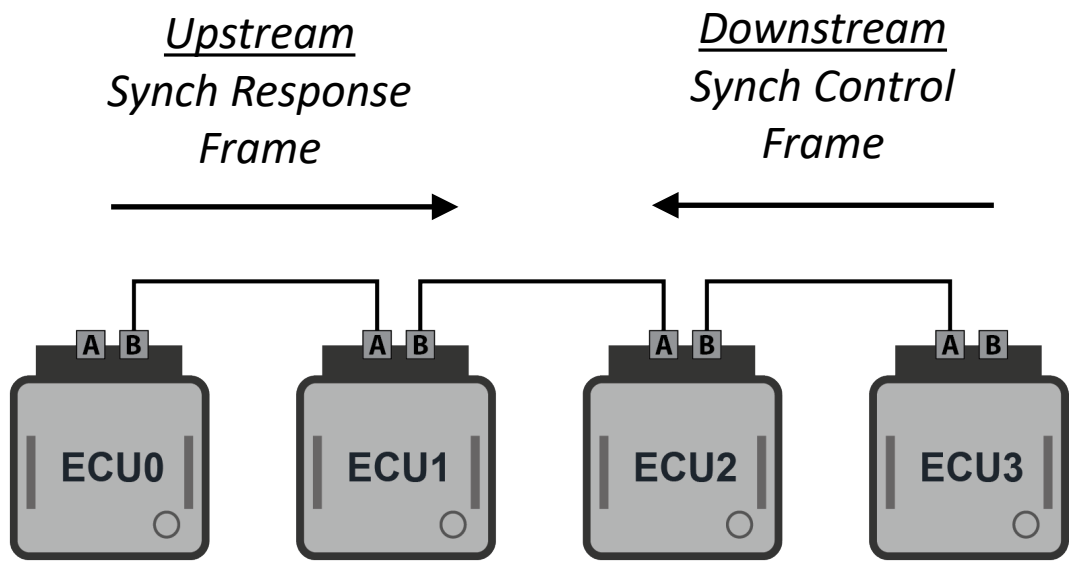
- Basics
  - Multidrop topology
  - UTP
  - Up to 10 Mbit/s (10 times greater than normal CAN)
- Pros
  - Great Clock synchronization
  - Deterministic (static frames)
- Cons
  - Must design the entire network at one time
  - All nodes must be aware of and programmed for the entire network design

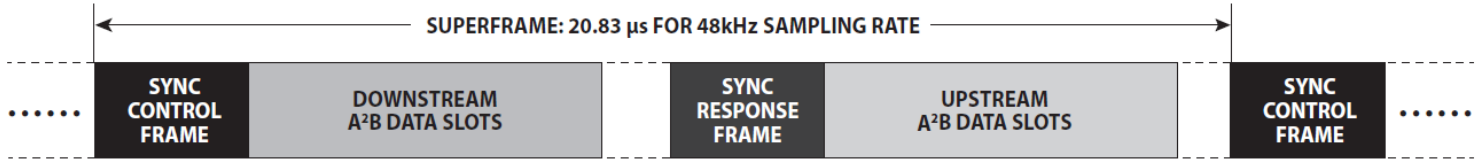




A²B – Automotive Audio Bus

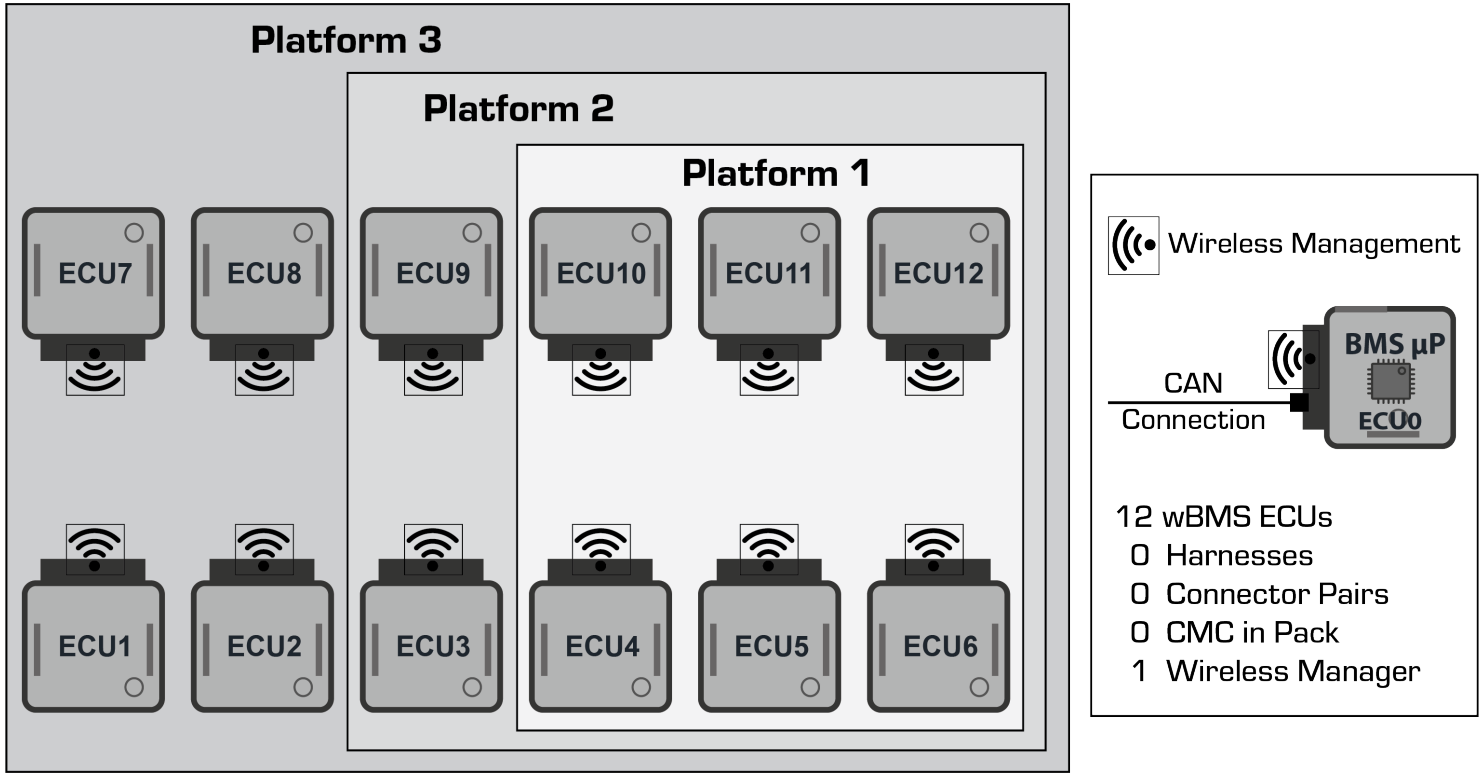
- Basics
  - Daisy-Chain
  - UTP
  - Up to 50 Mbit/s
  - 15 m between nodes, 40 m total
- Pros
  - Easy implementation & support for I2C
  - Synchronization built in
- Cons
  - Single source - wBMS
  - Specialized use cases



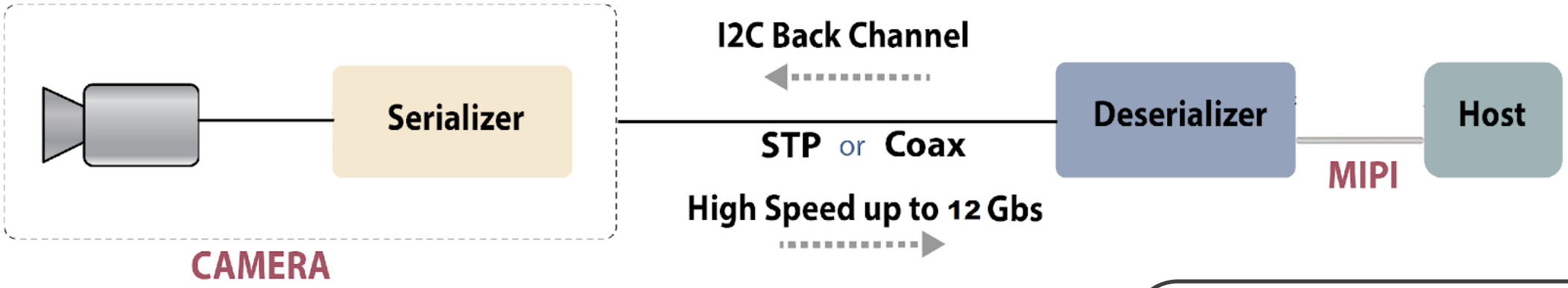


wBMS – Wireless Battery Management

- Basics
  - 2.5 GHz wireless
  - Up to 24 nodes / 288 cells
- Pros
  - No wires!
  - Low cost, low weight (air)
- Cons
  - Single source – Analog Devices
  - Specialized use cases



Serializer / De-Serializer – "SerDes"



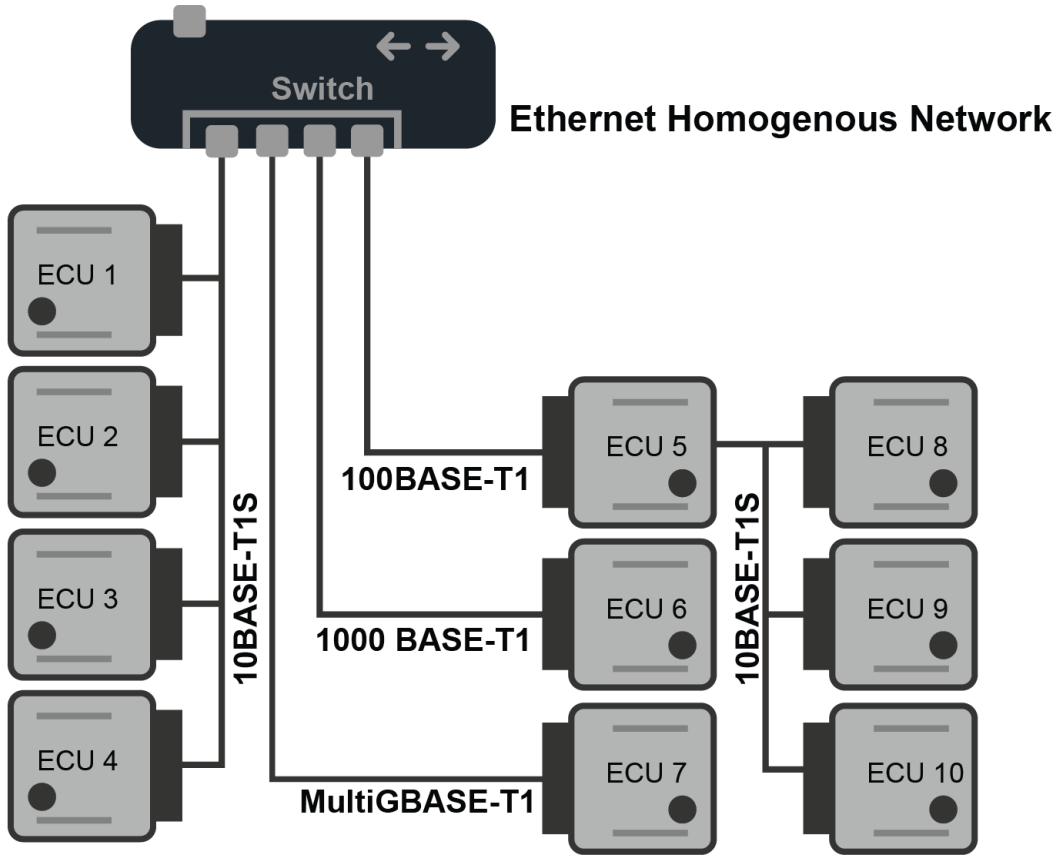
- Basics
  - 1.6 to 12Gbs
  - STP or COAX
  - 10 to 15 m
  - Point-to-point
- Pros
  - High Speed
  - Simple implementation
  - Camera / video support
- Cons
  - Proprietary. Standard being worked on ->
  - Point-to-point only

Texas Instruments — FPD-LINK
maxim integrated — GMSL
SONY — GVIF

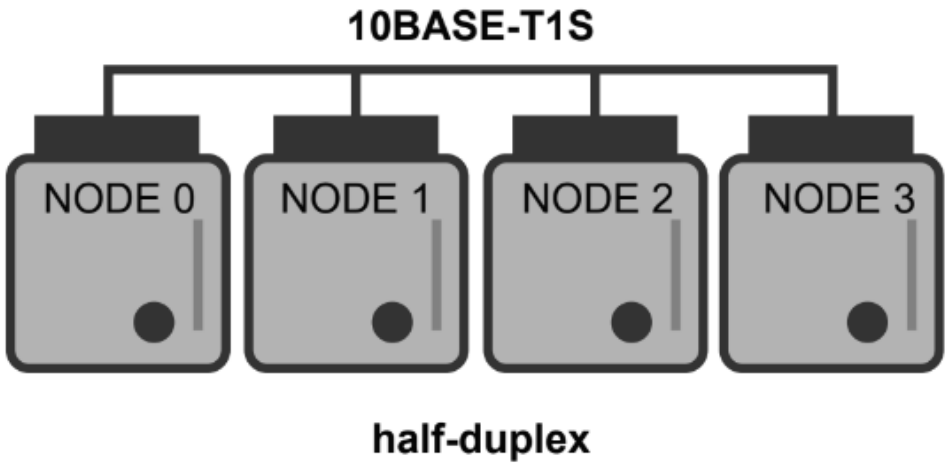
Automotive Ethernet

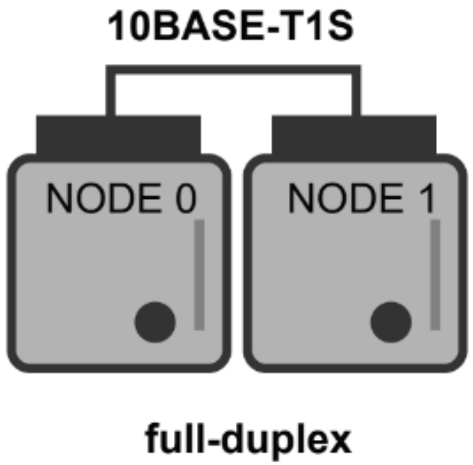
(100BASE-T1 / 1000BASE-T1 / MultiGBASE-T1)

- Pros
  - 10Mbps to 10Gpbs
    (each direction and each leg excluding 10BASE-T1S)
  - Widely used technology
    (much support)
  - Good clock synchronization technology available (gPTP)
  - History of adaptation to solve new problems.
- Cons
  - Requires a switch except for 10BASE-T1S
  - Not possible to add or remove nodes unless the switch has spare ports
  - Tools cannot just connect and sniff the bus



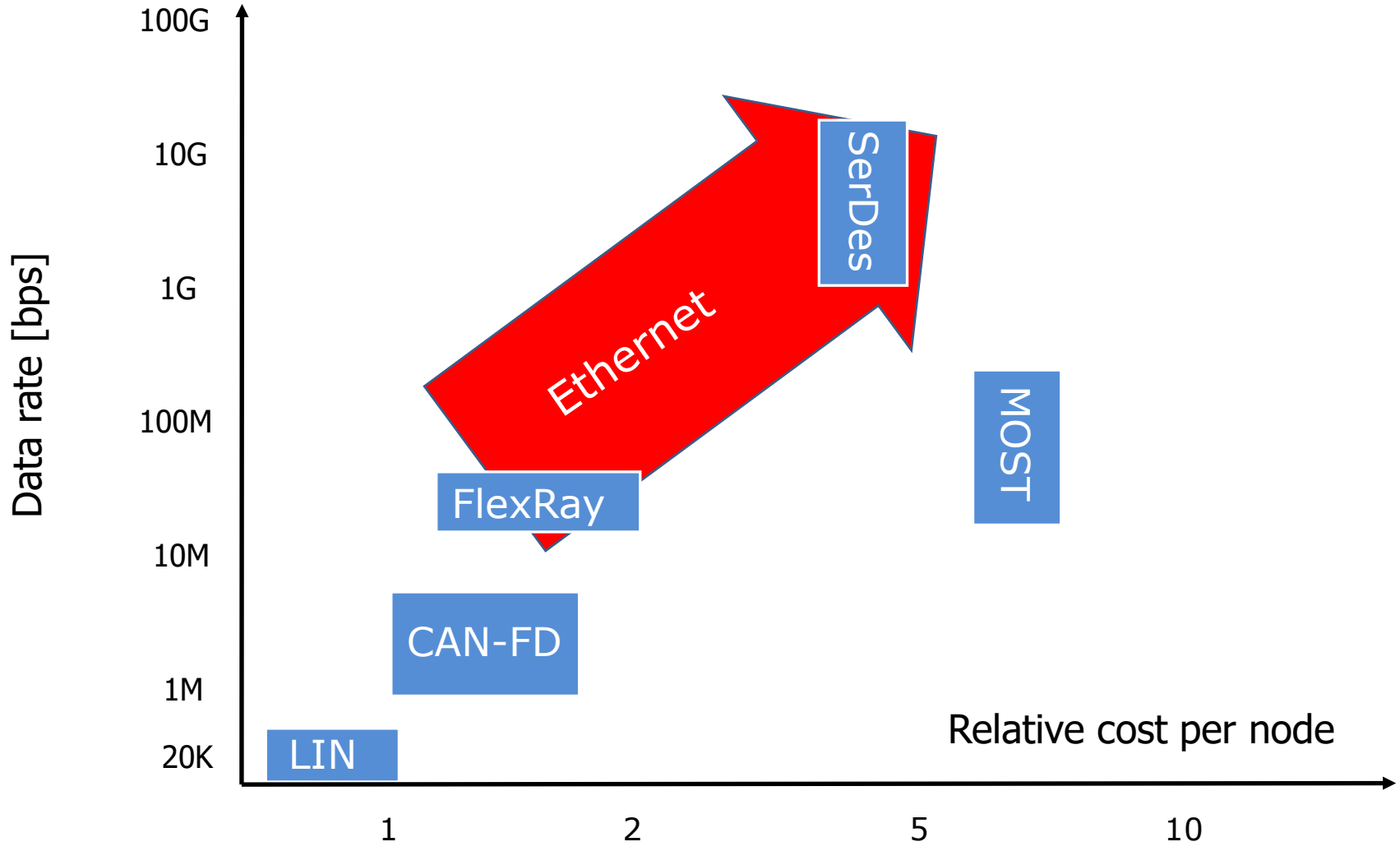
10BASE-T1S – Multi-Drop / BUS





- Pros
  - Multi-Drop / BUS Architecture
    Reduces Network Wiring Length
  - Enables bus utilization of greater than 90%+
  - Enables the Ethernet everywhere vehicle
- Cons
  - Number of nodes with standard wiring & 15m is limited (approx. 8 nodes)

Cost vs. Data Rate



Vehicle Network History and Trends

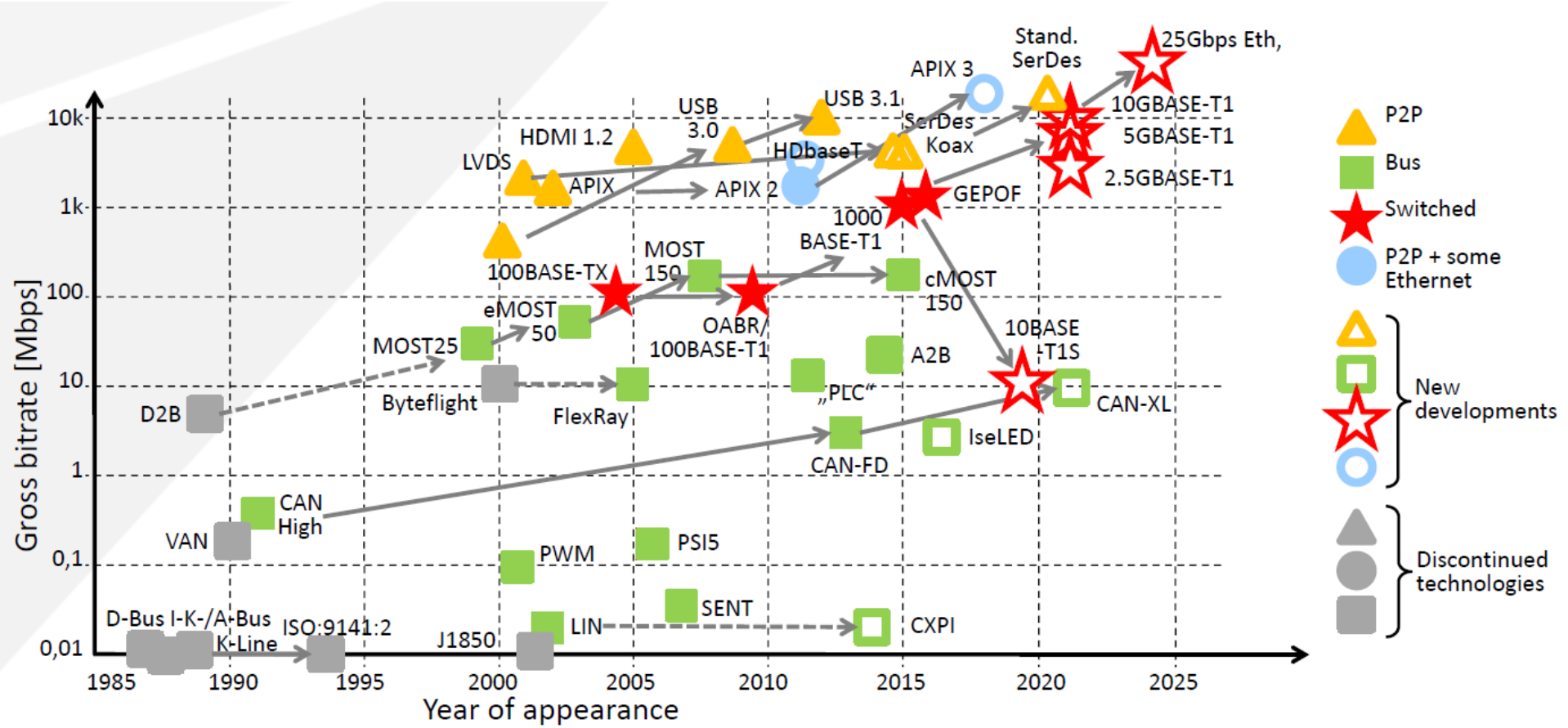


Image credit, "Empowering the In-Vehicle Network.",
Dr. Kirsten Matheus, BMW AG, 2019 Automotive Ethernet Congress, Munich

Automotive Network Architectures

Moving Away from Domain Architectures

- Domain Architectures were an improvement from previous architectures
- Domains segregated by network
- Advances in technology have made this this suboptimal
  - Cost
  - Weight
  - Manufacturing

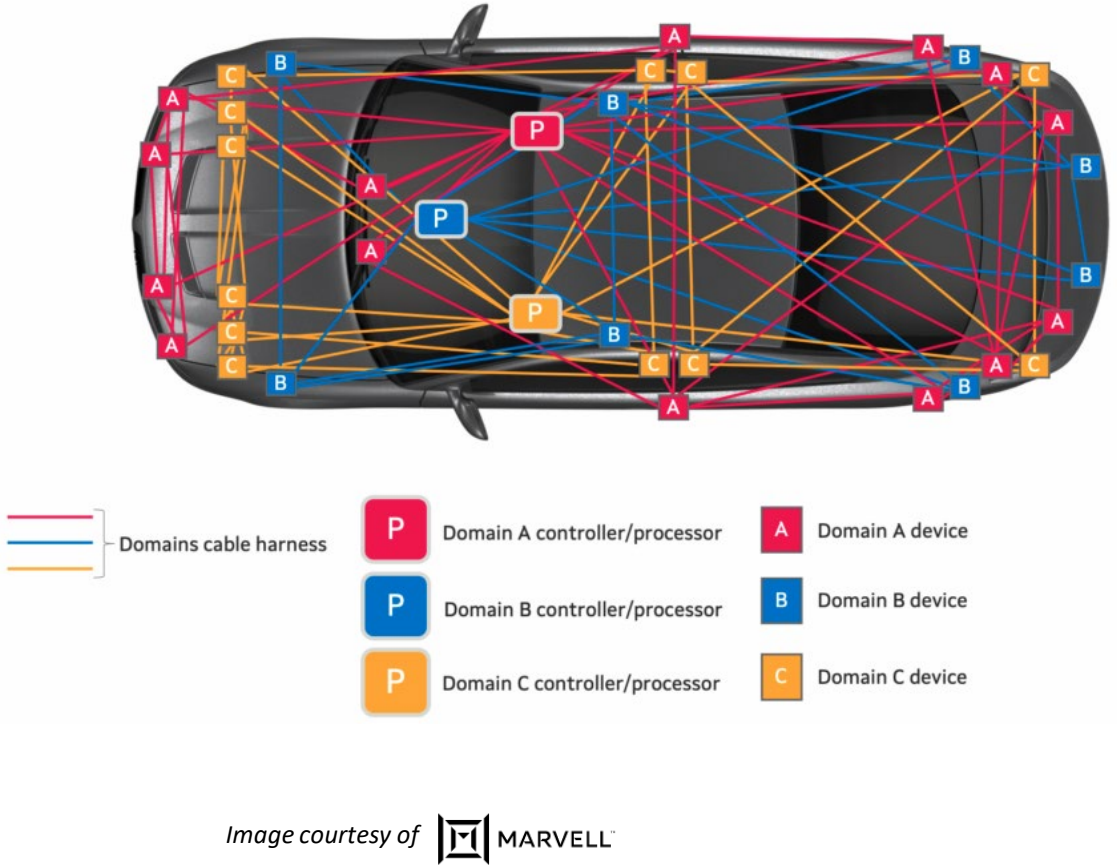


Image courtesy of MARVELL

Zonal Architectures Advantages

- Optimize Power and Signal Distribution System
  - Fewer network connections
    - Less cost
    - Less weight
    - Simpler assembly
    - Higher reliability (mechanically speaking)
- But not without challenges!
  - "Cost" of Optimization
  - Requires Higher Bandwidth!
  - QoS guarantees are now required
    - Shared bandwidth between subsystems
    - More failure modes and fault conditions

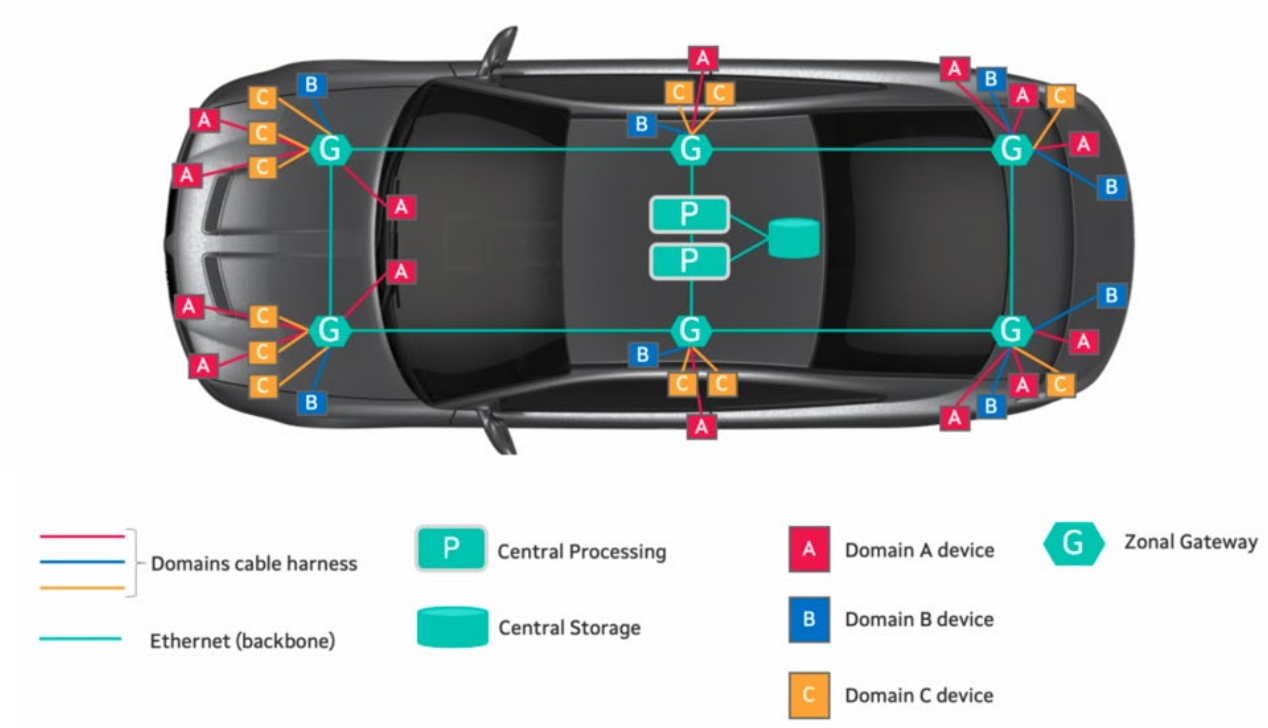
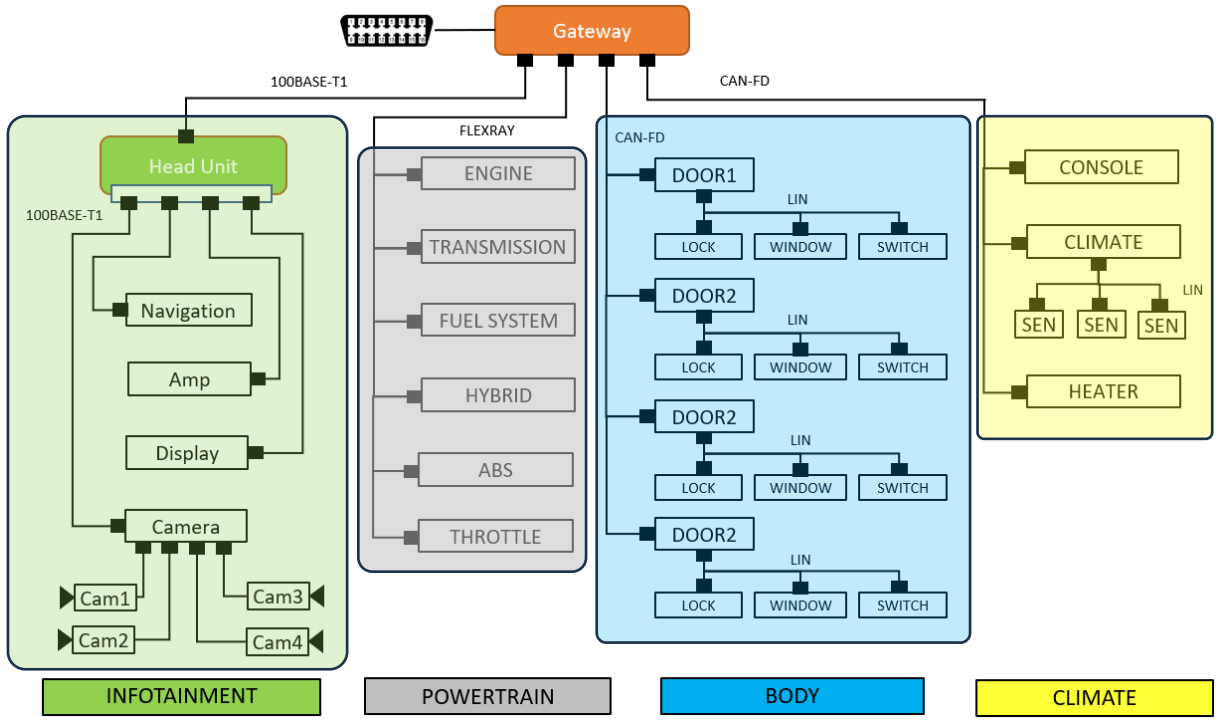


Image courtesy of MARVELL

Domain vs Zonal Architecture

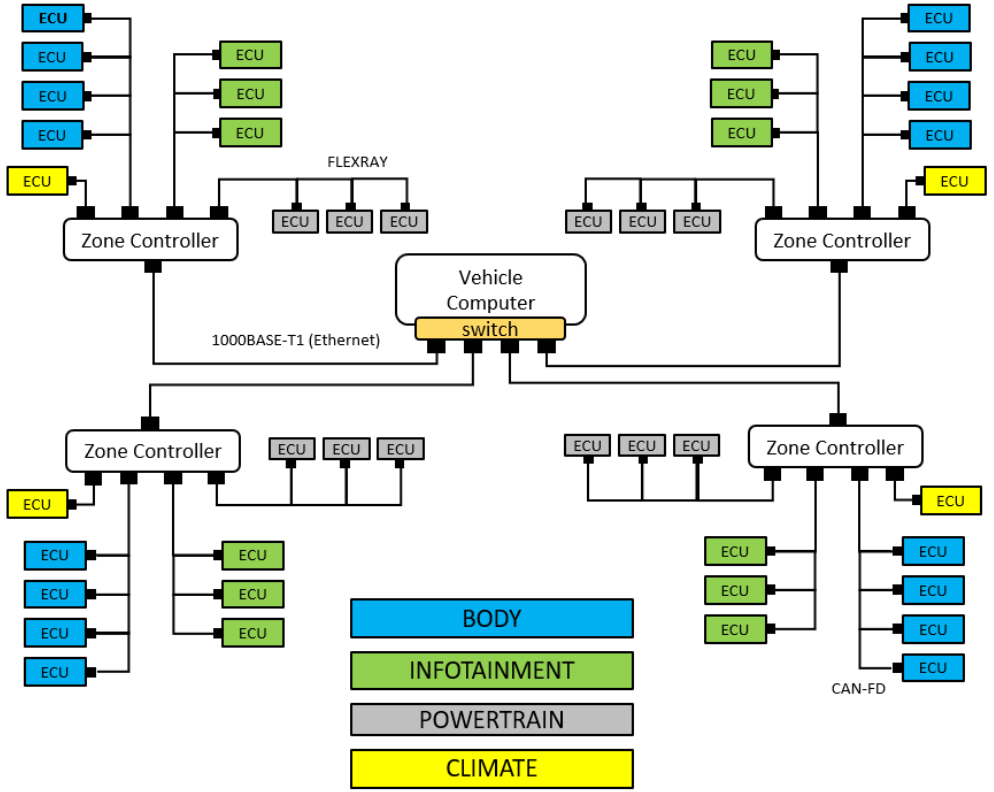
DOMAIN

Many variants depending on OEM. Many legacy and proprietary networks employed including CAN-FD, FlexRay, Ethernet, A2B, SENT, LIN, etc.



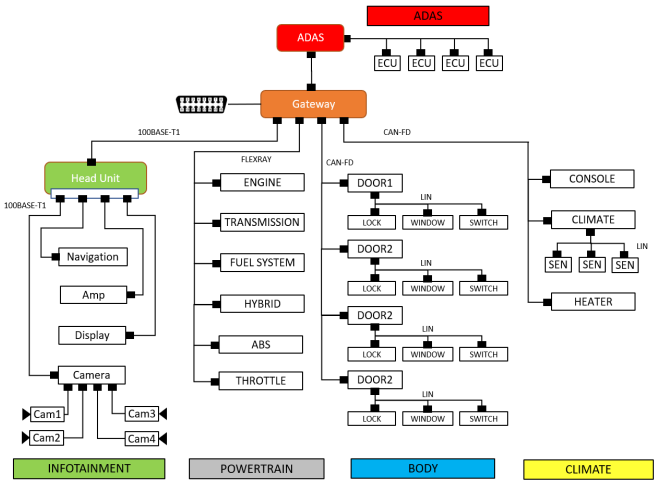
ZONAL

Many variants that include “Ethernet only” Zonal, and hybrid versions that include CAN-FD, LIN, FlexRay, etc. Backbone is always Ethernet.

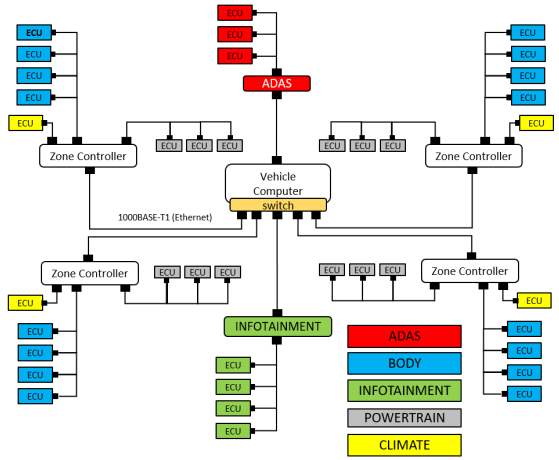


Drive Toward Zonal Model

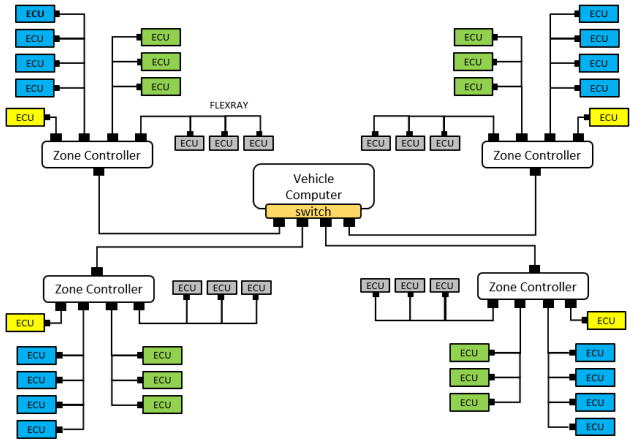
DOMAIN



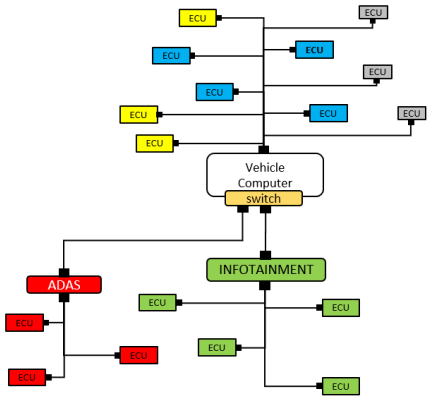
PARTIAL ZONE



FULL ZONE



CLUSTERD DOMAIN



OEM A

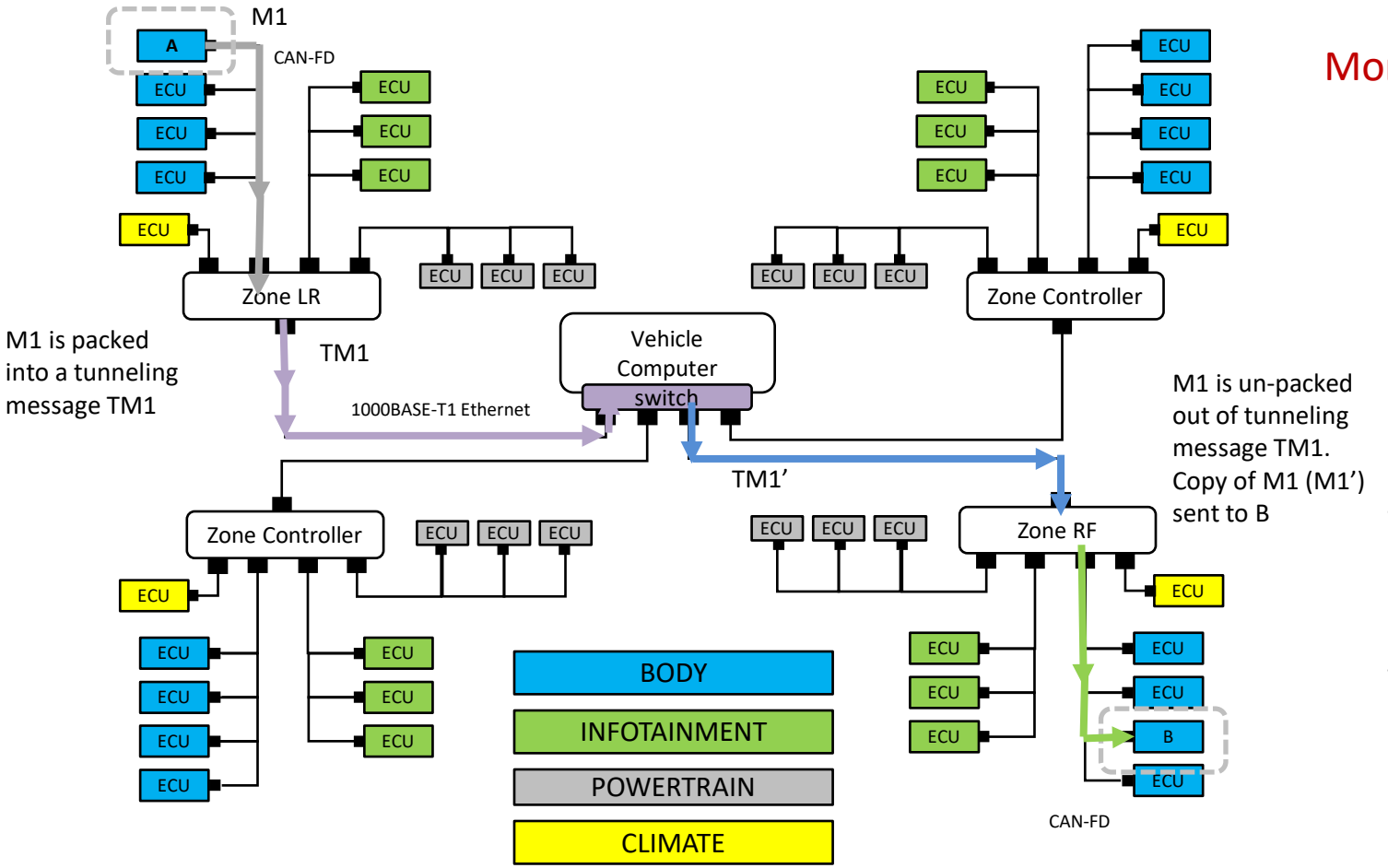
OEM B

OEM C

Legacy edge networks (CAN, LIN)

Ethernet Only Zonal

Zonal Architecture (example 1 with legacy networks)



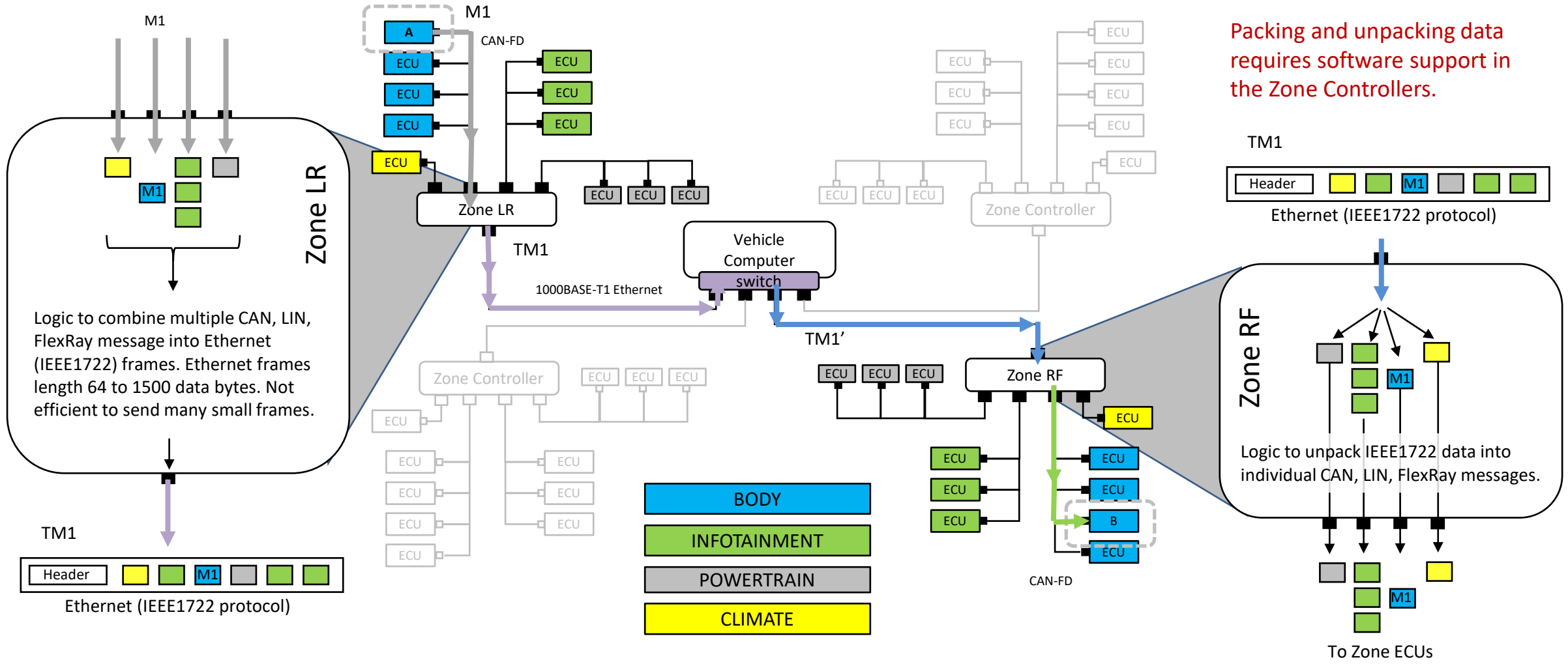
Monitoring and logging data is less straightforward

BODY Example: Say "A" needs to send a message M1 to "B"

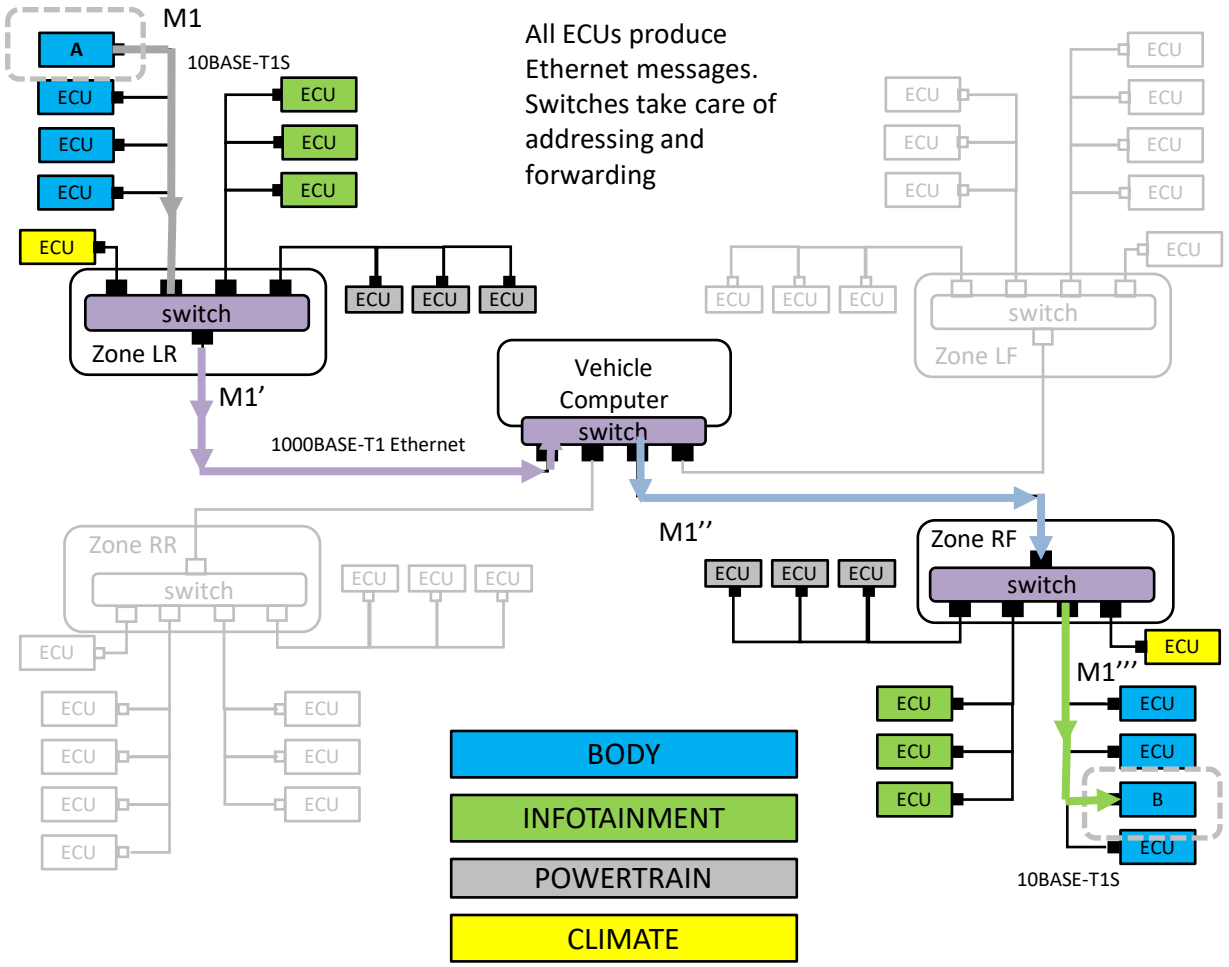
1. A sends CAN-FD message M1
2. Zonal LR consumes the message, must translate it for transport over Ethernet (likely IEEE 1722)
3. Ethernet data travels through 2 Zonal controllers and the Vehicle Computer Switch (each path is a copy of the Ethernet data)
4. Zone RF must un-pack the Ethernet Data translate it to CAN-FD and send M1' to "B"

NOTE: M1', M' is a copy of M1. There are 2 copies of M1. TM1 and TM1' carry the data of M1 in Ethernet messages

What happens "in the Zone?" (with CAN, LIN, FlexRay)



Zonal Architecture (example 2 Ethernet only)



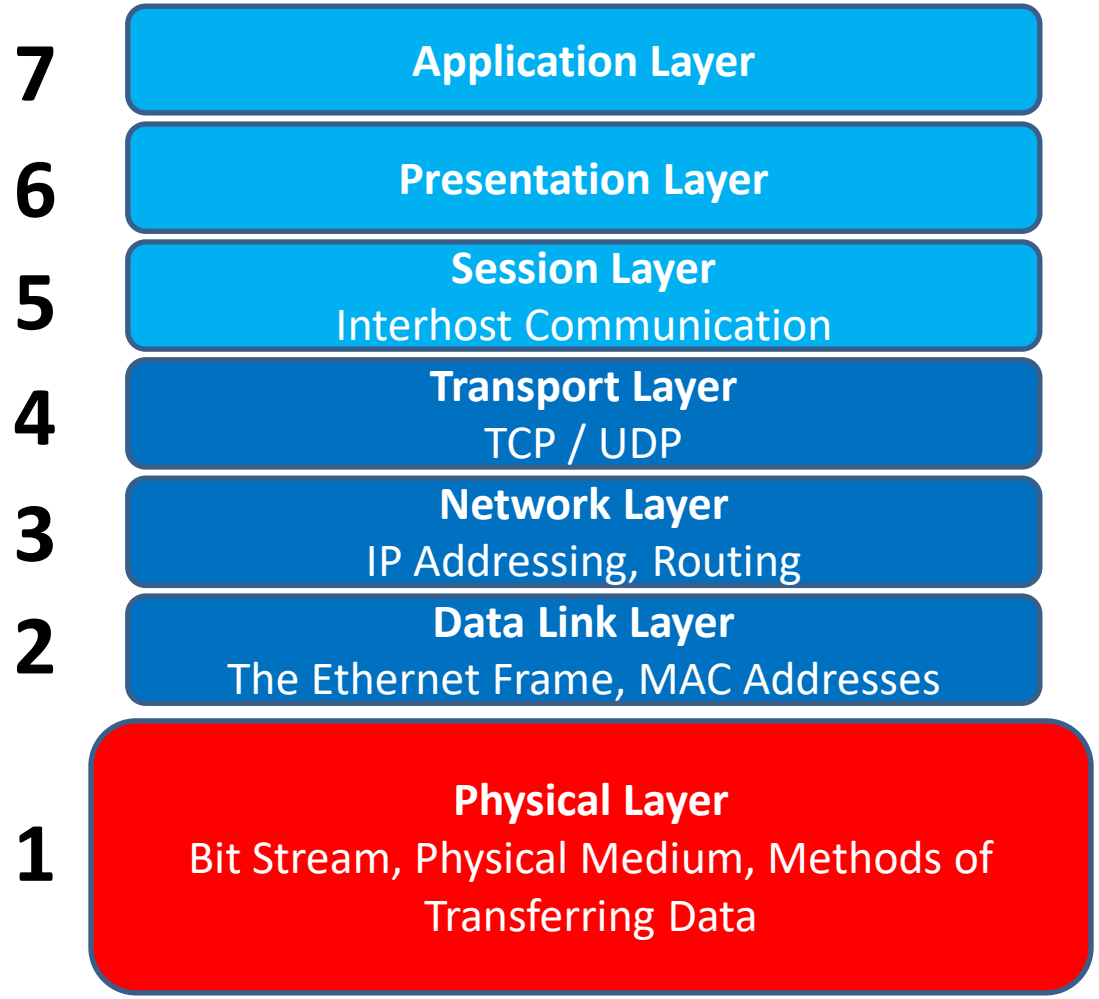
Ethernet only enables switches to route Ethernet messages with less or no software / firmware. Ethernet has message addressing & routing "built-in" or standardize.

BODY Example: Say "A" needs to send a message M1 to "B"

1. A sends CAN-FD message M1
2. Zonal LR Switch *forwards* M1 to Vehicle Computer M1' is a copy.
3. Ethernet data travels through 2 Zonal switches and the Vehicle Computer Switch there are 4 copies of M1 (M1, M1', M1'', M1''')
4. Zonal RF *forwards* and sends M1''' to "B"

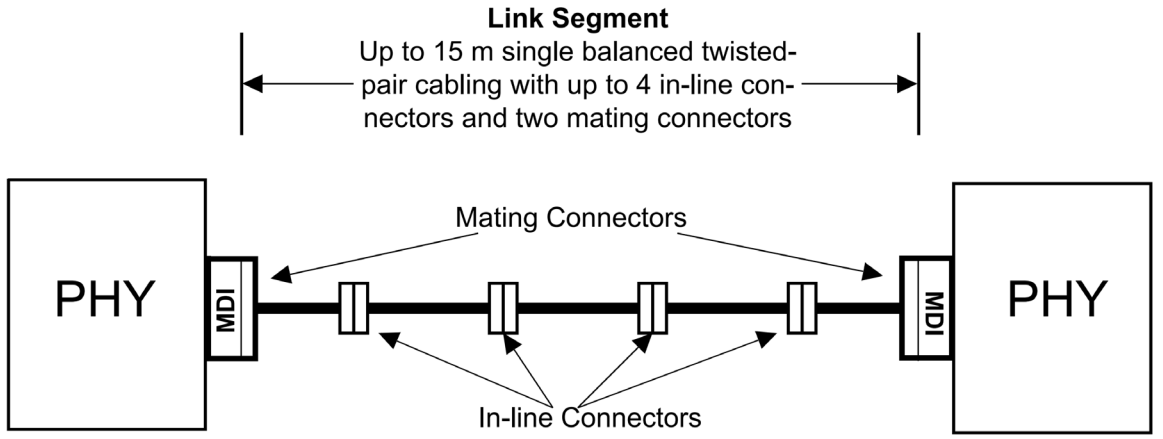
NOTE: M1', M1'', M1'' are a copies of M1. There are 3 copies of M1

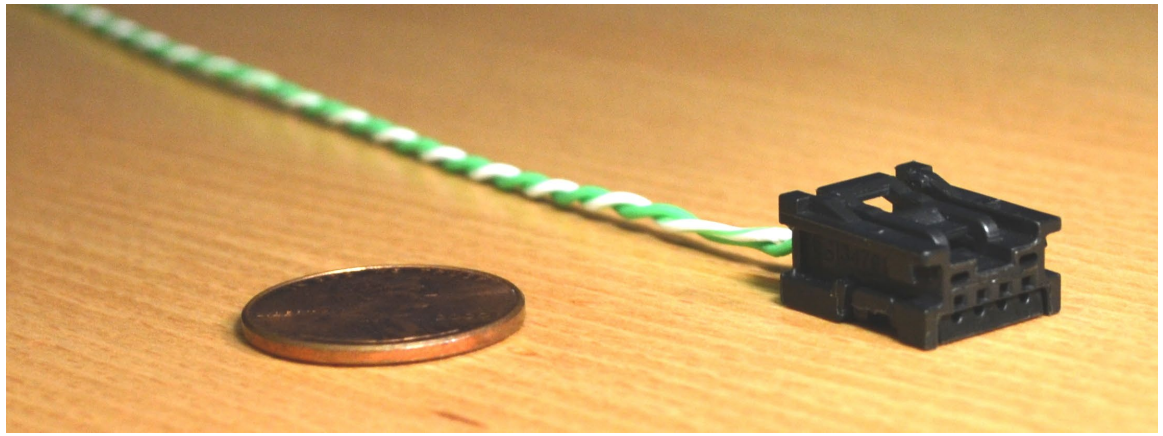
Physical Layer – 45min



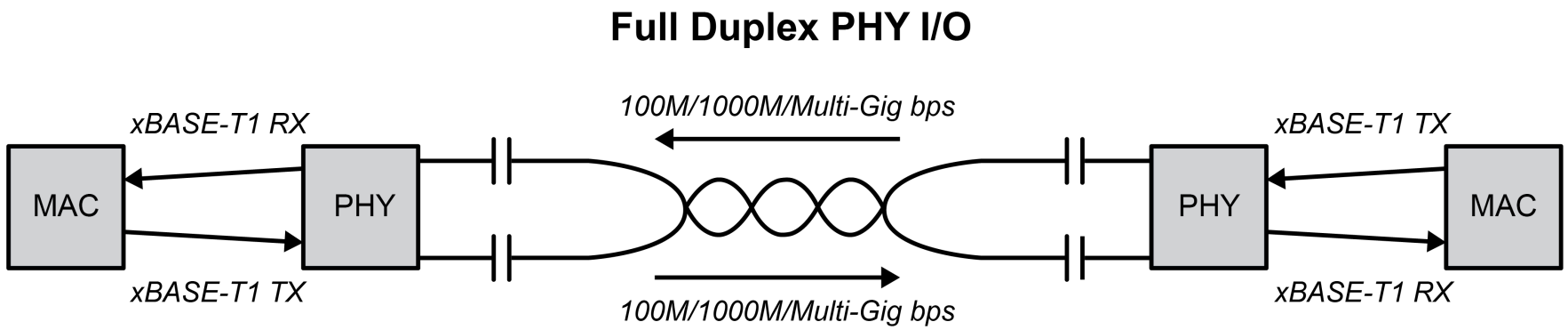
xBASE-T1 Physical Layer

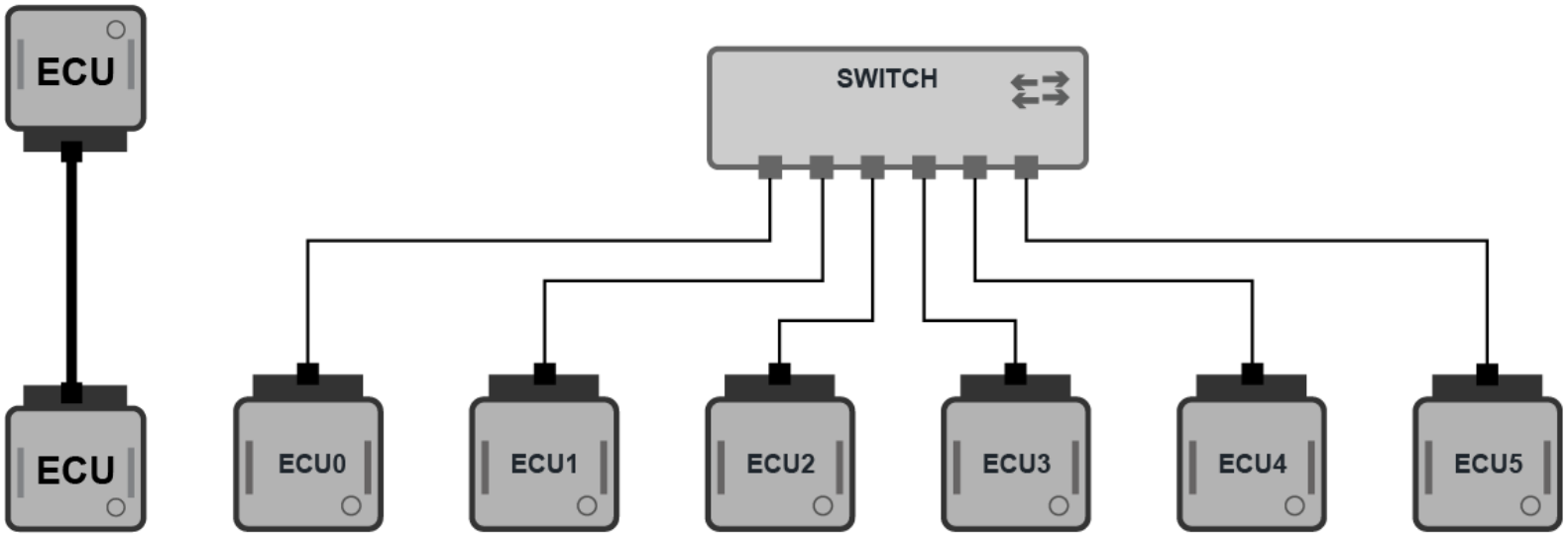
- 100 / 1000 / 2.5G / 5G / 10G
  - Share some common requirements
  - Requirements on cables & connector unique to speed grade. Open Alliance
- UTP (Unshielded Twisted Pair)
  - 100BASE-T1, 10BASE-T1S
- STP (Shielded Twisted Pair)
  - Optional for 1G, required for 2.5G and above
- 15 meters with 4 inline connectors
  - 11 meters with 25G and above.
- Cable and connector requirements unique to each speed grade through Open Alliance





xBASE-T1 Physical Layer

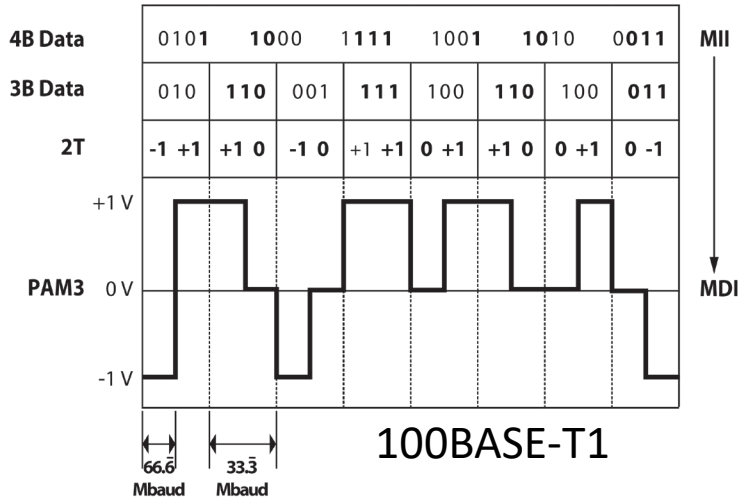




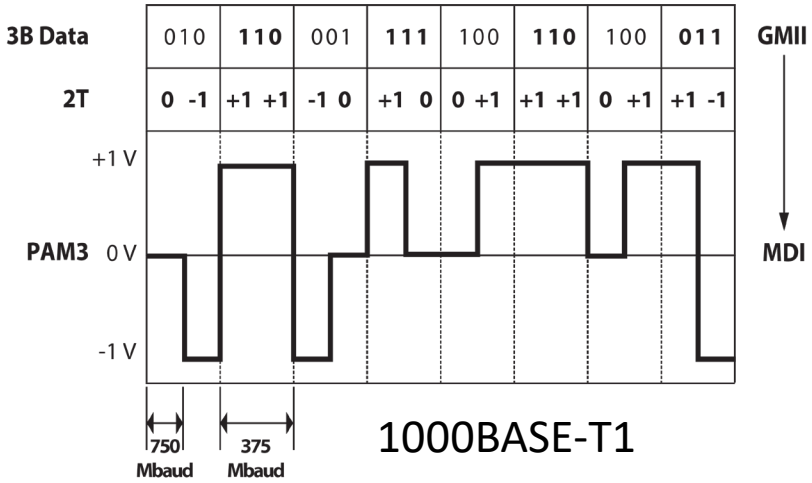
Each “leg” of a switched network is electrically its own point-to-point network.

100/1000BASE-T1 Physical Layers

	100BASE-T1	1000BASE-T1
Modulation	PAM3: 3 logical states (voltages)	
Link Voltage	2V pp	
Encoding	2 symbols represent 3 bits	
Clock Frequency	33MHz / 66 Mbaud	375 MHz / 750 Mbaud
Bitrate	3 x 33MHz = 100 bps	3 x 375MHz <> 1000 bps ???



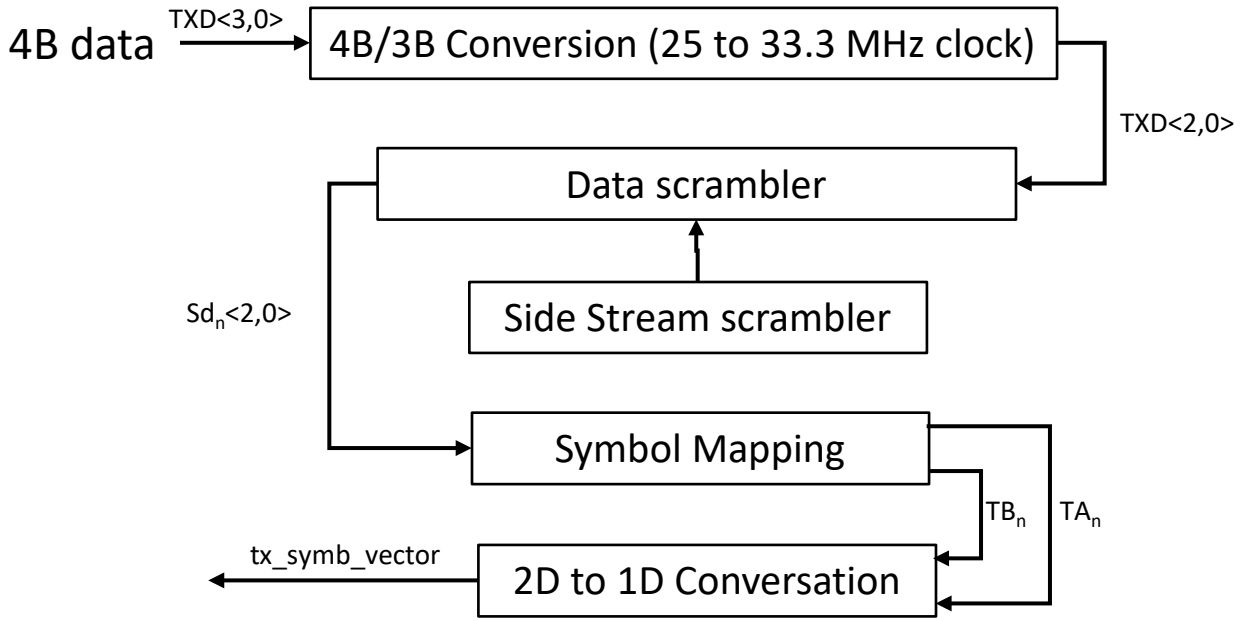
100BASE-T1



1000BASE-T1

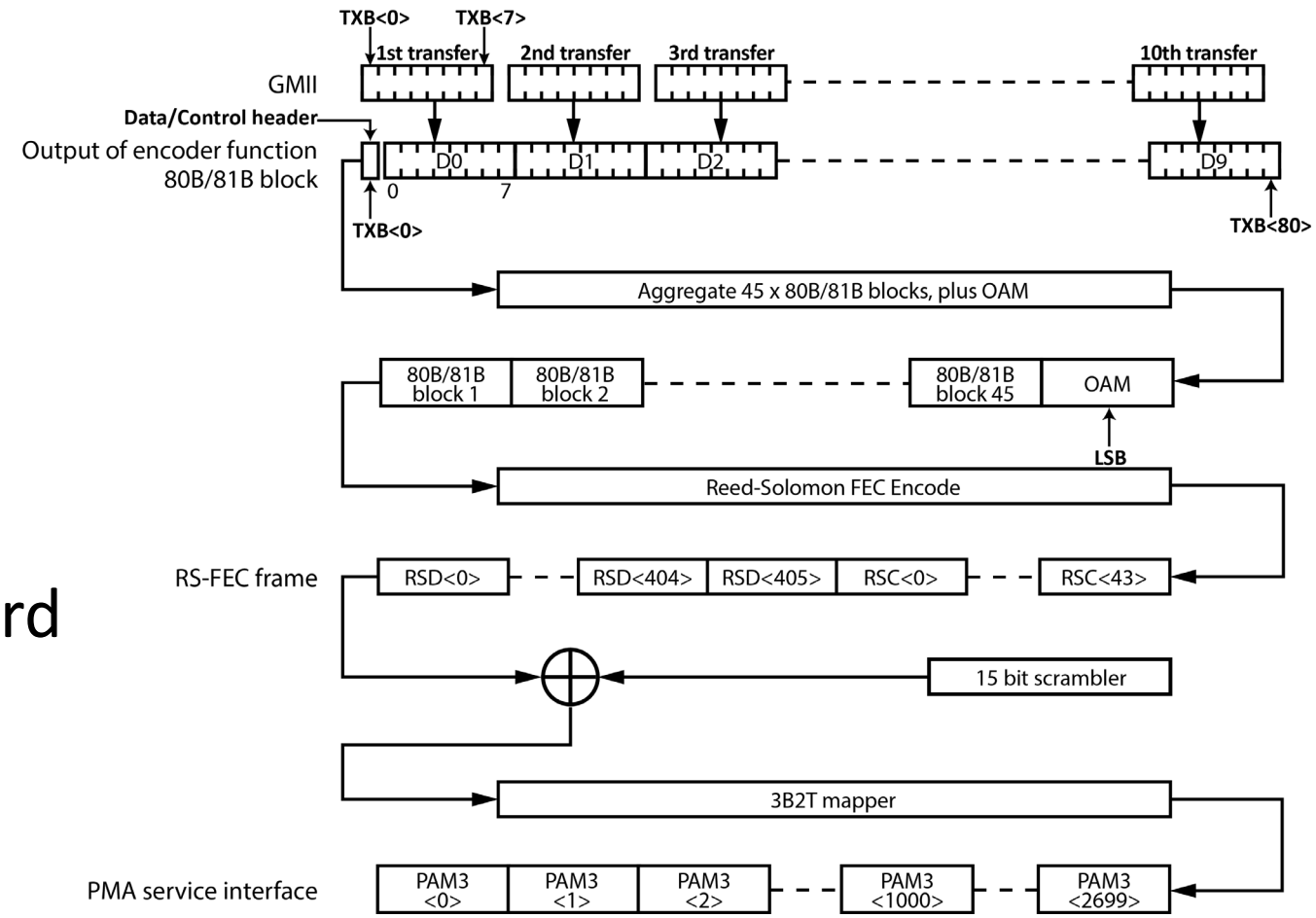
100BASE-T1 Physical Layer

1. 4B / 3B Conversion
2. Data Scrambler
3. 2T3B Symbol Mapping
4. 2D to 1D Conversion



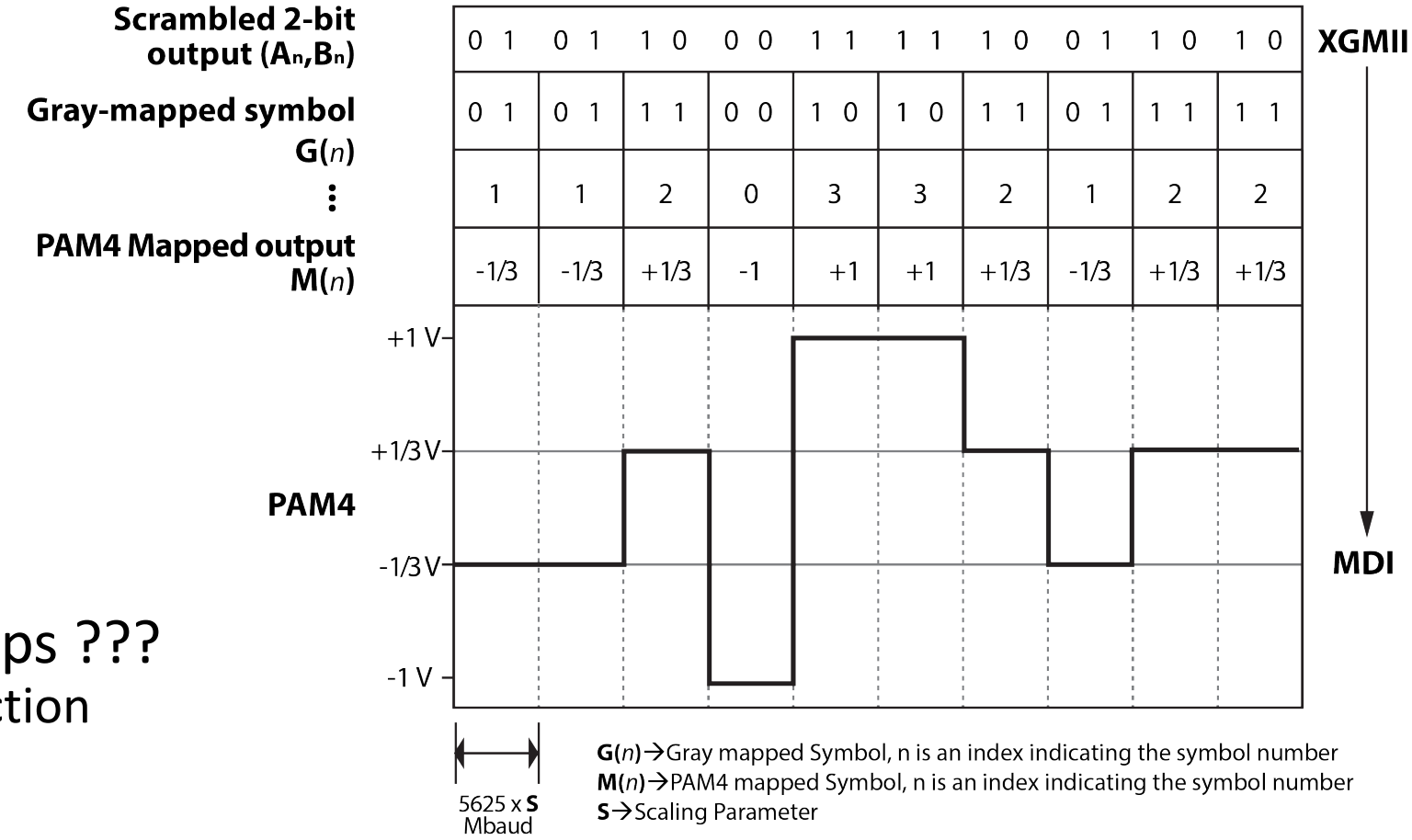
1000BASE-T1 Physical Layer

1. 80/81B - 80 bits of data 1 bit control:
   - 1 = data for 80 bits
   - 0 = control info in the block
2. 45 blocks combined with OAM
   - **O**perations, **A**dministration, **M**aintenance
3. RS-FEC – Reed-Solomon Forward Error Correction
4. Scrambler
5. 3B2T mapper



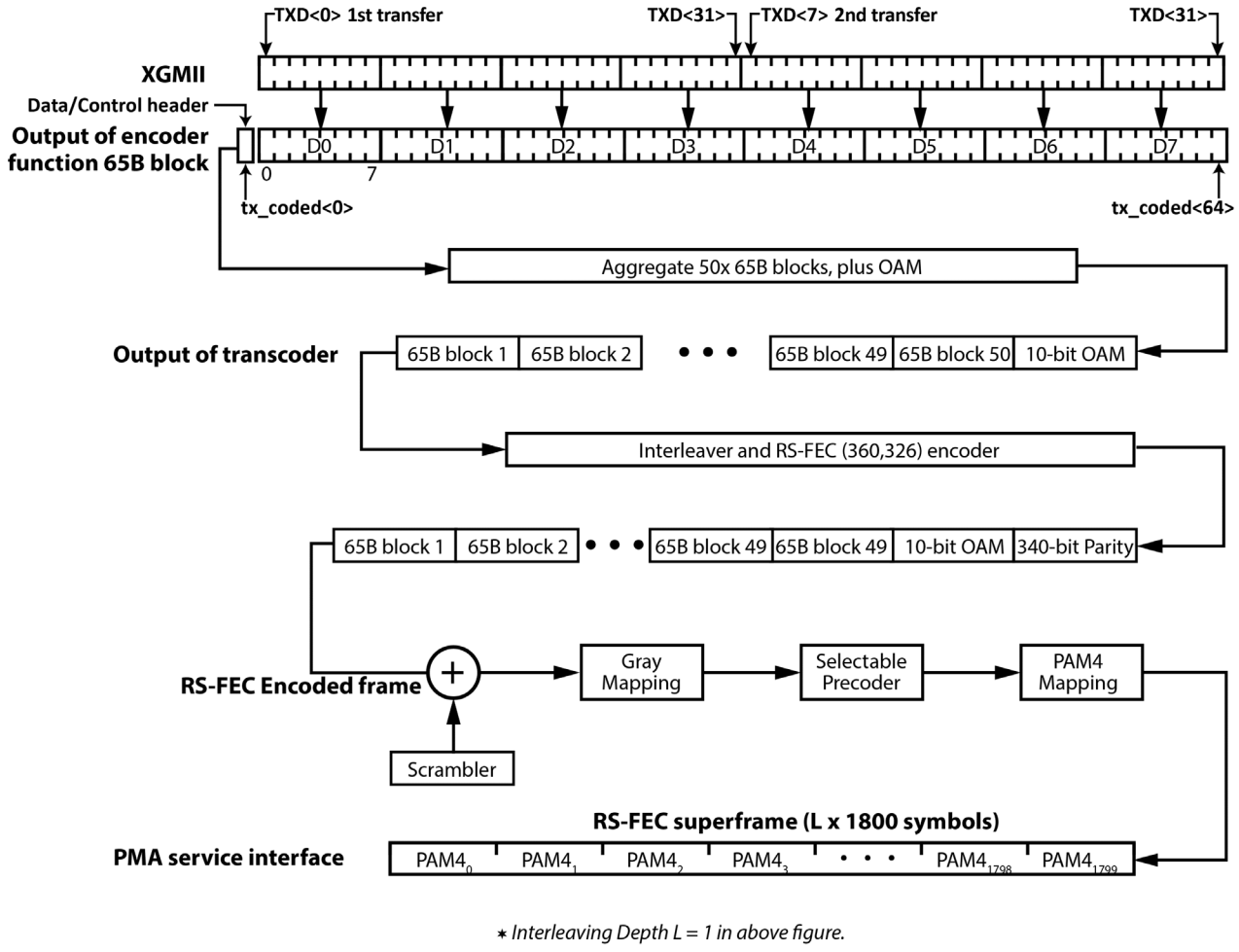
MultiGBASE-T1 Physical Layer

- PAM-4 (4 logical “states”)
- 2 bits encoded in 4 levels
- 2V max span signal
- 2/3 V span = 1 logic level
- Clock frequency
  - 10G: 5.625 Ghz
  - 5G: 2.8125 Ghz
  - 2.5G: 1.41 Ghz
- $2\ bits \times 5.625\ Ghz > 10$ Gbps ???
  - ~10% Overhead for error correction



MultiGBASE-T1 Physical Layer

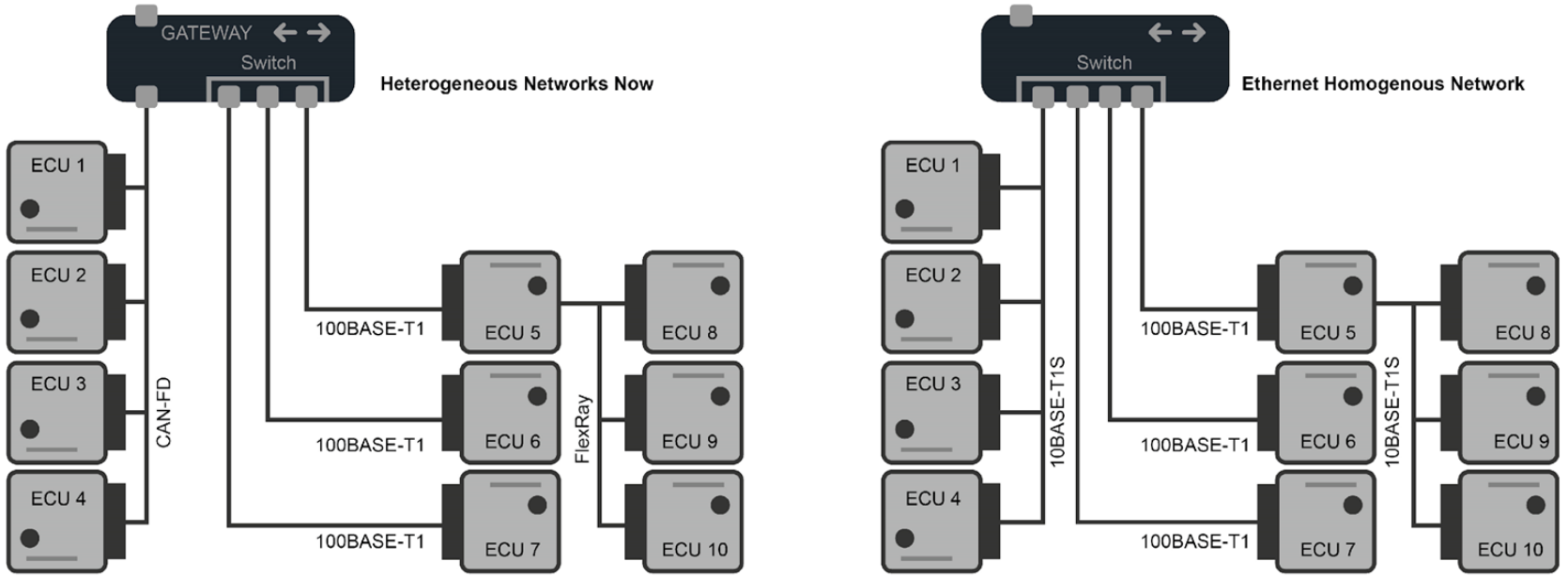
1. 64/65B - 64 bits of data 1 bit control:
   - 1 = data for 64 bits
   - 0 = control info in the block
2. 50 blocks combined with OAM
   - **O**perations, **A**dministration, **M**aintenance
3. Interleaver
4. RS-FEC – Forward Error Correction
5. Scrambler
6. Gray Mapping
7. Selectable Precoder
8. PAM4 Mapping



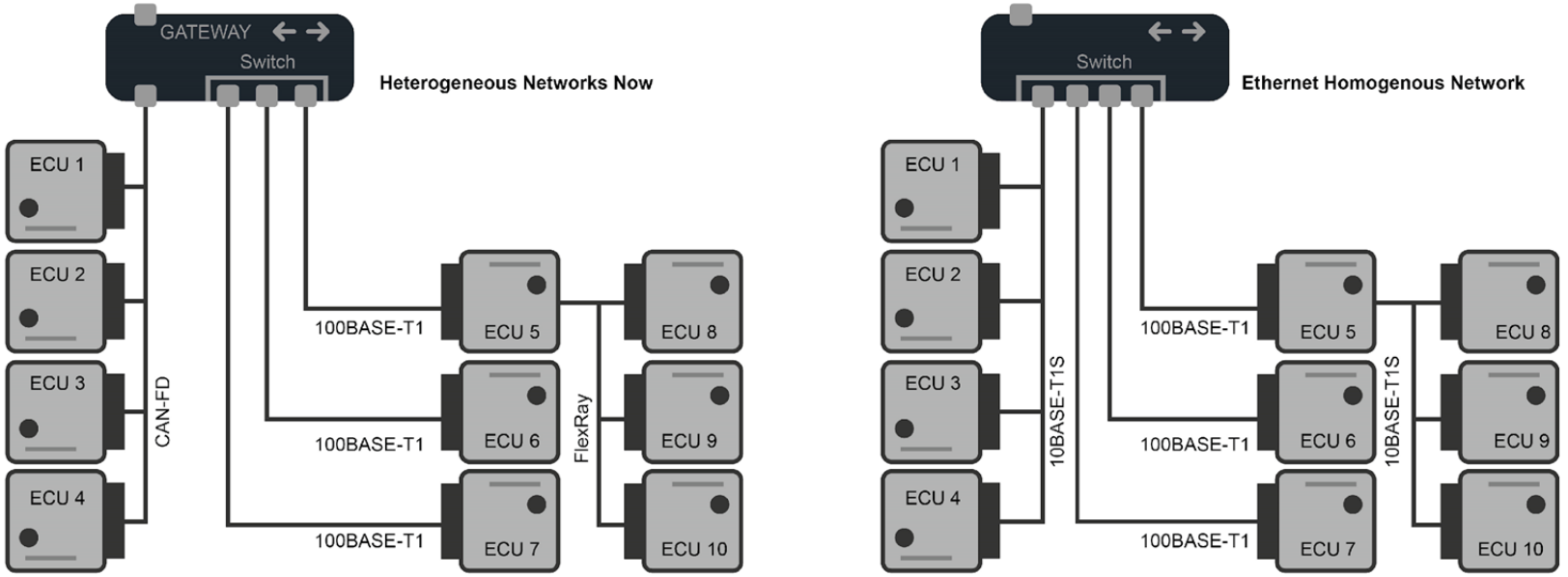
⋆ *Interleaving Depth L = 1 in above figure.*

Motivation for 10BASE-T1S

- Continuous growth of ECUs driven by electronic features.
- Numerous types of network in the vehicle. Ethernet, CAN-FD, LIN, FlexRay.
- Gateways are used to bridge different network types and functionality domains.
- 80% plus of communication between ECUs requires less than 10Mb/s of bandwidth.
- Complex gateways used to bridge networks.



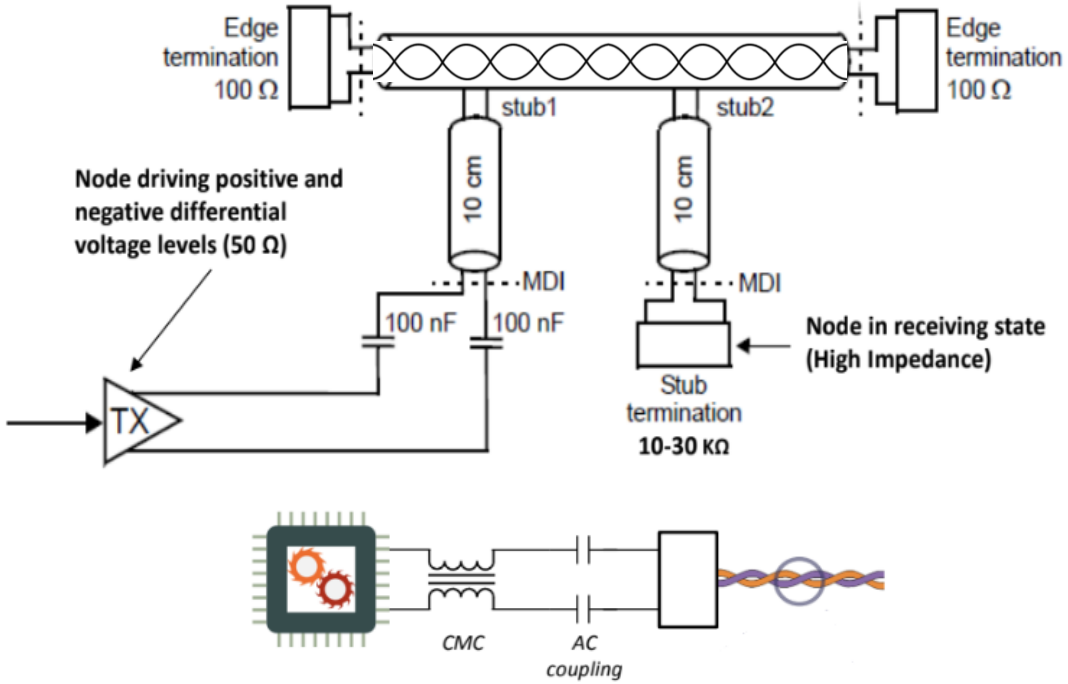
Goals for 10BASE-T1S



- Provide an Ethernet / IP based solution similar in cost to legacy networks (CAN-FD, FlexRay)
- Allow for an IP everywhere network. Simplifies network design and maintenance.
- Reduce dependency on gateways.
- Offer optional PoDL support (Power over Data Lines) to further reduce complexity and cost.
- BUS / Multi-drop architecture provides wiring cost benefits and reduces PHY count.

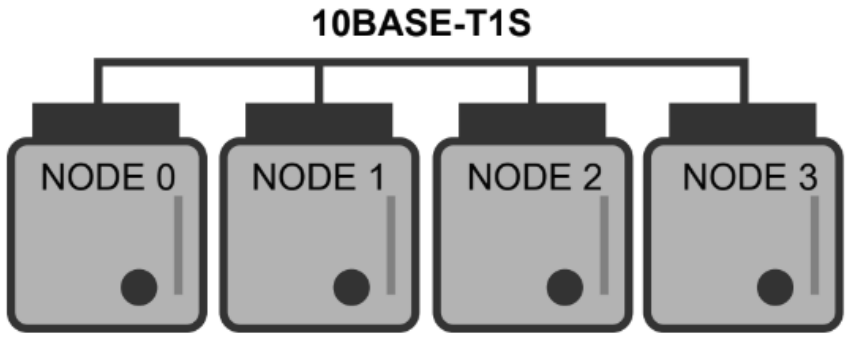
10BASE-T1S Basics

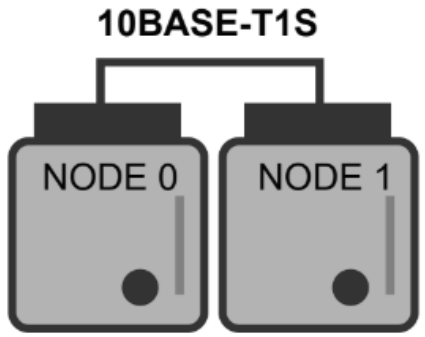
- STP (Single Twisted Pair) coper cabling similar to CAN-FD, FlexRay.
- Uses new PCLA (Physical Layer Collision Avoidance Method).
- BUS access method is deterministic unlike CAN / CAN-FD.
- At least 8 nodes 25 meters in reach.
- Supports PoDL (Power over Data Lines).
- 12.5MHz Baudrate * 4B/5B Encoding = 10Mbps



10BASE-T1S Low Cost / Flexibility

Supports mutually exclusive multi-drop half-duplex or point-to-point full-duplex modes





Typical DSP-based xBASE-T1 architecture needs

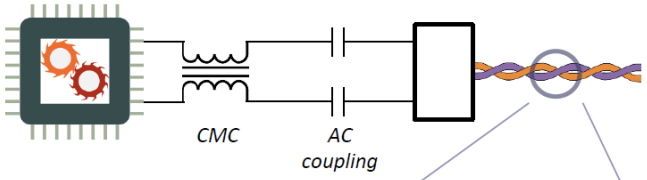
– Multi-bit, high-speed ADC
– Adaptive equalization
– Echo cancellation
– Complex clock recovery
– Baseline wander correction

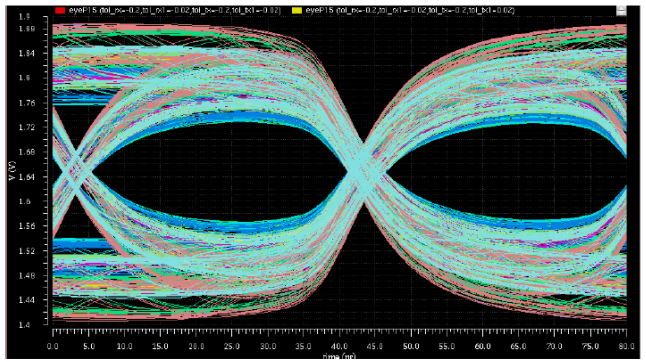
10BASE-T1S

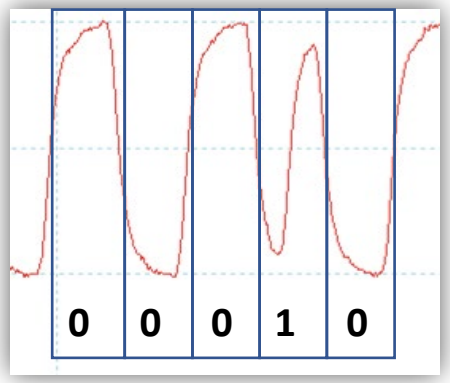
– Window comparator (2-level signal)
– Simple equalization (lower speed)
– No need for echo cancellation (half-duplex)
– No need for clock recovery (DME is self clocked)
– No need for wander correction (DME is balanced)

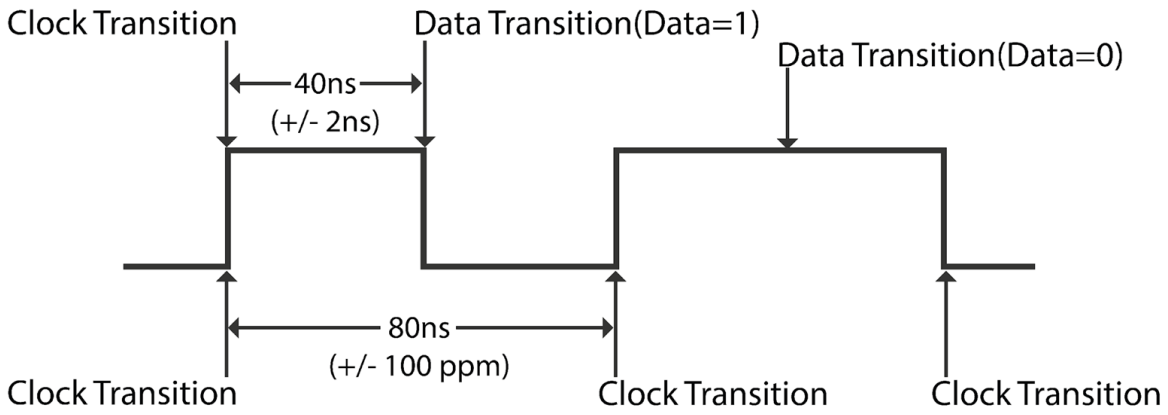
10BASE-T1S Line Encoding

- 1V peak-to-peak 20% margin of error
- Differential Manchester Encoding (DME)
  - At least one transition per clock period enables clock synchronization.
  - Values are encoded based on transition and not state or level. This provides better EMI Immunity.





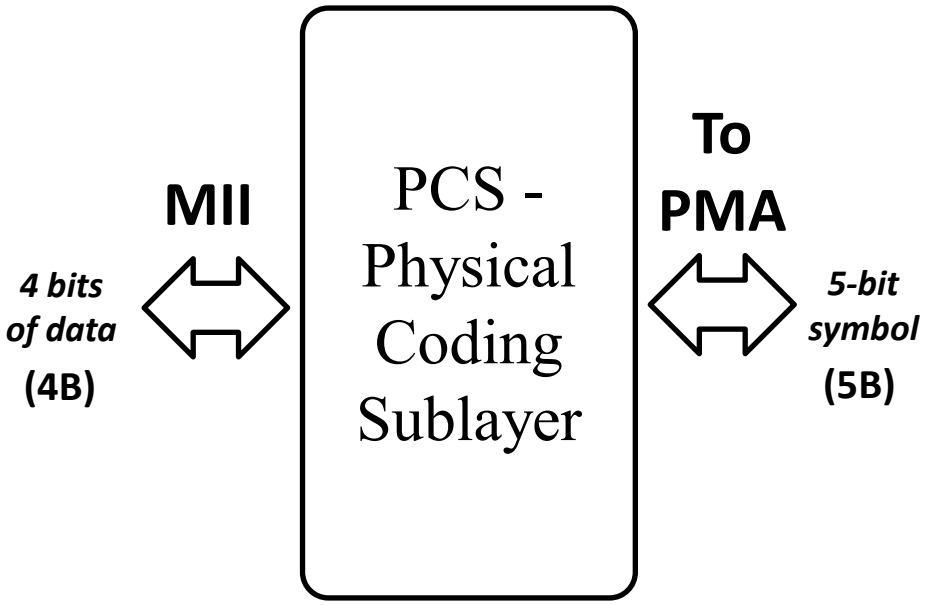




Differential Manchester Encoding

10BASE-T1S Line Encoding

4B/5B Encoding is used to allow for special PLCA symbols. ***(in addition to frame data)***



Name	4B	5B	Special function
0	0000	11110	—
1	0001	01001	—
2	0010	10100	—
3	0011	10101	—
4	0100	01010	—
5	0101	01011	—
6	0110	01110	—
7	0111	01111	—
8	1000	10010	—
9	1001	10011	—
A	1010	10110	—
B	1011	10111	—
C	1100	11010	—
D	1101	11011	—
E	1110	11100	—
F	1111	11101	—

I	N/A	11111	SILENCE
J	N/A	11000	SYNC / COMMIT
K	N/A	10001	ESDERR
T	N/A	01101	ESD / HB
R	N/A	00111	ESDOK / ESDBRS
H	N/A	00100	SSD
N	N/A	01000	BEACON
S	N/A	11001	ESDJAB

Methods for Handling Collisions

LIN - Master / Slave:

- Master tells all nodes when to transmit
- Driven by a Schedule Table in the master node

FlexRay – TDMA, Time Divided Media Access:

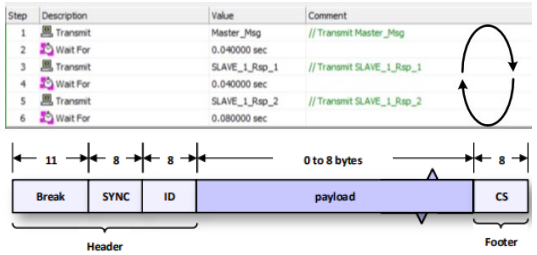
- All nodes are pre-programmed to know when they can / cannot transmit.
- Very reliable timing requirements

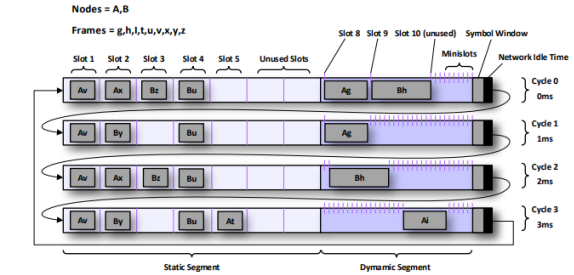
CAN – Non-Destructive Arbitration:

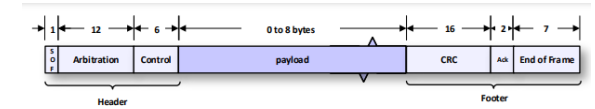
- All nodes transmit anytime but detect when a higher priority message is on the BUS to stop transmit.

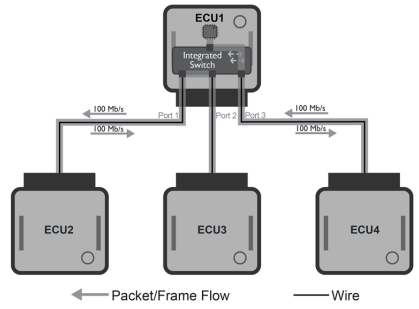
100BASE-T1, 1000BASE-T1, MultiGBASE-T1:

- Point-to-Point physical layer only.
- Full bandwidth in both directions all the time.
- No opportunity for collisions.



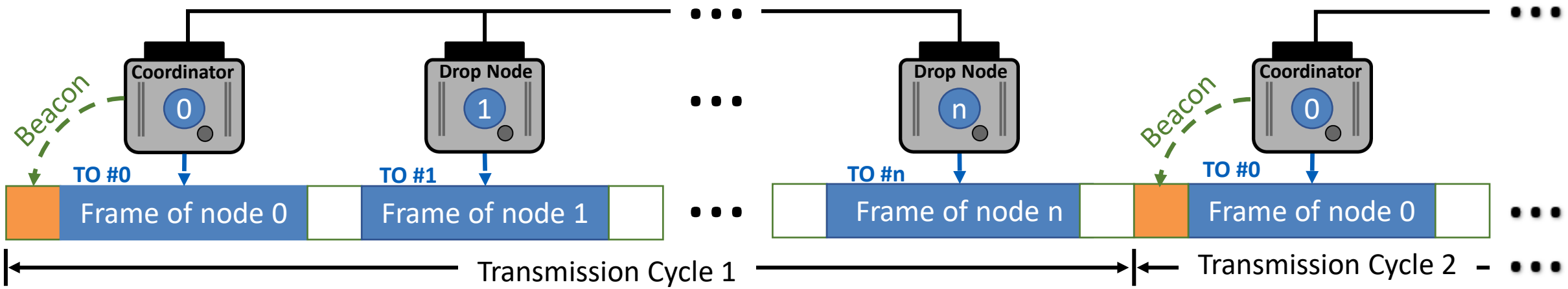






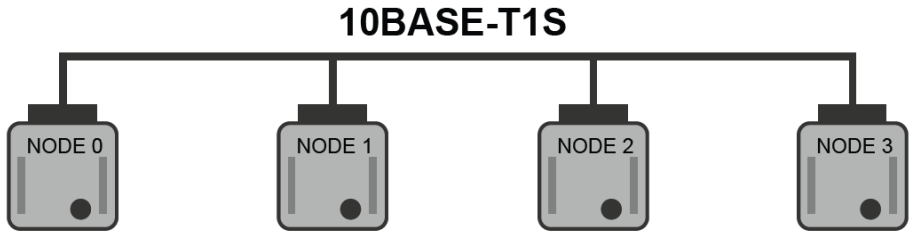
PHY Level Collision Avoidance (PLCA)

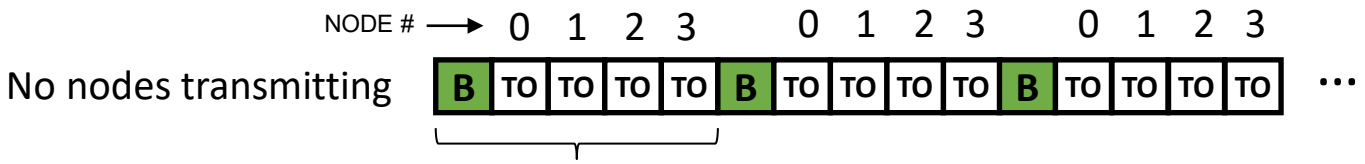
- Nodes on the BUS are assigned an IDs.
- ID 0 is the “Coordinator”.
- At the start of the transmission cycle the “Coordinator” sends a beacon.
- “Follower” nodes are given a “TO” (Transmit Opportunity) in order of their assigned IDs.
- Drop node forfeits TO if nothing is sent within the TXOpp Tmr. (32 bit-times by default)
- Round Robin - no handshaking, transmit opportunities are counted by each node.

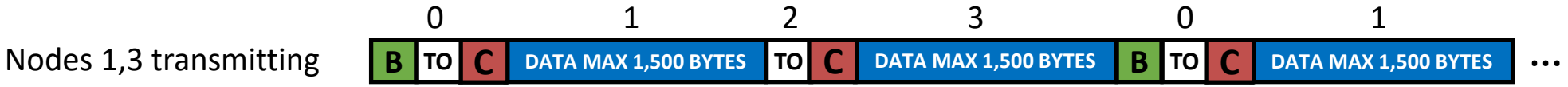


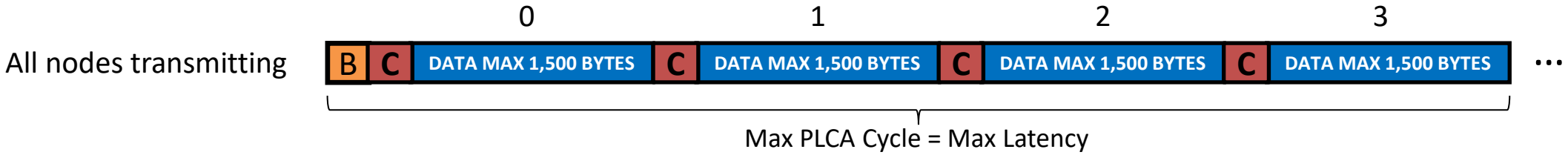
10BASE-T1S Transmission Cycle

Consider a 4-node network





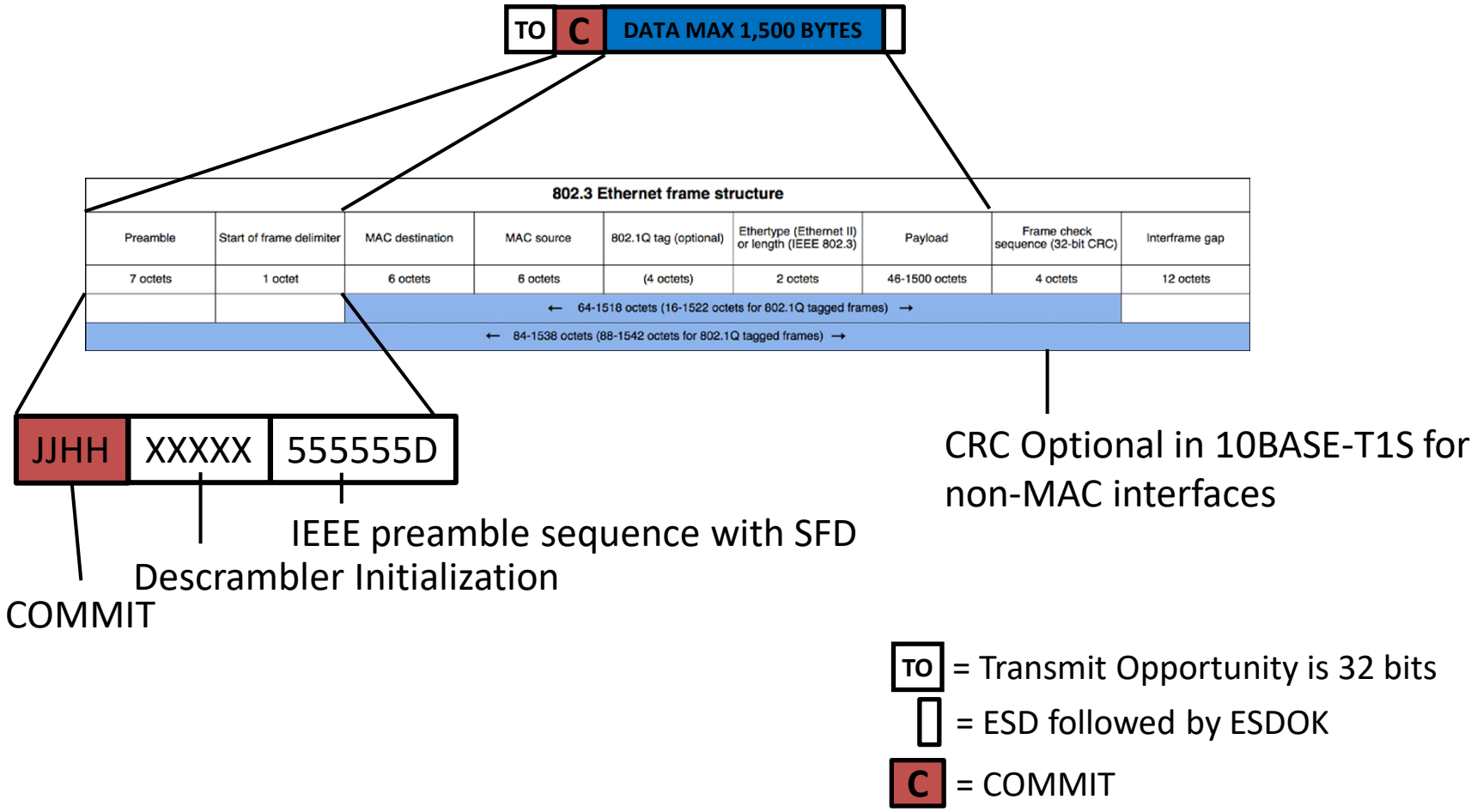




TO = Transmit Opportunity is 32 bits B = BEACON is 20 Bits C = COMMIT

* ESDBRS, ESDOK at end of data not shown

10BASE-T1S Preamble / Frame

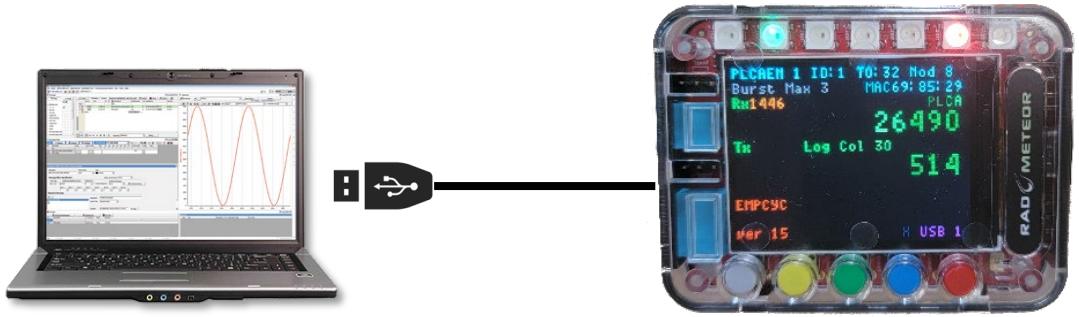


TO = Transmit Opportunity is 32 bits

[ ] = ESD followed by ESDOK

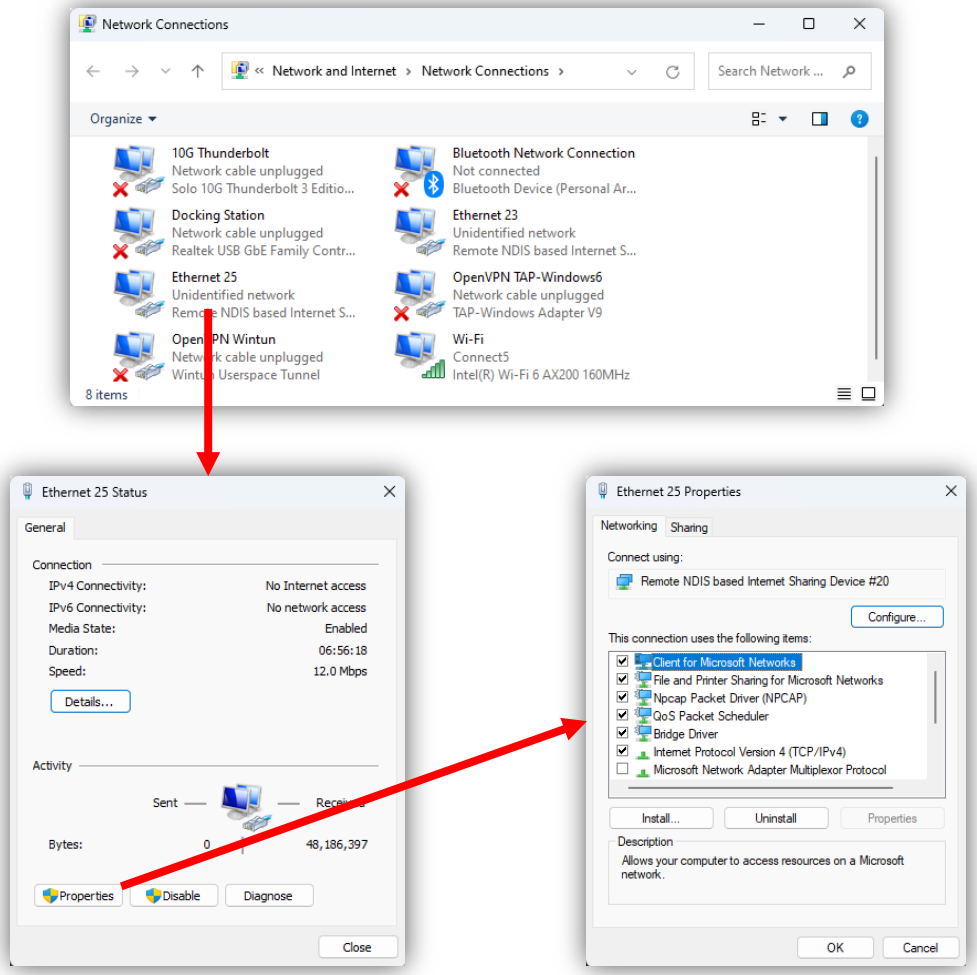
C = COMMIT

What is RAD-Meteor?

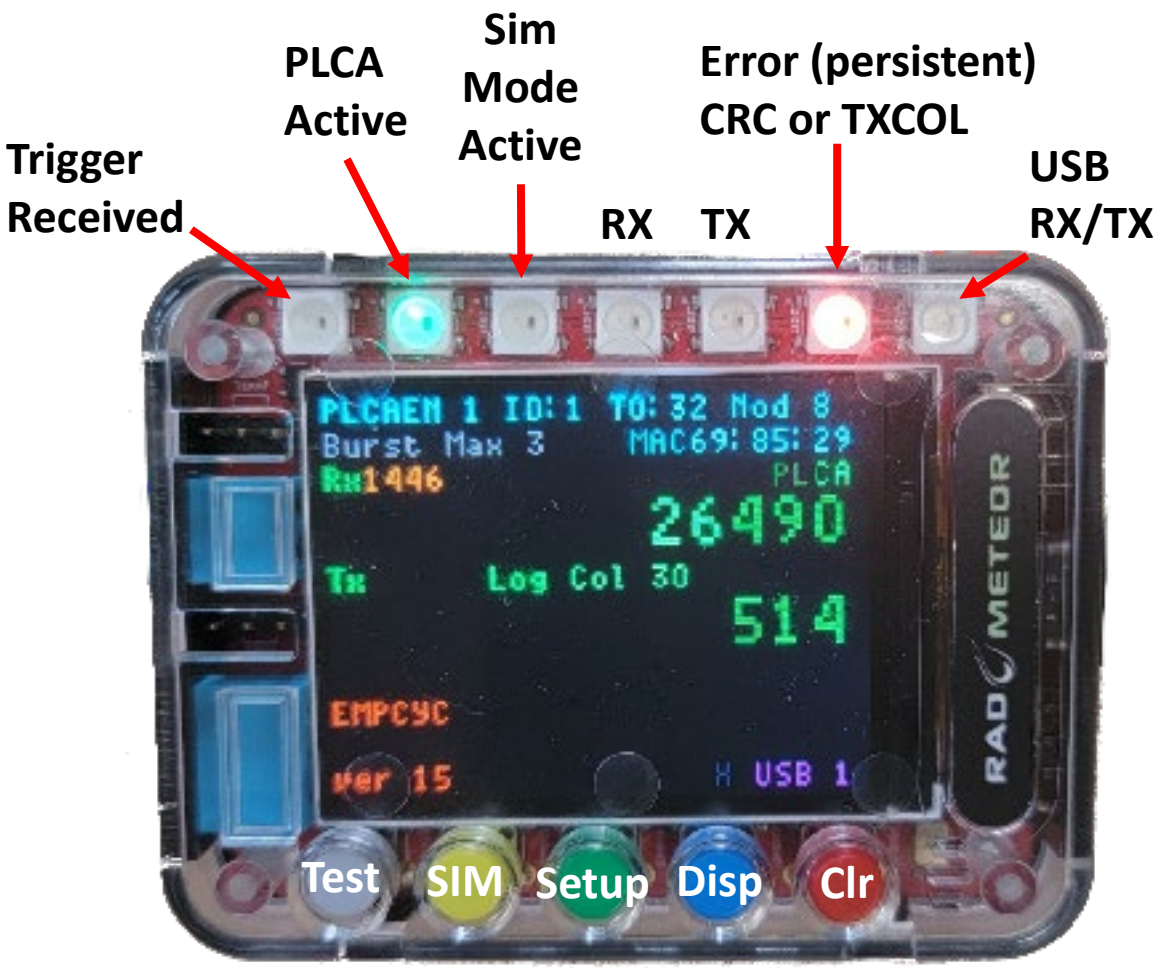


- 10BASE-T1S/USB Network Adapter
- Compatible with Windows/Linux
- *Aside from an incredibly slow link speed, no different than any other Ethernet connection to the computer*

From the command prompt, type "ncpa.cpl"



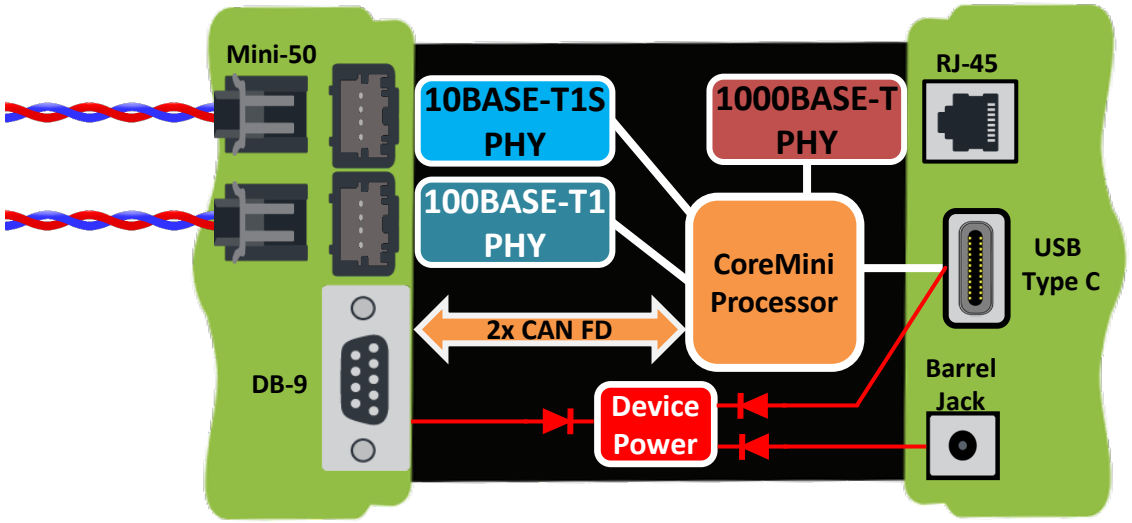
RAD Meteor User Interface



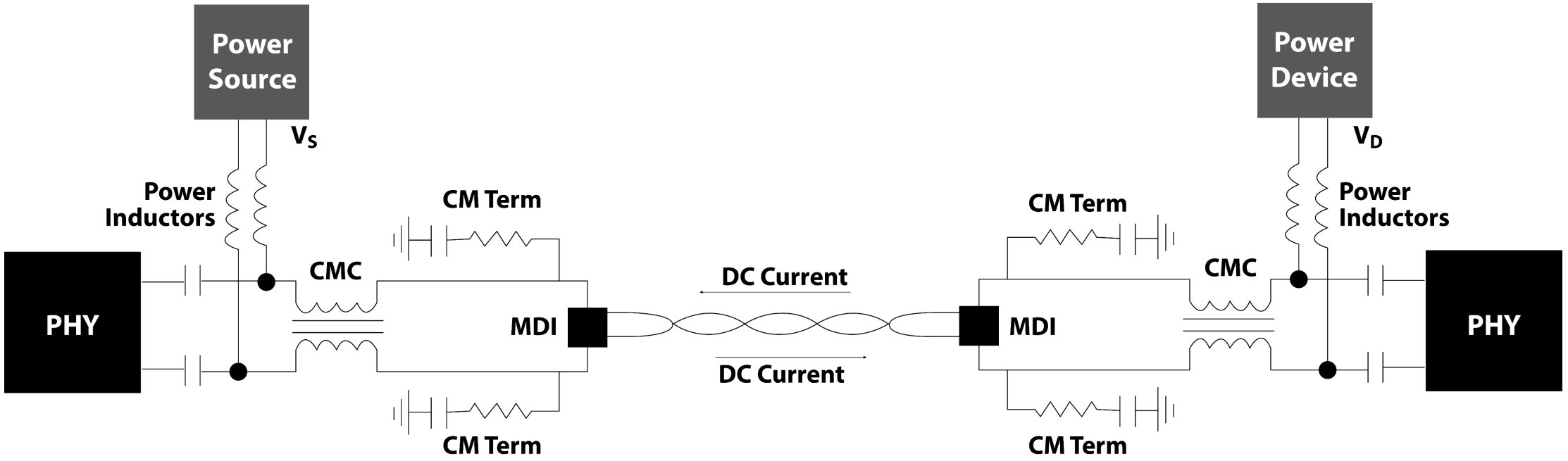
- Some LEDs are redundant with GUI
- Buttons enter menu system for
  - Enabling IEEE Test Modes
  - Enabling Node Sim Modes
  - Setup
    - PLCA Configuration
    - Scope Triggers
    - Sim Mode Configuration
  - Cycle through Display Modes
  - Clear statistics, error LED, and persistent indicators
- Inside menus, button context displayed on screen.

RAD-Comet Overview

- Network Interfaces
  - 1x 10BASE-T1S
  - 1x 100BASE-T1
  - 1x 10/100/1000BASE-T
  - 2x CAN-FD
- Applications
  - Full Vehicle Spy and Wireshark support
  - Media Converter for 10Base-T1S and 100Base-T1
  - Network Monitoring
  - ECU Simulation
  - Gateway applications between Ethernet and CANFD
  - USB interface for status register monitoring and configurations
- User interface
  - Buttons setting PHY modes
  - LED status indicators
- Device Power
  - USB
  - 6-40V (Barrel Jack / DB-9)

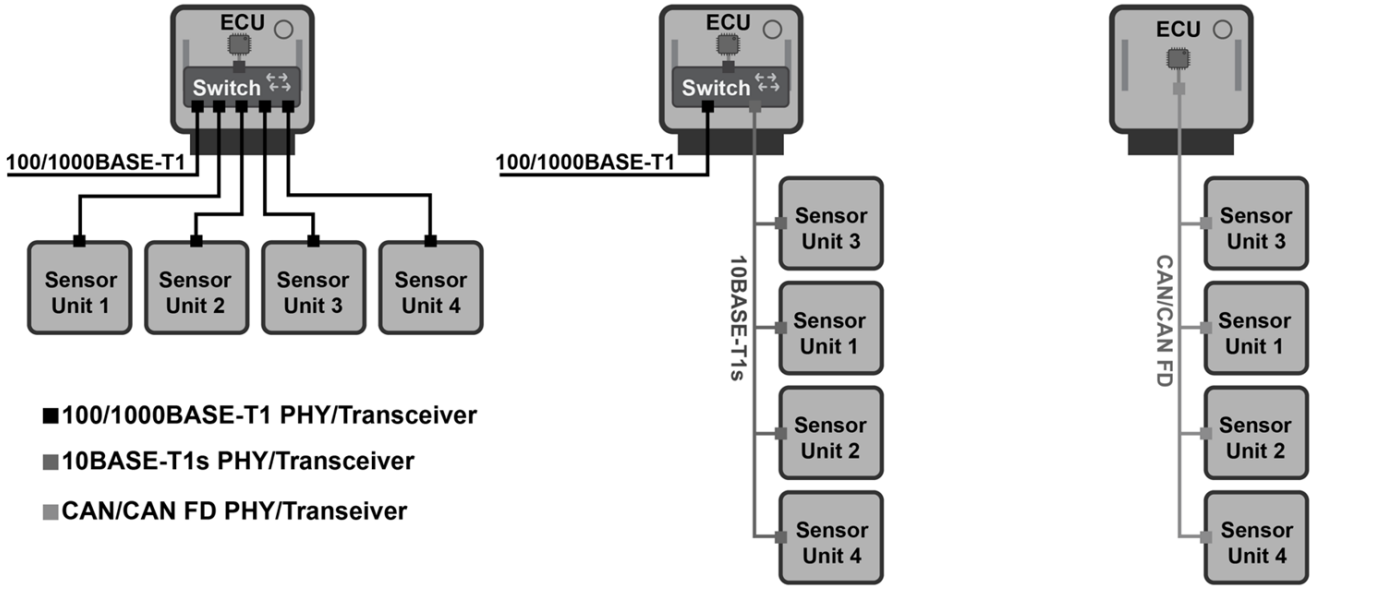


PoDL – Power Over Data Lines



BUS / Point-to-Point PHY Count Compared

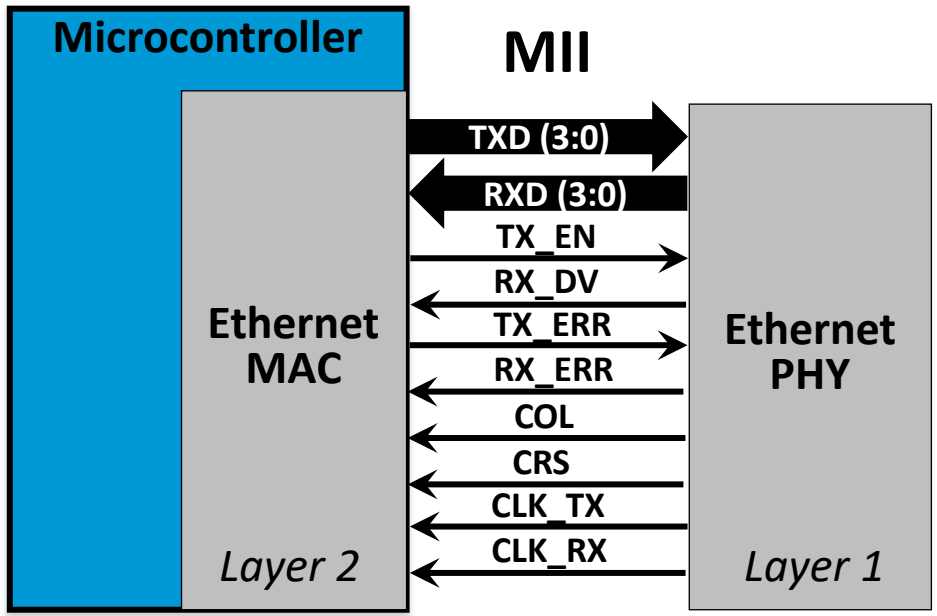
Point-to-Point verses Multi-drop (BUS) for 5 Nodes:



	100/1000BASE-T1	10BASE-T1s	CAN/CAN FD	***Advantages of 10BASE-T1s***
# of PHYs/total Connectors	8	5	5	Fewer PHYs needed
# of Connectors on ECU	4	1	1	Fewer connectors and less connector space needed on ECU
Cabling	4 cables	1 bus line	1 bus line	Less cabling, extendability, scalability
Bandwidth	≥ 100 Mbps	10 Mbps	≤ 10 Mbps	More bandwidth than CAN
Ethernet-based network	Yes	Yes	No	Seamless integration into overall Ethernet architecture

The Power of MII – 100 / 1000 / MultiGBASE-T1

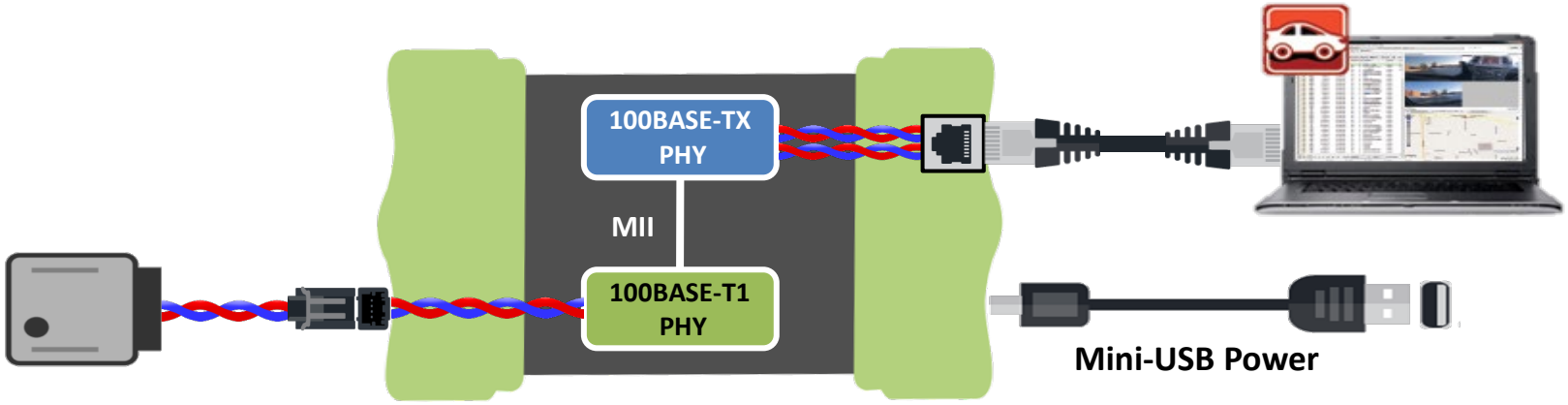
- MII
  - Media Independent Interface
  - Industry standard digital interface
  - enables different PHYs to be used with any MAC.
  - Evolved into a few variations
    - RMII: Reduced
    - GMII: Gigabit
    - RGMII: Reduced Gigabit
    - SGMII: Serial Gigabit



Swap out any Ethernet physical layer and reuse everything above

RAD-Moon Media Converter

- 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

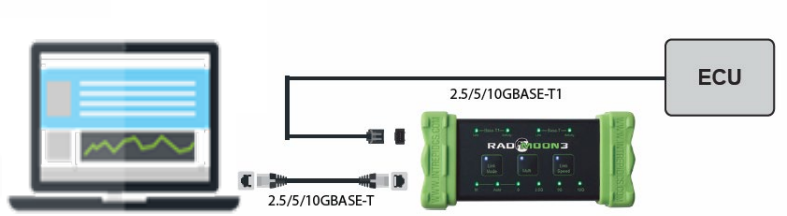
RAD-Moon2
100/1000BASE-T1 Media Converter

- 1000BASE-T1 Media Converter
- Marvell 88Q2112 PHY
- Connect between 1000BASE-T1 or 100BASE-T1 device to 100/1000BASE-T
- User Interface
  - PHY Clock Status & Configuration
  - Link Speed, Status & Activity
  - Protocol Indicators for IP/gPTP/AVTP
  - 12 Level SQI Bar Graph Indicator
- Other Features
  - Powered by USB 3.0 or Barrel Jack (4.5 – 40V)
  - T1 Connectors
    - MATEnet
    - H-MTD
  - PHY Register monitoring and updating over USB using Vehicle Spy or Intrepid's Open Source API

100/1000BASE-T1 Media Converter

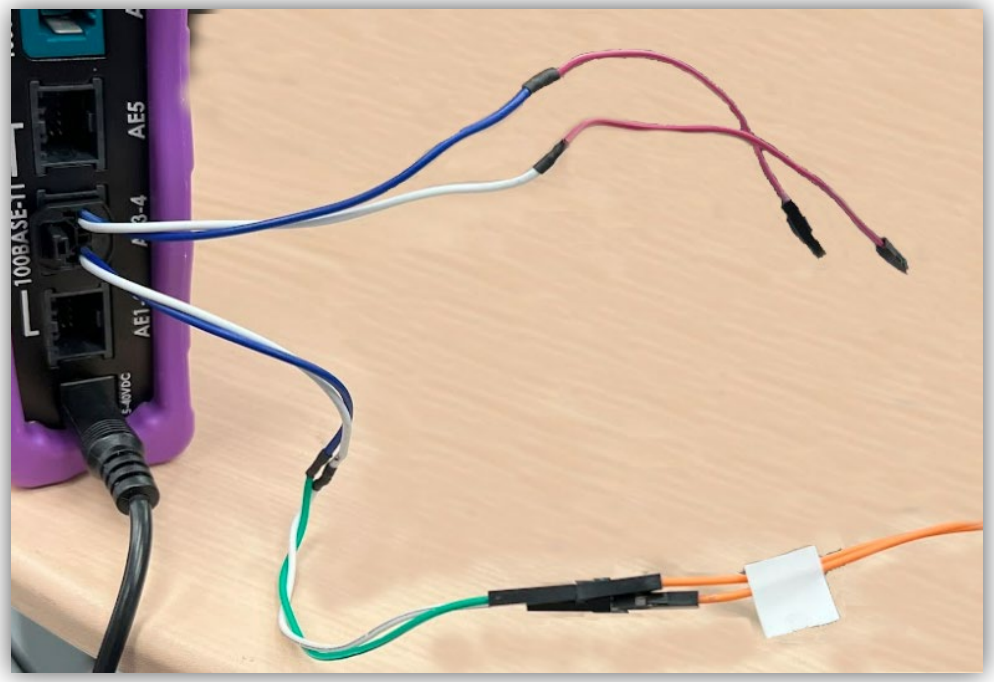
RAD-Moon3
MultiGBASE-T1 Media Converter

- MultiGBASE-T1 Media Converter
- Marvell 88Q4364 PHY
- Connect between a 2.5/5/10GBASE-T1 device to 2.5/5/10GBASE-T
- User Interface
  - PHY Clock Configuration & Status
  - Link Speed Configuration, Status, and Activity
  - 12 Level SQI Bar Graph Indicator
- Other Features
  - Power via Barrel Jack (4.5 – 40V)
  - H-MTD MultiGBASE-T1 Connector
  - PHY Register monitoring and updating over USB using Vehicle Spy or Intrepid's Open-Source API.
  - User Defined Button for use with API



Most Common Linking Problems

Rate my customers AE connections!
Would you expect any connection problems from that?



It's not ideal... lol might work, might not. Is there a problem?

It kinda works and kinda doesn't

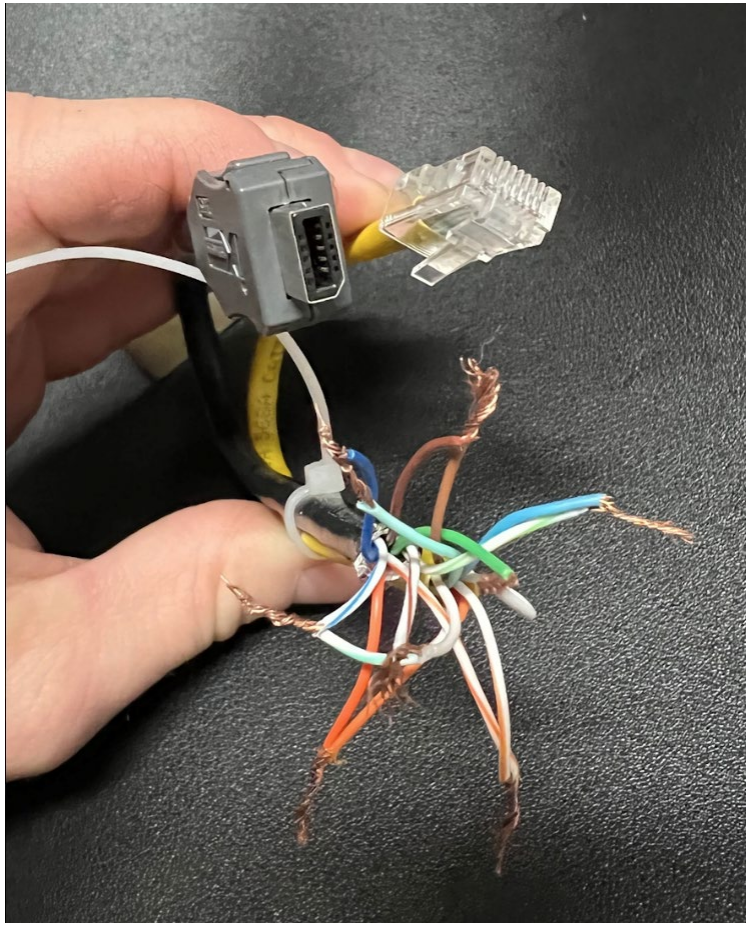
They lose connection seemly randomly

As I might expect.

It's called a single **twisted** pair for a reason.

i think there is a single twist in one of them

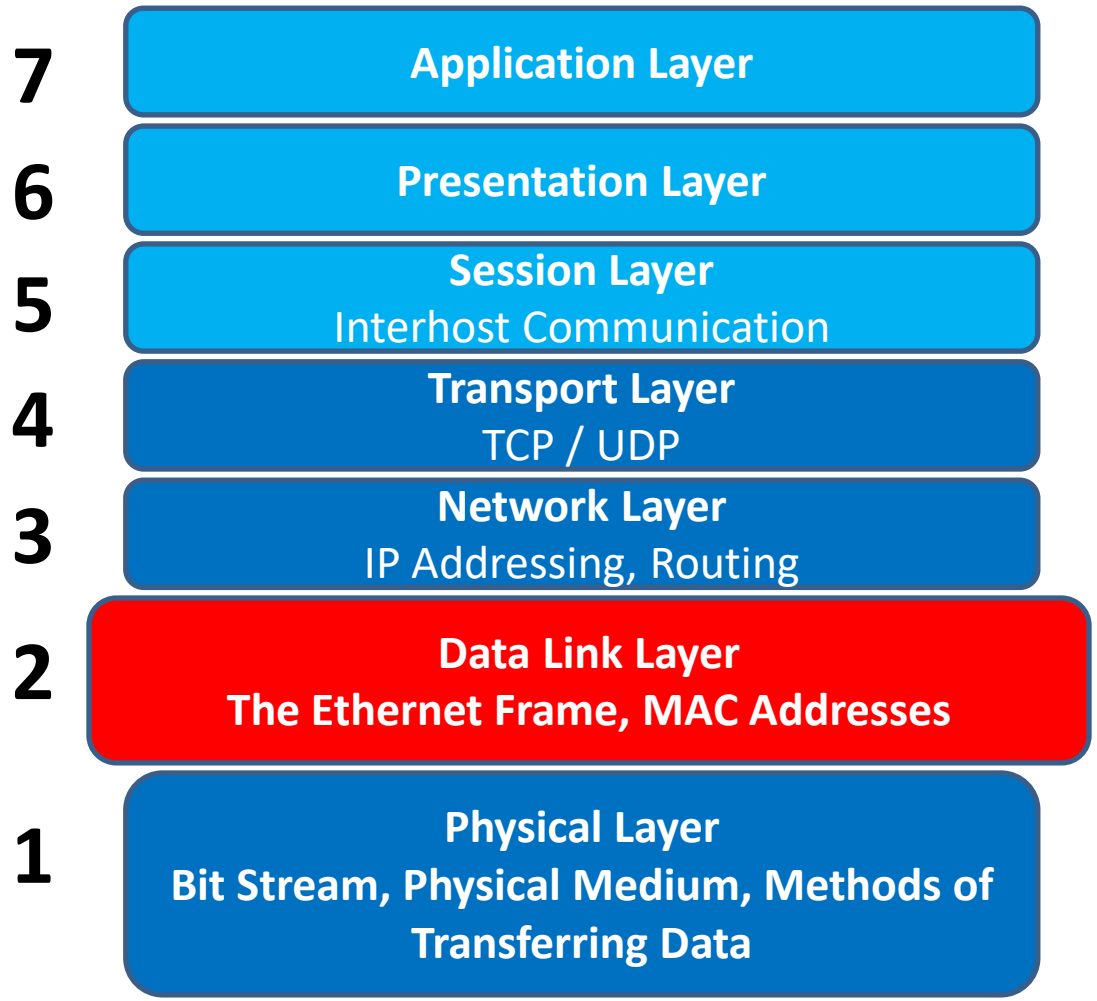
Another one for the Customer HoF



Less Common Linking Problems

- The Plug-and-Play consumer world has made us soft!
- Automotive is more a *Plug-and-Pray* environment
- Configuration Mismatch (Link Speed or Master/Slave)
  - When in doubt, turn off auto-config
  - or at least verify the configuration state as a result of auto-config
  - Double-check static configurations
- DUT Issues
  - Not powered
  - No firmware
  - Powered but asleep and waiting for Network Management
- Some problems remain a mystery (to me)

Physical Layer – 45min



The Ethernet Frame

- Lowest level data structure carrying all data on Ethernet
- Sometimes referred to as a “MAC Frame”
- Specified to meet the needs of OSI Layer 2
  - Device addressing
  - Message formatting
  - Error detection
  - QoS
- Frames can carry 46 to 1,500 bytes of data

- Max size= 1542 bytes = 12,336 bits
- Max Transmission Time
  - @100 Mbps = 123.4 µs
  - @1 Gbps = 12.3 µS
  - @10 Gbps = 1.3 µS

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) →								

Preamble / Start of Frame Delimiter

- Preamble: 7 octets* of 10101010
- Start of frame delimiter (SFD): 10101011
- Preamble provides signal edges so network device clocks can synchronize with each other

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) →								

**At one point in time, the term "byte" was considered hardware dependent. "Octet" has been used in countless standards to eliminate any ambiguity.*

Ethernet Addressing: the MAC Address

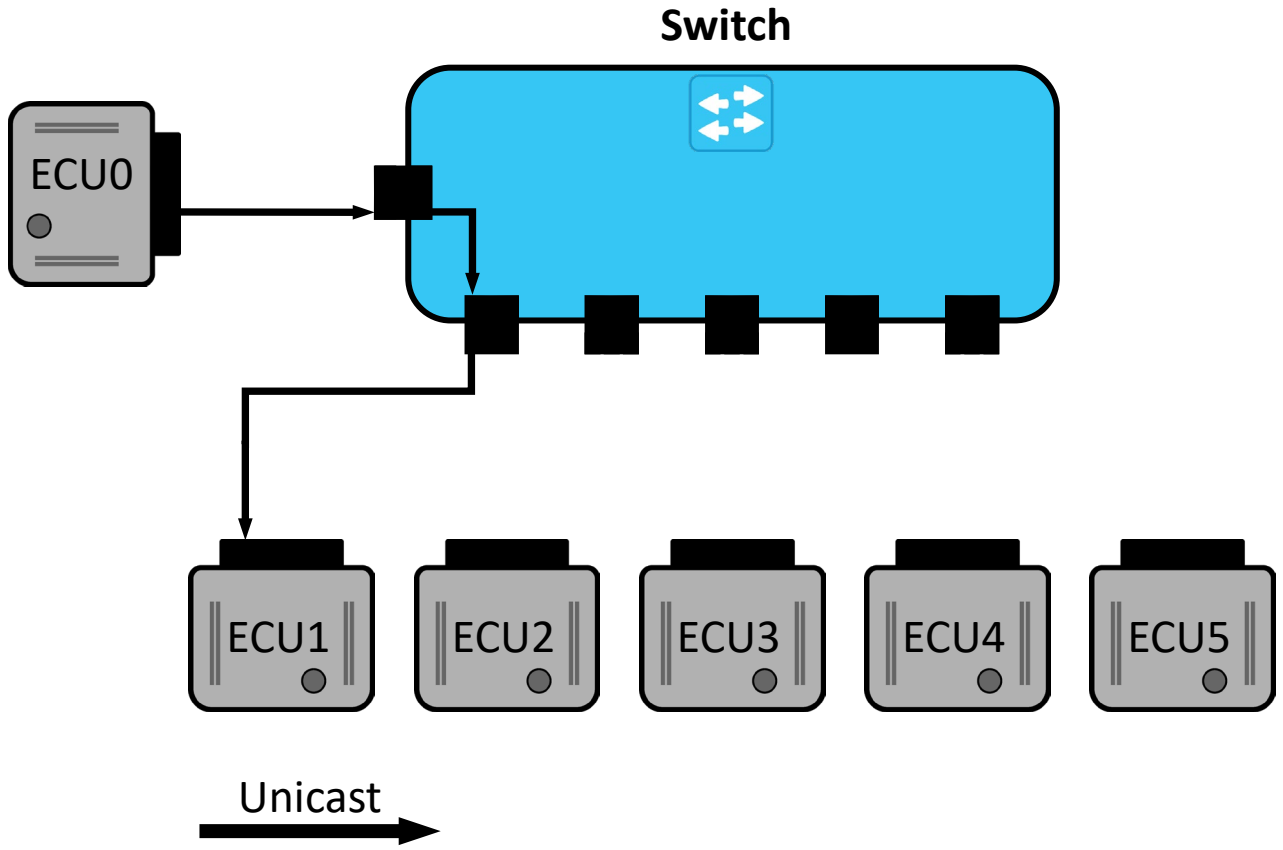
- Low-level / physical network address:
  - Programmed into hardware devices
  - 6 bytes long, each node globally unique *(usually)*
  - First 3 bytes is registered to an organization (OUI)
  - A MAC address is sometimes referred to as an Ethernet address
- Used to direct data on an Ethernet network:
  - 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) →								

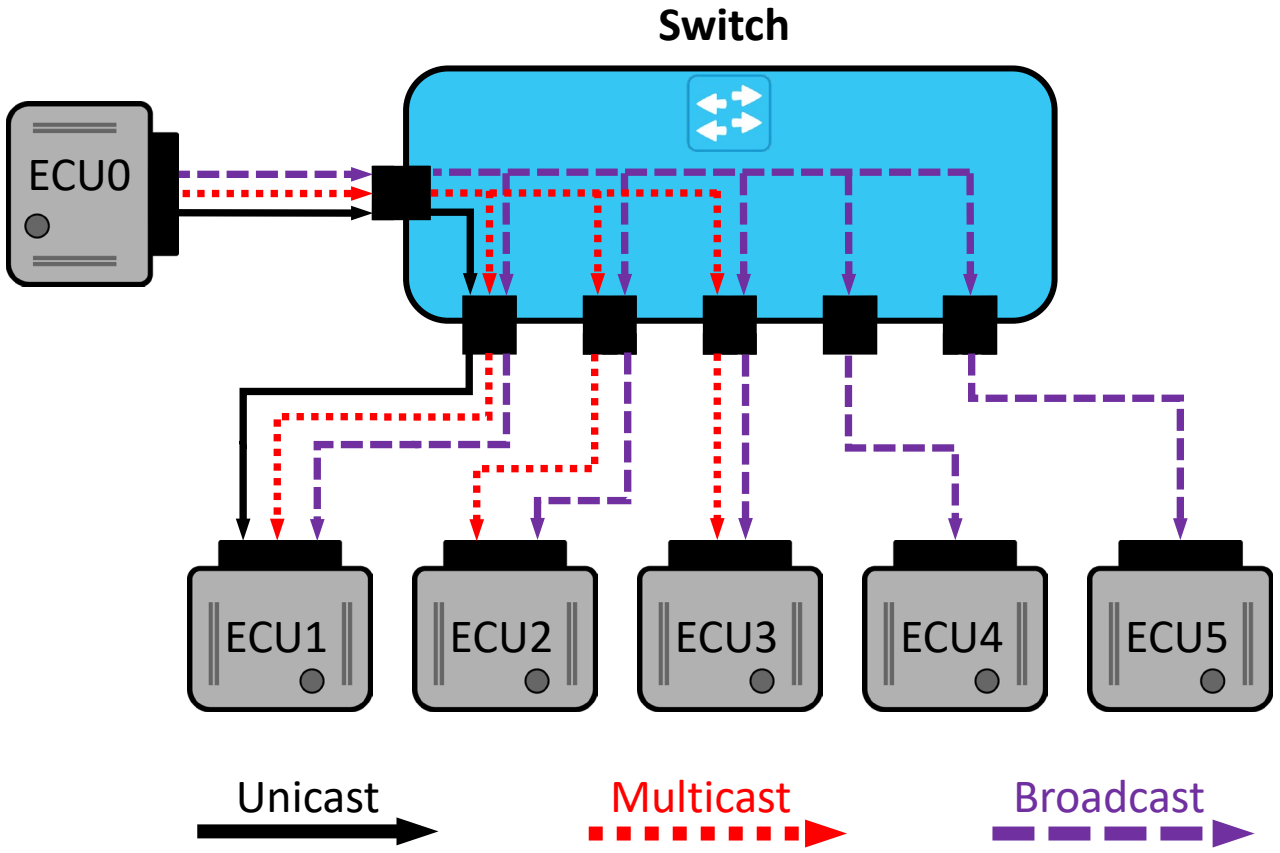
Unicast MAC Addresses

- Universally Administered Address (UAA)
  - Globally unique / Assigned by manufacturer using OUI
  - Example: **00**:XX:XX:XX:XX:XX
  - 2nd LSb of first byte of MAC address is “0”
    - xxxx.xx**0**x$_2$
- Locally Administered Address (LAA)
  - Designates the address is probably not unique outside an ***engineered network.***
    (Like say…., an automotive network)
  - Example: **02**:XX:XX:XX:XX:XX
  - 2nd LSb of first byte of MAC address is “1”
    - xxxx.xx**1**x$_2$



Multicast MAC Addresses

- Multicast: one to many (Streams)
  - Most commonly **01**:XX:XX:XX:XX:XX
  - LSb of the first octet of the Address = “1”
    - xxxx.xxx**1**$_2$
- 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
  - Value < 1536: indicate length (legacy support)
  - Value >= 1536: IEEE Assigned Values
    - 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

More on VLANS very soon…

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.

Payload

- Ethertype defines the header information and organization of the payload
- For example, in an IPv4 Ethertype indicates the beginning of the IP header starts here.

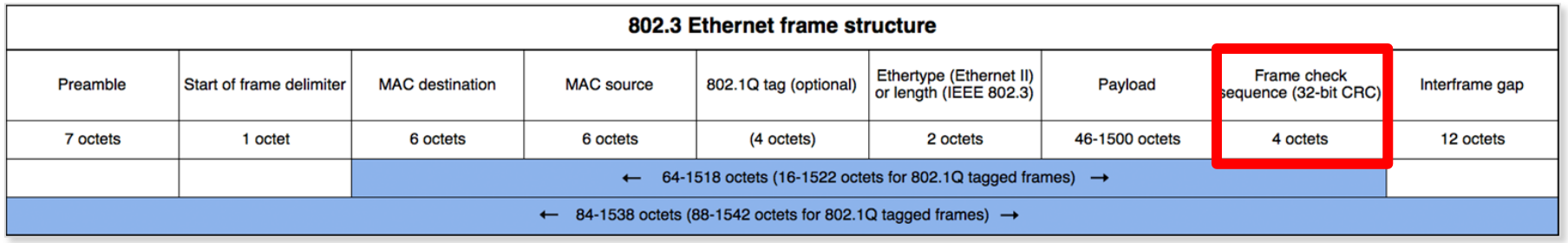
802.3 Ethernet frame structure

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

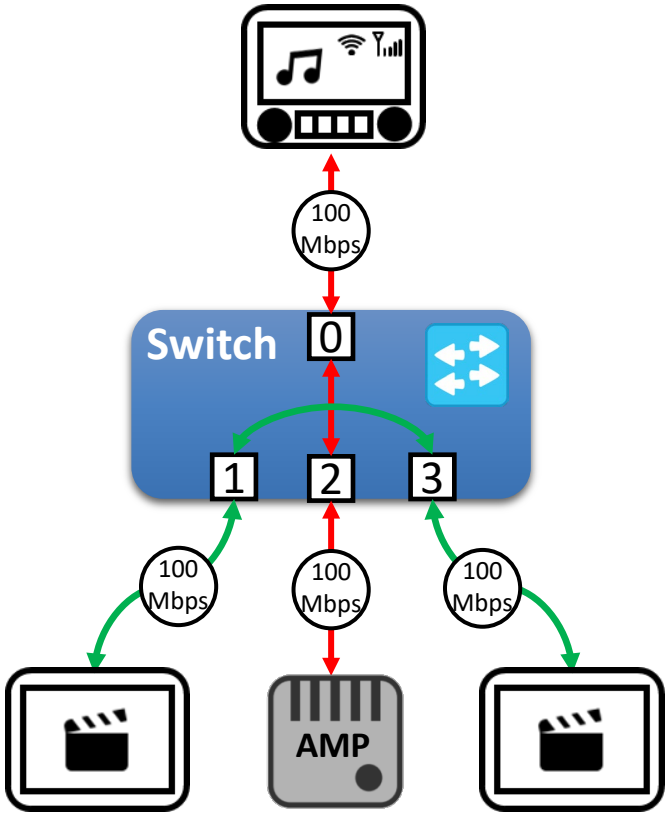
  (this is implemented at higher layers; hint: TCP)



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) →								

What does a Layer 2 Switch Do?

- Connect devices and deliver services and support protocols on Layer 2
- 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



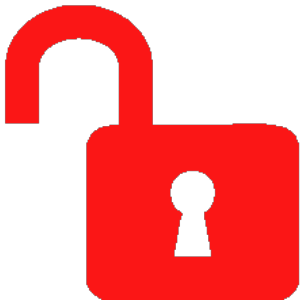
Two communications streams with an aggregate bandwidth of 400 Mbps

Intelligent Frame Forwarding

- Address Translation Unit
  - L2 Address Table
  - MAP 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

Layer 2 Forwarding Table Configurations

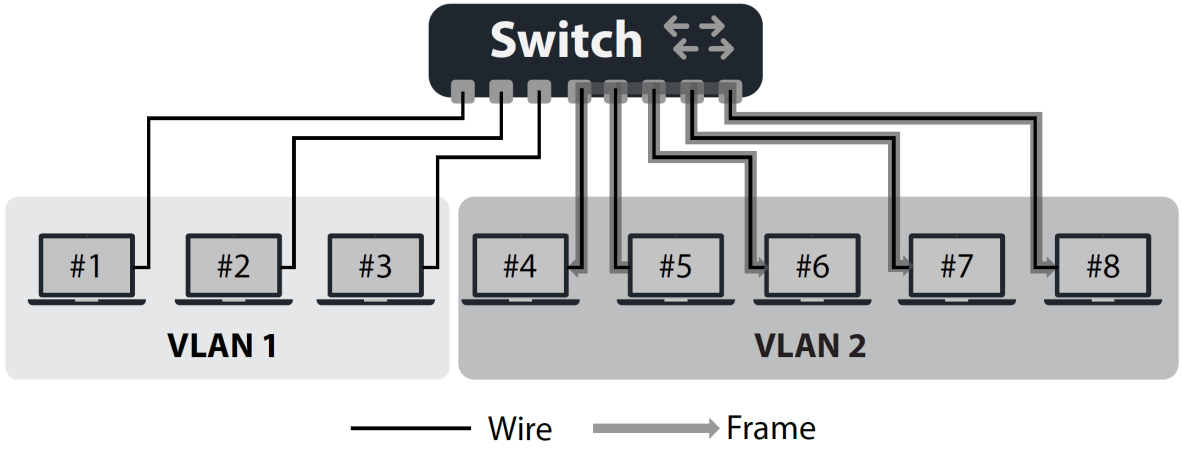


- Dynamic Table (Most common – “Plug & Play”)
  - Switch has no knowledge of connected devices after boot
  - “Flood” ports with Unknown Destination Address (DA)
  - Built from Source Address (SA) of frames received
  - Addresses removed if not received periodically

- Static Table
  - Pre-program L2 Address Table
  - Unknown Destination Address (DA)
    - Do nothing (Secure)
    - “Flood” ports (Plug & Play)

Virtual LANs (VLANs)

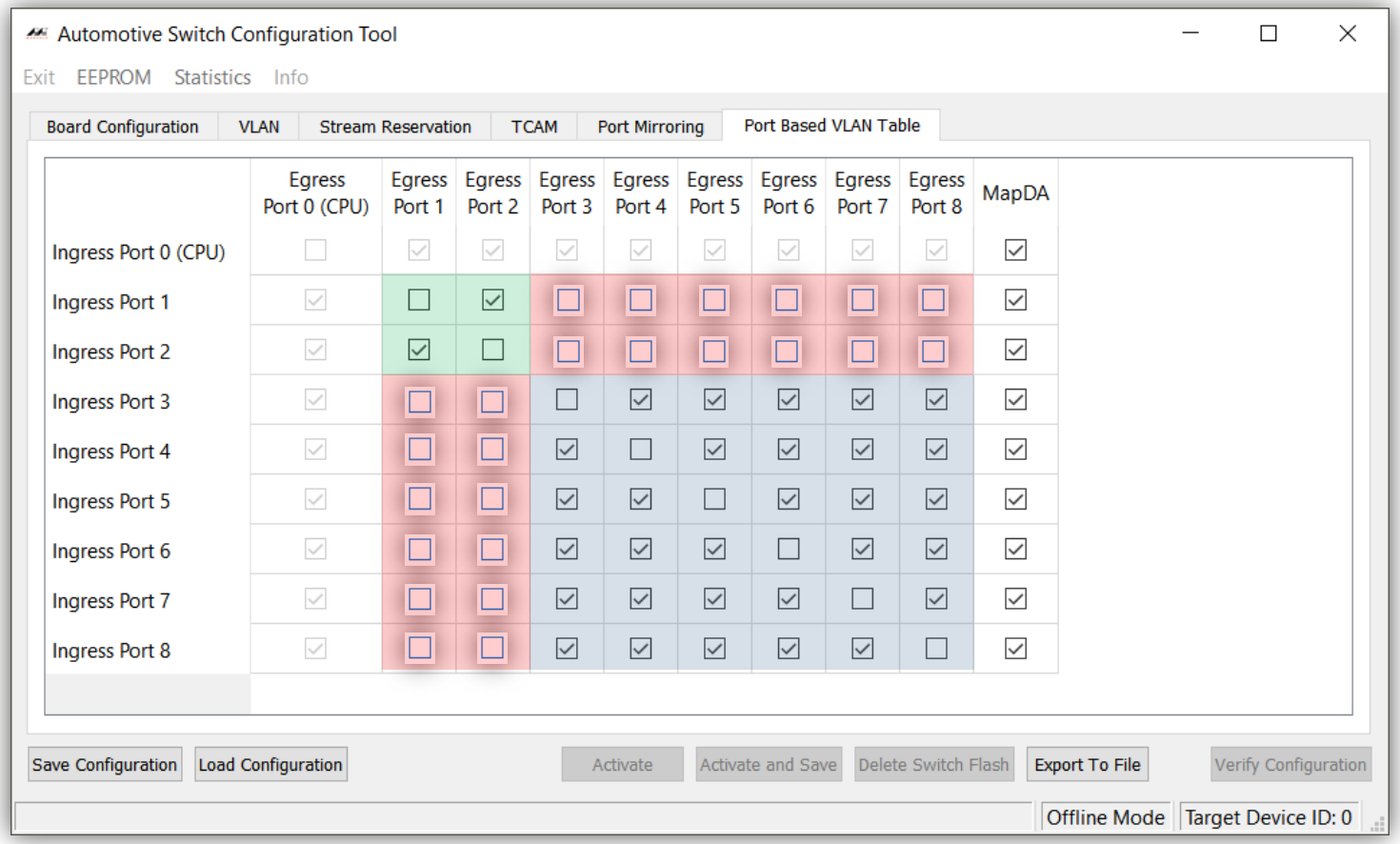
- QoS at Layer 2 in hardware
- Switch enforces forwarding restrictions based on VLAN configuration
- Each VLAN "sees" only its own traffic
- Used to optimize bandwidth use with least resources
- Two types of VLANs
  - Port Based VLAN
  - VLAN Tags in Ethernet Frame Header



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

Port Based VLAN

- Egress paths of each ingress port are explicitly enabled or disabled
- Example defines exclusive connection between Ports 1 and 2 (Green)
- Additional VLAN shared by Ports 3-8 (Blue)



IEEE 802.1Q – VLAN Tagging

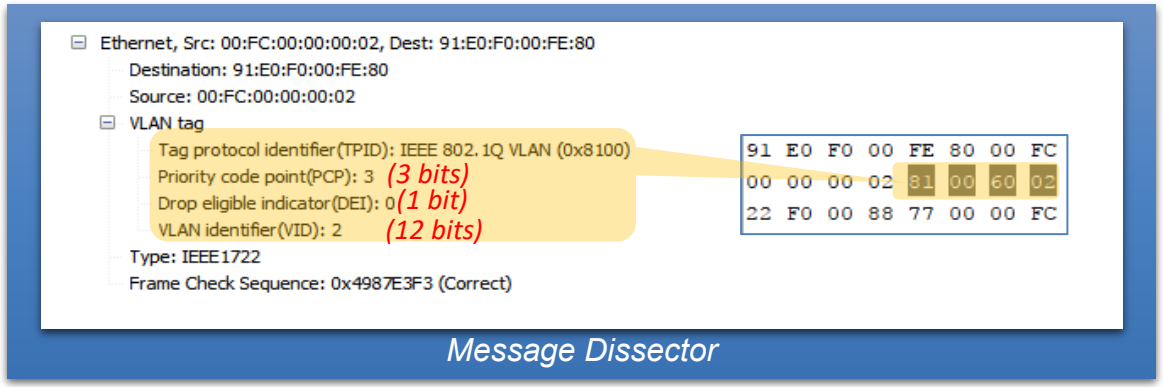
- Port Based VLAN
  - Static
  - “All or Nothing”
- VLAN Tagging
  - Optional content in Ethernet frame to isolate networks and control bandwidth.
  - Frames forwarded based on port membership of a VLAN.
  - Can be static or managed configuration
  - 2 octets following MAC SA
    - 0x8100 designates the frame as having a VLAN tag.
    - 0x9100 designates double VLAN tag
- May or may not see VLAN tag in Windows depending on NIC hardware and configuration.

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) →								

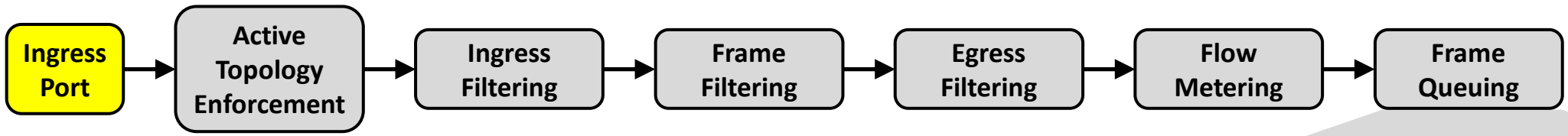
VLAN Tag Information

- VID
  - VLAN ID
  - 12-bit value identifying a VLAN.
  - Defines where the frame may or may not be forwarded by the switch
- DEI
  - Drop Eligible Indicator
  - QoS flag indicating to a switch that the frame can be dropped in congestion. (If switch is so configured)
- PCP
  - Priority Code Point
  - Indicates which priority queue should be used in forwarding the frame.

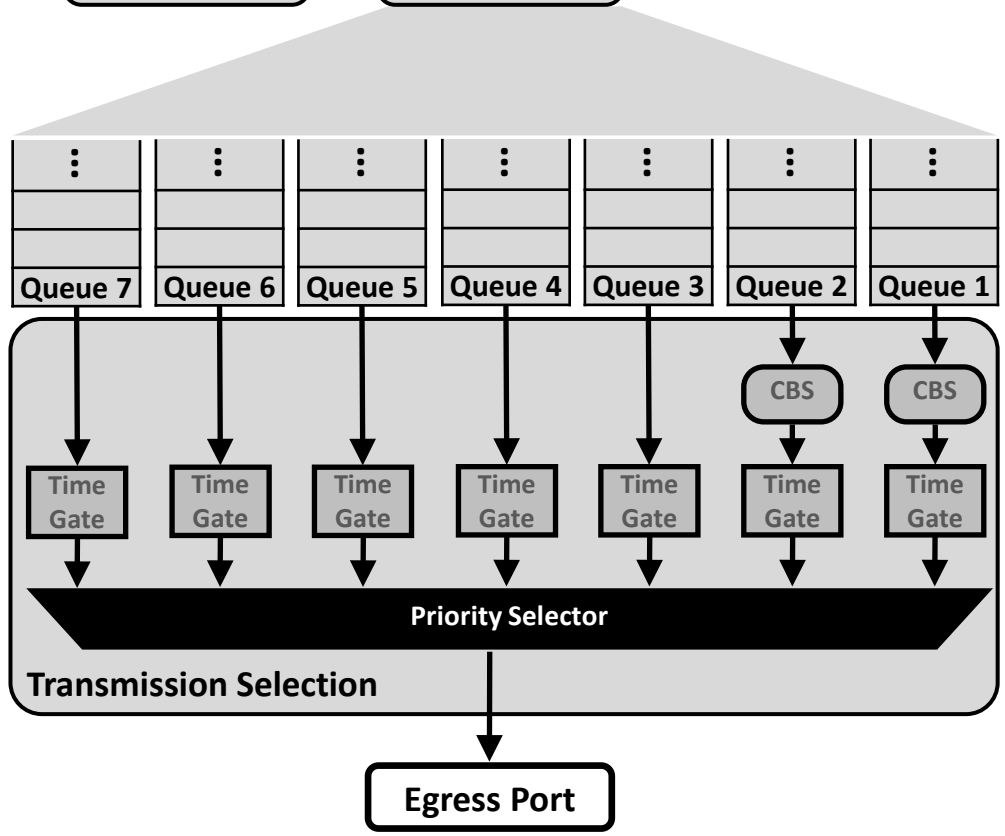


The term VLAN is commonly used to imply the VID. In other words, if someone references VLAN 2, what they really mean is a VLAN with a VID of 2

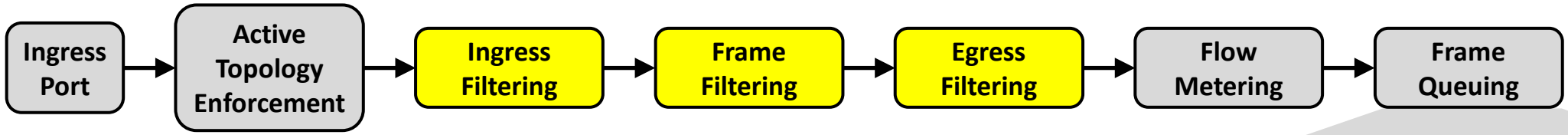
Switch Ingress



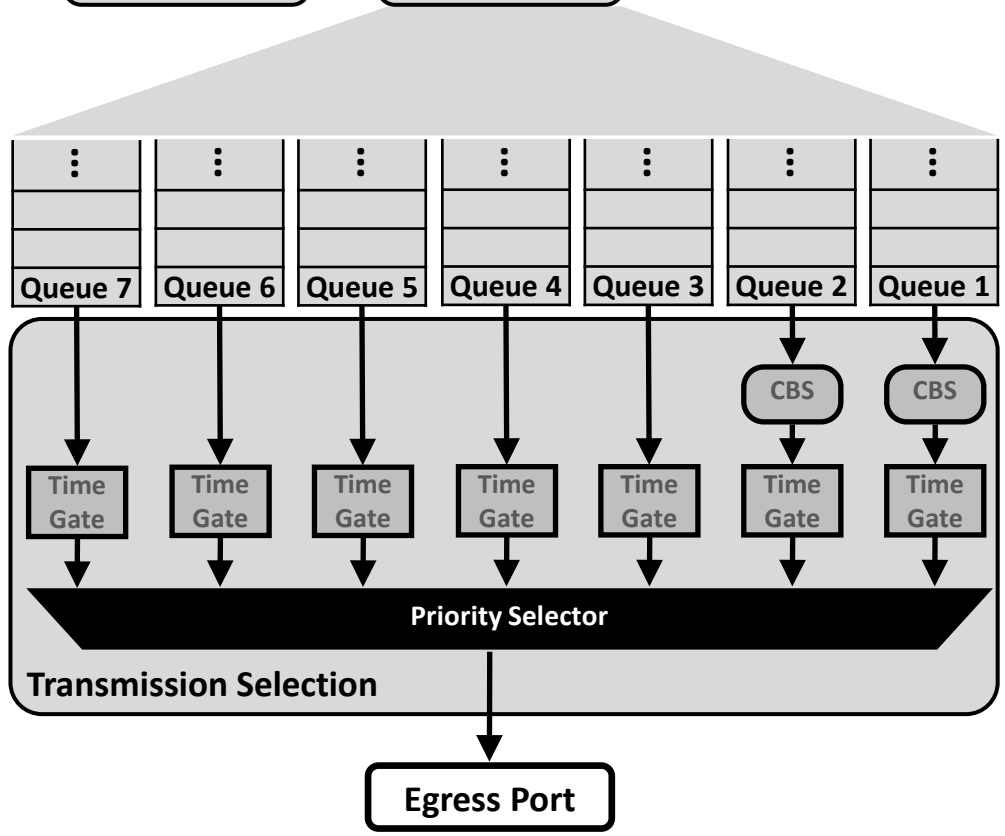
- Eliminate frames with errors, oversized frames, “runt frames” (<64 bytes)
- “Store & Forward” Device
  - Entire message must ingress switch before it is forwarded.
  - Required to check the FCS and drop the frame if it is corrupt.
  - Latency a function of the length of the frame
  - Opposite of “Cut-Through” device which allows egressing almost immediately after ingressing.



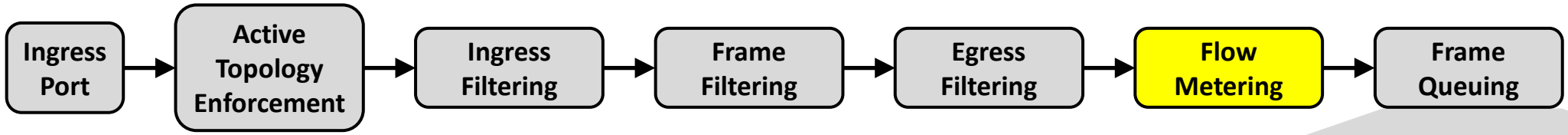
VLAN Enforcement and Filtering



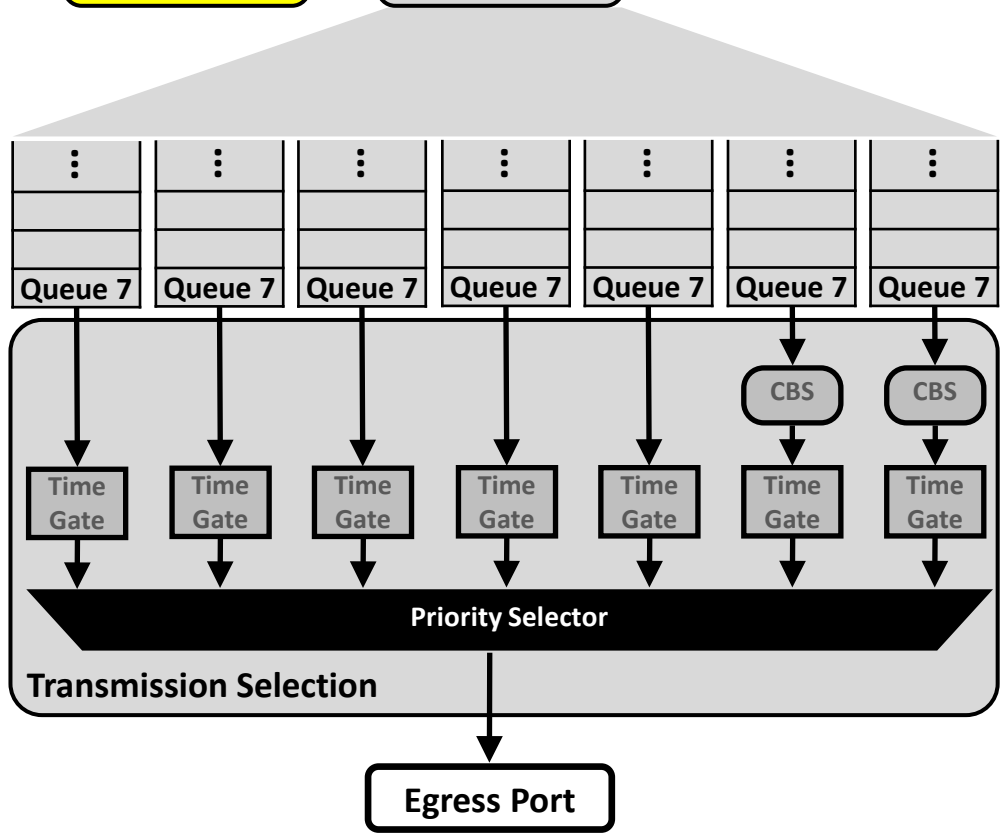
- Determines which ports the frame should forward the frame-based destination MAC address and VLAN information.
- Switch "Policies" enforced to trap or drop frames
  - VLANs (Tagged / Untagged / Unknown VLAN tags)
  - Unknown DA (Destination Address)
  - Reserved DA *(protocols like gPTP)*
- TCAM filtering to enable "actions" later in the forwarding process.



Flow Metering



As the name suggests, this is where a switch can restrict the flow of a stream if it exceeds a specified threshold that is defined in terms of frames per second or bits per second.



Network Traffic Metering

- Traffic metering
  - Method to restrict the *average* flow of traffic to not exceed a specified bandwidth
  - Not necessarily a strict bandwidth limit. It can be configured to allow bursts of traffic that exceed the bandwidth limit for a short time.
  - Although metering affects the egress of the traffic, understand that it is applied per ingress port.
  - Does not necessarily need to apply to all the traffic ingressing a given port; it can be selectively applied based on the MAC address and VLAN information in the Layer 2 header.
- The Token Bucket Algorithm
  - Metering algorithm used for Ethernet is described in the Metro Ethernet Forum Technical Specification 10.3 (MEF 10.3).
  - The algorithm itself does not shape the traffic, but "colors" each Ethernet frame (Red/Yellow/Green) based on how it compares to the allowable limits set.
    - Information Rate: The bandwidth limit (usually in bits-per-second)
    - Burst Size: An allowable amount of data that can exceed the information rate for a brief time. (usually in bits or bytes)
  - Switch configuration determines how each color is treated
    - Dropped
    - Tagged as "Drop Eligible"
    - Forwarded at lower priority

Single Token Bucket
2-color (Red/Green)

- Tokens
  - "Cost" of sending 1 bit = 1 Token 
  - Tokens accumulate in the bucket at the **Committed Information Rate** (CIR)
  - The maximum tokens accumulated is equal to the **Committed Burst Size** (CBS)
  - Tokens stop accumulating when the bucket is full
- Egressing Frames
  - If bucket contains *equal or more* tokens than bits in frame
    - Frame is compliant with limits and colored GREEN
    - Frame forwarded and Tokens removed from bucket
  - If bucket contains *less* tokens than bits in frame
    - Frame is not compliant with limits and colored RED
    - Disposition of frame depends on network configuration
      - Dropped
      - Forwarded with a lower priority and/or DEI bit is set *(Drop Eligible Indicator)*

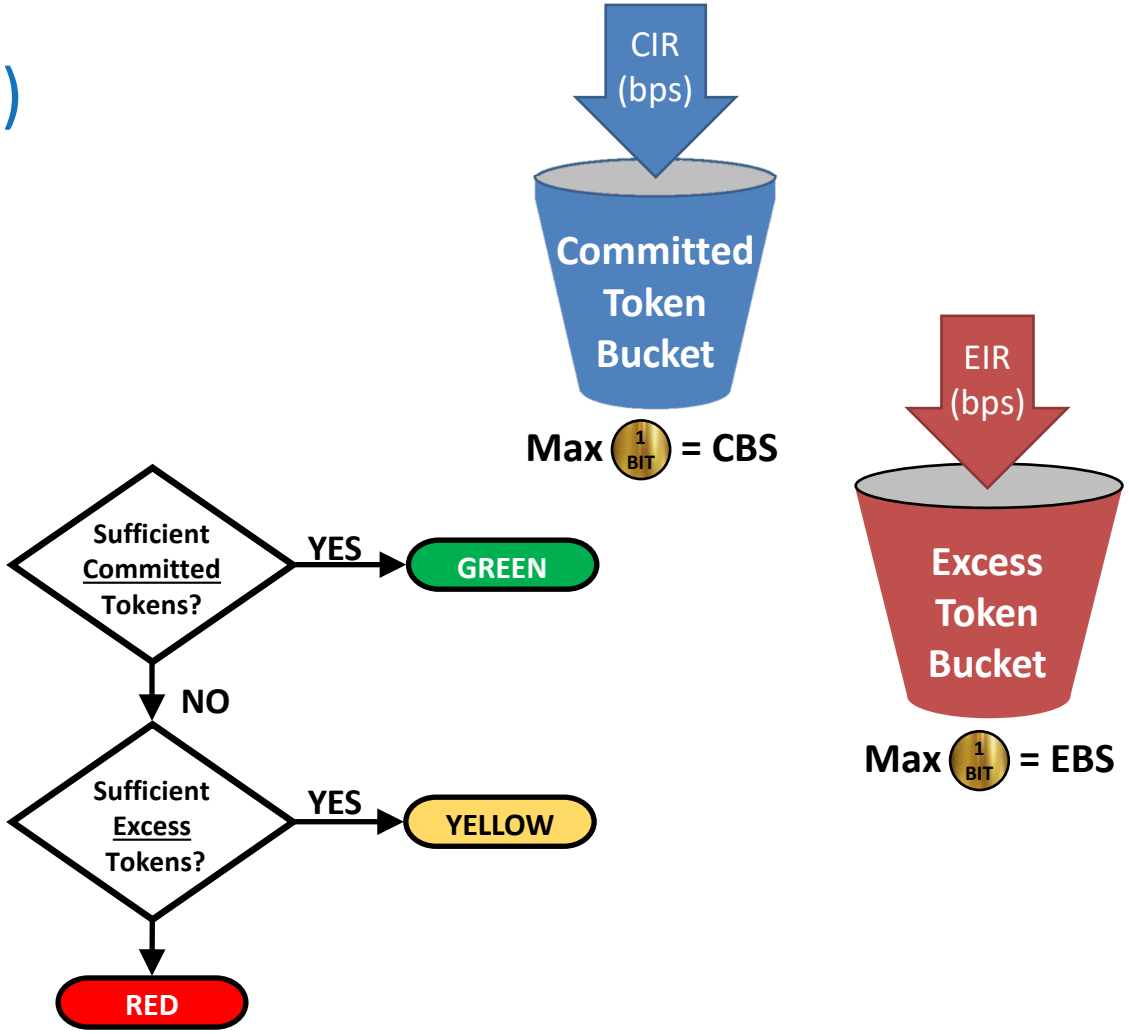
CIR = 100 bits/sec
CBS = 1000 bits

512-bit frame

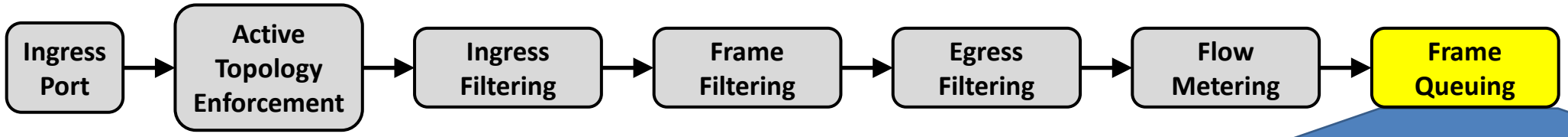
Dual Token Bucket

3-color (Red/Yellow/Green)

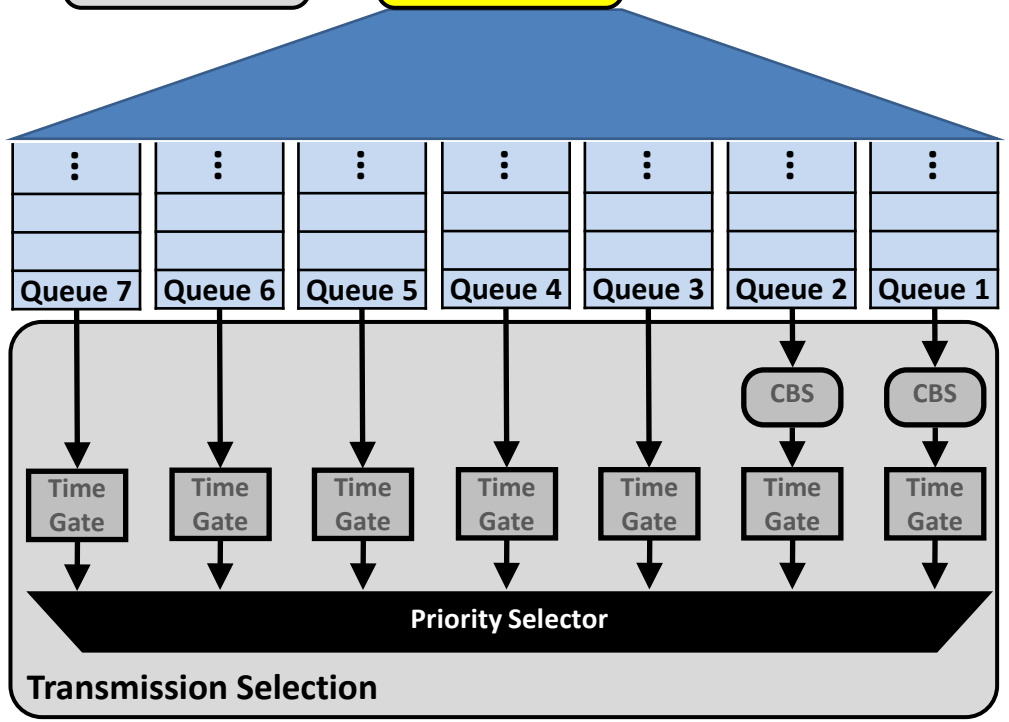
- Second Bucket
  - EIR (Excess Information Rate): The unacceptable limit for the average rate in bits/second.
  - EBS (Excess Burst Size): The unacceptable limit for the maximum number of bytes in a burst of traffic
- Egressing Frames with insufficient Committed Tokens are evaluated against Excess Tokens
- Some variations allow excess tokens from the Committed Bucket to overflow into the Excess Bucket.



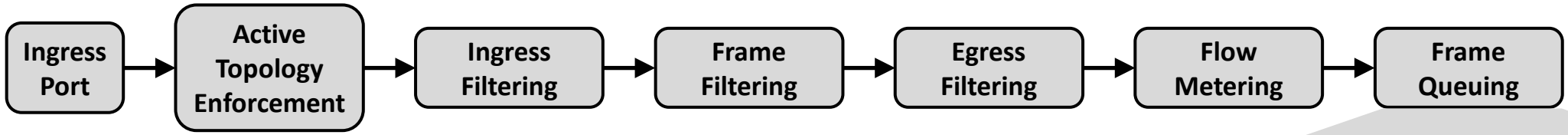
Frame Queuing



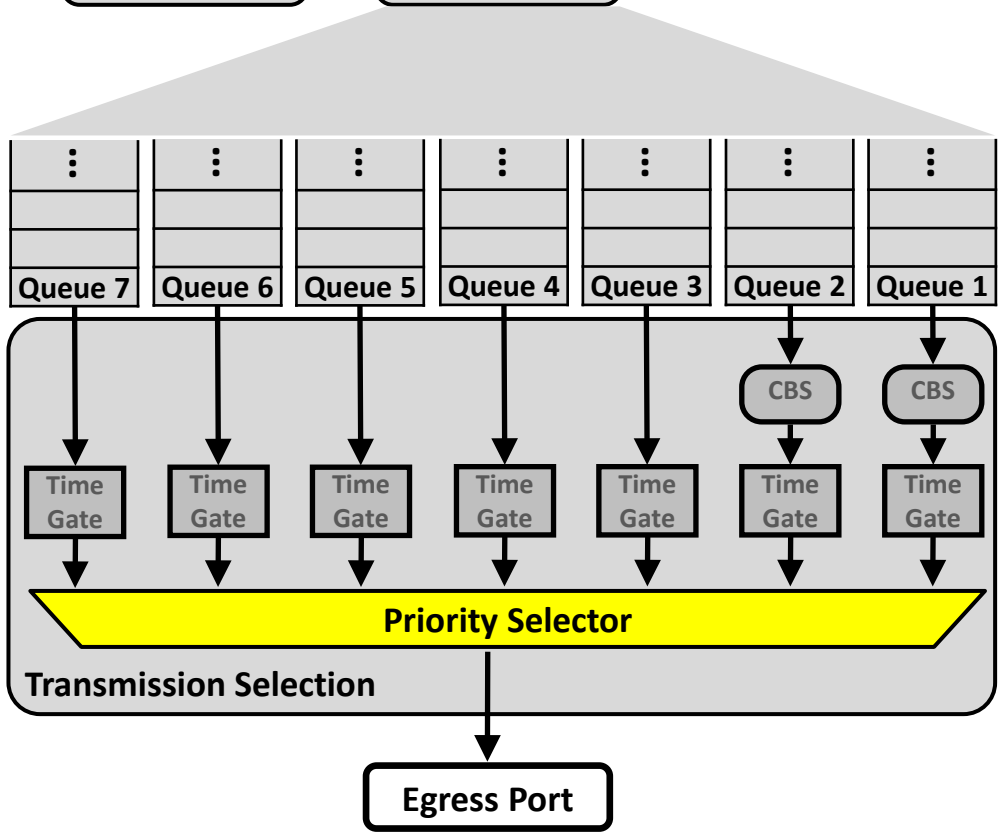
- Each port of a switch contains
  - up to 8 egress priority queues (PCP)
    - PCP determined by default or VLAN tag
  - assigned to up to 8 unique traffic classes.
- In addition to the queue granting a specific priority to the traffic class assigned to it, each queue may also be assigned one or more forms of QoS. (Quality of Service)



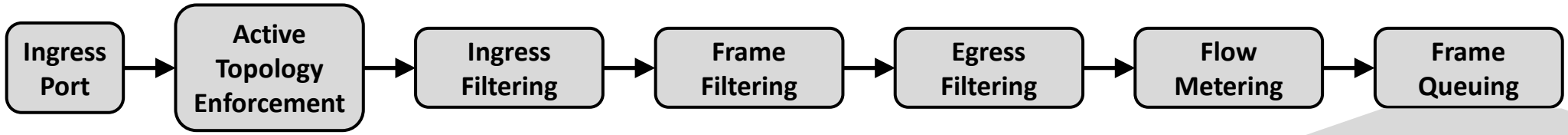
Transmission Selection



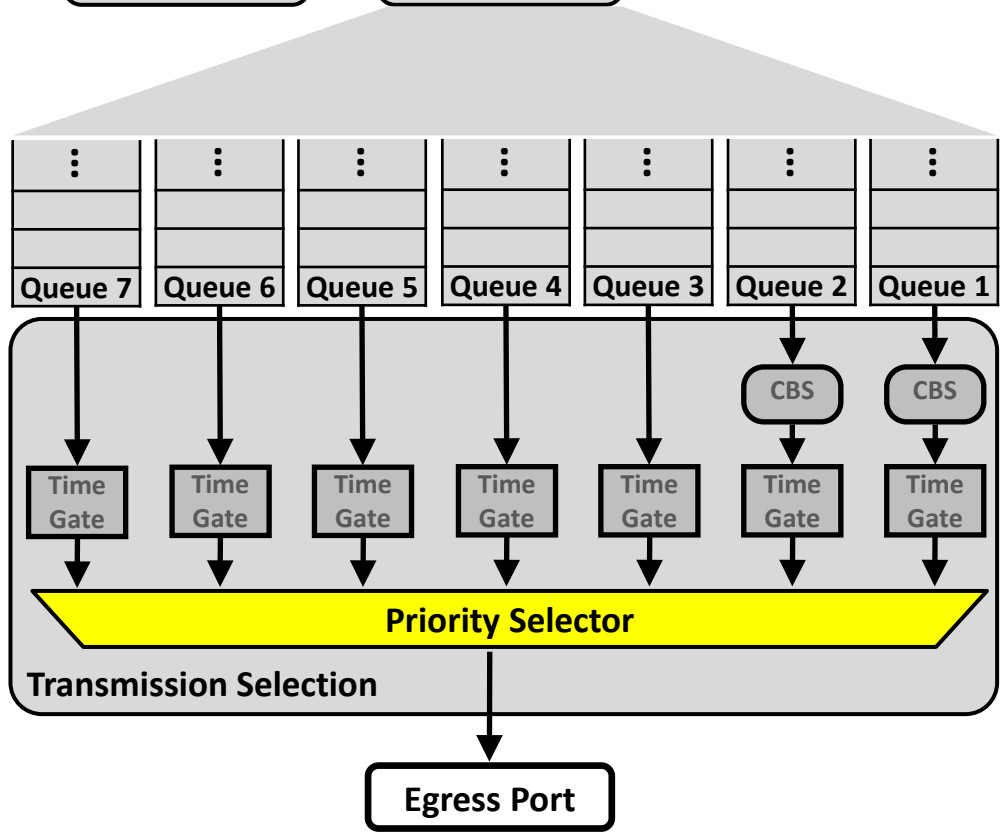
- There are many forms of QoS that dictate how the queues are emptied.
- Strict Priority:
  - Queues are emptied by order of priority
  - Frames may be transmitted from a queue, if and only if, all of the higher priority queues are empty.
  - Congestion Loss: Low priority queues overflow, and frames are dropped.



Enhanced Transmission Selection

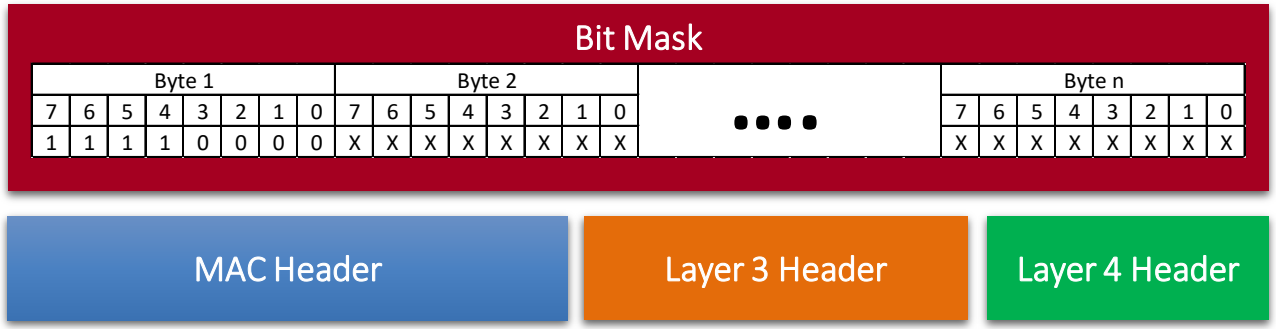


- Enhanced Transmission Selection:
  - Generic term for algorithms that allow the sharing of bandwidth between the different traffic classes.
  - The most known algorithm is weighted round-robin queuing.
    - Minimize congestion loss by periodically giving each queue the opportunity to transmit frames
    - "Weighted" implies higher priority queues have more time
- Other specialized forms of Transmission Selection exist for meeting specific QoS goals (AVB/TSN)
  - Eliminating Congestion Loss
  - Bounding Latency
  - Improving Determinism



What is TCAM?

- TCAM = Ternary Content Addressable Memory
- Technology behind Deep Packet Inspection
- Bit mask is applied to a range of bytes
- “Ternary” = 1,0,X
- “Hit” occurs when the bit pattern matches the mask



TCAM Actions

A “hit” can trigger the following *actions*

- Drop the message
- Mirror the message to a specific port(s)
- Override Destination Ports
- Manipulate VLAN tags
- Reprioritization
- “Trap” the message to a host microcontroller for specific handling in software
  - Deeper Inspection
  - Cybersecurity
  - Logging, network statistics, diagnostics, etc.
  - Complex ingress policing (e.g. temporal, adaptive, etc.)
  - Gateway to another network

TCAM Applications

- Stream Identification (AVB/TSN)
- Hardware filtering
  - *Any pattern or combination of patterns out to Layer 4 header!*
  - MAC(s)
  - VLAN/Ethertype
  - IP Address(s)
  - Port(s)
- Frame Dropping (AVB/TCP/UDP)
  - Simple means to create intermittent errors
  - Filtering out stream from relevant traffic
- Change VID, priorities
- Inject traffic
  - DoS
  - Spoofing

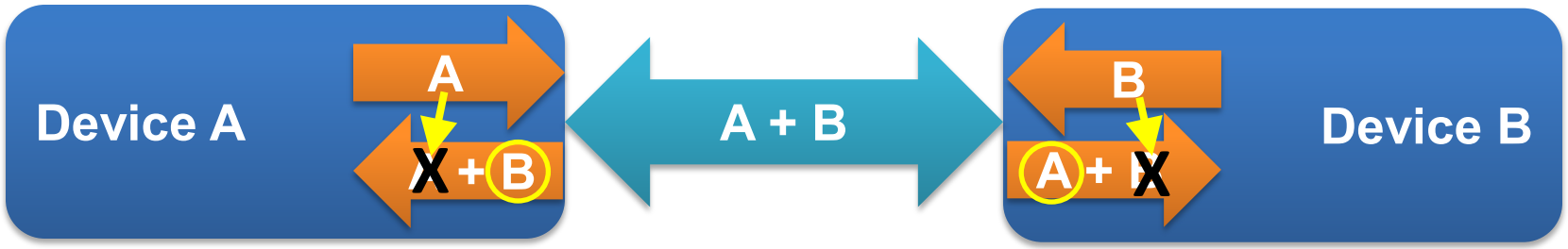
Traffic Monitoring in a Switched Network

- Bus topology (CAN/LIN/etc.) can be easily tapped
- Not possible with a switched topology like Automotive Ethernet
  - No shared bus
  - A probe on a switch's port will only see traffic sent to that port, and not any others
- Technologies like 100BASE-T1 are also designed for exactly two devices:
  - Complex signaling may be disrupted by the addition of a probe
  - The larger obstacle is that it is impossible to decode (next slide)

Why Can't I Just Probe 100/1000BASE-T1?

The price to be paid for having Full Duplex on single medium:

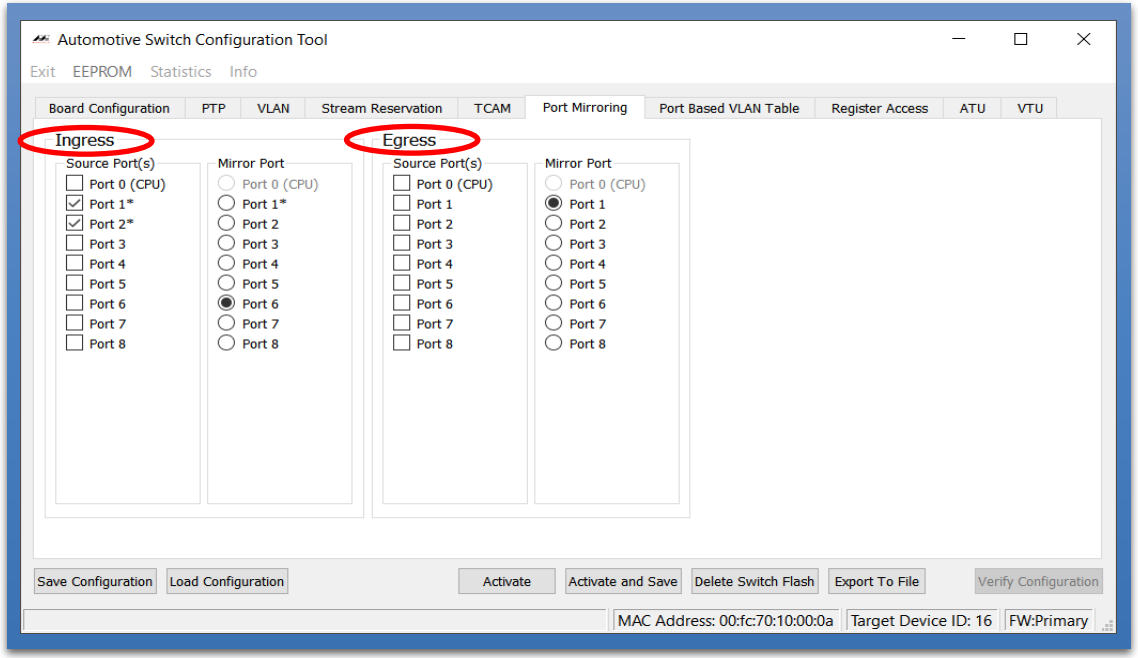
> *Even with an infinite impedance probe, you cannot separate the composite data stream without having knowledge of what is being sent by one of the devices.*



Similar to echo cancellation used in hands-free communication devices

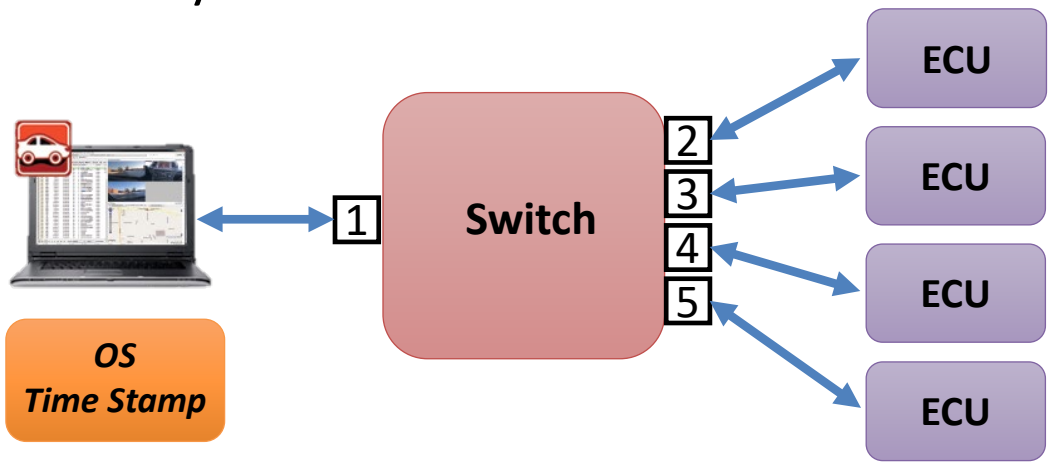
Port Mirroring

- Not all switches are configured the same way.
- This switch supports mirroring ingress and egress traffic on separate ports.



Port Mirroring / Monitoring Drawbacks

- Bad frames not forwarded
- Time Stamp Limitations
  - Needs embedded timestamp for any significant accuracy (can't use any switch)
  - Time stamped after frame forwarded, not when arrived on "the wire"
  - Switch queuing introduces nondeterministic latency
- Cannot strategically inject traffic
- Store & Forward Behavior
- Alternative to Port Mirroring
  - Active Taps
    - Precision time stamps
    - Inject Traffic



RAD-Jupiter

Managed Switch for Automotive Ethernet

7-Port Managed Switch (Marvell 88Q5050)

- 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
- Ingress Rate Limiting
- “Cut-Through” Forwarding

Integral CAN/LIN Interfaces

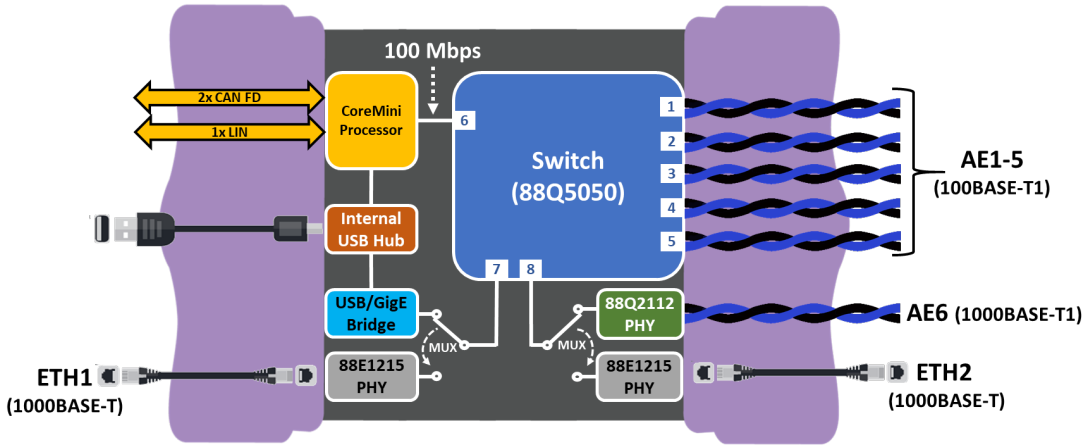
- 2x CAN-FD
- 1x LIN
- Embedded Function Block Execution

Use Cases

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

AVB/TSN

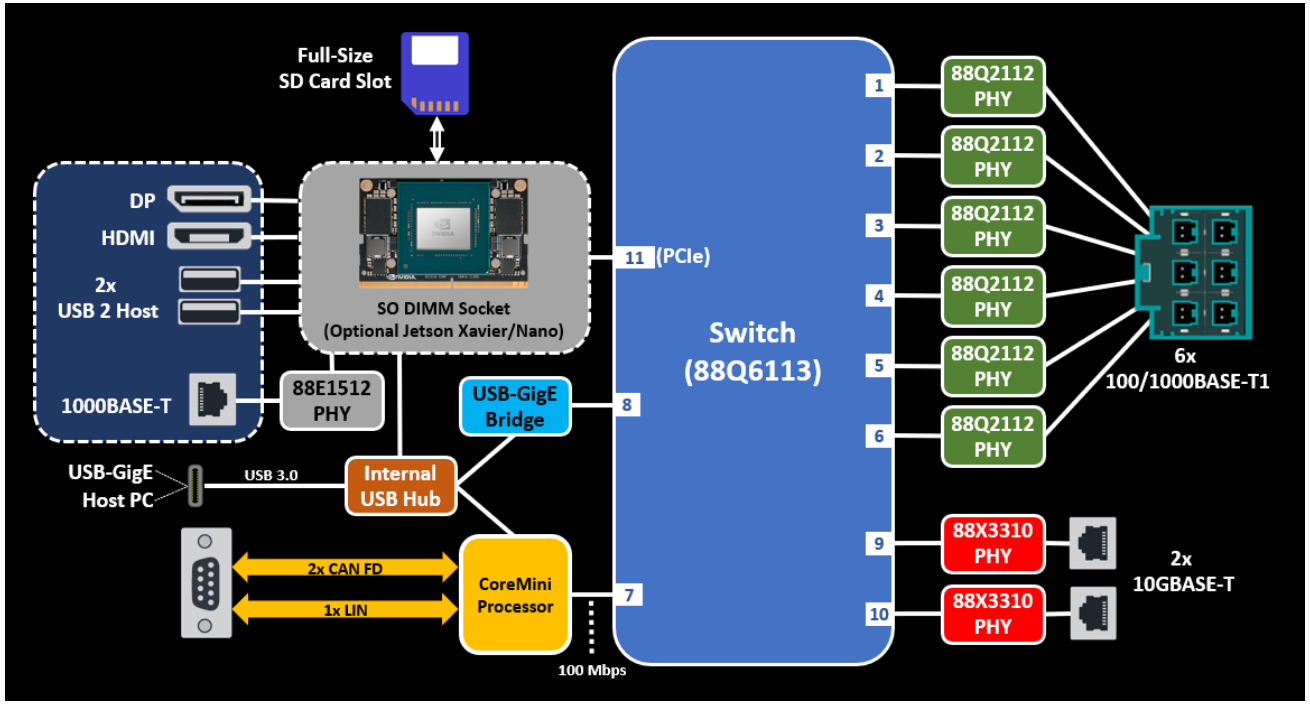
- gPTP
- FQTSS/CBS
- Static SRP



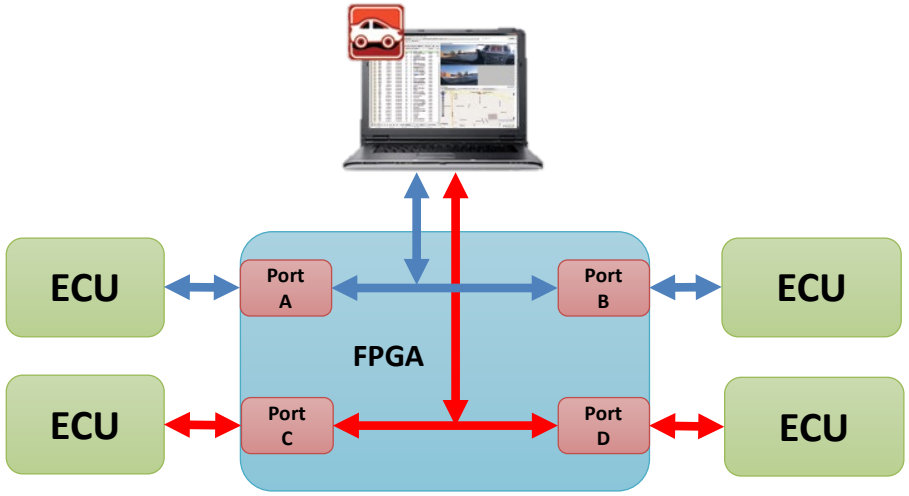
RAD Epsilon 10-Port Managed Switch

- Physical Layers
  - 6x 100/1000BASE-T1
  - 2x 10GBASE-T
  - USB3/GIGE Bridge
- QoS
  - AVB/TSN Protocol Support
    - gPTP
    - Qav: Credit Based Shaping
    - Qbv: Time Aware Shaping
  - Per Stream Filtering and Rate Limiting
  - Deep Packet Inspection (TCAM)
- PHY and Switch Register Access using VSPY or Intrepid Open-Source API.
- Integral CAN/LIN Interfaces
  - 2x CAN-FD
  - 1x LIN
  - Embedded Function Block Execution

Optional Nvidia Jetson Integration

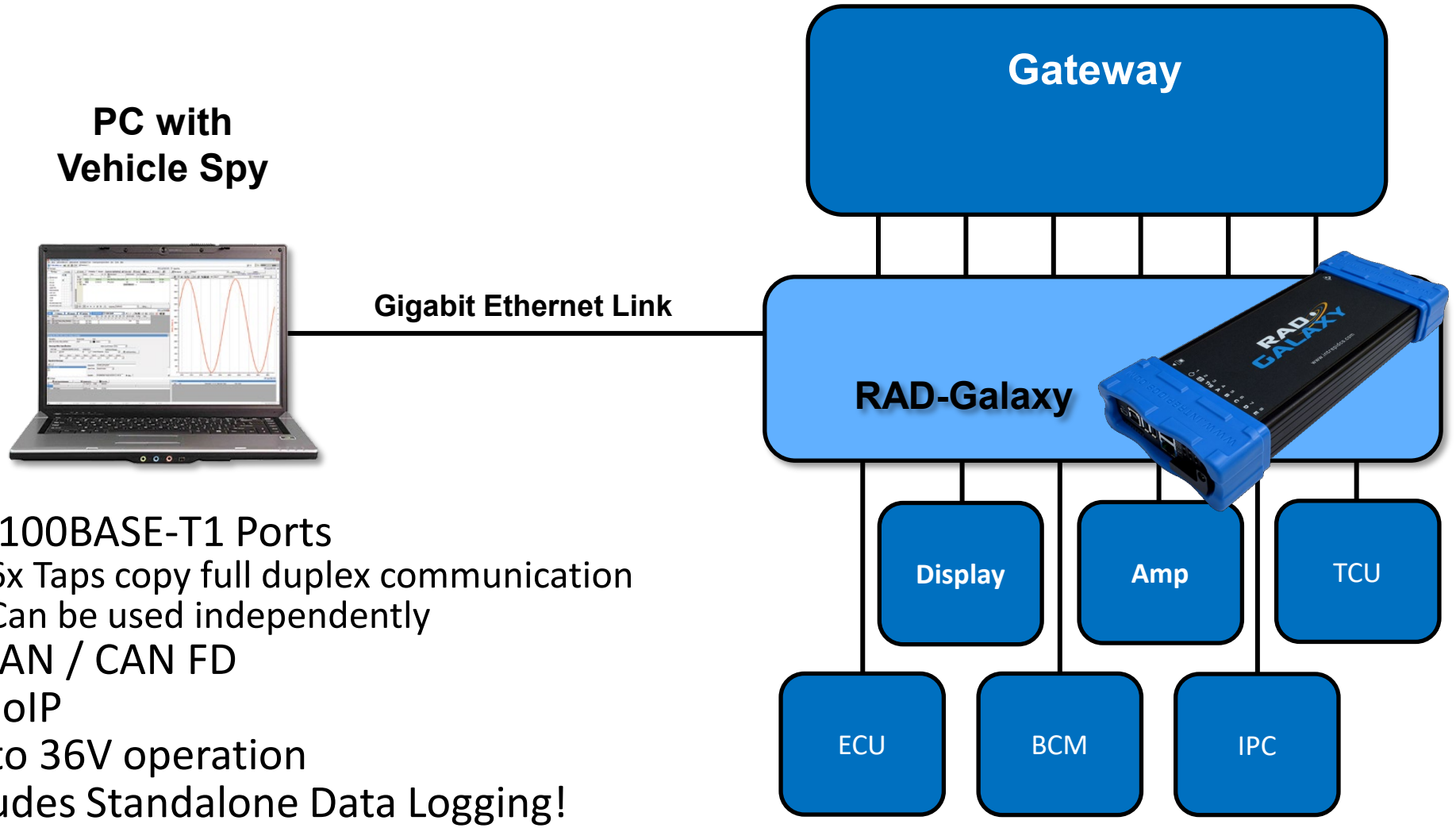


Active Tap
"Man in the Middle"



- Frame intercepted before immediate forwarding
- Time stamped as frame hits "the wire" and sent to PC
- Minimal latency if configured as cut-through
- Possible to inject traffic if configured as Store & Forward
- Bad frames are encapsulated and forwarded to PC

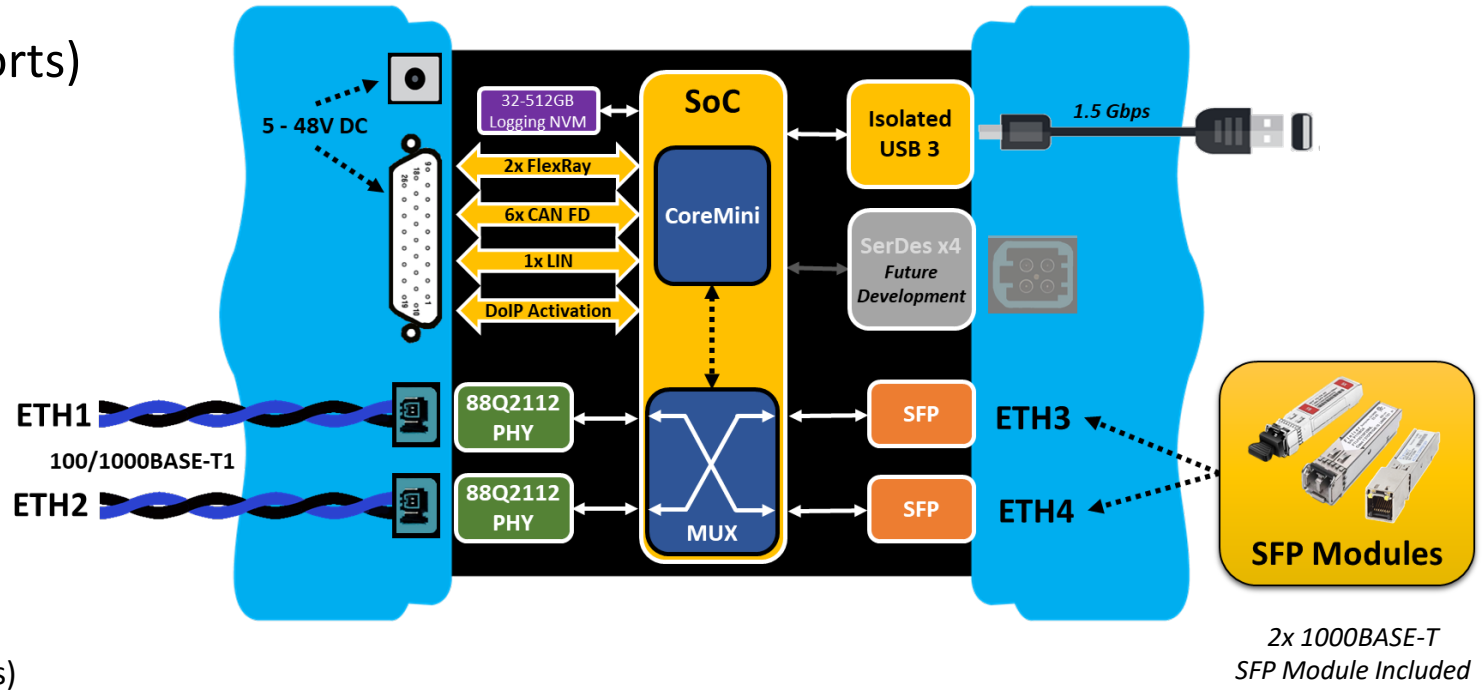
System Level Monitoring with RAD-Galaxy



- 12x 100BASE-T1 Ports
  - 6x Taps copy full duplex communication
  - Can be used independently
- 8x CAN / CAN FD
- 1x DoIP
- 4.5 to 36V operation
- Includes Standalone Data Logging!

RAD-Gigastar
Dual 1000BASE-T1 Active Tap

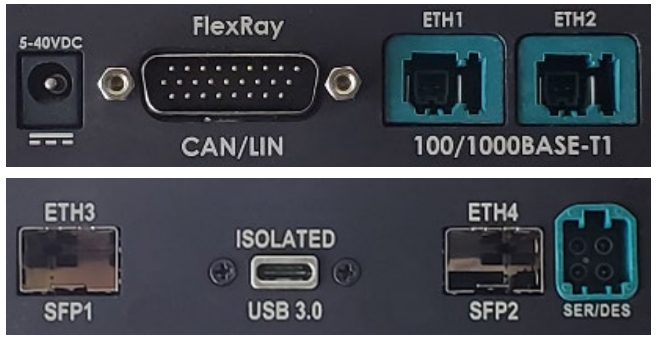
- Ethernet Ports
  - 2x 100/1000BASE-T1 Ports (Marvell 88Q2112 rev A2)
  - 2x SFP cages – Flexible media conversion
- Dual Ethernet Active TAP (using any 2 ports)
  - 100/1000BASE-T1 to 100/1000BASE-T1
  - 100/1000BASE-T1 to SFP
  - SFP to SFP
- Legacy Networks
  - 6x CAN / CAN-FD
  - 1x LIN/K-Line
  - 2x FlexRay (Rx Only)
  - 1x DoIP Activation Line
- 32GB – 512GB Internal Logging NVM
  - Not customer accessible/upgradable
  - Limited to 50-60 MByte/Sec (~400 – 480 Mbps)



2x 1000BASE-T SFP Module Included

RAD-Gigastar Applications

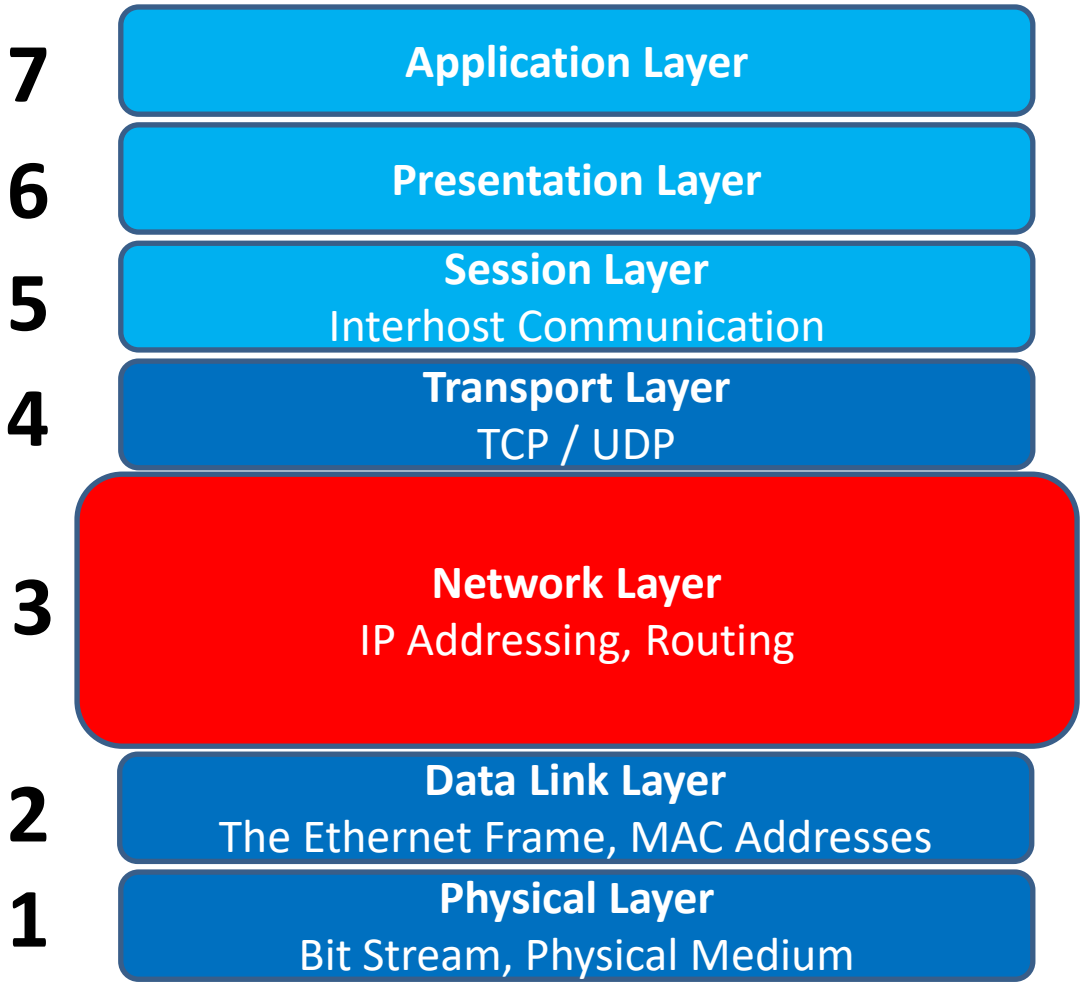
- Dual 100/1000BASE-T1 Active Tap
  - USB 3 Host Connection (1.5 Gbps)
  - Can host over 1000BASE-T with single Active Tap
- Gateway Functions
  - Any network to any network
  - On-the-fly Network Address Translation
- Stand Alone Data Logging
  - Axis camera hosting
  - ICS Device Hosting
- ECU and system-level automated testing
- SoAd / DoIP / ISO 15765 flashing over Automotive Ethernet or CAN FD
- Embedded Function Block Execution



How to Interact with Automotive Ethernet

1) Media Converter- Simply converts from Automotive Ethernet to “Regular” Ethernet to simulate a switch or module with your laptop
   - RAD-Moon 100BaseT1
   - RAD-Moon2 1000BaseT1
   - Rad-Moon3 2.5G/5G/10G BaseT1
   - Comet 10BaseT1S to 100/1000BaseT1(Q4) or 100/1000BaseT
2) Ethernet TAPS – “Man in the Middle” The only way to truly get all information- good frames and bad frames and inject faults and manipulate data
   - RAD-Galaxy- 8 CAN/FD and 12 100BaseT1 (6 TAPS)
   - Rad-Galaxy2 (Q4) 8 CAN/FD and 12 100/1000 BaseT1 (6TAPS)
   - RAD-GigaStar 6 CAN/FD and 2 100/1000 BaseT1; [possible to add 2 more via SFP’s but with degraded performance
   - Comet (Q4) 10Base T1 Tap
3) Switches – Can Mirror ports and “copy” data to your PC but will drop bad frames and timing is not deterministic
   - Jupiter
   - Epsilon

Network Layer



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 that frames arrive in order
  - No guarantee that frames arrive at all…..

Internet Protocol

- Created to enable communication between heterogeneous computer systems
  - Abstracts any Physical Addressing and replaces it with a “Logical” Addressing
- IP and Ethernet is non-deterministic
  - No guarantee that frames arrive in order
  - No guarantee that frames arrive at all…..
- Internet Protocol (IPv4 & IPv6) Key responsibilities:
  - Logical Addressing
  - Data encapsulation / message formatting
  - Routing (determining end to end path)
  - Fragmentation of packets and re-assembly

Ethertype:

IPv4 = 0x800

IPv6 = 0x86DD

Distinguishes IP traffic from all other traffic

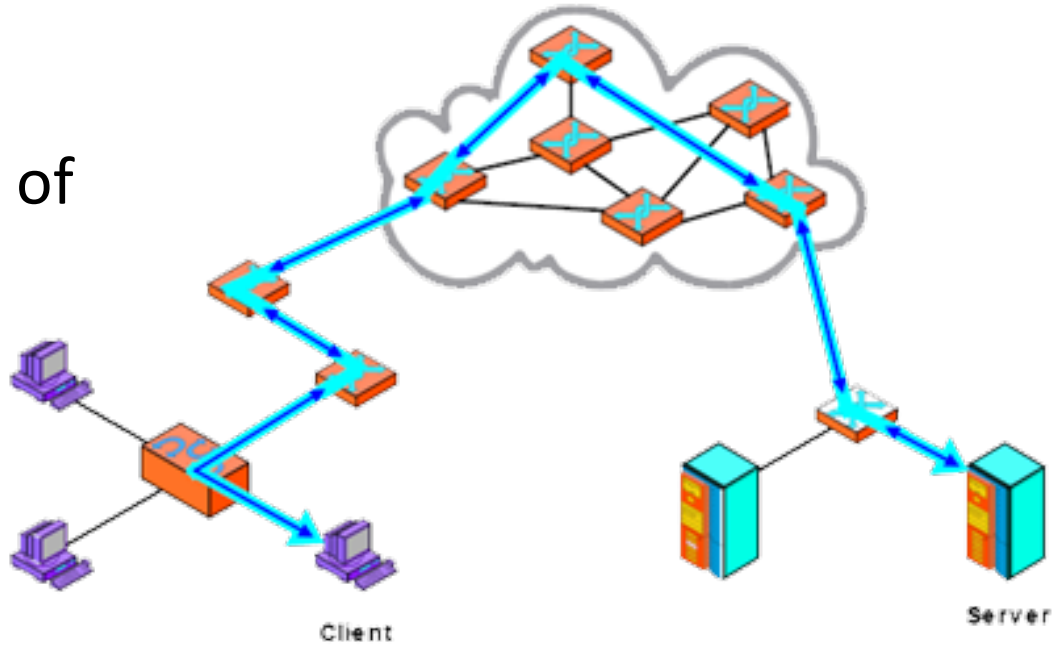
802.3 Ethernet frame structure

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 oc						
← 84-1538 octets (88-1542 octets for 802.1Q tagged frames) →								

IP Characteristics

- Low overhead
- Designed for routing from one device to another
- Universal addressing with independence of
  - Underlying protocols
  - Physical Media
- Connectionless
- Unacknowledged

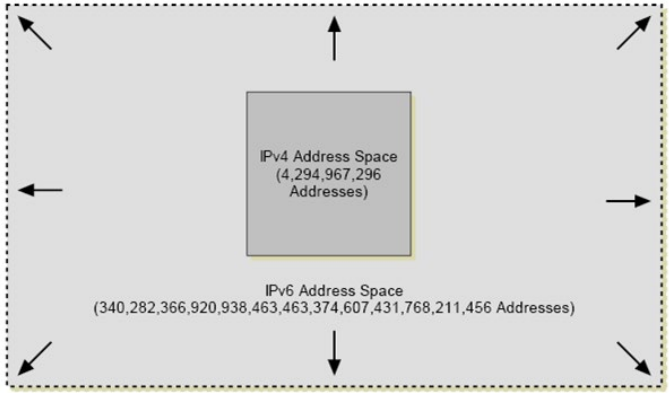
  (no guaranteed delivery)
- Nearly all traffic carried in IP packets
- Generally used with other protocols



IP Addresses

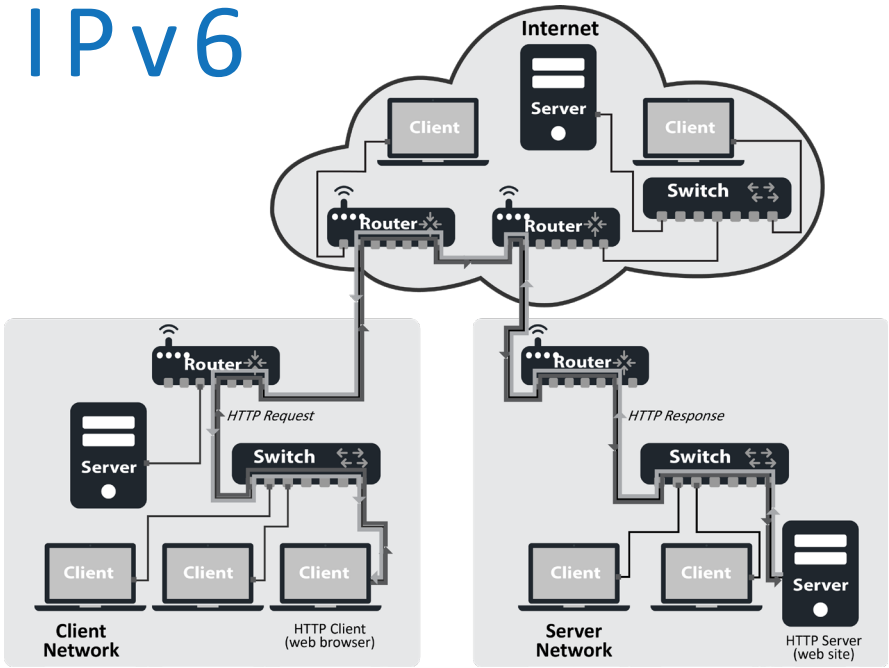
- IPv4's 32 bits equates to 4 billion unique addresses
- IPv6 was created out of concern
  - Internet growth will lead to address exhaustion.
  - 128-bit addresses
- IPv6 adoption slow
  - Techniques such as classless routing and Network Address Translation (NAT) have extended the life of IPv4
  - Overwhelming Inertia
    - Legacy Hardware/Software
    - ….and "it ain't broke!"

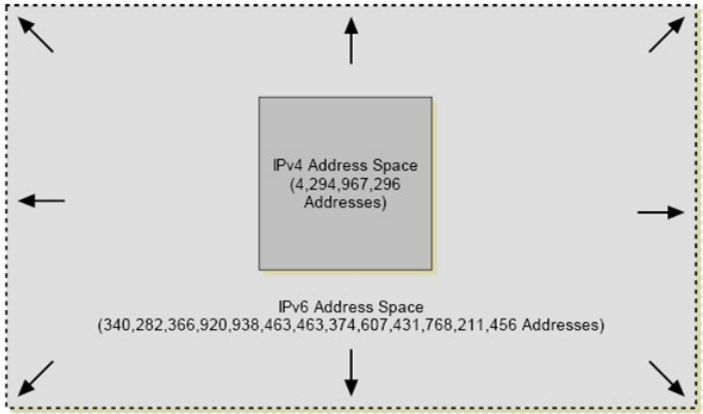
    (Imagine if an entire country changed from 110 Vac to 220 Vac)
- With a finite number of IPv4 addresses and continued Internet growth, IPv6 is inevitable.



Internet Protocol – IPv4 vs IPv6

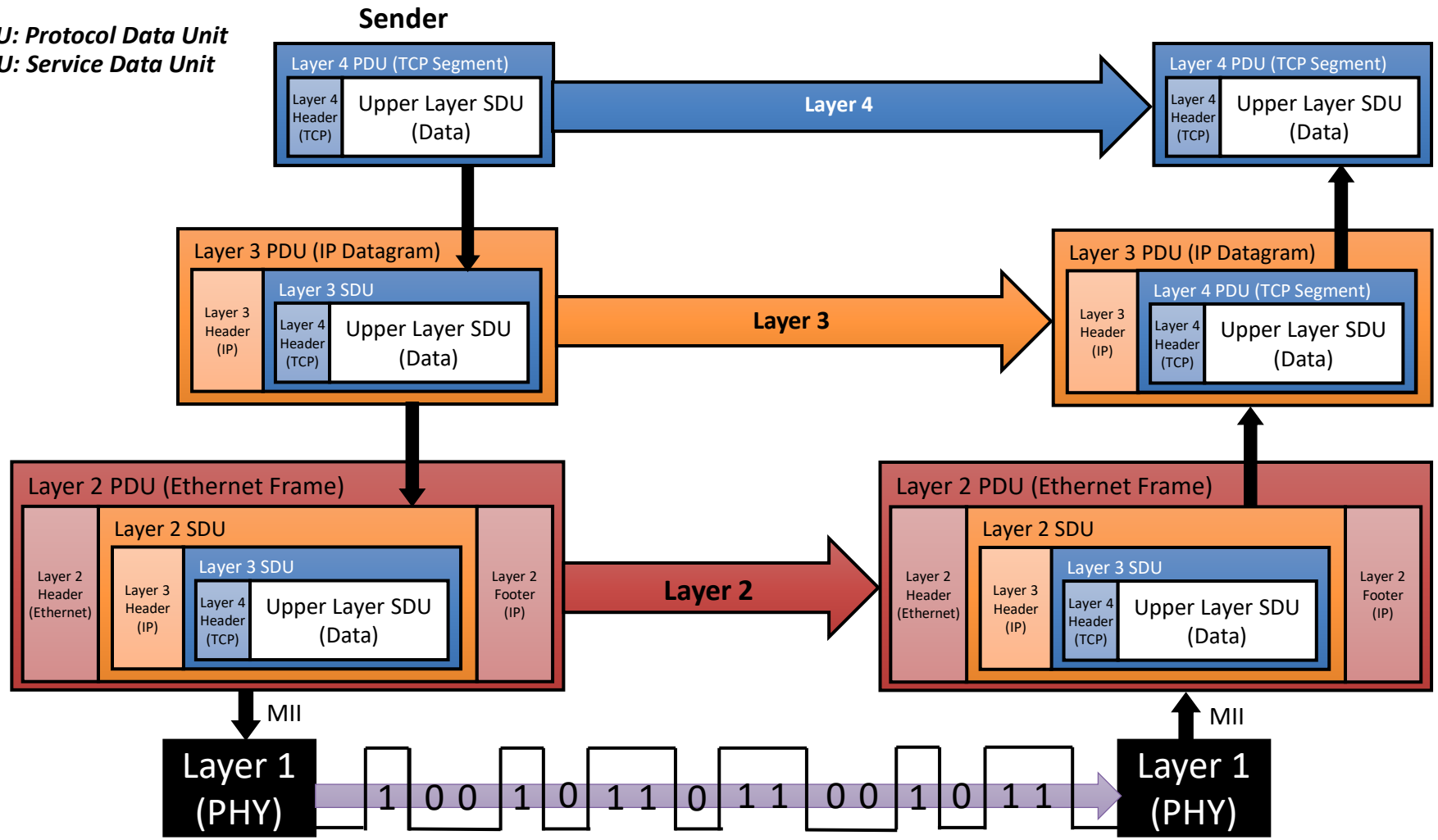
- IPv4's 32 bit addresses = 4 billion addresses (already gone!)
- IPv6 128 bit addresses = equates to $3.4x10^{38}$
- Improved hierarchal Address Space including the ability to add stateless, self-generation, autoconifg of IP address. Can be based on MAC address.
- Eliminate the need for Network Address Translation (NAT)
- Eliminate broadcasts messages. Uses only multicast addresses
- Introduces "anycast" = deliver to first host in group X.
- Enhanced security – built-in authentication headers and more



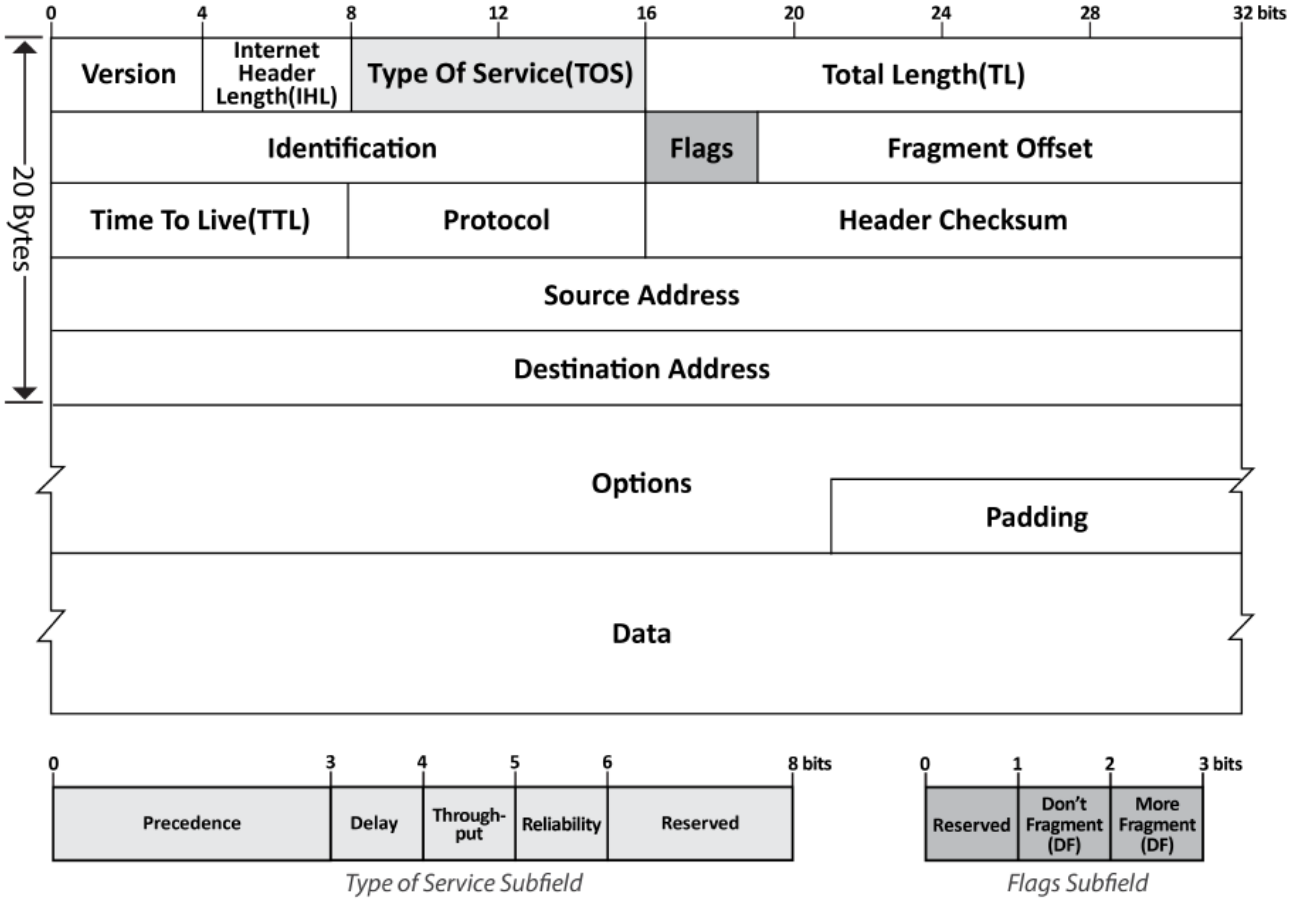


Message Encapsulation

PDU: Protocol Data Unit
SDU: Service Data Unit

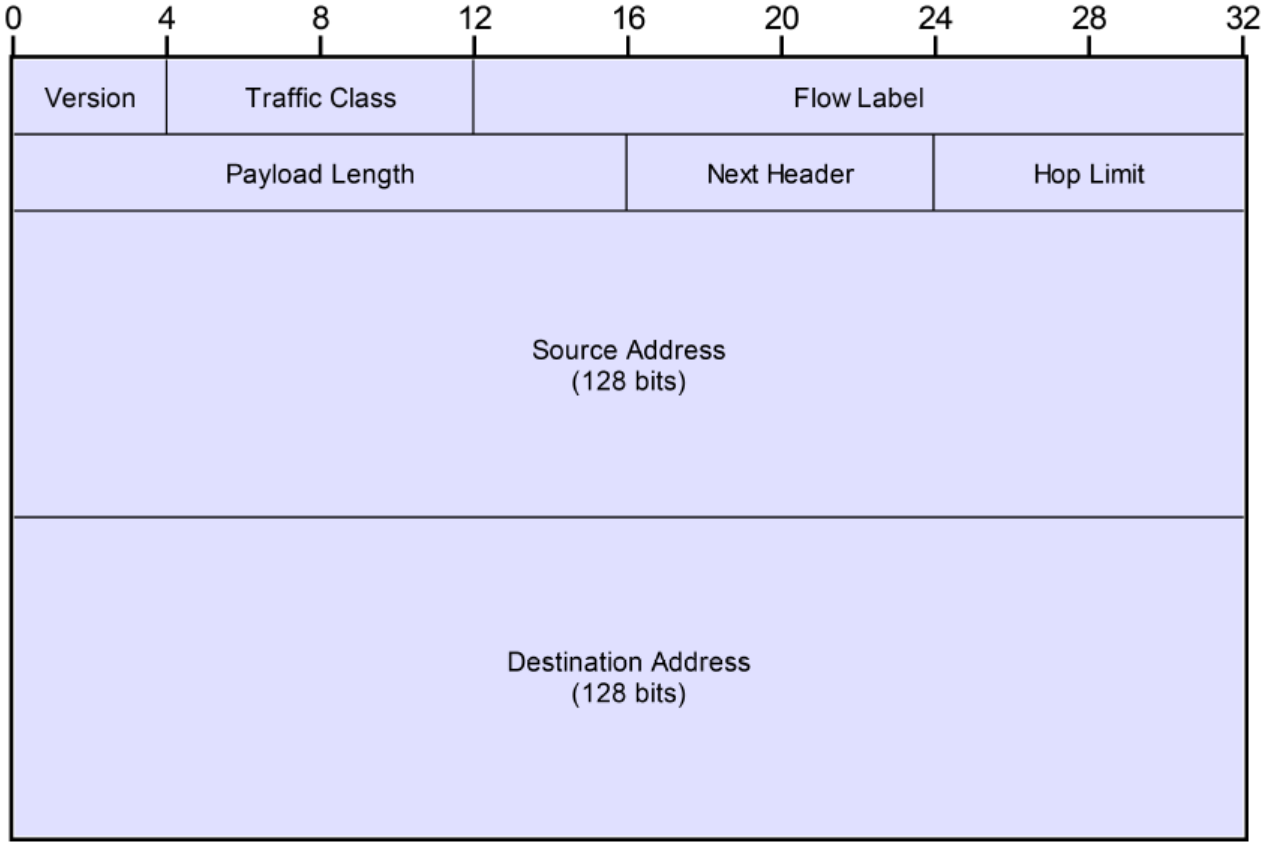


IPv4 Header



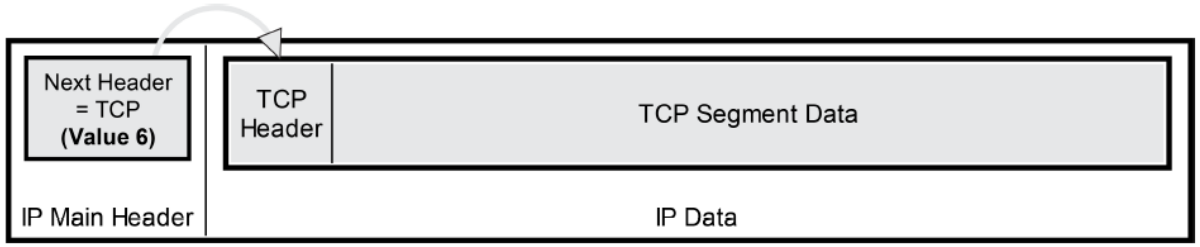
- **Version** – Value 4 (IPv4)
- **IHL** – Length of header in 32 bit words
- **TOS** – QoS. Redefined to Differentiated Services (DS)
- **Total Length** – Length of datagram fragment in bytes.
- **Identification** – Used to ID fragments
- **Flags** – Control of fragments
- **Fragment Offset** – position in overall datagram for this fragment
- **TTL** – Number of hops before being dropped
- **Protocol** – Next header (1 = ICMP, 6 = TCP, 17 = UDP)

IPv6 Header

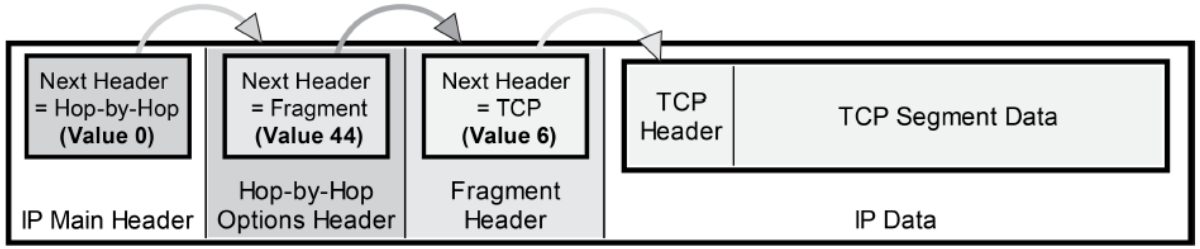


- **Version** – Value 6 (IPv6)
- **Traffic Class** – Replaces Type of Service (TOS). RFC3168 (QoS)
- **Flow Label** – RFC6437, support for real-time datagram delivery
- **Payload Length** – Length of payload and any extension headers
- **Next Header** – Replaces Protocol field in IPv4. Enables daisy chain of headers
- **Hop Limit** – Same as TTL but named better

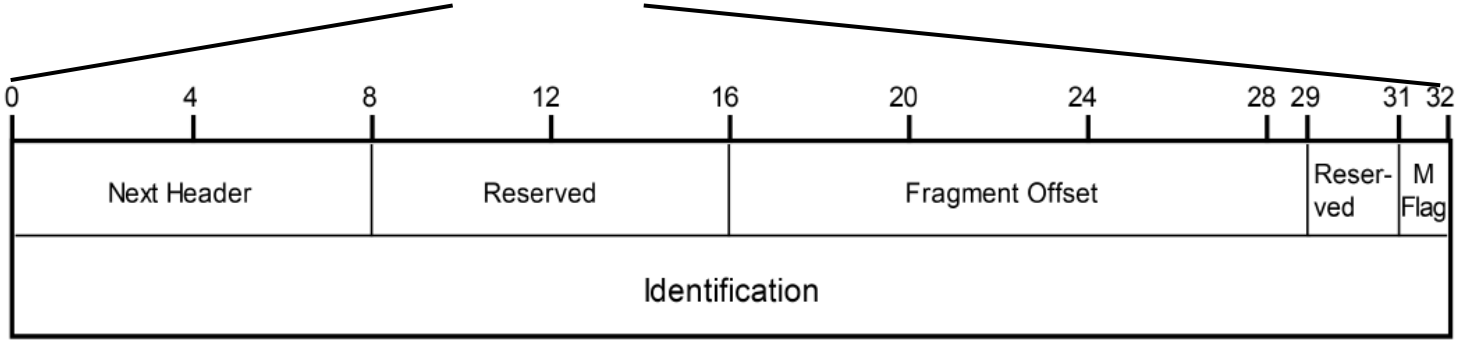
IPv6 Extension Header



IPv6 Datagram With No Extension Headers Carrying TCP Segment



IPv6 Datagram With Two Extension Headers Carrying TCP Segment



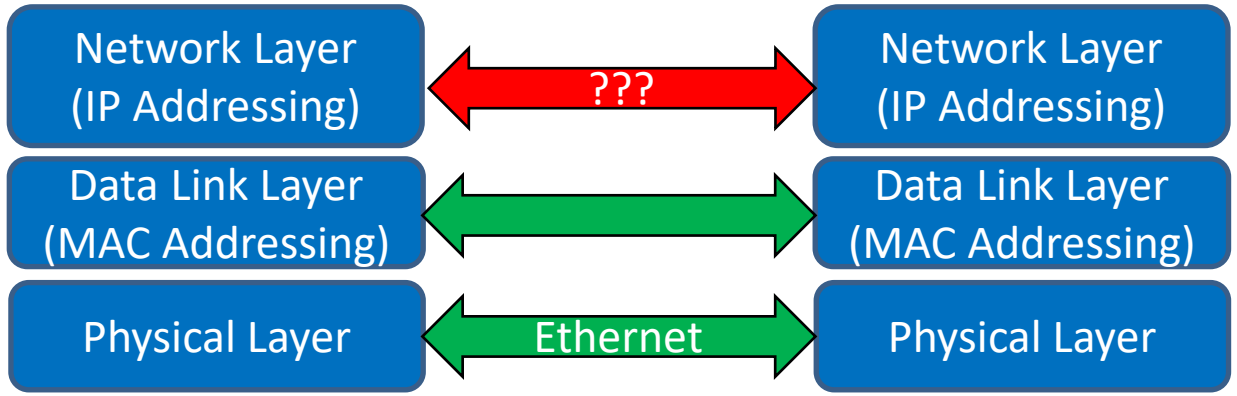
- **Next Header** – Value of next protocol header
- **Reserved** – Not used
- **Fragment Offset** – Position of this segment in the overall datagram.
- **Reserved** – No used
- **M Flag** – More Fragments. 1=More fragments
- **Identification** – Specific value common to all fragments in this datagram

How is This Going to Work?

IP provides **abstraction from the MAC address….**

But Ethernet traffic is **forwarded using MAC addresses…..**

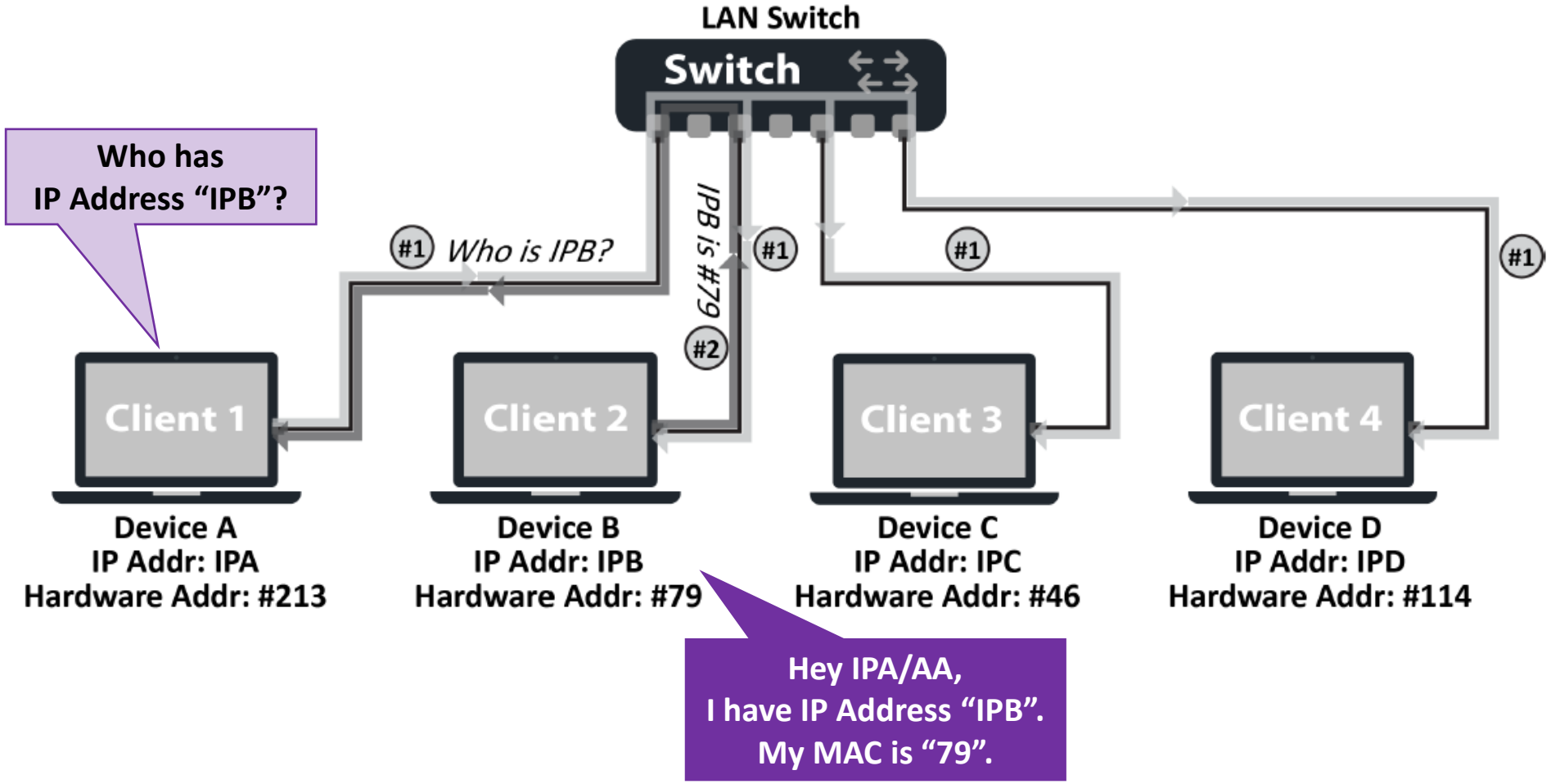
So how does an IP frame get routed where it needs to go?



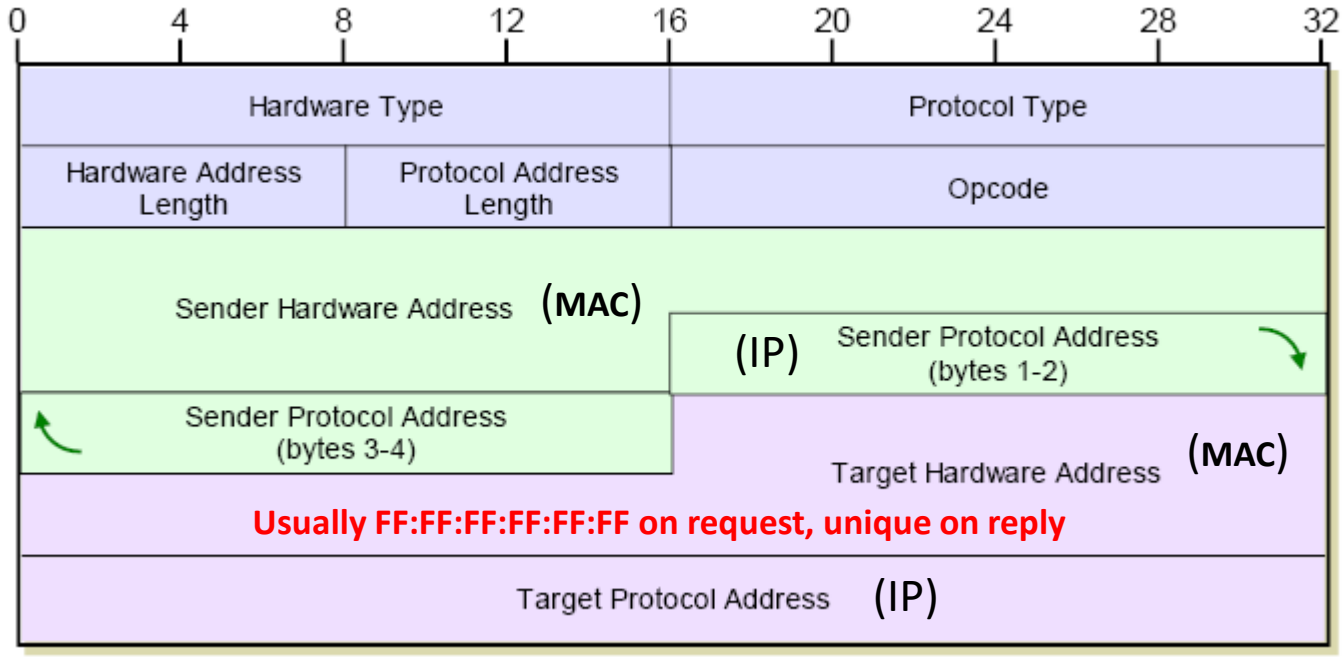
2 Options:

1. Hard coded addresses (defeats the purpose of abstraction…)
2. “Discovery” through a higher-level protocol.

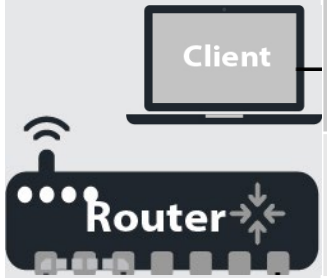
Address Resolution Protocol (ARP) IPv4 only



ARP – Header
IPv4 only



Neighbor Discovery Protocol - NDP



Message	ICMP Type	Source Address	Destination Address
Router Solicitation (RS)	133	Unspecified ::	All-routers multicast FF02::2
Router Advertisement (RA)	134	Router link-local address FE80::X	All-nodes multicast FF02::1
Neighbor Solicitation (NS)	135	Link-local address or unspecified if duplicate address detection (DAD)	All-solicited nodes multicast FF02::1:FFxx:xxxx Where xx:xxxx = IP of dest
Neighbor Advertisement (NA)	136	Link-local address FE80::x	Link-layer address, or all nodes multicast FF02::1
Redirect (RE)	137	Used to re-direct hosts to a more preferable router	

Internet Control Message Protocol (ICMP)

Same format for IPv6 and IPv4

ICMP Header Format

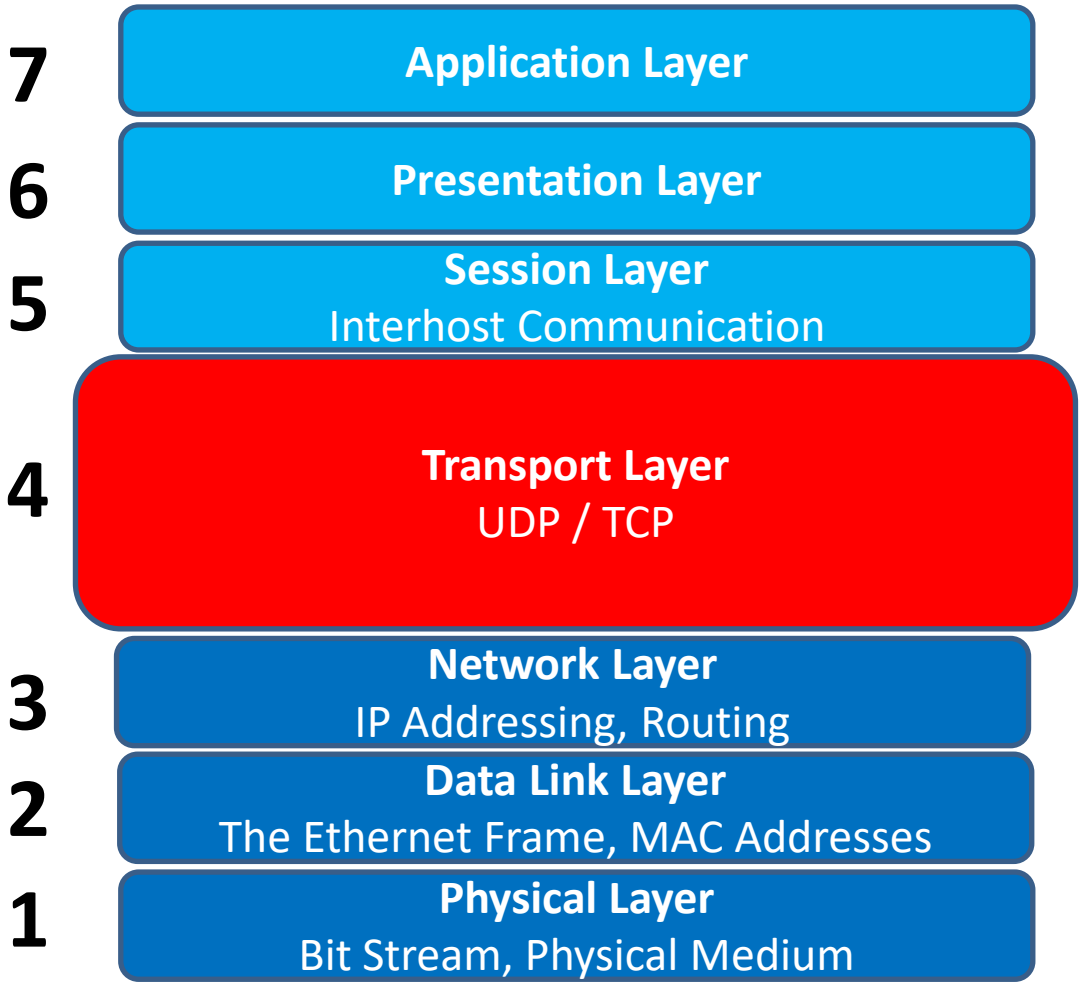
Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Type								Code								Checksum															
4	32	Rest of Header																															

ICMP v4 (examples):
8 = Echo Request (ping)
0 = Echo Reply
3 = Destination Unreachable
ICMP v6 (examples):
1 = Destination Unreachable
3 = Time exceeded
135 = Neighbor solicitation

ICMP Code:
Message subtype or details about an error

Rest of Header:
Format depends on the Type/Code

Transport Layer



TCP verses UDP

TCP

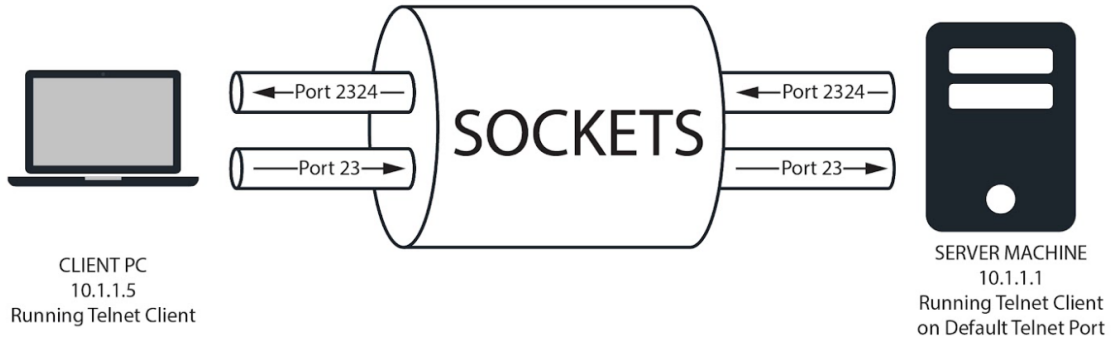
- Connection Oriented
  - Defined start and end of connection
- More overhead compared to UDP
- Reliable connection
  - Confirmation of data delivery
  - Sender is aware of errors
  - Data is delivered in order
- Flow Control
  - Data is sent at a rate at or slower than the max for the entire path
- Data can flow in both directions with one connection

UDP

- Non-Connection Oriented
  - Fire and forget
- Less overhead compared to TCP (simpler)
- No built-in error discovery
  - No error awareness at L4
- No flow Control
  - Data sent at the rate of the sender
- Data can flow in both directions

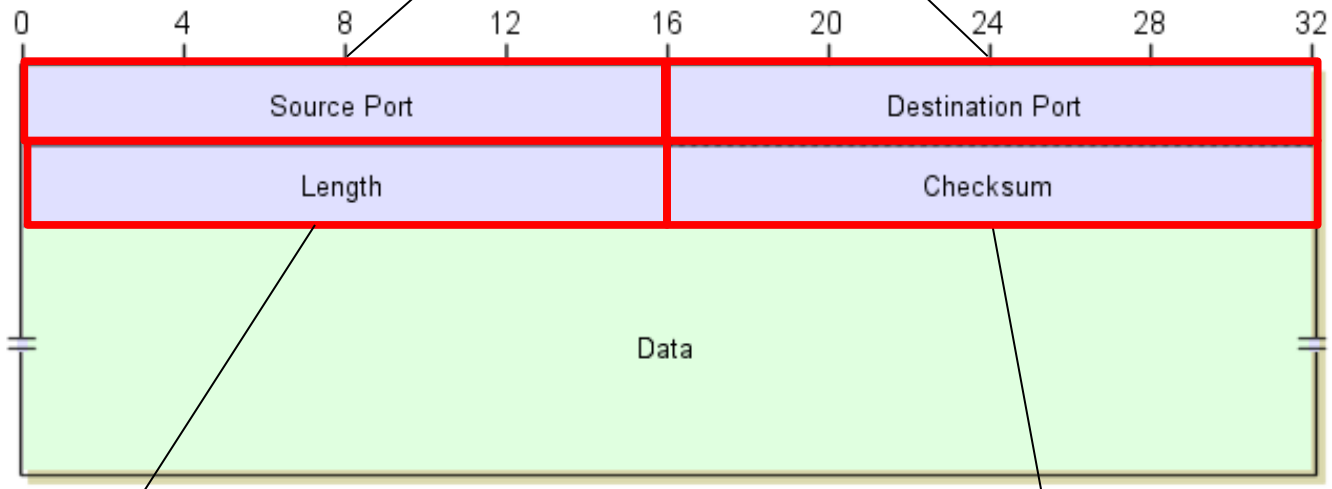
TCP/UDP Process-Level Addressing: **Ports**

- 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)



UDP Header

Source and Destination Ports –
Assigned to specific processes



Length of UDP (up to 64K bytes)

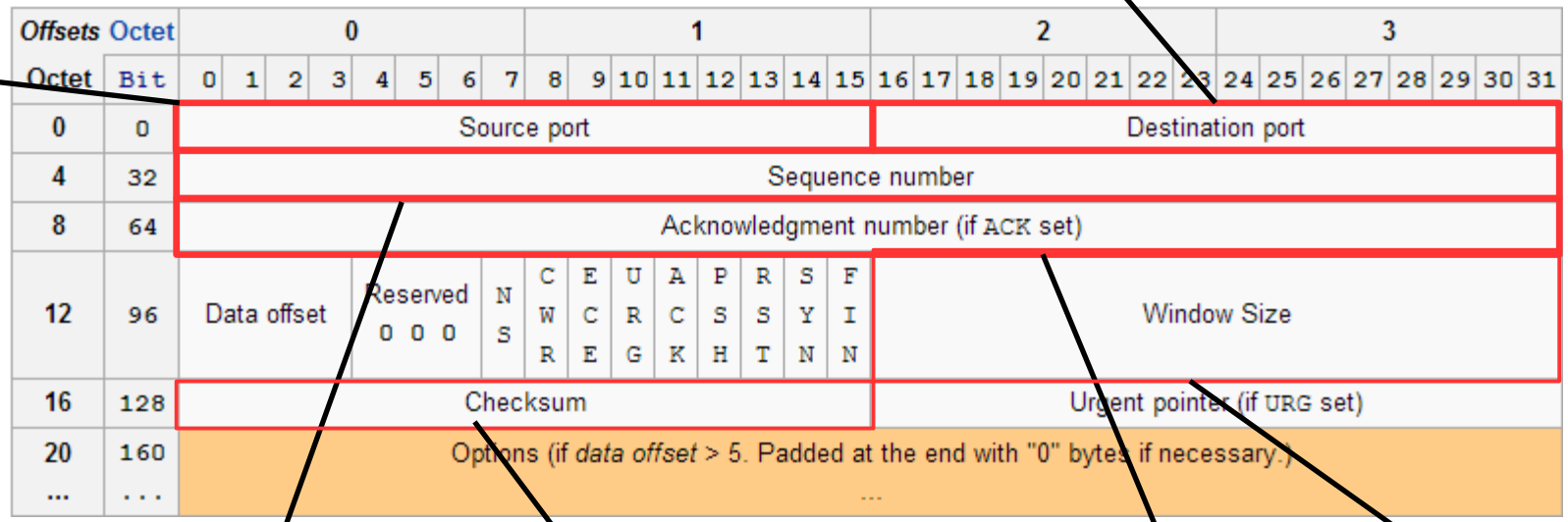
Optional checksum, 0 = no checksum,
All 1's = 0 checksum

The TCP Header

TCP has IP protocol number 0x06

Destination port – same as UDP

Source port –
same use as UDP



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	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0				NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size														
16	128	Checksum																	Urgent pointer (if URG set)														
20	160	Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.)																															
...	...	...																															

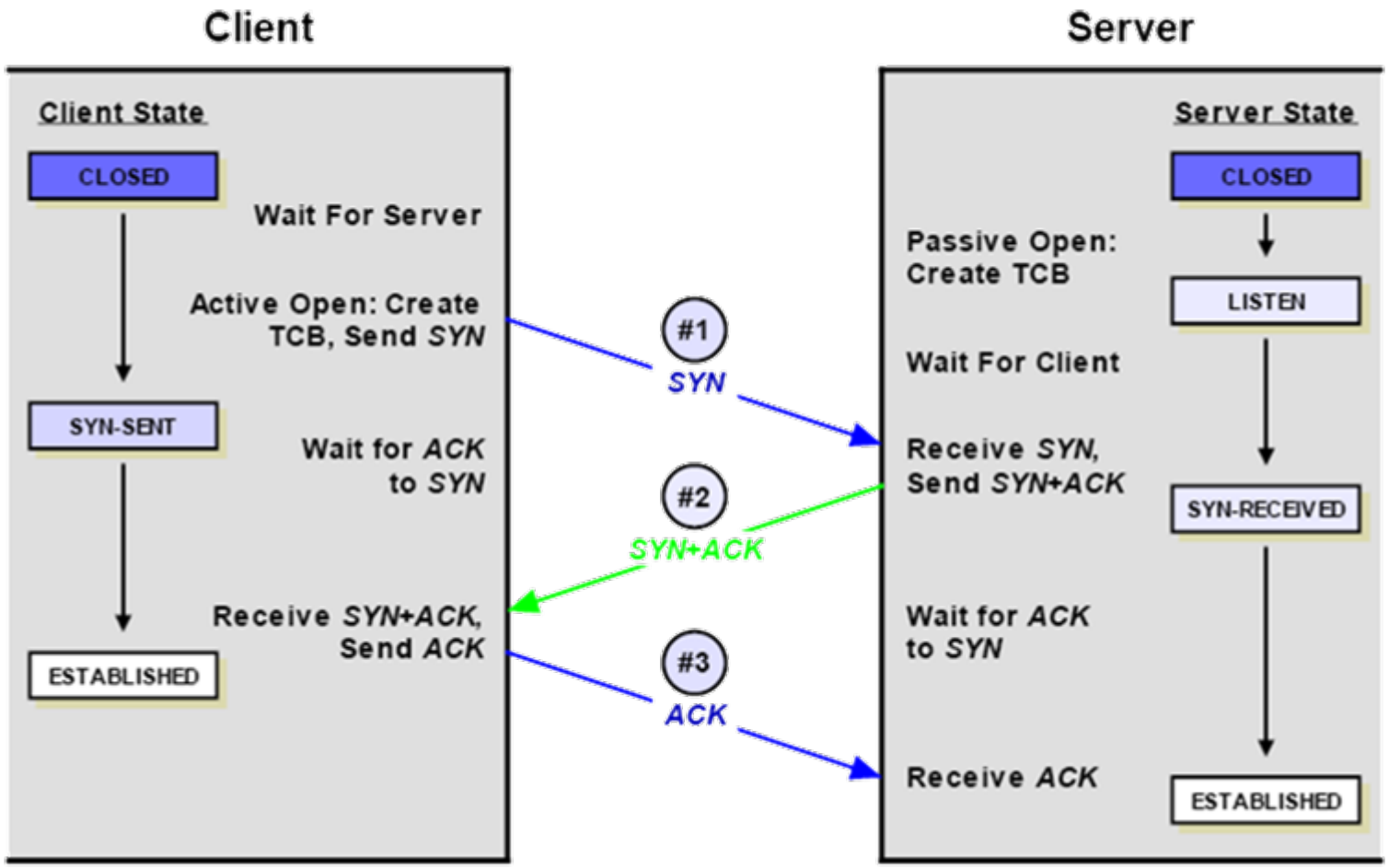
SEQ# – Tracks bytes sent

Checksum of header **and data**

ACK# - Tracks bytes received

The maximum number of bytes the sender is able to receive with no ACK (flow control). Set by receiver.

TCP "Three-Way Handshake"



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

How does TCP guarantee delivery?

By explicitly acknowledging each packet received

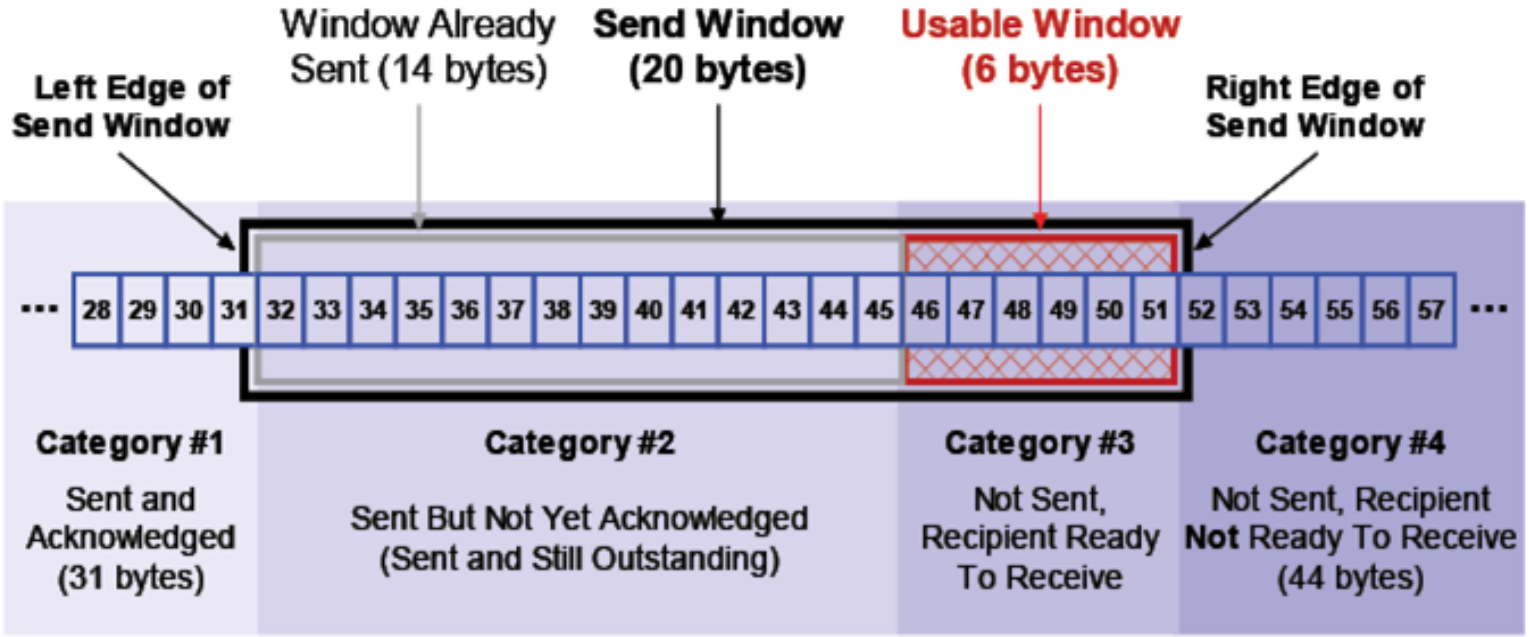
- Obvious cost in overhead and performance
- For a packet to be successfully read by an application, it must be received, then acknowledged back to the sender
- If no acknowledgment, the packet is retransmitted

TCP is also *stream-oriented*

- Application layer does not see individual packets, just a seamless stream of bytes
- TCP is well suited for data that must arrive exactly as it was sent, exactly in the order it was sent
- TCP also has flow control to deal with asynchronous receive/transmit speeds

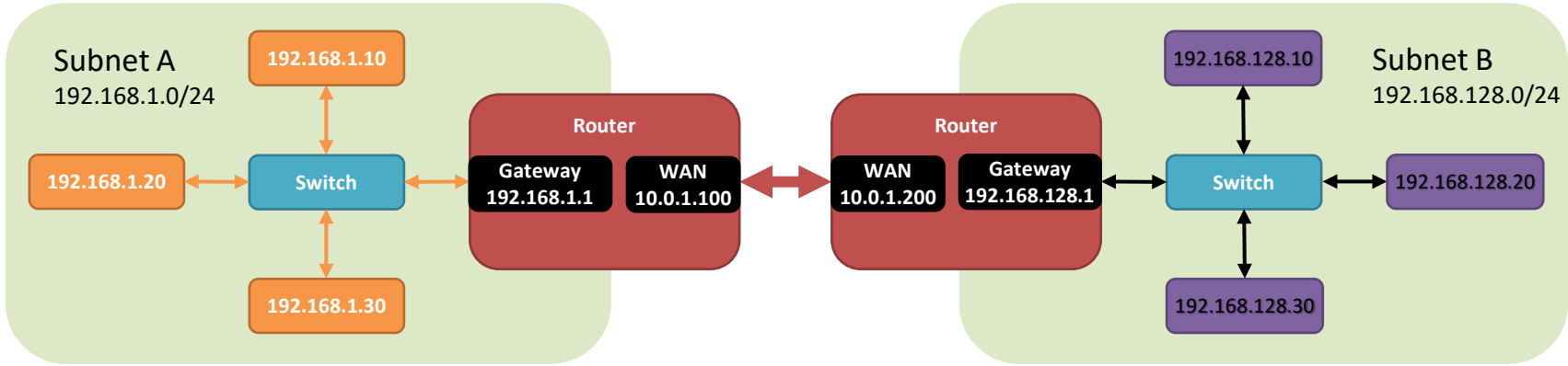
TCP Sliding Window System

- Used to keep track of bytes sent and received
- Special pointer maintained for each connection
- Sometimes called “bytes in flight”



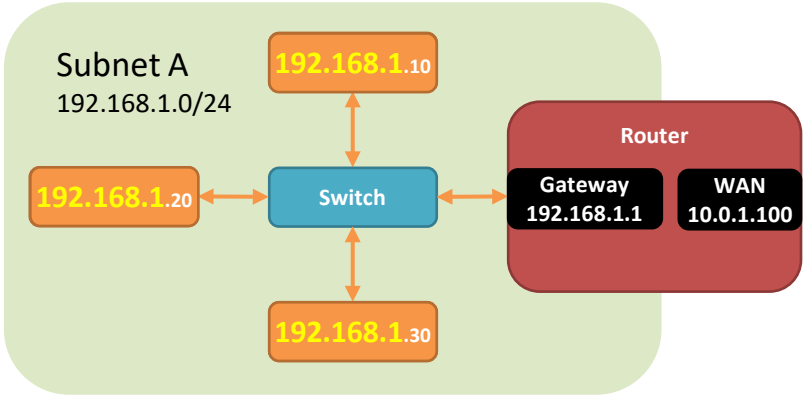
Subnets and Gateways

- A *subnet* (or subnetwork) is a logical grouping of network devices defined by a range of IP Addresses
  - A device can send a message directly to another on the same subnet
  - A destination outside the subnet will be sent to the *gateway* address (router)



Example Subnet

	# Networks	Addresses /Network	Example	Subnet Mask
Class A	128	16K	10.0.0.0/8	255.0.0.0
Class B	16K	64K	172.16.0.0/16	255.255.0.0
Class C	2M	256	192.168.1.0/24	255.255.255.0
Class D	NA	NA	224.1.1.1	multicast
Class E	Reserved / Not Defined			

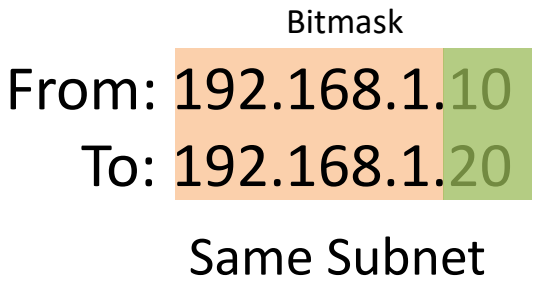


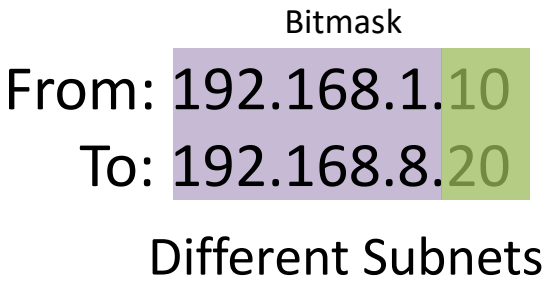
Subnet A: 192.168.1.0/24

- 192.168 designates a private subnet
- The 24 indicates that each device on the subnet shares the same 24 MSb.
- Only 256 unique addresses

Subnet Masks

- A *subnet mask* determines if a destination address is inside or outside a subnet.
  - The 24-bit subnet mask for the subnet defined in the last slide is 255.255.255.0
  - Another representation if this is FF.FF.FF.00 (bitmask)
  - Apply the bitmask to both addresses and if the values match, they are on the same subnet





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