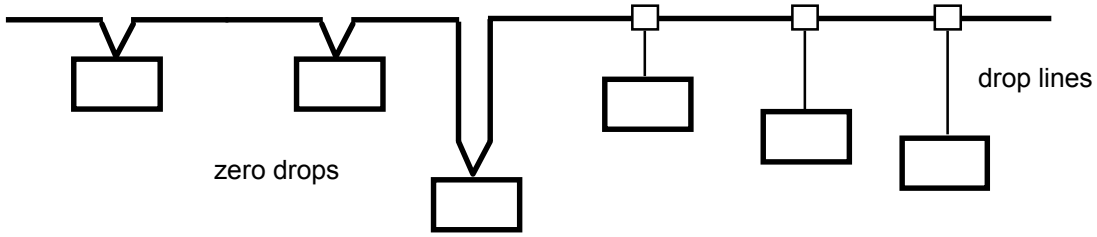
CAN (Controller Area Network)

- **CAN is open technology supporting multiple applications**
- **Chips available today from Intel, Motorola, Philips/Signetics, NEC, Hitachi, Siemens**
- **Volumes from multiple industry usage insures downward price pressure -**over 5 million chips in 1995
- **Network has flexibility for now and future**
  - Master/slave, multiple master, and peer-to-peer
- **Currently in use in automobiles**
  - An excellent proxy for industrial applications
  - Temperature extremes, shock/vibration, high noise environment

General Features



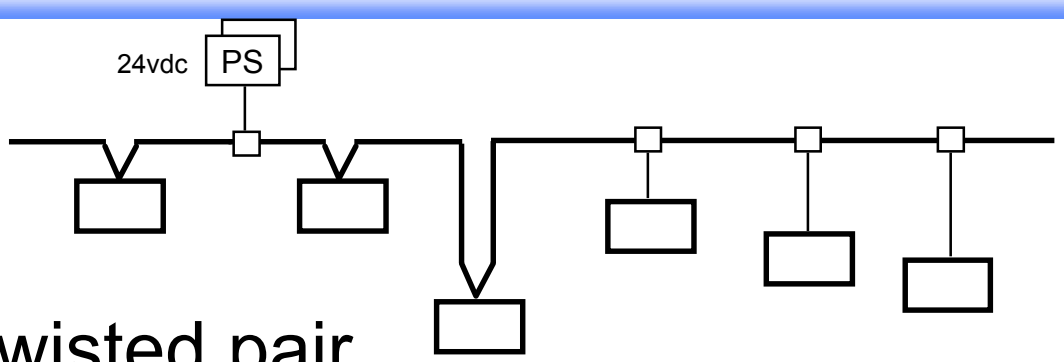
- Trunk line, drop line configuration
- Node removal without breaking trunk line
- Up to 64 addressable nodes
- Signal and 24Vdc Power in same cable
- Selectable Data Rates (125k, 250k, 500k)
- Both Sealed and Open-Style connections
  - zero node separation
- 121 ohm terminator at each trunk line end

Speeds, Distances, and Drops

Data Rate	Trunk Distance (thick cable)	Drop Length	
		Max drop	Cumulative
125K	**500m** (1640 ft)	**6m** (20 ft)	**156m** (512 ft)
250K	**250m** (820 ft)	**6m** (20 ft)	**78m** (256 ft)
500K	**100m** (328 ft)	**6m** (20 ft)	**39m** (128 ft)

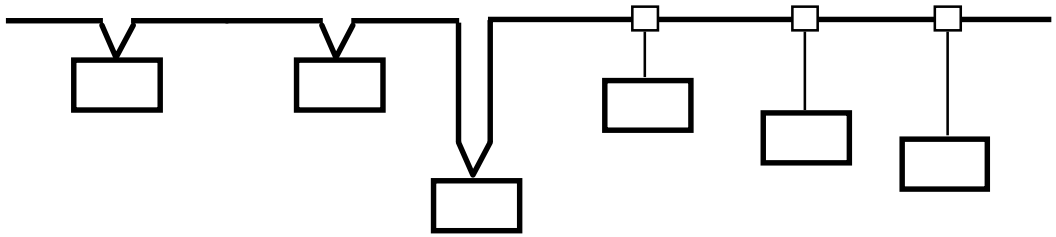
NOTE: Thin cable may be used as trunk. Maximum distance is 100 meters, regardless of data rate.

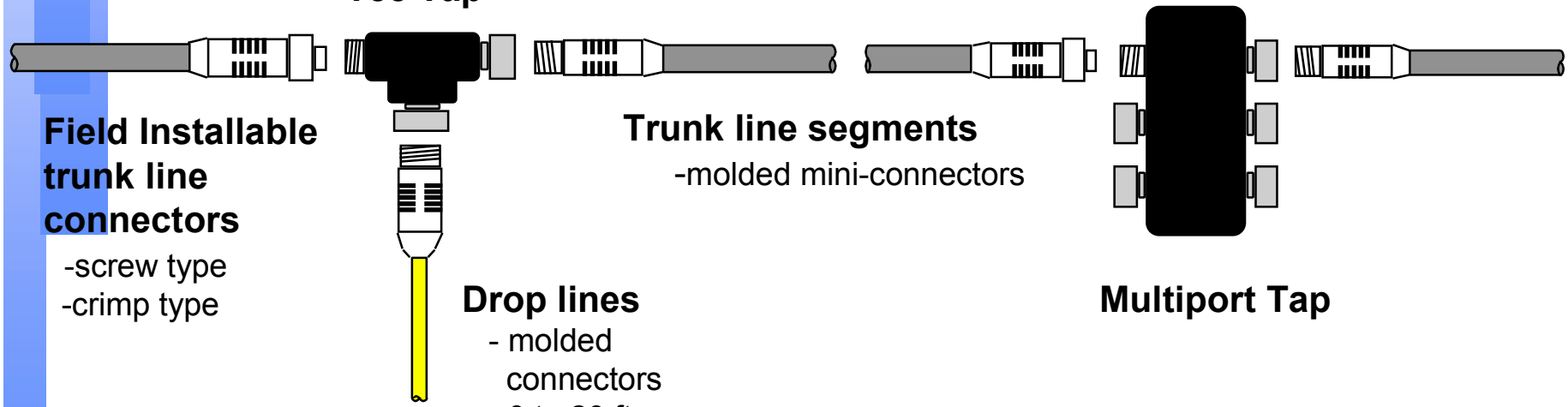
Power and Signal



- Two twisted pair
  - Signal pair: low loss, high velocity with foil shield
  - Power pair: up to 8A capacity with foil shield
    - NOTE: Class II NEC Code limits current to 4A on any segment
  - Overall braid with drain wire
- Sensors can be powered direct from bus
- Opto-isolation for self powered devices
  - e.g. drive, PLC, weigh scale, etc.
- Multiple power supplies can be used
  - used for additional power or as back-up

Typical Sealed-Style Taps





Tee Tap

Field Installable trunk line connectors

-screw type
-crimp type

Trunk line segments

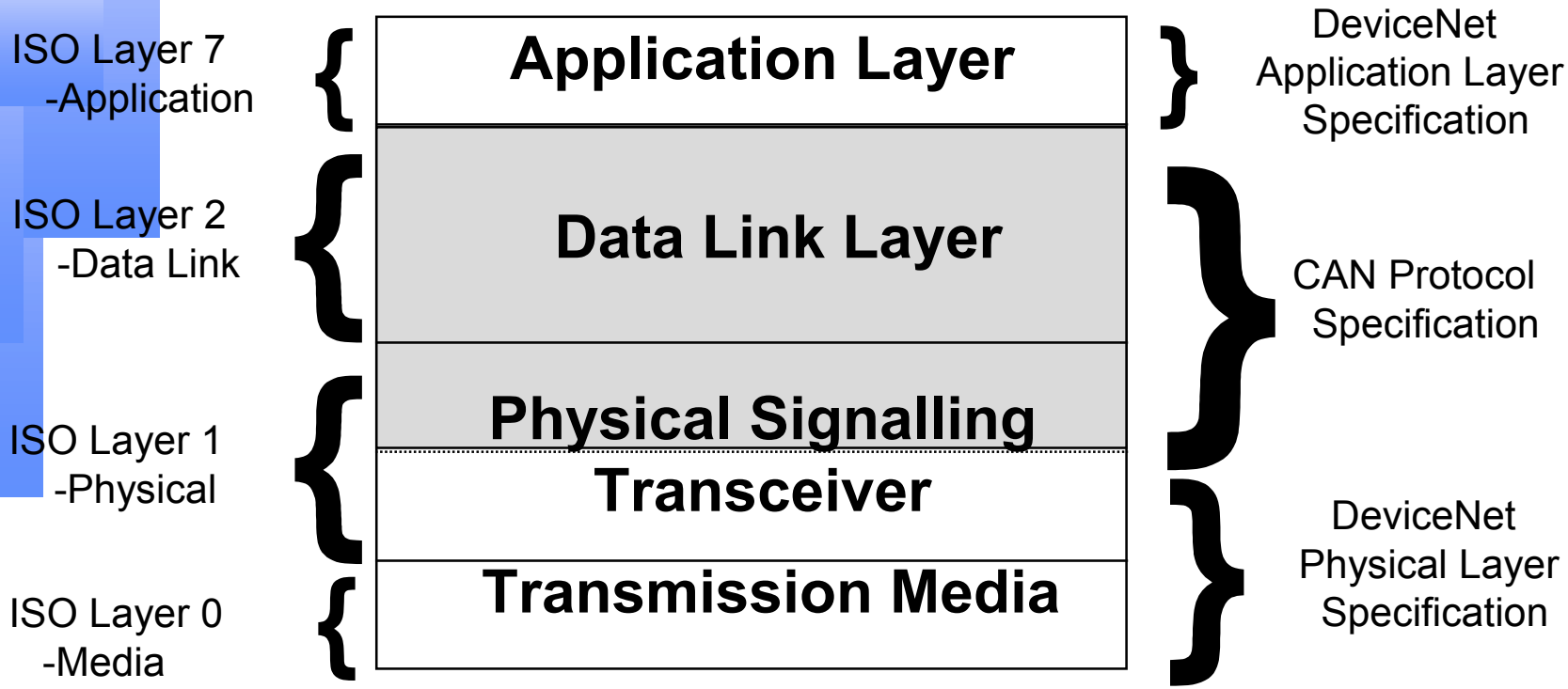
-molded mini-connectors

Drop lines

- molded connectors
- 0 to 20 ft.
- mini or micro at sensor

Multiport Tap

CAN in the Stack



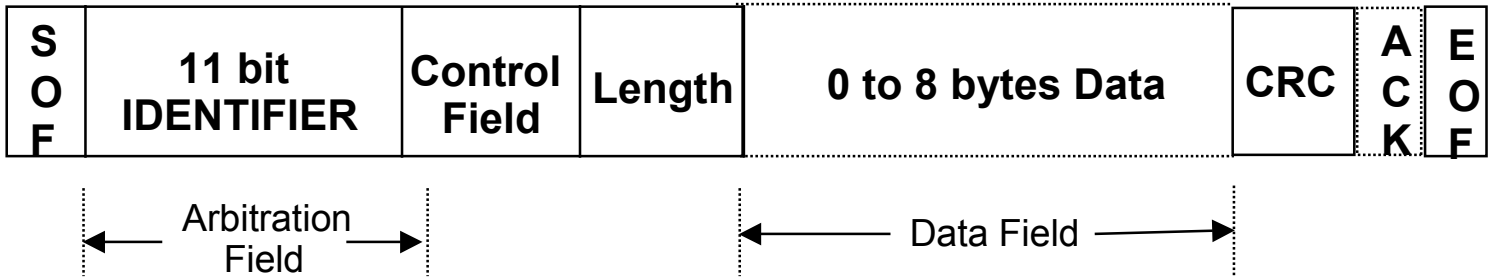
Data Link Layer Characteristics

- **CSMA/NBA** - **C**arrier **S**ense **M**ultiple **A**ccess with **N**on-destructive **B**itwise **A**rbitration
- Any node can access bus when quiet
- Data portion of packet can be 0 to 8 bytes long

•Non-destructive bit-wise arbitration allows 100% utilization and message priority based on 11-bit packet identifier

•CAN provides automatic error detection, signaling, and retries

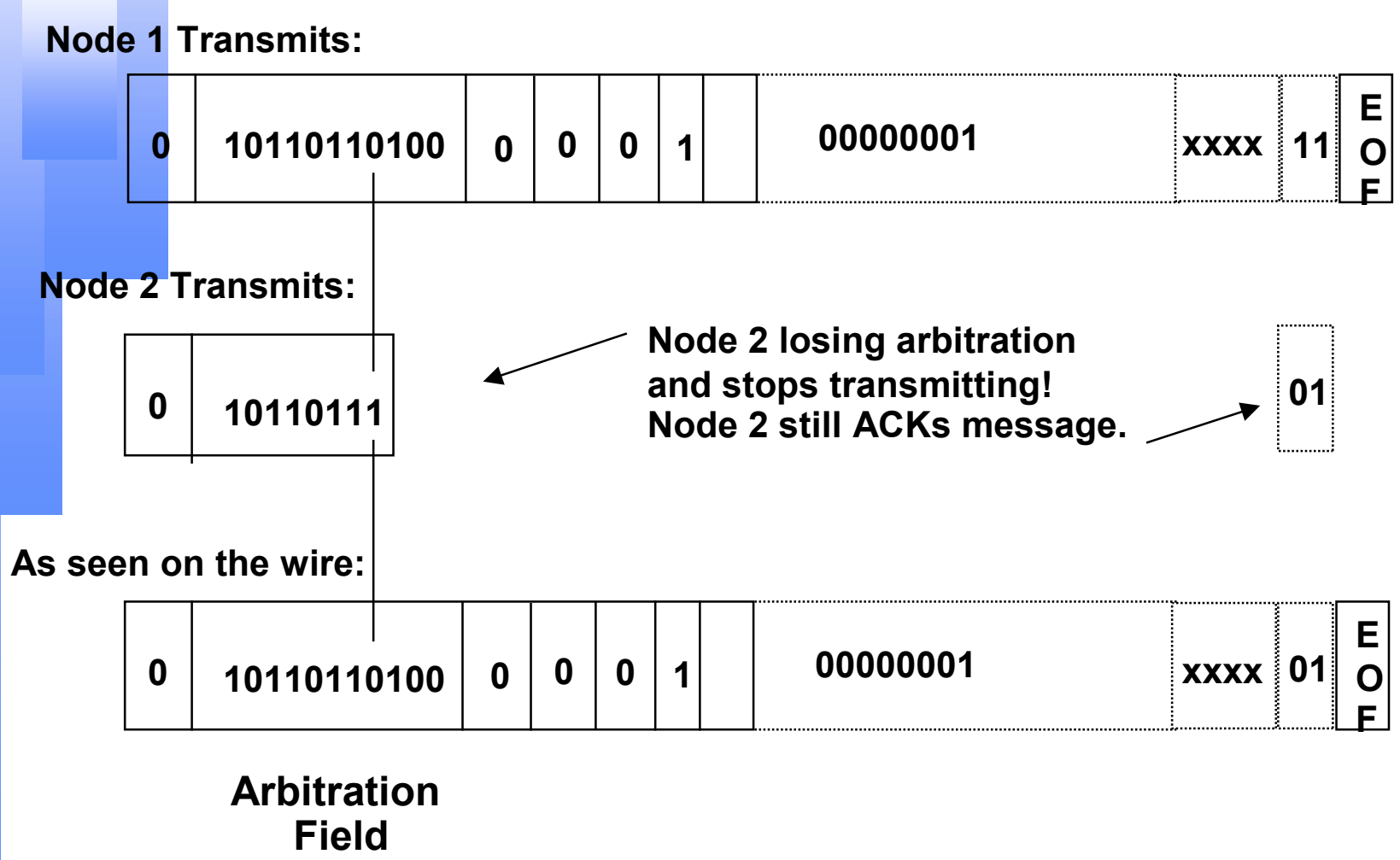
CAN Data Frame Overview



SOF - Start of Frame
LEN - Data Length Code
CRC - Cyclic Redundancy Code (CRC 16)

ACK - Acknowledgment

CAN Arbitration Example



CAN Error Detection

- Bit Errors
  - Transmitting node checks bit on bus versus what it sent
- Stuff Error
  - After 5 consecutive bits of same value, transmitter must insert opposite value bit
- Acknowledgment Error
  - All nodes respond in the ACK slot if they receive the message properly
- CRC Error
  - 16 bit transmitted value recalculated by receiving node
- Form Error
  - check for delimiter and other packet formats violations

DeviceNet Supports Multiple Network Models and Data Movement

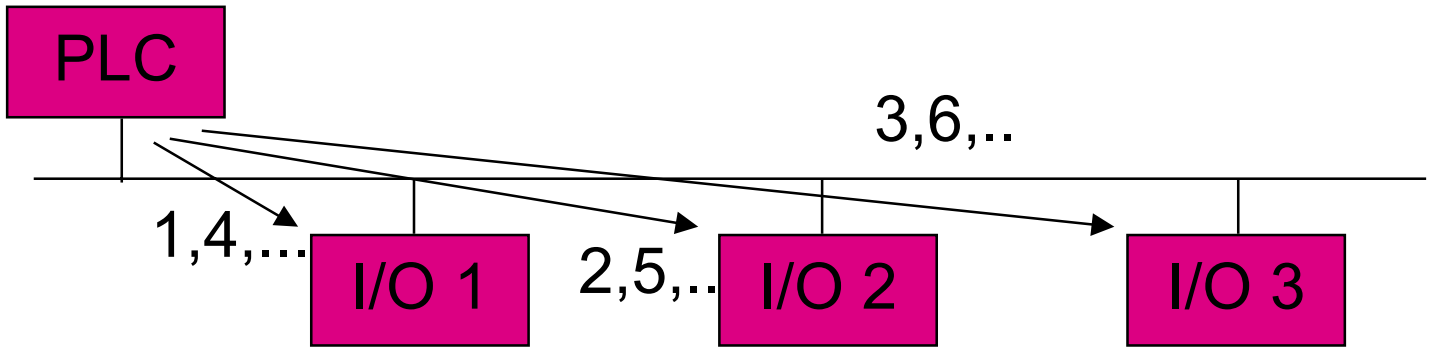
- Master/Slave
- Peer-to-Peer
- Multi-master

- Change of State data
- Cyclic Data Production
- Strobed
- Polled data

Producer/Consumer Paradigm allows for multiple model support vs. limited Source/Destination

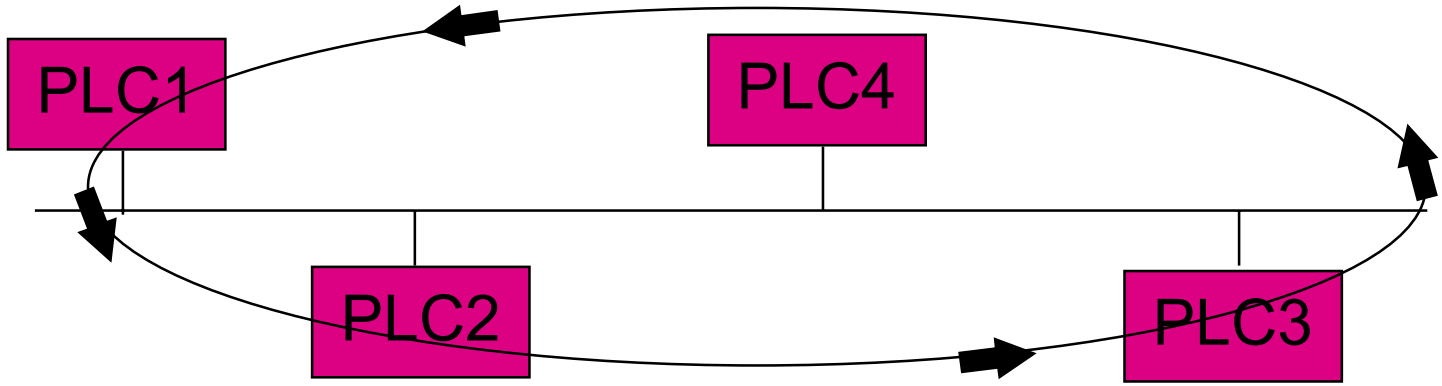
Network Models - Master/Slave

- The simplest and most understood; “polling”
- The PLC or scanner is the master and I/O devices are the slaves
  - The slaves speak only when spoken to
  - Only one master per network (“single master”)
  - Deterministic but not repeatable
- Network examples - Remote I/O, Profibus DP, Interbus-S, Seriplex, LON



Network Models - Peer-to-Peer

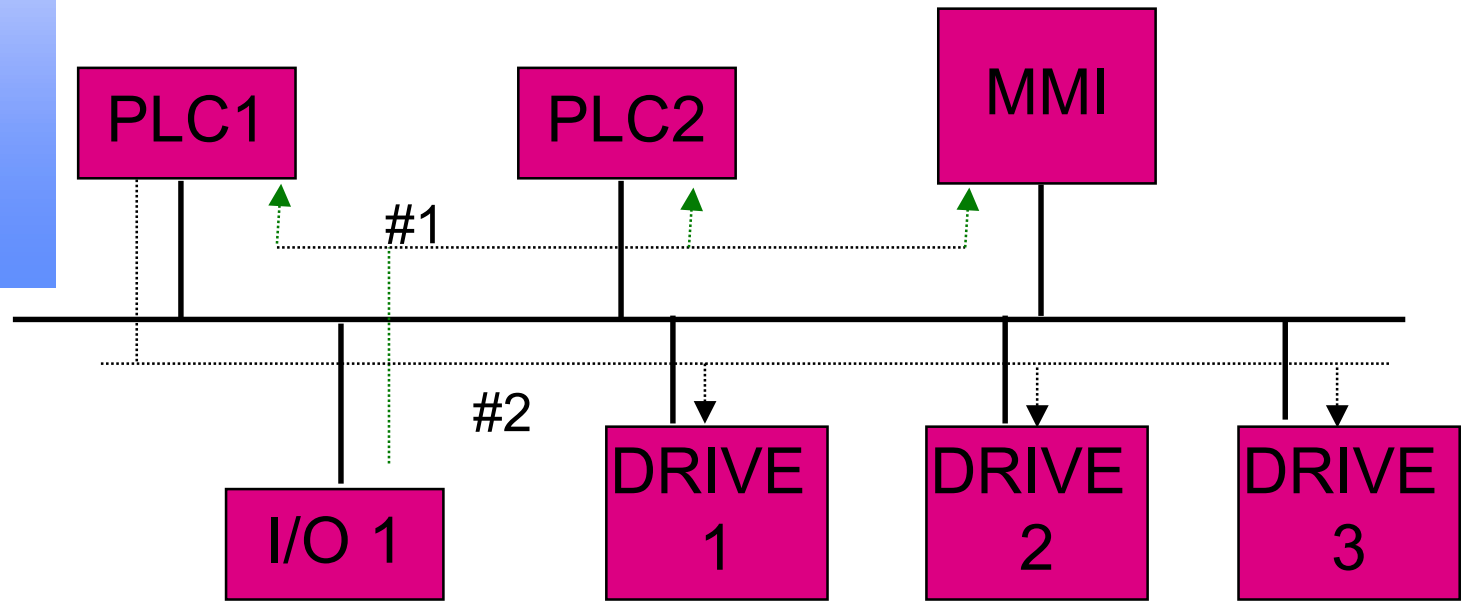
- Peer-to-peer are generally token pass networks
  - Each device can send messages only when they have the token
  - The token gets passed based on node number (round robin) or possibly via user defined priority list
- No sense of mastership or priority
- Not deterministic
- Network examples - DH+, DH485, LON, Profibus FMS



Producer/Consumer

- Data is identified as to it's content
  - No more Source/Destination requirements
  - No sense of mastership
- Allows the functionality of the Source/Destination models: Master/Slave and Peer-to-Peer
- Additional models are allowed because relationships can be built dynamically:
  - Multicast - one to many, many to one
  - Change of state
  - Cyclic, time based
- Superior performance because bandwidth is not wasted
- Network examples - DeviceNet, ControlNet, FIP, Fieldbus Foundation

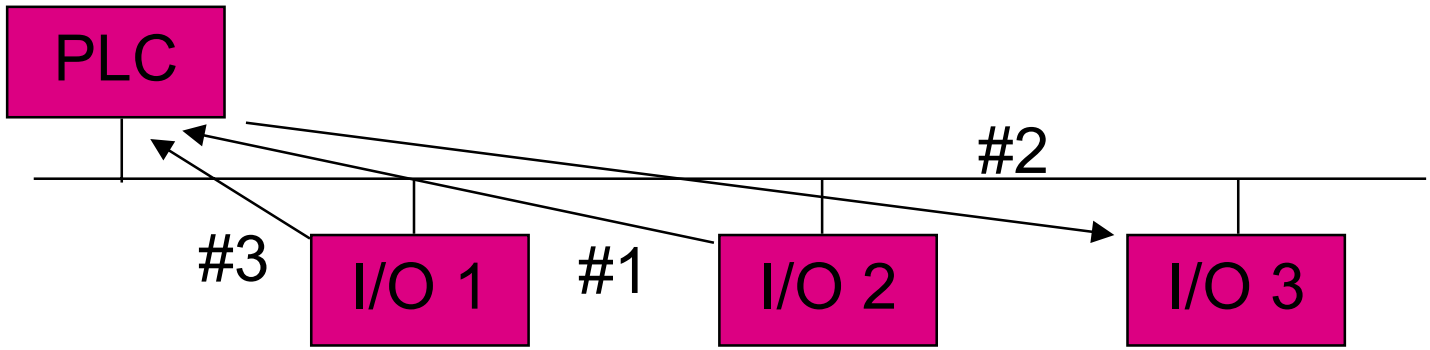
Network Models - Multi-master & Multicast



- Transaction #1 - position reference from I/O Rack #1 is broadcasted to PLC1, PLC2, and the MMI at the same time
- Transaction #2 - speed command is sent to all three drives at the same time

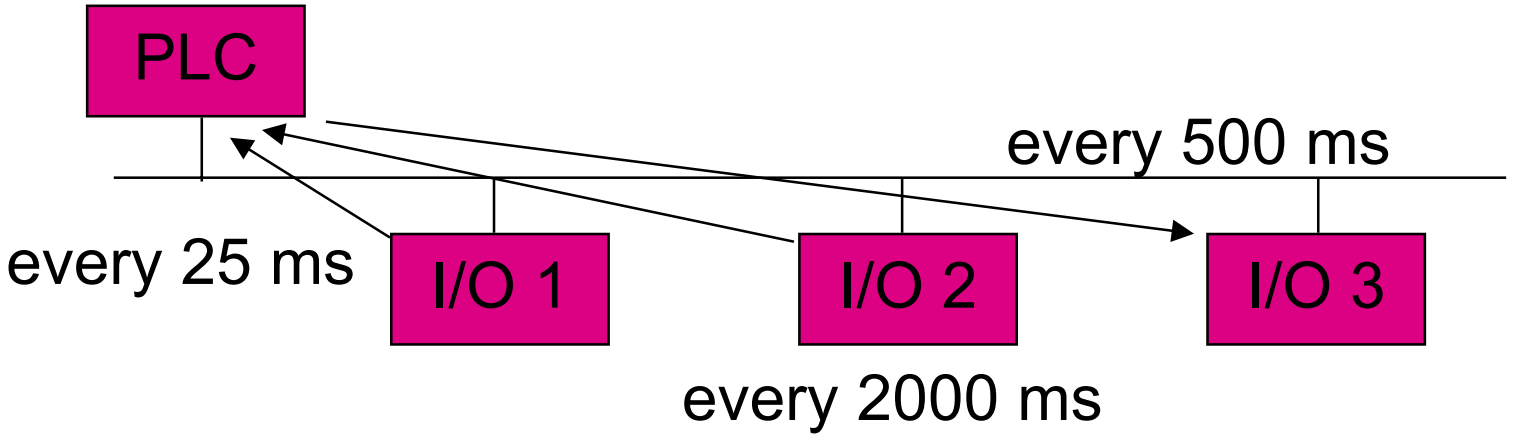
Data Movement - Change of State

- Rather than a master going through a polling list (scanning), devices report data (input or output) on a change-of-state basis as the events happen
- Change of State is more efficient for discrete applications
  - Network traffic is significantly reduced
  - Performance is greatly improved
- Background heartbeat for device health
- Can be used in Master/Slave, Peer-to-Peer, or Multi-master environments



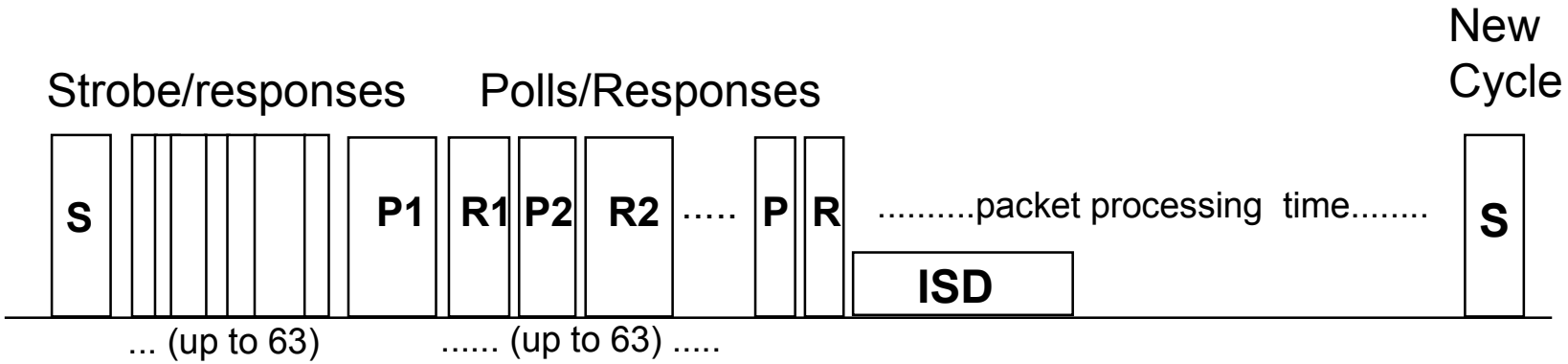
Data Movement - Cyclic Data Production

- Devices report data on a user-configured time increment basis (input or output)
- Cyclic Data Production is more efficient for applications with slowly changing I/O (analog)
  - Network traffic is reduced
  - Performance is repeatable
- Can be used in Master/Slave, Peer-to-Peer, or Multimaster environments



Scan Cycle

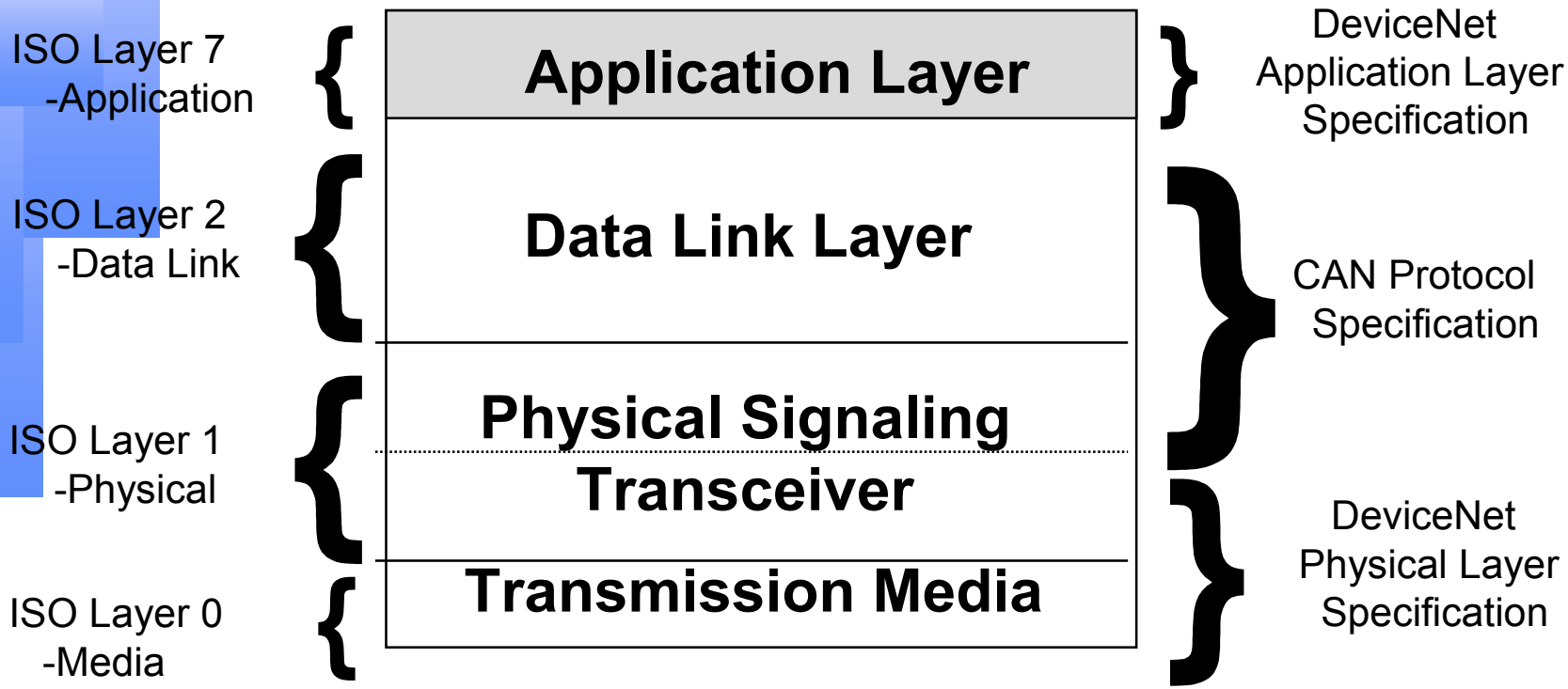
- STROBE: This multicast message starts off the scan cycle. Strobable slaves respond based on their latency.
- POLL: Sent out even as strobe responses are being received, as bandwidth allows.
- INTER SCAN DELAY: User selectable minimum quiet time to allow other devices access to the network. Scanner will not start another scan cycle (even if packet processing is complete).



C.O.S./Cyclic Traffic

- Devices report only when necessary
- More efficient since only data changes are transmitted
- Configurable for Ack or no Ack
- Used along with Poll & Strobe
- Optional heartbeat can be utilized to assure node is still active

Application Layer



Functions of Application Layer

- CAN Identifier Assignment
  - establishes priority in arbitration process
  - used by receiving nodes to screen for “their” messages
- Two Messaging Types
  - I/O Messages for Time Critical control data
  - Explicit Messages for typical Client/Server functions
  - Fragmentation supported for data greater than 8 bytes
- Duplicate Node Address Detection
  - each node must pass before going on line
- Device Application Data Consistency
  - Identity data: Type, Vendor, Cat. #, Serial #, ...
  - Comm Link data: Node Address, Baud Rate, ...
  - Device Config data: e.g., drive - Accel/Decel, Freq Control, ...

Device Configuration Support

- Provide for User Friendly configuration
  - Computer based, notebook, palmtop, etc.
- Electronic Data Sheet (EDS)
  - standardized ASCII file format
  - provides description of device attributes
    - name, ranges, eng. units, data type, etc.
  - public attributes from device profiles
  - vendor specific attributes
  - device vendor does once
    - all software vendors use as input
- Parameter Object
  - same content as EDS, but on board the device itself
  - no mismatches between tool and device/version

Device Interchangeability

- Standardized “Data Sets” (profiles) for various device types
- Allows user to substitute “logically” equivalent devices among vendors
  - only provides for same device types, data structures and meaning
  - NOT complete functional interchangeability
- User still has to determine “application” equivalency
  - accuracy, life, mechanical strength and mounting, environmental ratings, response time, capacity, etc.
  - this is the same as when replacing a device connected to an I/O point
  - substitution with another vendor’s product not likely if user has utilized any vendor specific parameters
- System can “key” devices to prevent illegal substitutions
  - For example, system can be configured to not accept a “reflective” photoeye for a “diffuse” photoeye