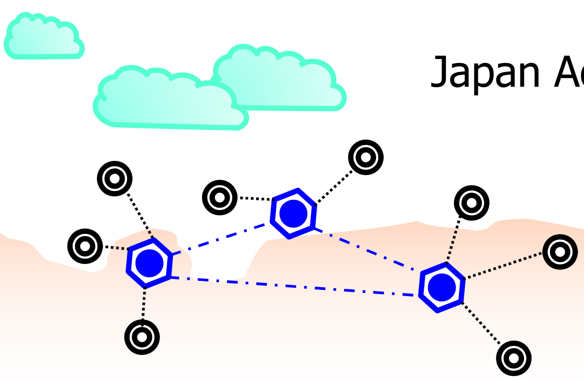
I226
Computer Networks

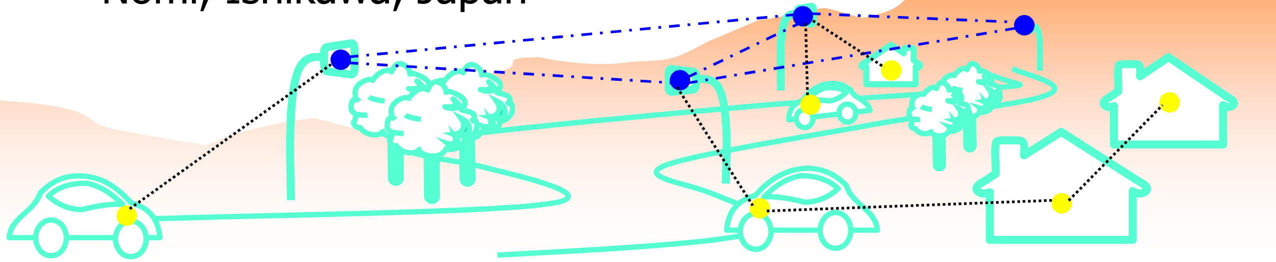
Chapter 3

Data Link Layer

Assoc. Prof. Yuto Lim

School of Information Science
Japan Advanced Institute of Science and Technology
Nomi, Ishikawa, Japan

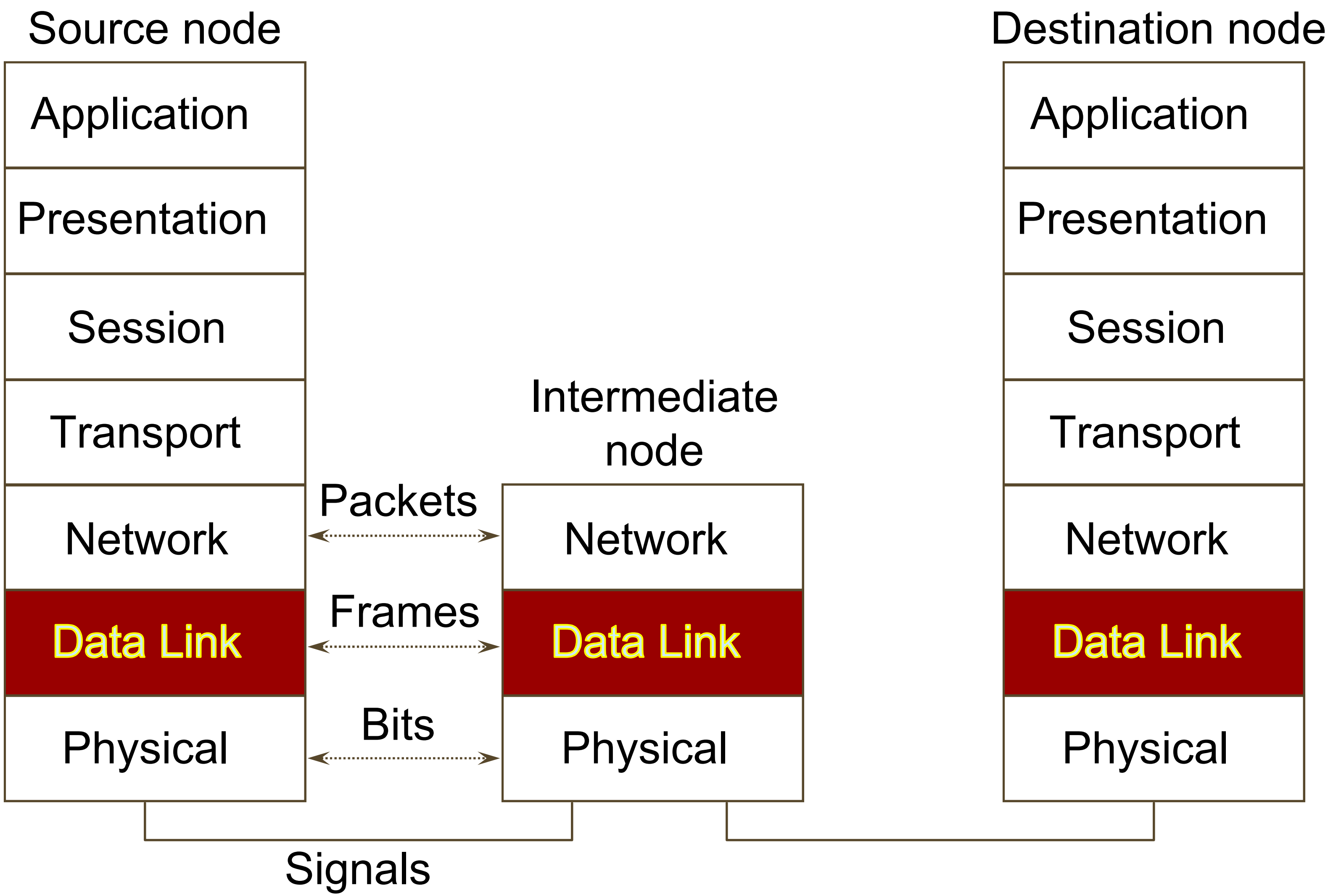




Objectives of this Chapter

- Provide an understanding what are the three functions of data link layer
- Explain in-depth knowledge on how the error detection using cyclic redundancy check (CRC) and the error correction using hamming code
- Give an explanation of three different data link protocols; byte-count-oriented, byte-oriented, and bit-oriented
- Give an explanation of different type of medium access control (MAC) protocols for point-to-multipoint configuration

Data Link Layer



Outline

- Functions of Data Link Layer
  - Framing
  - Flow Control
  - Error Handling
    - Error Detection and Correction
    - Error Control
- Data Link Protocols
  - DDCMP, BSC (BISYNC), HDLC
  - Others (LAPB, LAPD, LAPF, ATM)
- Medium Access Control Protocols
  - ALOHA, CSMA
  - Ethernet: CSMA/CD, Token Ring, FDDI

Position of LLC and MAC

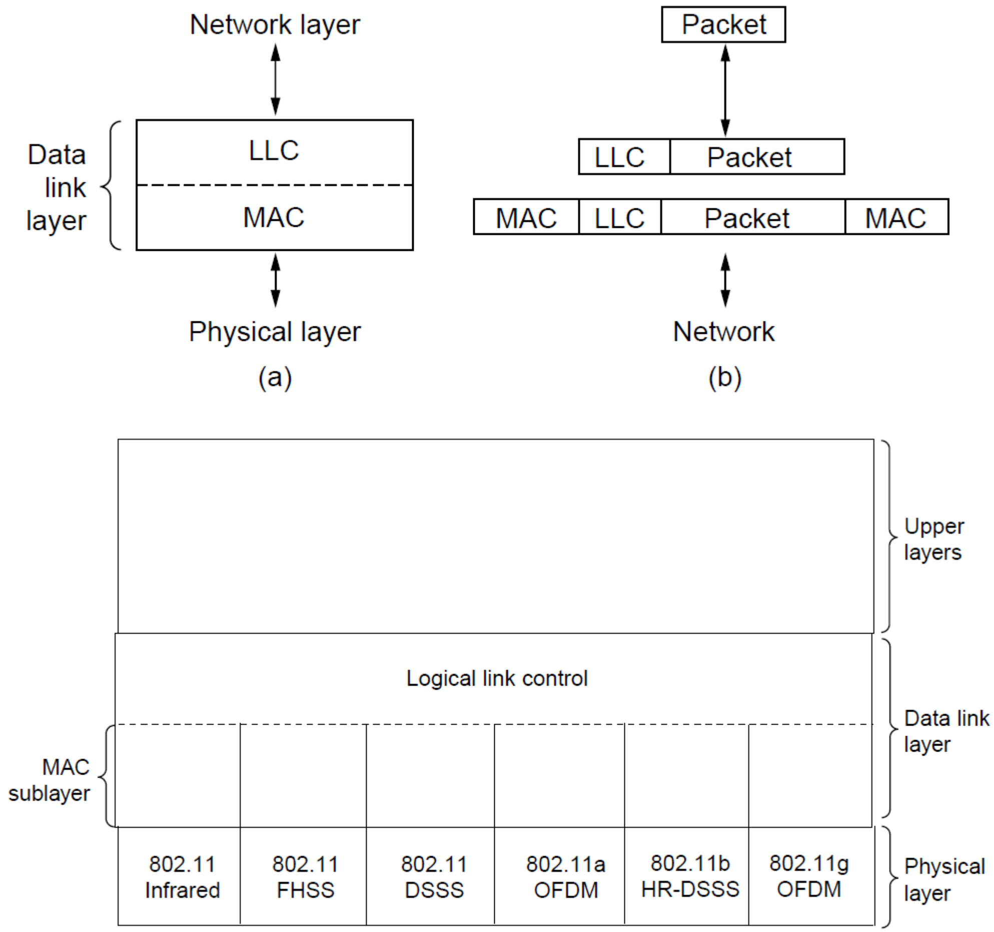
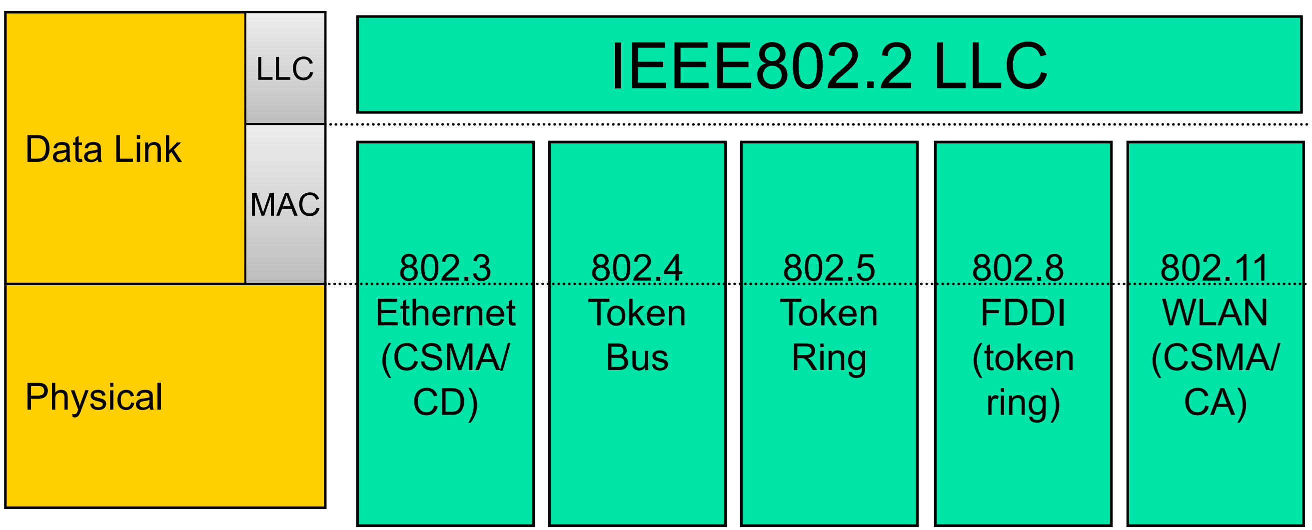


Figure: Position of LLC

LLC and MAC in IEEE Standardization

- Logical link control (LLC) layer and media access control (MAC) in IEEE standardization



Functions of Data Link Layer

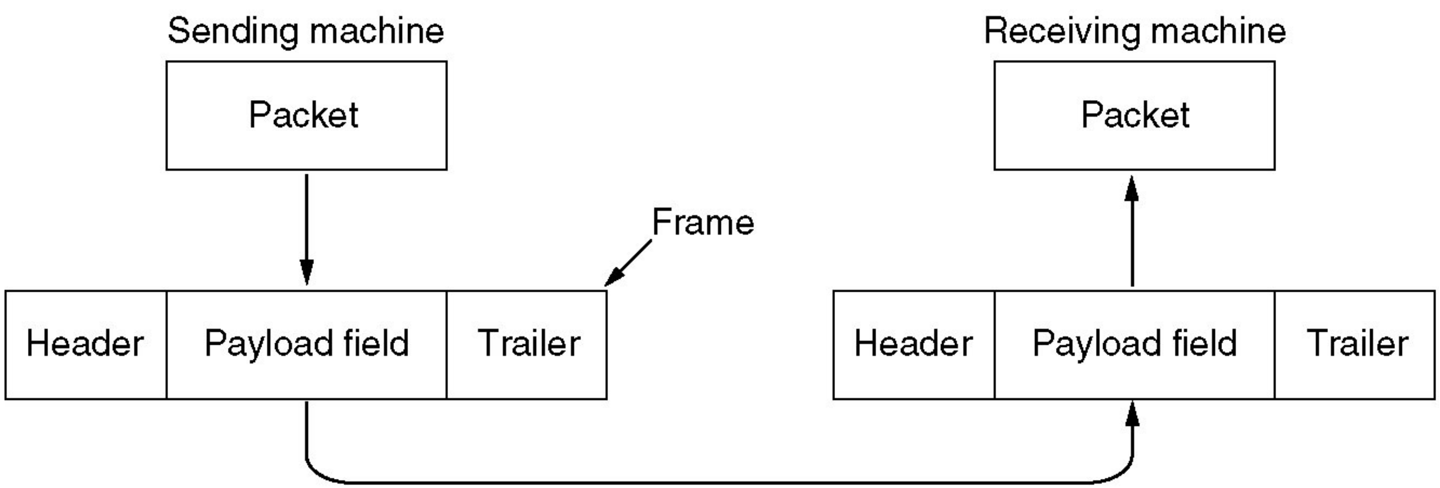
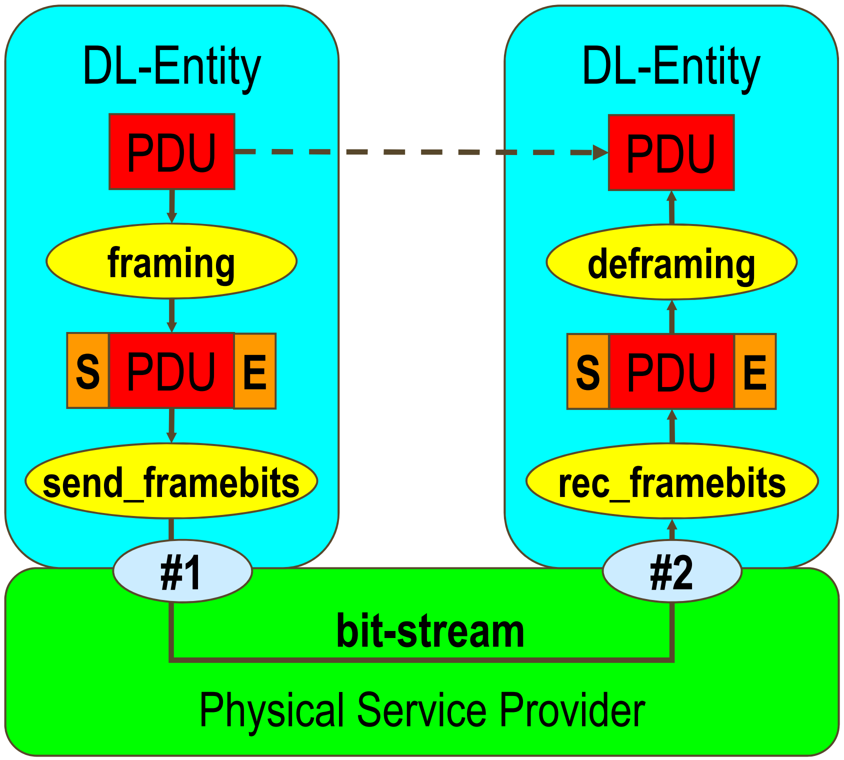


Figure: Relationship between packets and frames

- <u>Framing</u> – provide service interface to the network layer
- <u>Flow control</u> – regulating data flow
  - Slow receivers not swamped by fast senders
- <u>Error Handling</u> – dealing with transmission errors

Framing

- DL-Entity can transmit a bit-streams (or bit-sequences) using the Physical Service Provider (PSP)
- Given the protocol data unit (PDU) to be send to the peer protocol entity it turns it into a frame, meaning
  - It adds a start-flag (S) and an end-flag (E) to the PDU so that the receiving protocol entity can recognize as frame
  - Framed PDU is send as a bit-stream from sending protocol entity to receiving protocol entity using the PSP



Flow Control

- To provide the sending entity does not overwhelm the receiving entity
  - recipient needs some time to process incoming frames
  - flow control prevents buffer overflow – if sender sends faster than recipient processes, then buffer overflow occurs

- 2 approaches are used

  - Feedback-based flow control – the receiver sends back information to the sender giving it permission to resend or at least telling the sender how the receiver is doing

  - Rate-based flow control – the protocol has a built-in mechanism that limits the rate at which sender may transmit data, without using feedback from the receiver

- Rate-based flow control are never used in the data link layer

Flow Control (cont.)

- Performance Metrics
  - Transmission time (delay) – time taken to emit all bits into medium
  - Propagation time (delay) – time for a bit to traverse the link
  - Processing time (delay) – time spent at the recipient or intermediate node for processing
  - Queuing time (delay) – waiting time at the queue to be sent out

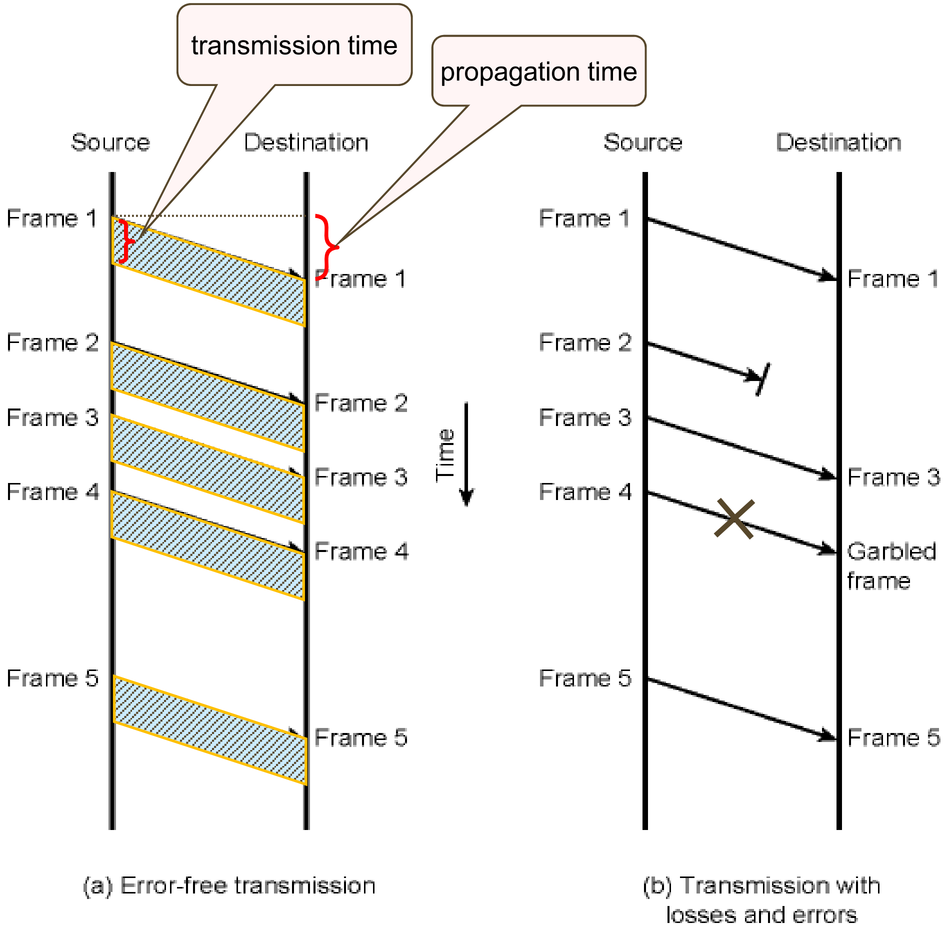


Figure: Model of Frame Transmission

Flow Control (cont.)

- 2 methods to control the flow of data across communications links

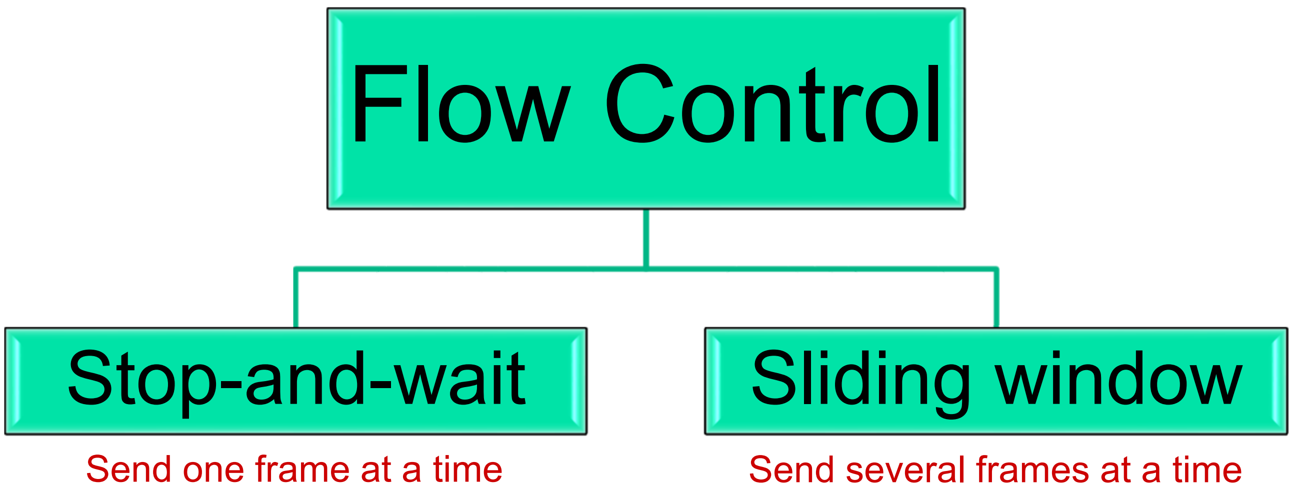


Figure: Categories of flow control

Flow Control: Stop-and-wait

- Operation
  - source transmits frame, while destination receives frame and replies with ACK
  - source waits for ACK before sending next frame
- Destination can stop flow by not sending ACK
- Efficient for large frames, but inefficient for smaller frames
- Large frame can split into small frames, fragmentation
  - make buffer size is smaller at receiver
  - when whole frame received, retransmission of smaller frames is needed if error is detected
  - prevents one station occupying medium for long periods
- Channel utilization is higher when
  - the transmission time (T) is longer than the propagation time (D), or
  - frame length is larger than the bit length of the link

Flow Control: Stop-and-wait (cont.)

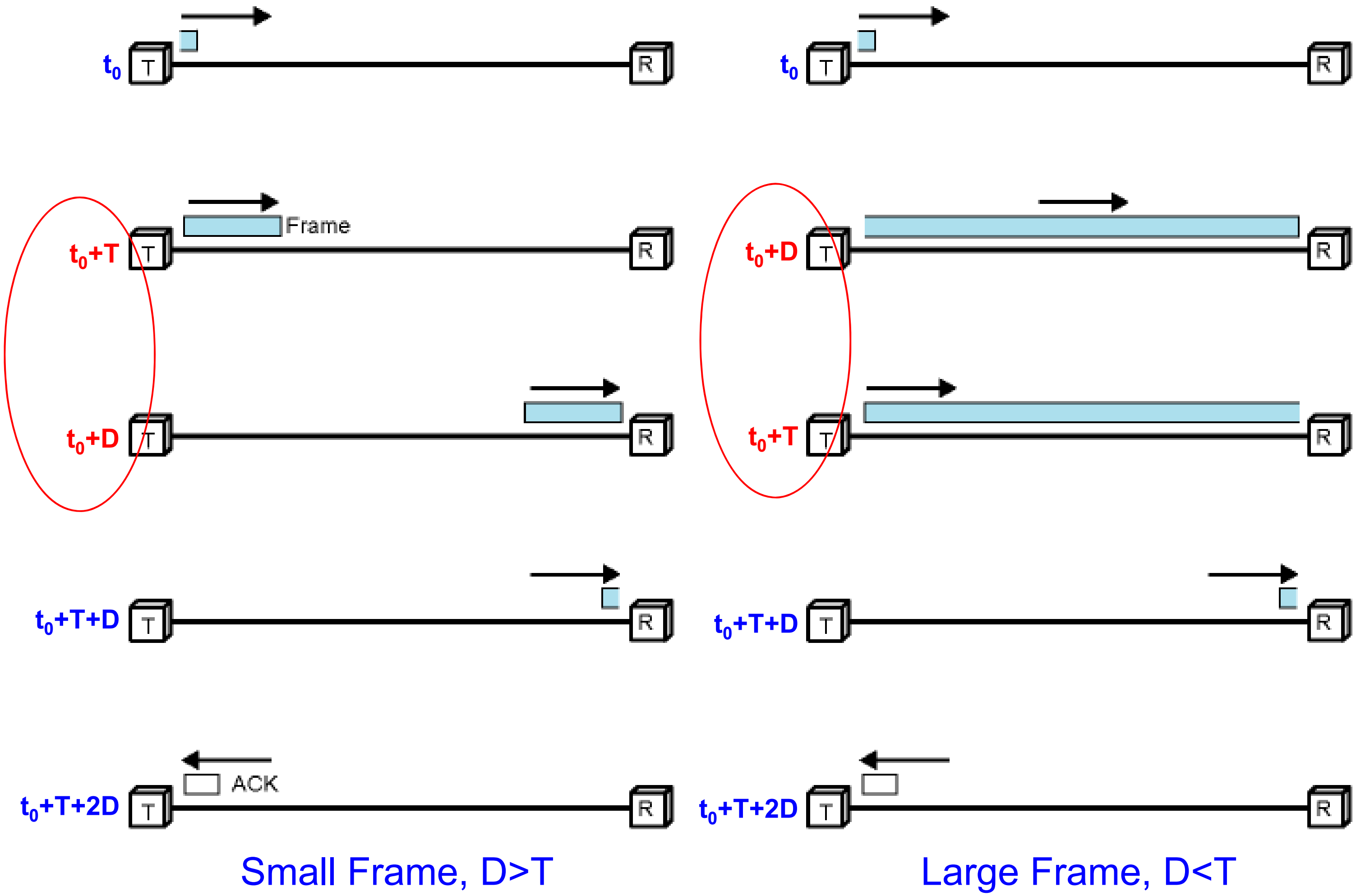


Figure: Link utilization, where D is propagation time, T is transmission time

Flow Control: Sliding Window

- Stop-and-wait problem cannot send multiple frames
- Receiver has buffer of W (window size) frames
- Transmitter can send up to W frames without ACK
- Each frame is numbered
  - Sequence no. bounded by size of the seq. no. field (k bits)
  - Thus, frames are numbered modulo 2^k ($0 \ldots 2^k - 1$)
- ACK includes number of next frame expected

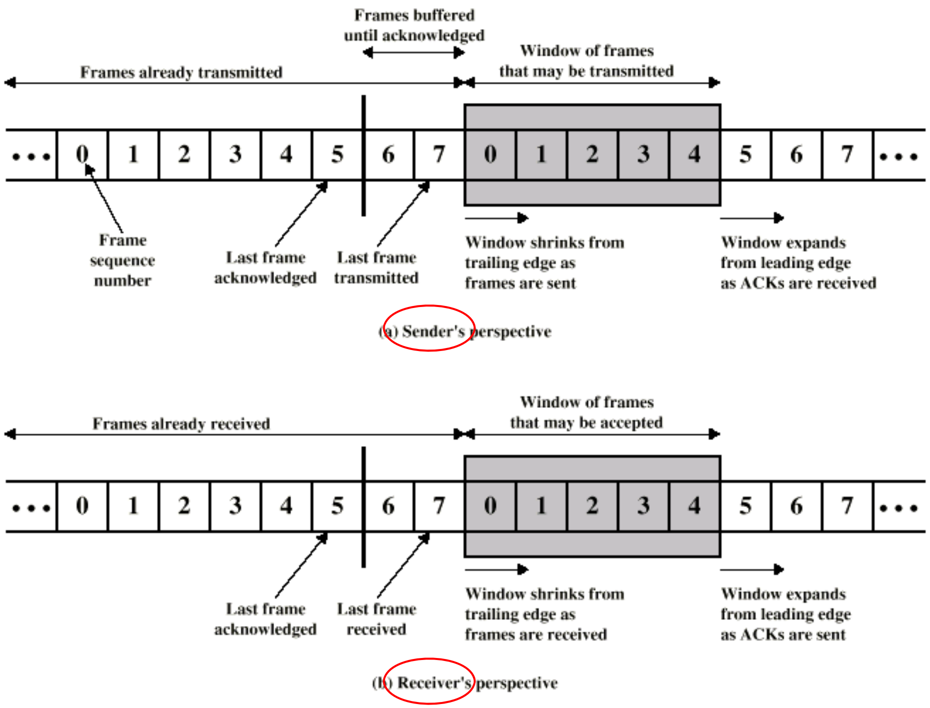
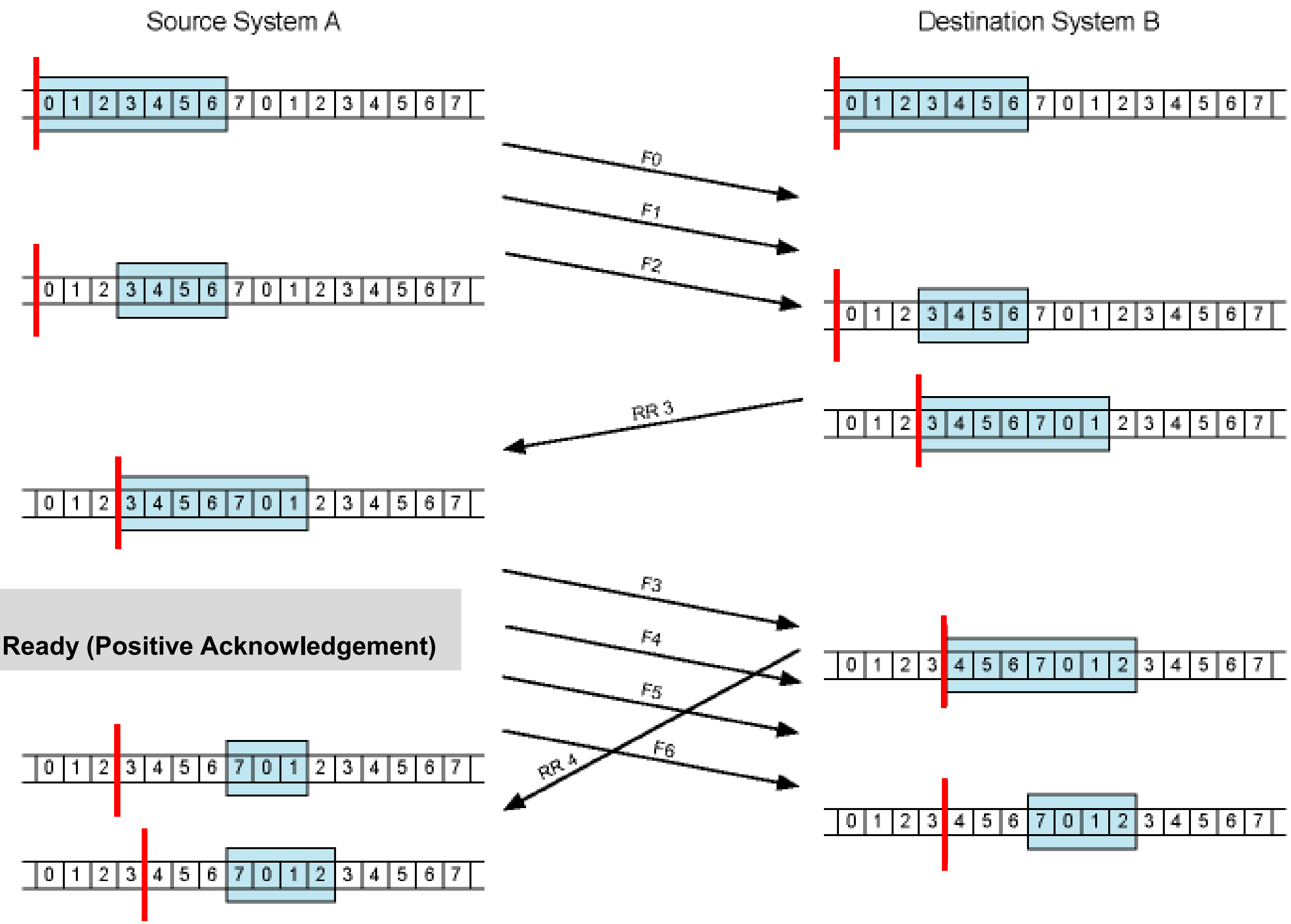


Figure: Example of a Sliding Window Protocol (W = 7)

Flow Control: Sliding Window (cont.)



F = Frame
RR = Receive Ready (Positive Acknowledgement)

Figure: Example of a Sliding Window Protocol (W = 7)

Error Detection and Correction

- In previous slides, we assume that flow control mechanism where frames are transmitted without errors
  - In real life any transmission facility may introduce errors
- Errors that can occur are
  - Errors in bits, e.g., a ‘0’ is received instead of a ‘1’; or vice versa. This error is caused by the Physical Service Provider
  - Frame may lost, e.g., bits come in too fast. This error is caused by the data link layer itself
- We have to detect errors. If possible, correct the errors
- 2 methods
  - Error detection & retransmission – Code a PDU such that at the receiver side the error can be detected and the receiver asks the sender to send the PDU again
  - Error correction – Code a PDU such that at the receiver side the errors can be restored

Error Detection

- Additional bits added by transmitter as error detection code
  - Receiver checks this code
- Parity
  - Single bit added to the end of the data
  - Value of parity bit is such that data and parity have even (even parity) or odd (odd parity) number of ones
  - Even number of bit errors goes undetected, thus not so useful
- There are many Codes for error detection, we discuss
  - 1-Dimensional Parity Check Code
  - 2-Dimensional Parity Check Code
  - Cyclic Redundancy Check (CRC) Code

Parity Check Code

Information Word (PDU)								Code Word (new PDU)							
0	1	0	1	0	0	1	⇒	0	1	0	1	0	0	1	1
1	1	0	1	0	0	1	⇒	1	1	0	1	0	0	1	0
1	0	1	1	1	1	0	⇒	1	0	1	1	1	1	0	1
0	0	0	1	1	1	0	⇒	0	0	0	1	1	1	0	1
0	1	1	0	1	0	0	⇒	0	1	1	0	1	0	0	1
1	0	1	1	1	1	1	⇒	1	0	1	1	1	1	1	0

Figure: 1-Dimensional (Even Parity)

- Method: add an extra bit to that PDU so the total number of 1’s in the new PDU is even (called even parity) or odd (called odd parity)
- Most 3 bit errors can be detected, but it cannot infer which bit is wrong
- Given a PDU of length b, the overhead of this code is: $100/b$ %

Information word (PDU)								Code word (new PDU)							
0	1	0	1	0	0	1	⇒	0	1	0	1	0	0	1	1
1	1	0	1	0	0	1	⇒	1	1	0	1	0	0	1	0
1	0	1	1	1	1	0	⇒	1	0	1	1	1	1	0	1
0	0	0	1	1	1	0	⇒	0	0	0	1	1	1	0	1
0	1	1	0	1	0	0	⇒	0	1	1	0	1	0	0	1
1	0	1	1	1	1	1	⇒	1	0	1	1	1	1	1	0
								1	1	1	1	0	1	1	0

Figure: 2-Dimensional

- Method: for each row we add an extra bit so that the total number of ‘1’ in the row becomes even. We add an extra row of bits so that the number of 1’s in each column becomes even
- Most 4 bit errors can be detected. This code can detect errors that occur in a row (called burst-errors)
- The overhead of the 2-Dimensional parity check is larger

Cyclic Redundancy Check

- Given the *PDU* (i.e., a sequence of bits) and a generator *G*:
  - This is a particular bit-sequence, it is part of the protocol (hence sending and receiving data-link protocol entity both know them)
  - Let *G* consist of $r+1$ bits
- We add *r* 0-bits to the *PDU*, let this be *PDU'*
- Now divide the *PDU'* by *G* (so called modulo-2 arithmetic is used), this gives a rest *R*
- Now we calculate a bit-sequence *T* such that $T = PDU' - R$
  - *T* will be transmitted
  - It can be proven that *T* can always be divided by *G*

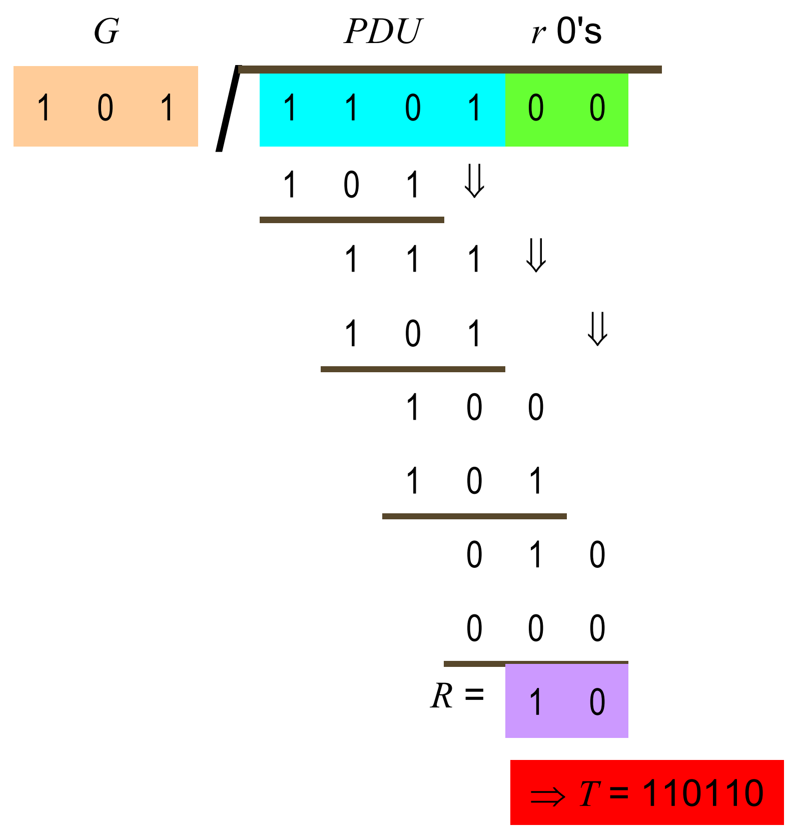


Figure: Binary division in a CRC generator

Cyclic Redundancy Check (cont.)

- CRC generators are subject of design and standardization. The goal here is to let them have strong properties like
  - Detect all single and double errors
  - Detect all burst of 16 bits and less
- Example generators are
  - CRC-8 100000111
  - CRC-10 11000110011
  - CRC-12 1100000000101
  - CRC-16 11000000000000101
  - CRC-CCITT (ITU-T) 10001000000100001
  - CRC-32 100000100110000010001110110110111
- Highly efficient codes
  - Overhead of CRC-16 Code for a PDU of size 12000 bits (1500 bytes) as in Ethernet: 0.14%

Error Correction: Hamming Code

- Hamming code is <u>well known</u> in the field of error correcting codes
- Hamming code can correct 1 error only
- Hamming Code is written as: Hamming b-r
  - b is the number of information bits
  - r is the number of control bits
- The code in Hamming 7-4 is

_	_	_	_	P	_	_	_	P	_	P	P
12	11	10	9	8	7	6	5	4	3	2	1

Example

- What are the values for the other parity bits?

1	1	0	1		0	1	1		0		
12	11	10	9	8	7	6	5	4	3	2	1

  - Answer: The completed code word is shown below

    Bit 1 checks the digits, 1, 3, 5, 7, 9, and 11, so its value is ‘1’
    Bit 2 checks the digits, 2, 3, 6, 7, 10, and 11, so its value is ‘0’
    Bit 4 checks the digits, 4, 5, 6, 7, and 12, so its value is ‘1’
    Bit 8 checks the digits, 8, 9, 10, 11, and 12, so its value is ‘1’

1	1	0	1	1	0	1	1	1	0	0	1
12	11	10	9	8	7	6	5	4	3	2	1

Example

- Show how to identify the error that is occurred at?

error

1	1	0	1	1	0	1	1	1	0	0	1
12	11	10	9	8	7	6	5	4	3	2	1

Sender

1	1	0	1	1	0	1	0	1	0	0	1
12	11	10	9	8	7	6	5	4	3	2	1

Receiver

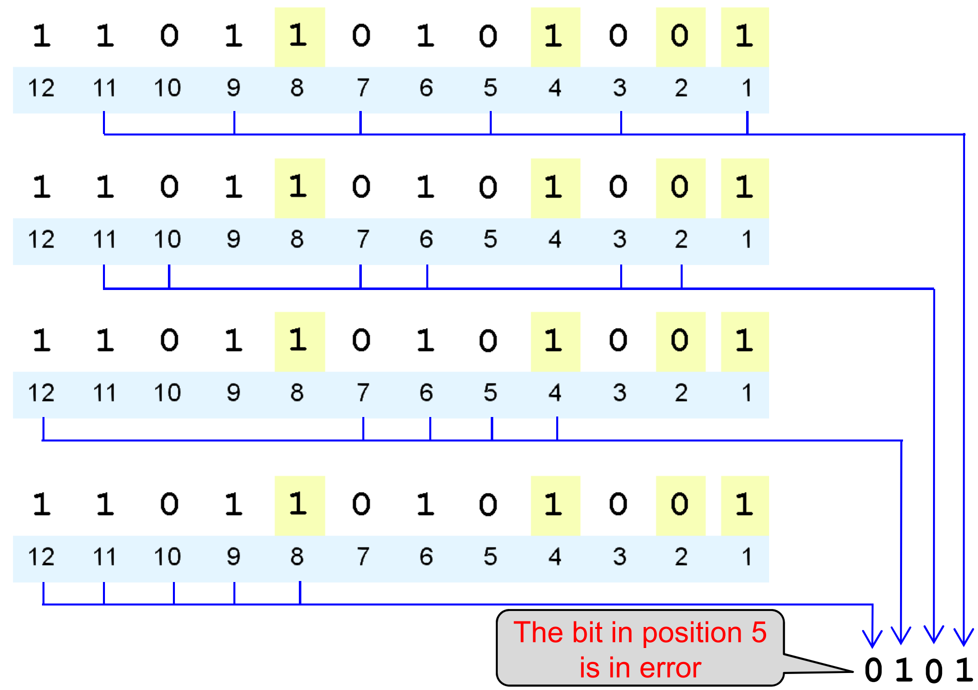
- Answer:

  Bit 1: bit 1, 3, 5, 7, 9, 11

  Bit 2: bit 2, 3, 6, 7, 10, 11

  Bit 4: bit 4, 5, 6, 7, 12

  Bit 8: bit 8, 9, 10, 11, 12



Error Control

- In the data link layer, the error control refers to methods of error detection and retransmission
- Automatic repeat request (ARQ) means retransmission of data in 3 cases:
  - Damaged frame
  - Lost frame
  - Lost Acknowledgement frame

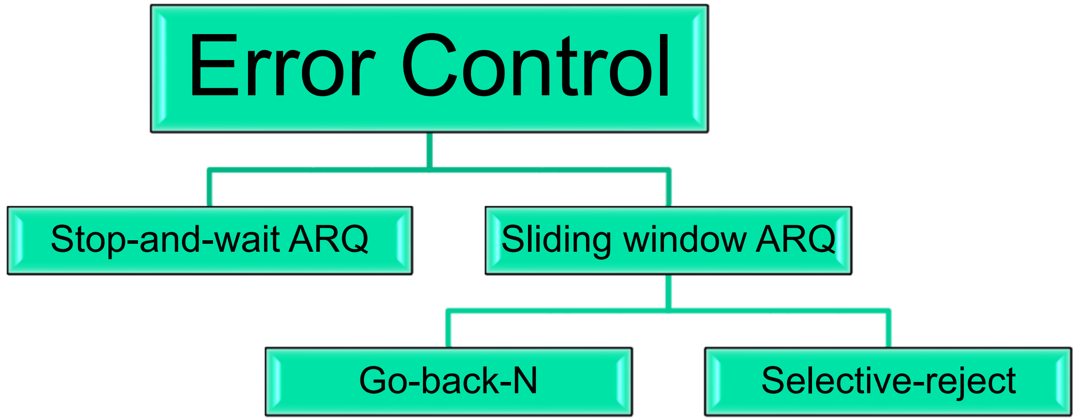
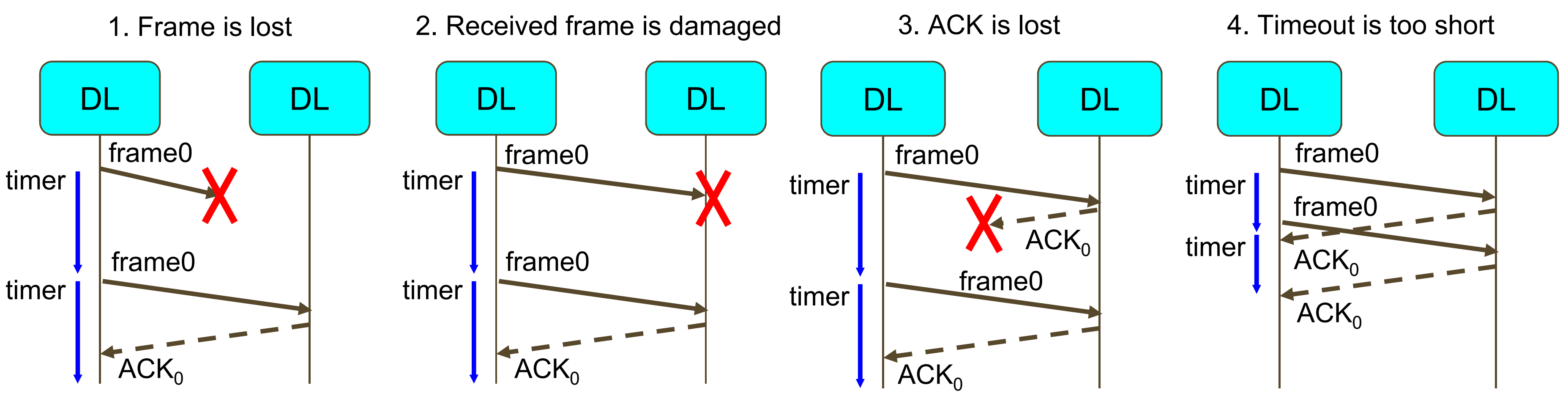


Figure: Categories of error control

Stop-and-wait ARQ

- Source transmits single frame and wait for ACK
- If received frame is damaged, discard it
  - If transmitter receives no ACK within timeout, retransmits
- If ACK damaged, transmitter will not recognize it
  - Transmitter will retransmit
  - Receiver gets two copies of frame, but disregards one of them
  - Use ACK_0 and ACK_1 (ACK_i means “I am ready to receive frame i”)



Sliding Window ARQ: Go-Back-N

- Stop-and-wait ARQ is simple, but inefficient
- If no error, ACK as usual with next frame expected
  - ACK_i means "I am ready to receive frame i" and "I received all frames between i and my previous ACK"
- Source uses window to control the no. of unacknowledged frames
- If error, reply with rejection negative ACK (NACK)
  - Discard that frame and all future frames until the frame in error received correctly
  - Transmitter must go back and retransmit that frame and all subsequent frames

Sliding Window ARQ: Go-Back-N (cont.)

- Control variables:
  - S – holds the sequence number of the recently sent frame
  - S_F – holds sequence number of the first frame in the window
  - S_L – holds the sequence number of the last frame
  - R – sequence number of the frame expected to be received
- Inefficient
  - All out of order received frames are discarded
- There is a problem in a noisy link
  - Many frames must be retransmitted → bandwidth consuming
- Solution
  - Re-send only the damaged frames
  - Selective Repeat ARQ to avoid unnecessary retransmissions

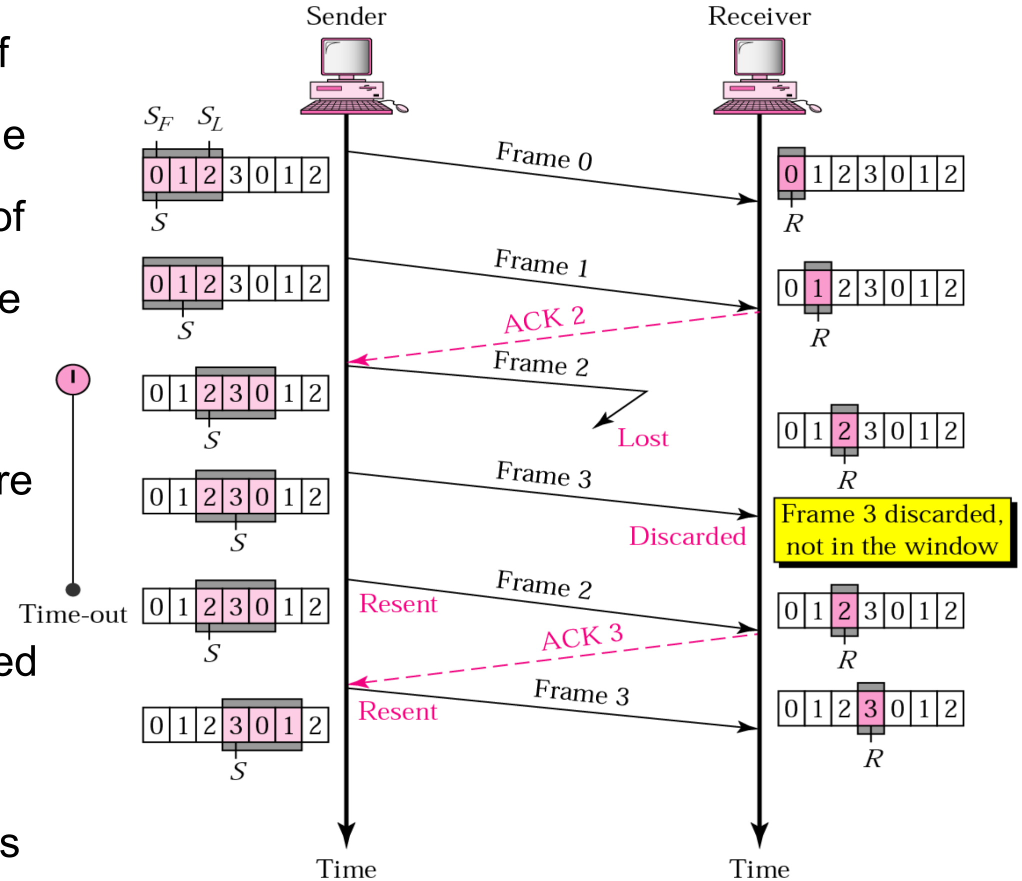


Figure: Lost frame case

Sliding Window ARQ: Selective-Reject

- Processing at the receiver more complex
- The window size is reduced to one half of 2^m
- Both the transmitter and the receiver have the same window size
- Receiver expects frames within the range of the sequence numbers
- Retransmission triggered with NACK and not with expired timer

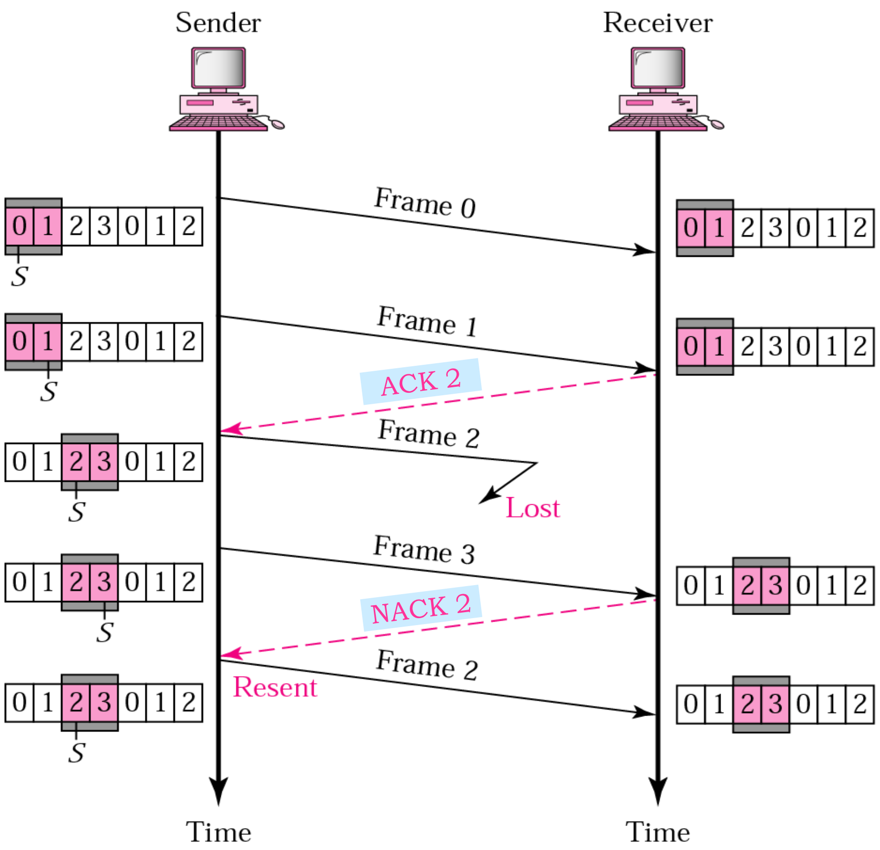


Figure: Lost frame case

Data Link Protocols

- 2 subgroups
  - Asynchronous protocols
  - Synchronous protocols
- Asynchronous protocols feature start and stop bits and variable length gaps between characters
  - Start/stop bits
  - Parity checking
  - Character oriented
  - Less expensive and less complicated equipment
  - For PCs, examples
    - XMODEM – simple, less reliable error checking
    - YMODEM – reliable, multiple files transfer
    - ZMODEM – fast, good failure recovery
    - KERMIT – reliable, fast file transfer, PC & mainframe
    - Serial Line Internet Protocol (SLIP) – full-duplex, IP over asynchronous dial-up or leased lines, no error correction
    - Point-to-point Protocol (PPP) – PC to a TCP/IP network, full-duplex for synchronous and asynchronous transmission, authentication, compression, error correction, and packet sequencing

Data Link Protocols (cont.)

- Synchronous protocols are divided into 3 classes:
  - Byte-count-oriented protocols
    - Special character for start of the header, count field, message, block check character (BCC)
    - E.g.,: DEC's Digital Data Communication Message Protocol (DDCMP)
  - Byte-oriented protocols, interpret a transmission frame as a succession of characters (one byte)
    - Special character for start and end of message
    - E.g.,: Binary Synchronous Communication Protocol (BSC or BISYNC)
  - Bit-oriented protocols, interpret a transmission frame as a succession of individual bits
    - Use flag character for start and end of message
    - E.g.,: IBM's Synchronous Data Link Control (SDLC) and ISO's High-level Data Link control (HDLC)

DDCMP

- Usage
  - Digital Network Architecture (DNA)
  - High-bandwidth and high-latency (satellite) links
- Data message and control message
- Error checking
  - Use block check character
  - Unique and increasing sequence number for sending message
  - ACK indicates the last message received
- Advantages
  - no “data transparency” problem (i.e., the user wishes to send an arbitrary data stream but the protocol itself needs to use control characters which could occur within that data stream)
  - Variable length of data
  - Only one control character: SOH (start of heading)
  - Easy implement for full-duplex and message sequence

BSC or BISYNC

- By IBM for 6-bit transcode (SBT), ASCII, EBCDIC
- SYN at start and middle of transmission
- Point to point and multipoint (polling)
- ARQ approach for error checking (ACK1, ACK0, NAK)
- Advantages
  - Provide both modes: transparency and non-transparency
  - Efficient, understandable, and widely used
  - Point-to-point & multipoint operations
- Disadvantages
  - Code dependent
  - Half-duplex protocol
  - Cumbersome for transparency mode

HDLC

- Support half/full – duplex over point-to-point and multipoint links
- HDLC station types
  - Primary station that controls the medium by sending “command”
  - Secondary station that “response” to the primary station
  - Combined station that can both command and response
- 3 configurations of all stations
  - Unbalanced (master/slave)
  - Symmetrical
  - Balanced

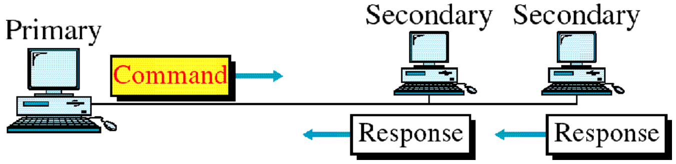


Figure: Unbalanced

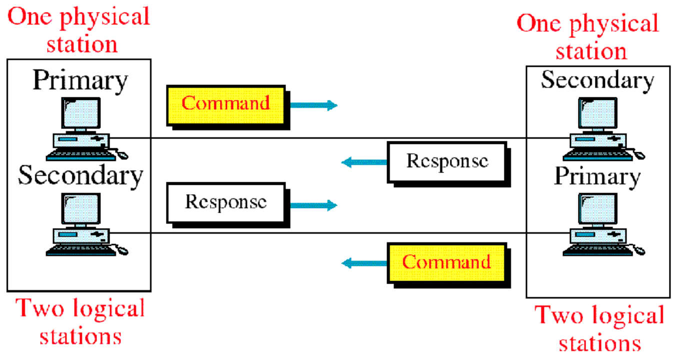


Figure: Symmetrical

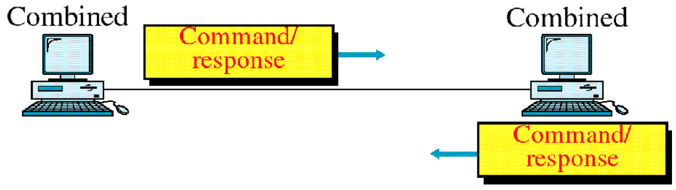


Figure: Balanced

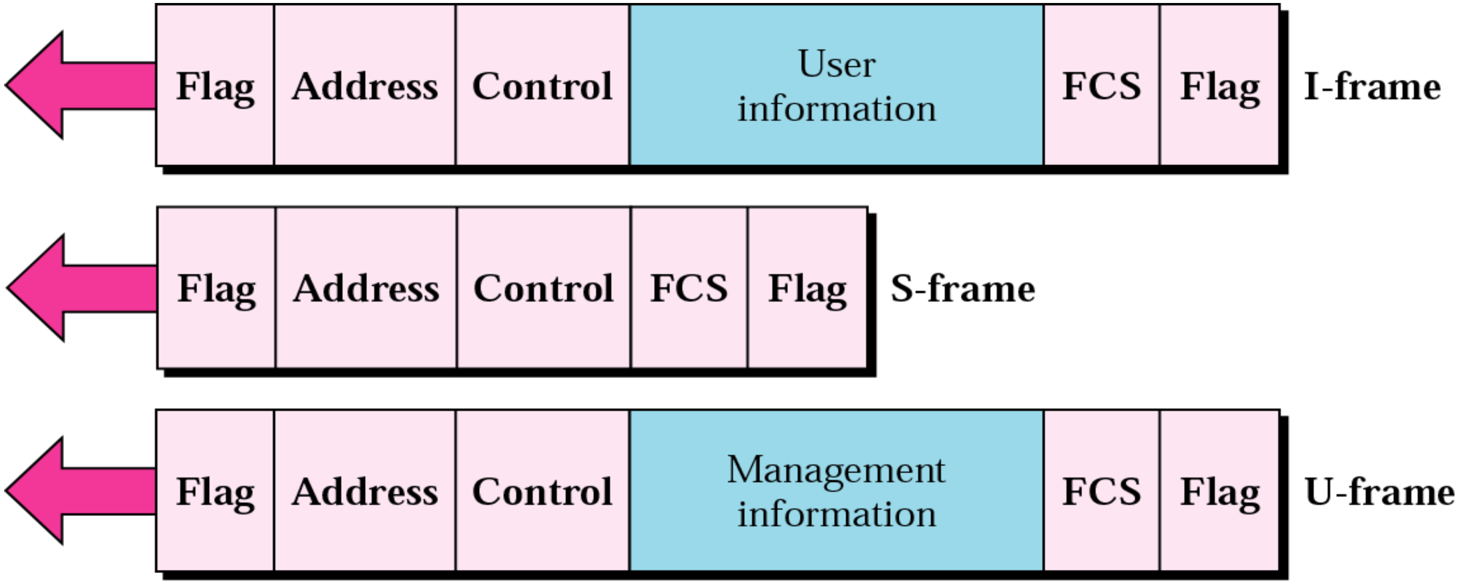
HDLC (cont.)

- Operating modes
  - Normal response mode (NRM) for a primary node and one or more secondary modes on a circuit (polling)
  - Asynchronous balanced mode (ABM) for nodes with peers (most used for efficiency with no polling in full duplex)
  - Asynchronous response mode (ARM) for primary and secondary nodes with same transmission right (rarely used)
- Mode describes “who controls the link”

	NRM	ARM	ABM
Station type	Primary & secondary	Primary & secondary	Combined
Initiator	Primary	Either	Any

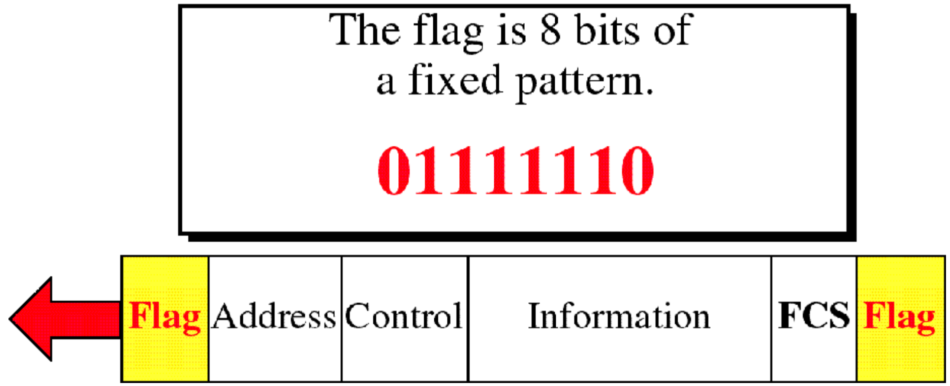
HDLC (cont.)

- Frames
  - Information or I-frame: (data)
  - Supervisory or S-frame: control acknowledge
  - Unnumbered or U-frame: (operation mode, start, termination)



HDLC (cont.)

- Flag '01111110'
  - Bit stuffing 0 after five 1s by hardware
  - For synchronization

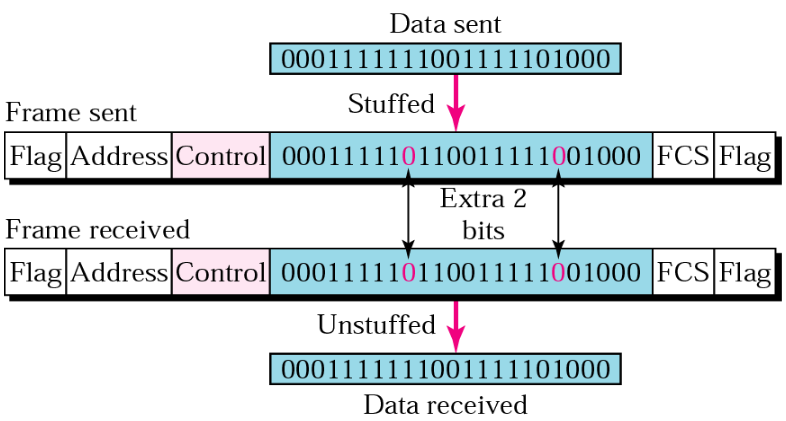


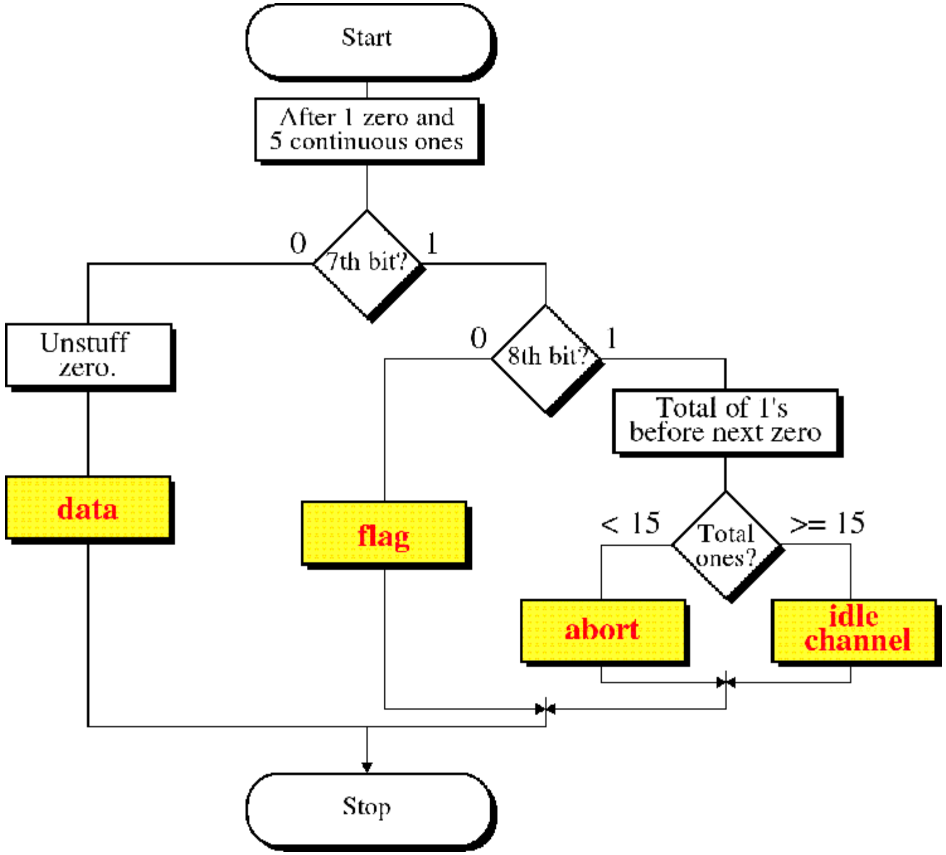
- Other fields
  - Address field
  - Control field: type of frame, sequence number for information frames
  - Information field: multiple of 8 bits
  - Frame check sequence (FCS) field: error checking

- Frame flow
  - Initialization phase, data transfer phase, and disconnect phase

HDLC (cont.)

- Bit stuffing
  - How to differentiate data and flag?
  - Adding one extra 0 whenever there are five consecutive 1s in the data





Other Data Link Control Protocols

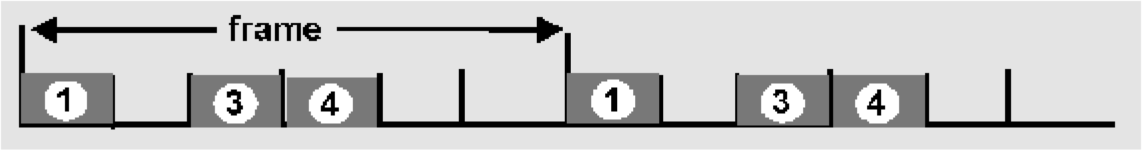
- Link access procedure, balanced (LAPB)
  - Part of X.25 (ITU-T) DTE and packet switching network
  - Full-duplex, point-to-point link between user
  - Subset of HDLC – ABM (Async. Balanced Mode)
  - HDLC frame format
- Link access procedure, D-channel (LAPD)
  - Part of ISDN (ITU-T) and ISDN network
  - ABM
  - Always 7-bit sequence numbers (no 3-bit)
  - 16-bit address field and 16-bit CRC
- Link access procedure for frame (LAPF), mode bearer service
  - High-speed packet switching network on low error rate digital circuits
- Asynchronous transfer mode (ATM)
  - Data transfer on high-speed, digital, error free network

Medium Access Control Protocols

- Network links:
  - Point-to-point: PPP, HDLC, etc
  - Point-to-multipoint (broadcast) :TDMA, CSMA, Token Ring, etc
- Medium access (MA) protocols for a broadcast channel of rate R bps have the following characteristics:
  - When one node is active, throughput is R bps
  - For N nodes, each has average R/N bps over some suitable interval of time
  - Decentralized, no master node
  - Simple and inexpensive
- MA protocol category
  - Channel partitioning
  - Controlled access (taking turn)
  - Random access

Channel partitioning

- Time division multiplexing access (TDMA)
  - Time frame, N time slots
  - Perfectly fair, avoids collisions
  - Poor bandwidth utilization
  - E.g.,: 6-station LAN, 1,3,4 have frame, slots 2,5,6 idle

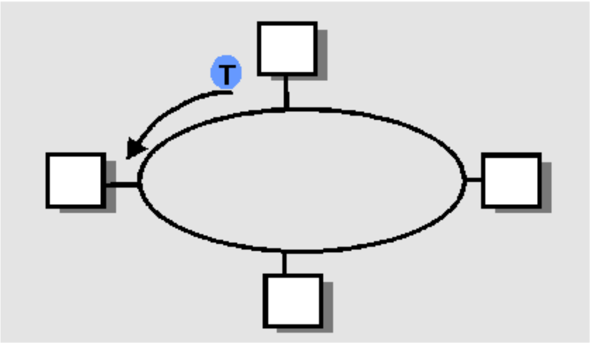


- Frequency division multiplexing access (FDMA)
  - Avoids collisions but poor bandwidth utilization
- Code division multiplexing access (CDMA)
  - CDMA code, orthogonal
  - Chip rate is much faster than transmission rate
  - Encoding, $Z_{i,m} = d_i . c_m$
  - Decoding

$$\frac{1}{M}\sum_{m=1}^{M} Z_{i,m} . c_m$$

Controlled Access

- Controlled access protocol
  - Reservation
  - Polling

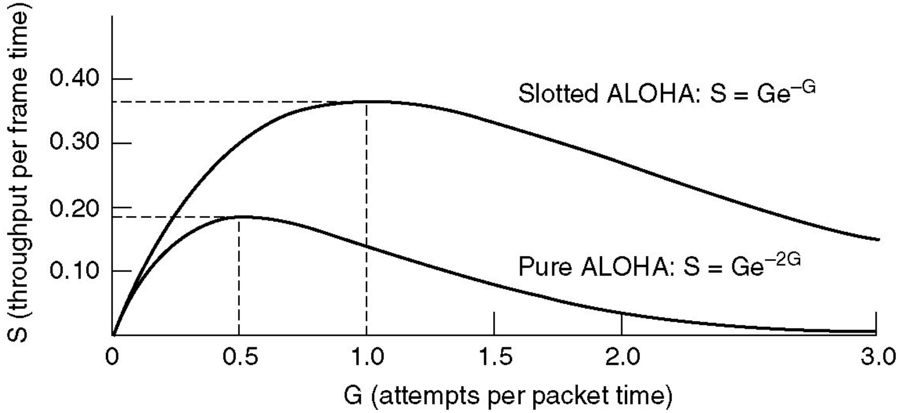


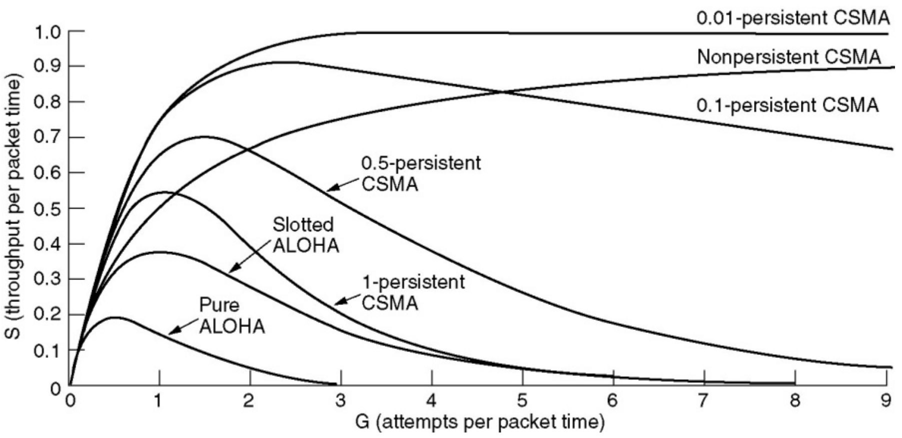
- Token ring
  - Control a token passed from one node to next sequentially
  - Wait for the token
  - Captures the token
  - If it has data frame to send, then send it
  - If allocated time is expired, remove the token, else send more frames

- Fiber distributed data interface (FDDI)
  - The same as token ring, but token is removed by the destination

Random Access

- When there is a collision, sender waits for random length of time and retransmits the frame
  - ALOHA
    - Pure ALOHA efficiency = 0.184
    - Slotted ALOHA efficiency = 0.368
  - Carrier sense multiple access (CSMA)





Carrier Sense Multiple Access

- Listen before talk
- No detection
- Non-persistent
  - Longer delay
- Persistent
  - 1 persistent (Ethernet, CSMA/CD)
  - p persistent (WiFi, CSMA/CA)

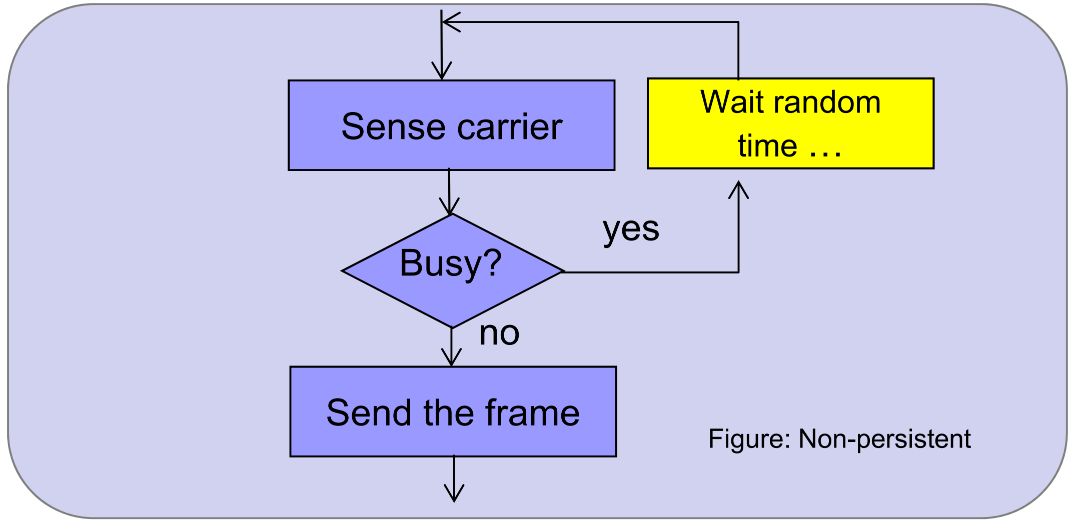


Figure: Non-persistent

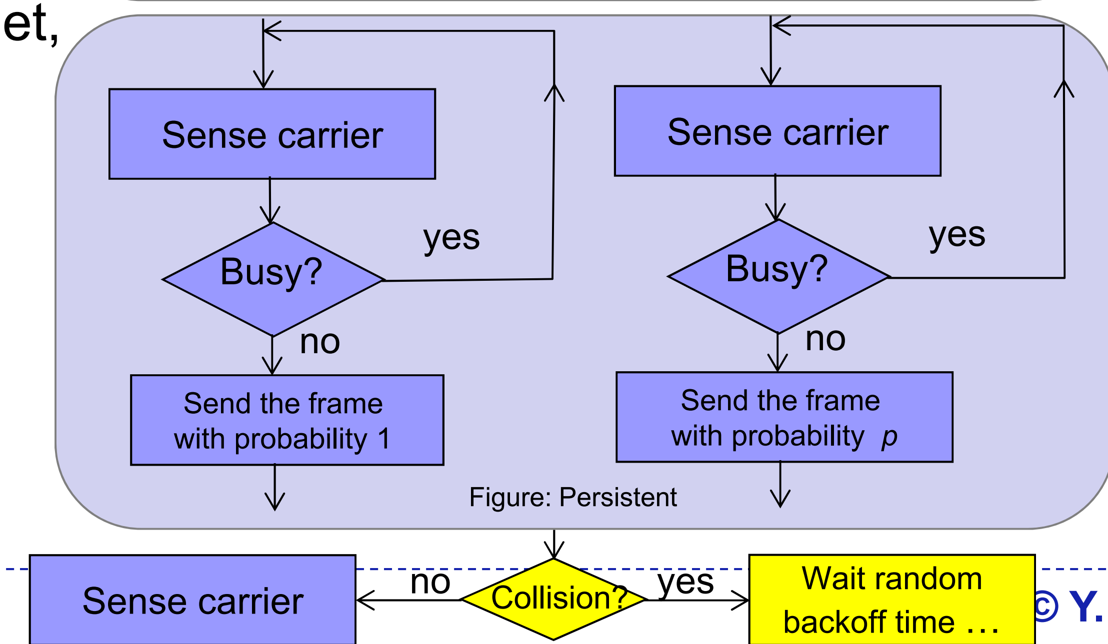


Figure: Persistent

Carrier Sense Multiple Access (cont.)

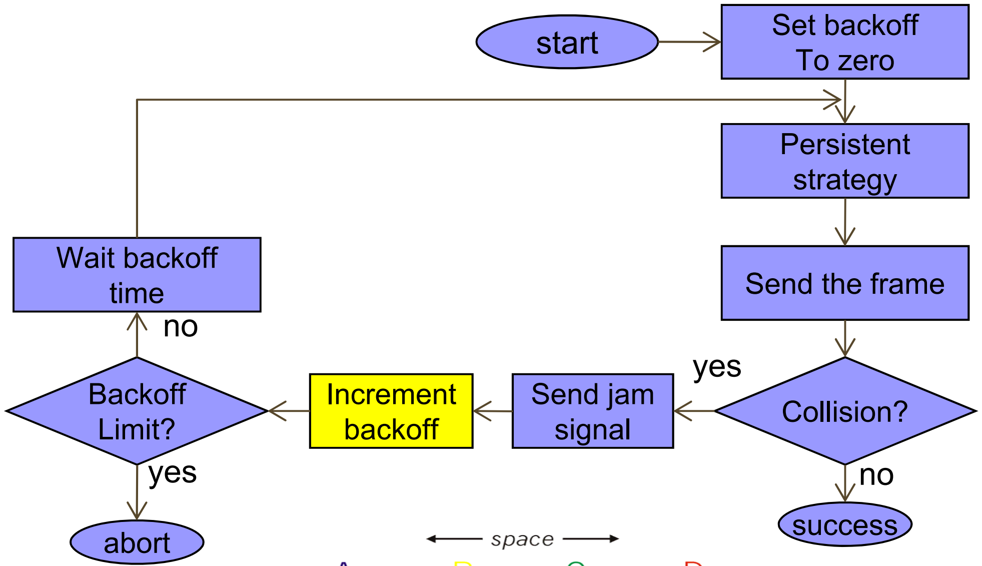
- Non-persistent (detect only once before send a frame)
  - If the channel is busy the station does not continually check it for detecting the end of ongoing transmission. It waits for a random time then checks the channel. If the channel is idle, sends the frame
    - Better channel utilization but longer delay compared to 1–persistent

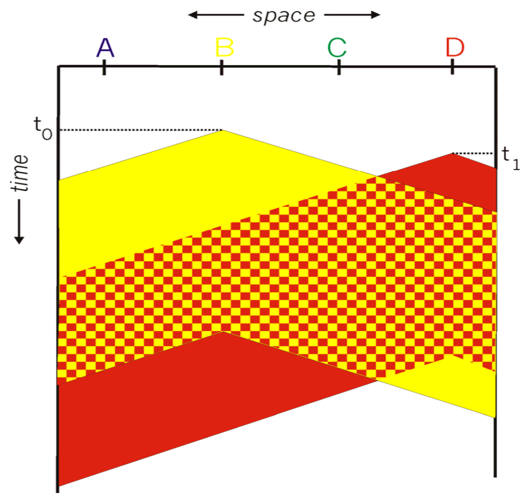
- Persistent (keep detecting before send a frame)
  - 1-persistent (used in CSMA/CD Ethernet): Stations continually checks the channel. If the channel is free sends frame instantly
    - Longer the propagation delay, the protocol performance more worse
    - Even when the delay is 0, collision can be happened. If two stations become ready in the middle of the transmission of a third one, both with start transmitting as soon as they find the channel empty after the 3rd stations transmission is over

  - p-persistent (used in CSMA/CA WiFi): when a station is has data to send, it senses the channel. If it is idle, it transmits with probability p. Otherwise it defers to the next slot with probability q = 1-p. The process repeat until either the frame has been transmitted or another station has begun transmission

CSMA/CD

- First listen, if the channel is busy, use exponential backoff, e.g., 2^N X max_prop_time
- If collision occurs, abort the transmission
- Waits a random period of time, and then tries again
- Why collision?
  - Propagation delay means two nodes may not hear each other's transmission





Local Area Network (LAN)

- In LAN, one broadcast channel
- MAC address (LAN address or physical address), unique
- Most dominant technology is Ethernet
- Address resolution protocol (ARP)
  - Table that resolves LAN address to IP
  - ARP frame is broadcasted (LAN add FF-FF-FF-FF) to get the LAN address of a particular computer with a given IP

IP Address (32 bits)	MAC Address (48 bits)	TTL
111.111.111.111	F0-23-A7-B0-00-3C	20

LAN Operation

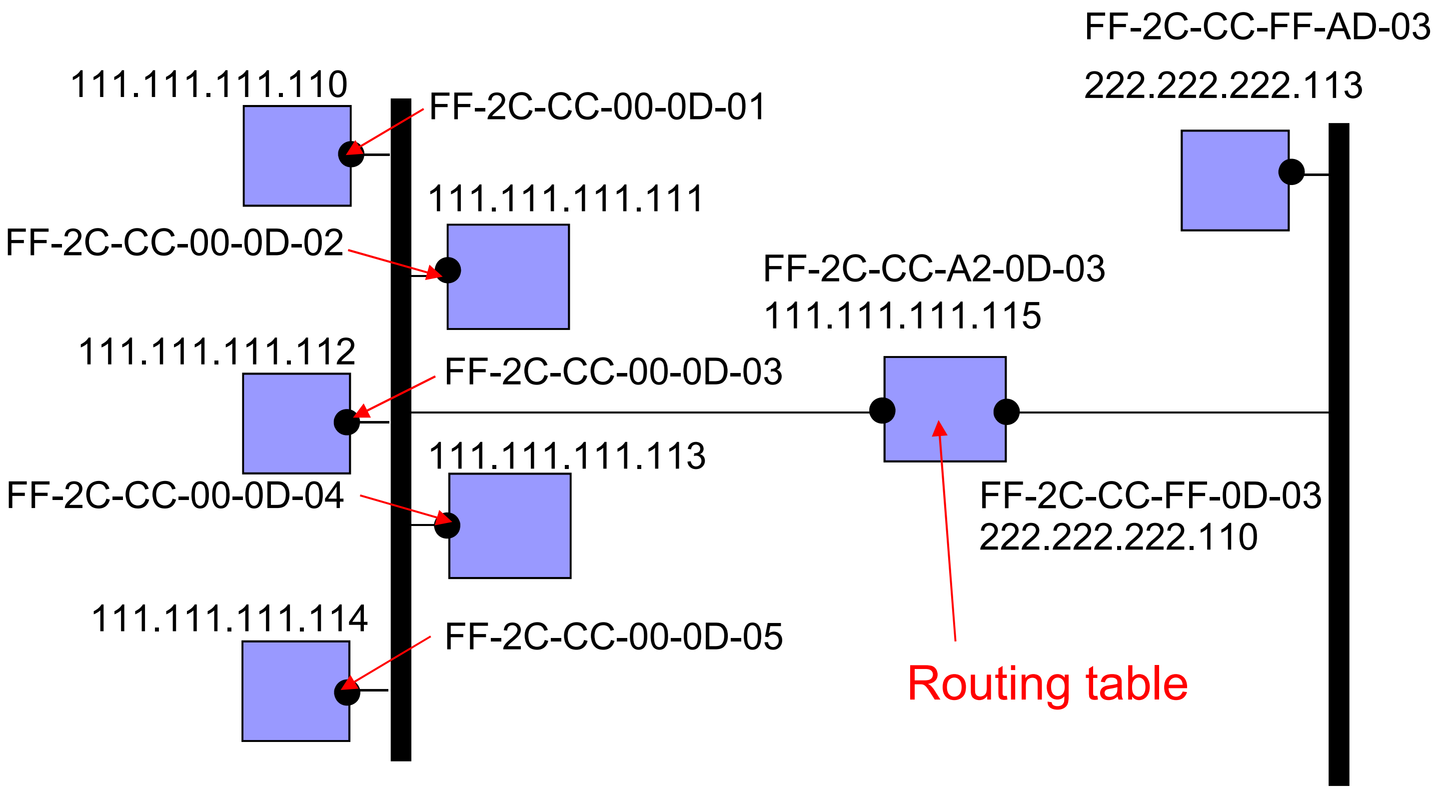


Figure: ARP query packet uses MAC broadcast address

Ethernet

- First developed in 1976, Xerox's Palo Alto Research Center
- Ethernet provides unreliable connection-less service: no handshaking, no ACK
- Data Link Layer
  - Logical Link control (LLC) sublayer
  - Media Access Control (MAC) sublayer
- LAN topology
  - Bus or star
- MAC sublayer
  - Govern the access method
    - Access method: traditional Ethernet uses 1-persistent CSMA/CD
- Ethernet Frame
  - Preamble (7 bytes) – alternating 0, 1
  - Start Field Delimiter (1 byte) – 10101011
  - Destination Address (6 bytes)
  - Source Address (6 bytes)
  - Length/Type of Protocol Data Unit (PDU) (2 bytes)
    - For <1518 it defines the length. If >1536 it defines type
  - Data and Padding (min 46 bytes, max 1500 bytes)
  - CRC (4 bytes)

Ethernet Address

- Embedded into the Network Interface Card (NIC)
- 6-bytes
- Expressed in hex notation. e.g.,:
  - 06-01-02-01-2C-4B
- Unicast or multicast
  - LSB of the first byte 0: unicast
  - LSB of the first byte 1: multicast

Ethernet CSMA/CD Operation

- Adapter obtains a network-layer PDU from its parent node, prepares an Ethernet frame, and puts the frame in the adapter buffer

- If the adapter senses that the channel is idle, it starts to transmit the frame. If the adapter senses that the channel is busy, it waits until it senses no signal energy plus 96 bits time and then transmits the frame

- While transmitting, the adapter monitors for the presence of signal energy from other adapters. If the adapter finds some signal energy from other sources before completing its transmission, it aborts instantly and sends a 48 bit jam signal

- After aborting, the adapter enters into a backoff phase. Specifically, when transmitting a given frame, after experiencing the n collision in for this frame, the adapter chooses a value for K at random from $\{0,1,2, . . ., 2^m-1\}$ where $m := min(n,10).i$ The adapter then waits $K \cdot 512$ bit times

Ethernet CSMA/CD Operation (cont.)

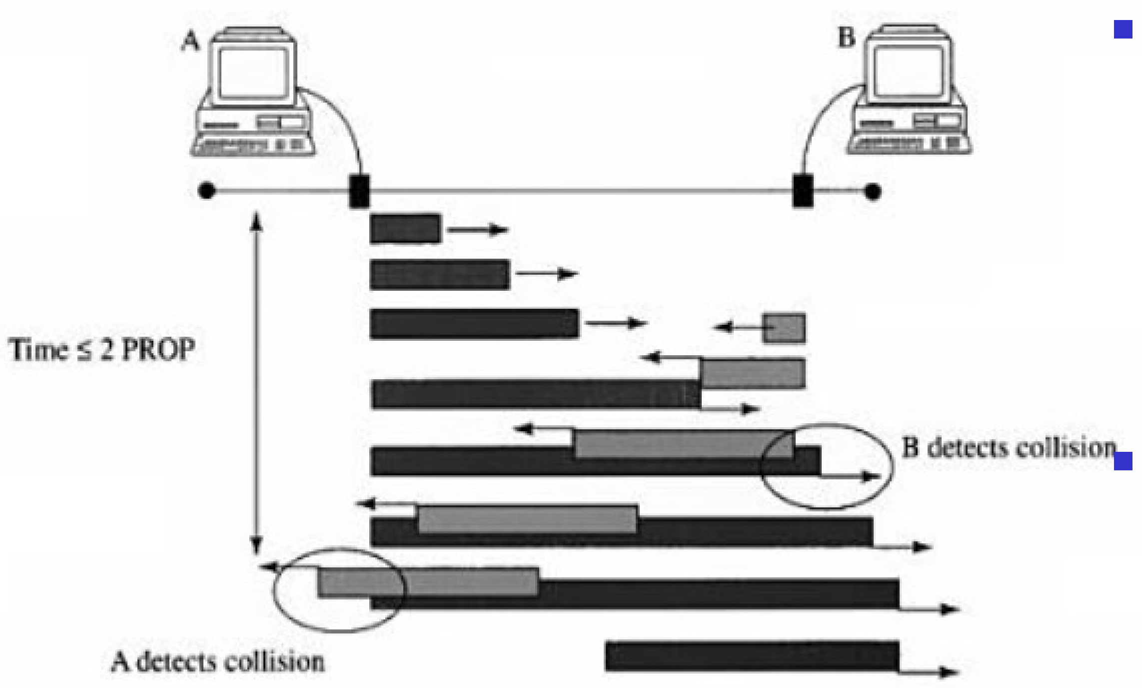
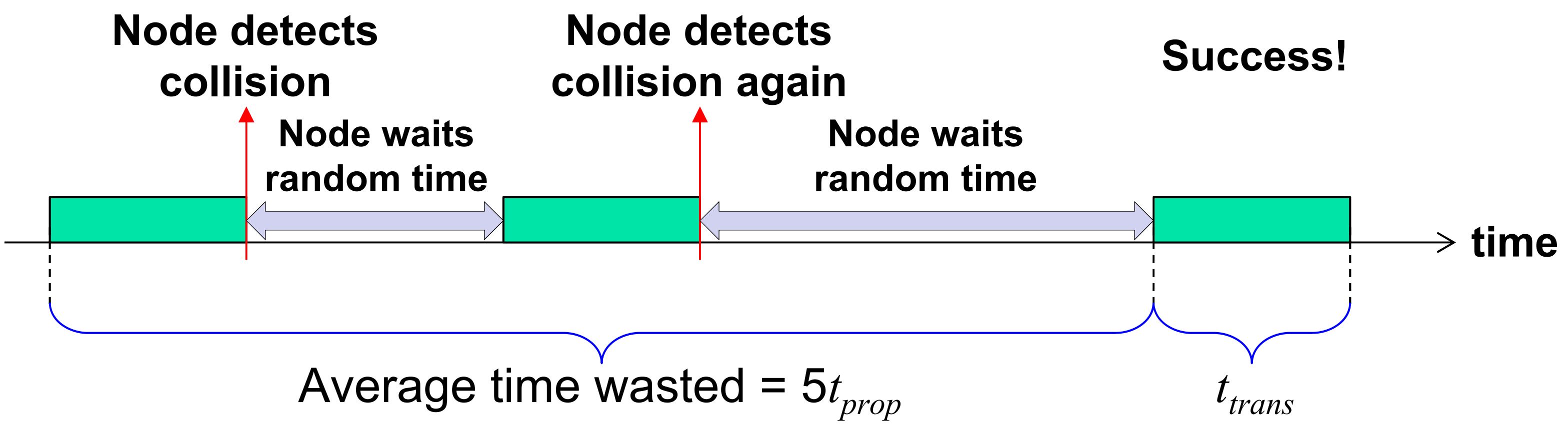


Figure: Maximum time until a node detects a collision is TWICE the propagation time of a signal between the nodes

- CSMA/CD requires that A detects the collision before it has stopped transmitting its frame
  - transmission time of smallest frame > round-trip propagation time
- Ethernet designs the smallest frame is 64 bytes for 2.5 km maximum distance
  - Transmission time of 64-byte is 51.2 μs
  - Propagation time of 2.5-km is 18 μs

Ethernet CSMA/CD Operation (cont.)



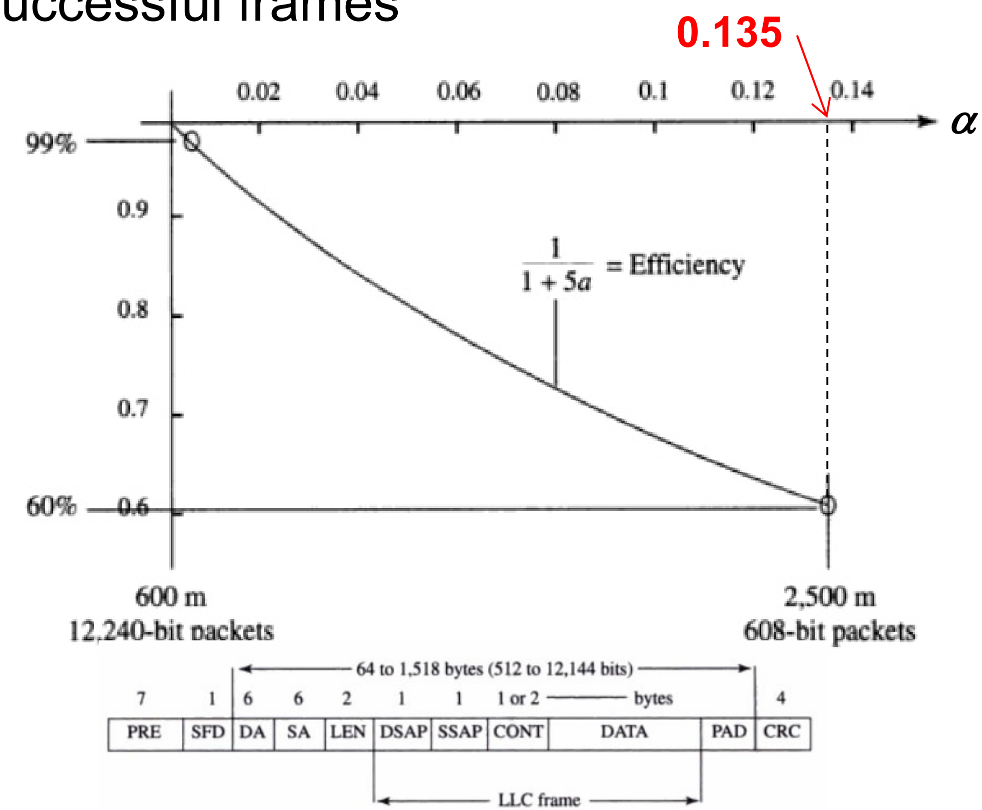
- Figure above shows the sequence of events when a node transmits a frame
- Let t_{prop} denote the max prop delay, t_{trans} be the time to transmit maximum size Ethernet frame
- When many nodes transmit, they waste, an amount of average time = 5 x t_{prop} per successful transmission

Efficiency of the CSMA/CD

- Efficiency (η) drops when the no. of nodes increases
- Typically, the efficiency of 10 Mbps is 80%. This means that 8 Mbps are used to transmit successful frames

$$\eta = \frac{1}{1+5\alpha},$$

$$where\ \alpha = \frac{t_{prop}}{t_{trans}}$$



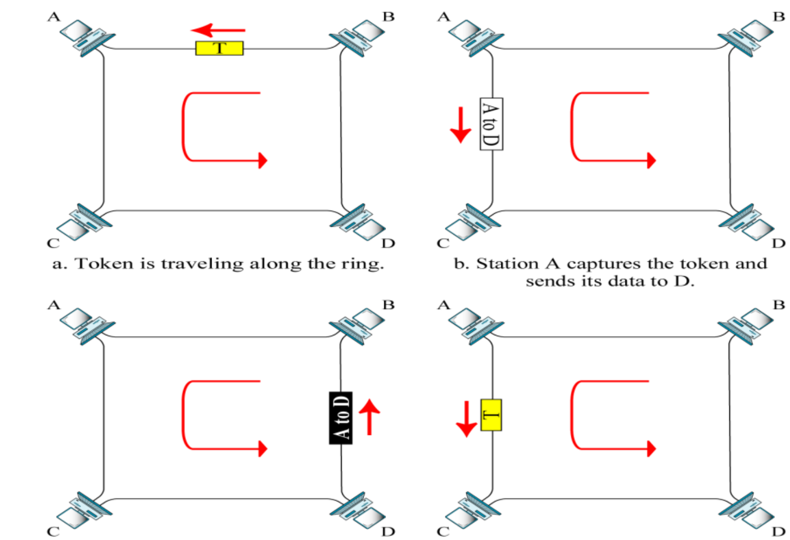
- From graph, α = 0.135, transmission time of 608-bit is 60.8 μs
- Thus, propagation time = α x t_{trans} = 0.135 x 60.8 μs = 8.2 μs

Ethernet Technologies

- 10Base2
  - Coaxial cable, bus topology, 10 Mbps
  - Max node distance is 185m
- 10BaseT
  - Twisted pair copper wire, star topology, 10Mbps
  - Max node distance is 200m
- 100BaseT
  - Category-5 cable
  - Use 4B5B encoding
- Gigabit Ethernet
  - Both fiber and twisted-pair

Token Ring

- Bus topology and collision-free using tokens
- Used for factory automation and process control. Other LANs are not suitable for this purpose
- Token Bus has no commercial application in data communications
- Token Ring allows each station to send one frame per turn
- Access method: Token passing (IEEE802.5 standard)
  - 4 Mbps
  - max token holding time: 10 ms (limits frame length)
  - SD, ED mark start, end of frame
  - AC: access control byte
    - Token bit: value 0 means token can be seized, value 1 means data follows FC
    - Priority bits: priority of frame
    - Reservation bits: station can write these bits to prevent stations with lower priority frame from seizing token after token becomes free



a. Token is traveling along the ring.
b. Station A captures the token and sends its data to D.
c. Station D copies the frame and sends the data back to the ring.
d. Station A receives the frame and releases the token.

SD	AC	FC

SD	AC	FC	dest addr	src addr	data	checksum	ED	FS

Figure: Frame format

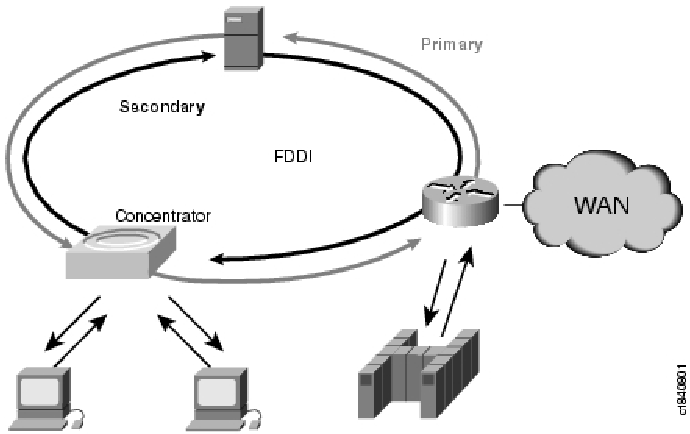
Token Maintenance

- To overcome error conditions, one station is designated as the active monitor
  - Periodically issues an `active_monitor_present` control frame to assure other stations that there is an active monitor on the ring
  - To detect a lost-token condition, the monitor uses a valid-frame timer that is greater than the time required to traverse the ring
  - The timer is reset every valid token or data frame
  - If the time expires, the monitor issues a priority 0 token
  - If it sees a persistently circulating data frame with the monitor bit set, it absorbs it and transmits a priority 0 token
  - No token should circulate completely around the ring at a constant nonzero priority level
  - If the active monitor detects another active monitor, it immediately goes into standby status

- Advantage
  - Flexible control over access that it provides

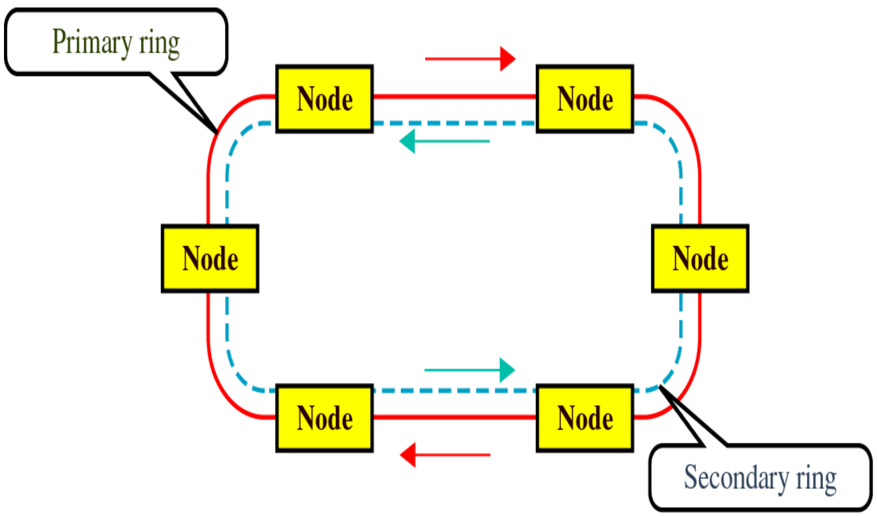
- Disadvantage
  - Requirement for token maintenance
  - Loss of token prevents further utilization of the ring
  - Duplication of the token also disrupt ring operation
  - One station must be selected as monitor to ensure that exactly one token is on the ring and to reinsert a free token if necessary

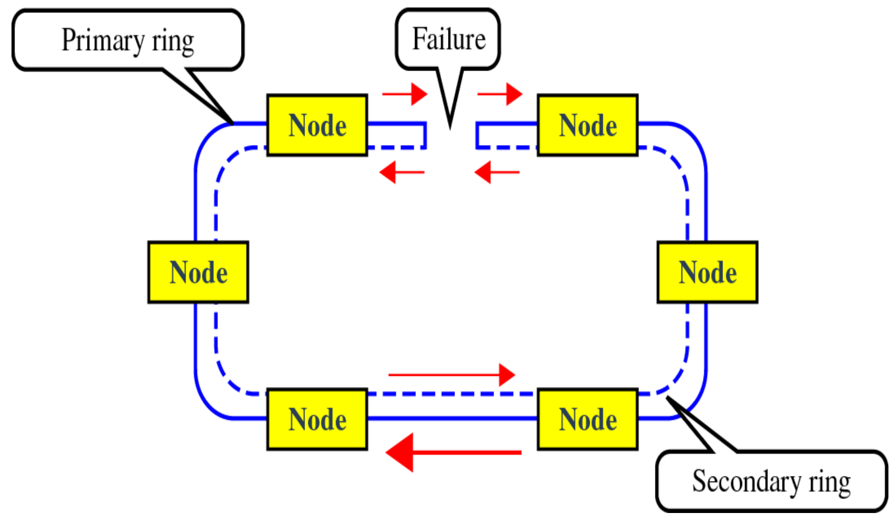
Fiber Distributed Data Interface (FDDI)



- FDDI is standardized by ANSI and ITU-T
  - 100 Mbps token ring LAN/WAN specification
  - Distances of up to 200 km
  - Up to 1000 hosts attached
- Uses optical fiber cabling and CDDI is the copper version of FDDI
- High reliability (dual rings) and immune to interference
- FDDI operation: FDDI modifies the IEEE802.5 protocol
  - To transmit data, a station must first capture the token
  - Then it transmits a frame and removes it when it comes around again
- Difference between FDDI and 802.5 is that in 802.5 a station may not generate a new token until its frame has gone all the way around and come back
  - With FDDI, the amount of time wasted waiting for the frame is substantial due to the large distances. For this reason, a station is allowed to put a new token back onto the ring as soon as it has finished transmitting its frame

FDDI Dual Ring Operation





- FDDI consists of 2 counter-rotating rings
- In the even of failure of both rings at one point, the two rings can joined together to form a single long ring

Comparison

Network	Access Method	Signaling	Data Rate	Error Control
Ethernet	CSMA/CD	Manchester	1, 10 Mbps	No
Fast Ethernet	CSMA/CD	Several	100 Mbps	No
Gigabit Ethernet	CSMA/CD	Several	1 Gbps	No
Token Ring	Token passing	Differential Manchester	4, 16 Mbps	Yes
FDDI	Token passing	4B/5B, NRZ-I	100 Mbps	Yes

Announcement

- Next is Chapter 4 Network Layer I
- 09:00 ~ 10:40 on 24 October (Monday)