Data-Link Layer

Dr. Miled M. Tezeghdanti

November 12, 2010

Data Link Layer Functions

- Framing
- Error Control
- Flow Control

Framing

- Framing is the process of locating the beginning and end of a message, at the receiving end of a link
- Framing Mechanisms
  - Character counter
  - Start Character and End Character with "Character stuffing"
  - Start Flag and End Flag with "Bit Stuffing"
    - Transparency with used encoding (ASCII, EBCDIC)
  - Violation of Physical layer encoding
    - Start and End of the frame are represented with symbols that are different from symbols used for bits 0 and 1
    - Manchester Encoding 0: Bottom-Up Transition 1: Top-Down Transition Start and End of the frame: continuous signal

Character Counter - Example

Decimal Data: 210-197-113-90

Hexadecimal Data: 0xD2-0xC5-0x71-0x5A

Binary Data: 11010010-11000101-01110001-01011010

Transmission Order: Bytes: letf to right, bits: right to left

Data on the Wire: 01001011-10100011-10001110-01011010

Frame
00100000010010111010001110001110010110 10
Length Data

Byte Stuffing - Example 1

Decimal Data: 210-197-113-90

Hexadecimal Data: 0xD2-0xC5-0x71-0x5A

Binary Data: 11010010-11000101-01110001-01011010

Transmission Order: Bytes: letf to right, bits: right to left

Data on the Wire: 01001011-10100011-10001110-01011010

Frame
01111110010010111010001110001110010110100111110
Start Flag Data End Flag

Byte Stuffing - Example 2

Decimal Data: 210-126-113-90

Hexadecimal Data: 0xD2-0x7E-0x71-0x5A

Binary Data: 11010010-01111110-01110001-01011010

Transmission Order: Bytes: letf to right, bits: right to left

Data on the Wire: 01001011-10111110-01111010-10001110-01011010

Frame Stuffed Byte
01111110010010111011111001111010100011100101101001111110
Start Flag Data End Flag

Byte Stuffing - Example 3

Decimal Data: 210-125-113-90

Hexadecimal Data: 0xD2-0x7D-0x71-0x5A

Binary Data: 11010010-01111101-01110001-01011010

Transmission Order: Bytes: letf to right, bits: right to left

Data on the Wire: 01001011-10111110-10111010-10001110-01011010

Frame Stuffed Byte

01111110010010111011111010111010100011100101101001111110

Start Flag Data End Flag

Bit Stuffing - Example 1

Decimal Data: 210-197-113-90

Hexadecimal Data: 0xD2-0xC5-0x71-0x5A

Binary Data: 11010010-11000101-01110001-01011010

Transmission Order: Bytes: letf to right, bits: right to left

Data on the Wire: 01001011-10100011-10001110-01011010

Frame

01111110010010111010001110001110010110100111110

Start Flag Data End Flag

Bit Stuffing - Example 2

Decimal Data: 210-126-113-90

Hexadecimal Data: 0xD2-0x7E-0x71-0x5A

Binary Data: 11010010-01111110-01110001-01011010

Transmission Order: Bytes: letf to right, bits: right to left

Data on the Wire: 01001011-01111110-10001110-01011010

Frame Stuffed Bit

01111110010010111111010100011100101101001111110

Start Flag Data End Flag

Bit Stuffing - Example 3

Decimal Data: 210-71-113-90

Hexadecimal Data: 0xD2-0x47-0x71-0x5A

Binary Data: 11010010-01000111-01110001-01011010

Transmission Order: Bytes: letf to right, bits: right to left

Data on the Wire: 01001011-11100010-10001110-01011010

Frame Stuffed Bit

01111110010010111110000101000111001011010 01111110

Start Flag Data End Flag

Error Control

- Single Error
  - Single bit inversion
  - 01001101 $\longrightarrow$ 01001001
- Double Error
  - Two bit inversions
  - 01001101 $\longrightarrow$ 01011001
- Burst Error: A burst error is a group of bits in which the first bit and the last bit are in error and the intervening bits may or may not be in error.
  - Many successive corrupted bits
  - 01001101 $\longrightarrow$ 00010111
- Transmission errors are caused by noise present in the communication channel

Error Detection

- How can we be sure that the received frame does not contain errors?
- Possible Solutions:
  - Send frame twice (or many times)
    - Bandwidth wasting
    - More delay to wait for the second frame
  - Send double copies of data in the same frame.
    - Bandwidth wasting
  - Use algorithms that can detect errors by adding control information (small size) to the frame.
    - Efficient Solution
    - Depends on the used algorithm

Parity

- Segment data in blocks of m bits
- Count the number of bits that are set to 1 in each block of m bits and add a parity bit at the end of each block.
  - If the number is odd, add bit 1 to the end of the block.
  - If the number is even, add bit 0 to the end of the block
- Send blocks of $(m + 1)$ bits
- It is the easiest method to detect single errors.
  - Each single error is detected
  - All odd multiple errors are detected
  - All even errors are not detected
- Problem: Parity bit inversion!

Parity

- Single Error
  - 0100110101000111 $\longrightarrow$ 0100110101010111
- Double Error
  - 0100110101000111 $\longrightarrow$ 0100110001010111
- Detected Multiple Errors
  - 0100110101000111 $\longrightarrow$ 0100100001010111
- Parity Bit Inversion
  - 0100110101000111 $\longrightarrow$ 0100110101000110

m-out-of-n Code

- With n bits, we can represent 2^n symbols
- If we reduce the number of useful symbols, non-used configurations may be used for error detection
- Encoding is selected in order that an error change a useful symbol to no-used symbol
- It is not an economic encoding but it is easy to implement

m-out-of-n Code

- Example
  - 2-out-of-5 code
    - 11000
    - 10100
    - 10010
    - 10001
    - 01100
    - 01010
    - 01001
    - 00110
    - 00101
    - 00011
  - Every single error is detectable
  - Double error is not detectable

Polynomial Codes

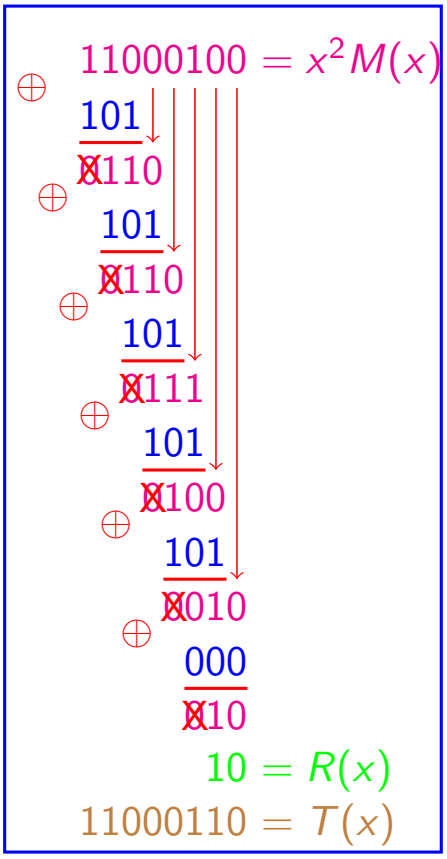
- For each m bits sequence, determine corresponding polynomial of degree $(m-1)$ and with 0 and 1 as coefficients
- Example
  - 11001101
  - 11001101
    - Corresponding Polynomial
    - $P(x) = 1 * x^7 + 1 * x^6 + 0 * x^5 + 0 * x^4 + 1 * x^3 + 1 * x^2 + 0 * x^1 + 1 * x^0$
    - $P(x) = 1 * x^7 + 1 * x^6 + 1 * x^3 + 1 * x^2 + 1 * x^0$
- Addition and subtraction are identical to the XOR operator

Polynomial Codes

- Sender and receiver must agree upon a generator polynomial of the form: $G(x) = x^r + \ldots + 1$
- Algorithm:
  - For each frame of m bits, compute corresponding polynomial $M(x)$
  - Add r zero bits at the end of the frame, corresponding polynomial becomes $x^r M(x)$
  - Divide $x^r M(x)$ by $G(x)$, $R(x)$ is the remainder of the division
  - The frame to transmit is $T(x) = x^r M(x) - R(x)$
  - $T(x)$ is divisible by $G(x)$
  - Receiver must check that the received frame is divisible by $G(x)$

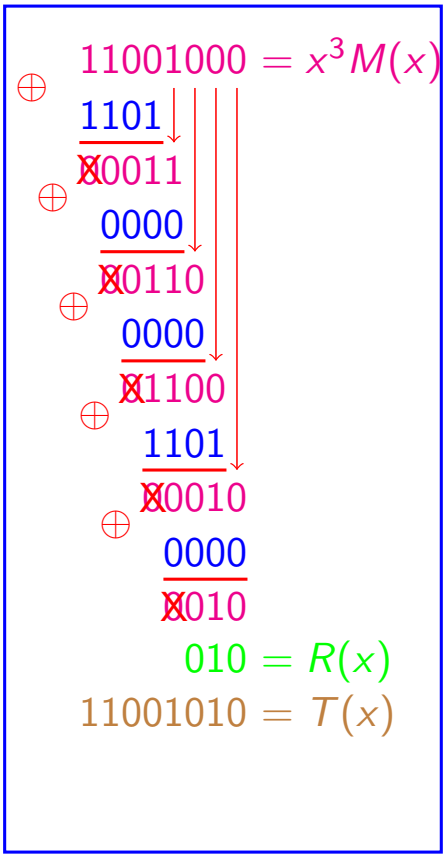
Polynomial Codes

- Example ($r = 2$)
  - $G(x) = x^2 + 1 = 101$
  - Message to transmit 110001
    - $M(x) = x^5 + x^4 + 1$
    - $x^2M(x) = x^7 + x^6 + x^2 = 11000100$
    - $R(x) = x = 10$
    - $T(x) = x^7 + x^6 + x^2 + x = 11000110$
  - Frame to transmit 11000110



Polynomial Codes

- Example ($r = 3$)
  - $G(x) = x^3 + x^2 + 1 = 1101$
  - Message to transmit 11001
    - $M(x) = x^4 + x^3 + 1$
    - $x^3M(x) = x^7 + x^6 + x^3 = 11001000$
    - $R(x) = x = 10$
    - $T(x) = x^7 + x^6 + x^3 + x = 11001010$
  - Frame to transmit 11001010



Polynomial Codes

- Good choice of $G(x)$ allows the detection of:
  - All single errors
    - If $G(x)$ contains two non-zero terms
  - All double errors
    - If $G(x)$ is not divisible by X and $(X^r + 1)$
- Example
  - CRC-16 (Cyclic Redundancy Check)
    - $G(x) = x^{16} + x^{15} + x^2 + 1$
  - CRC-CCITT
    - $G(x) = x^{16} + x^{12} + x^5 + 1$
- CRC is generally computed by Hardware

Error Detection Proporties of CRC-16

- The CRC-16 polynomial has the following error detection properties:
  1. It will detect all errors that change an odd number of bits
  2. It will detect all errors that change two bits provided that the block length is less than 32767 bits including the CRC bits
  3. It will detect all errors that consist of a single burst error of 16 or fewer bits
  4. It will detect all errors that consist of two occurrences of two adjacent bits in error provided that the block length is less than 32767 bits including the CRC bits
  5. It will detect all except the fraction $\frac{1}{2^{15}}$ of errors that consist of a single burst error of 17 bits
  6. It will detect all except the fraction $\frac{1}{2^{16}}$ of errors that consist of a single burst error of 18 or more bits
  7. It will not detect some errors that change four bits. For example, it will not detect the error pattern that is identical to the CRC polynomial.

Error Correction

- When an error is detected
  - Ask the sender to retransmit the frame
  - Correct the frame
- Detection does not mean correction
  - When we detect an error in a frame, this means that this frame contains an error but we can't determine which bits are in error
- If we can determine which bits are in error, we can correct them
  - Two possible values
  - To correct a bit in error, we have only to invert it

Hamming Code

- Hamming Distance
  - Number of bits that are different between two words of the code
  - Example
    - A = 01001101, B = 01001001, Hamming Distance = 1
    - A = 01001101, B = 11001001, Hamming Distance = 2
- Hamming Code
  - Number bits beginning from left and from 1
  - Bits that are power of 2 are control bits $(1, 2, 4, 8, 16, \ldots)$
  - Other bits are data bits
  - Control bit number 2^r is a parity bit over data bits that they have non-zero coefficient for 2^r in their binary representation
  - If the receiver notices that control bits i, j, and k are wrong then the data bit (i + j + k) is inverted

Hamming Code

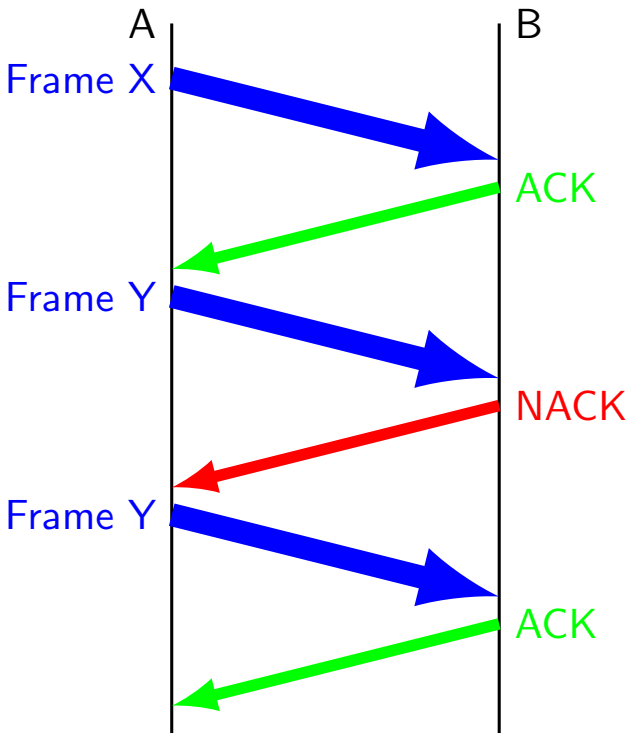
- Example
  - Byte Transmission
  - Control bits are 1, 2, 4, and 8
  - Data bits are 3, 5, 6, and 7
  - Data to transmit
    - $ab0c110d$
  - Binary Decomposition
    - $3 = 1 + 2, 5 = 1 + 4, 6 = 2 + 4, 7 = 1 + 2 + 4$
  - $a = parity(3, 5, 7) = parity(0, 1, 0) = 1$
  - $b = parity(3, 6, 7) = parity(0, 1, 0) = 1$
  - $c = parity(5, 6, 7) = parity(1, 1, 0) = 0$
  - $d = parity() = parity() = 0$
  - $11001100 \longrightarrow 11001000; 2 + 4 = 6$ (bit 6 is inverted)

Acknowledgement Mechanism

- How the sender could be sure that the receiver has received the frame?
- Perfect Transmission Channel
  - No Noise (No Error)
  - No Failure (No Loss)
  - Good Synchronization
    - Each transmitted frame is always correctly received by the receiver
- Reality is different!

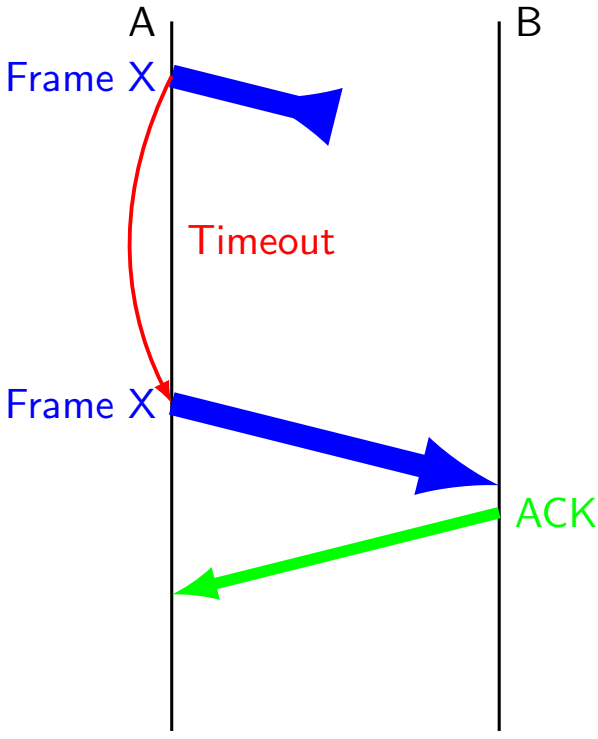
Send-and-Wait

- The sender transmits the frame and waits from the acknowledgement from the receiver
- The acknowledgement may be positive or negative (if the frame contains errors)
- When the acknowledgement is negative, the sender retransmits the frame
- Easy to implement



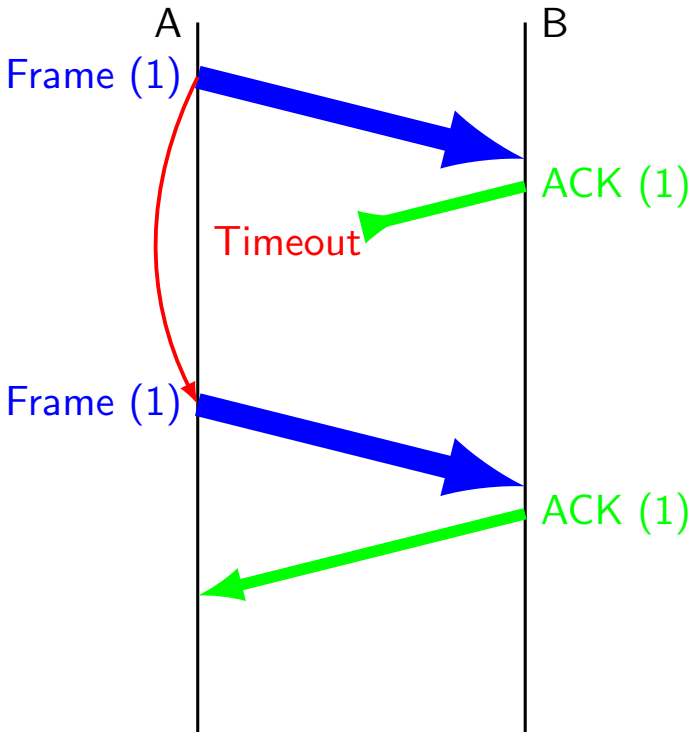
Loss Management

- What we have to do when the frame does not arrive to the receiver?
- Solution
  - Use of a timer
    - If the sender does not receive an acknowledgement before the timer expiration, he retransmits the frame.
    - Waiting time before retransmission must be precisely selected



Duplicates Management

- When the acknowledgement does not arrive to the sender, the latter will retransmit the same frame which will be received twice by the receiver
  - How the receiver can know that it is the same frame?
- Solution
  - Frame Numbering (Sequence Number)



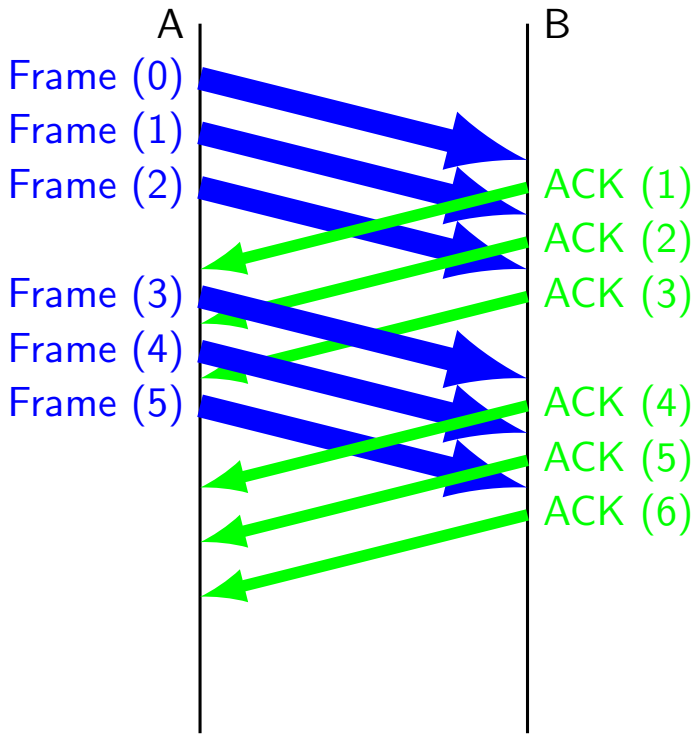
Send-and-Wait

- Performances
  - Sender spends half of the time waiting for the acknowledgement
  - Under-use of transmission channel bandwidth
  - Performances depend on
    - The size of the frame
    - The error probability over the channel
    - The loss probability

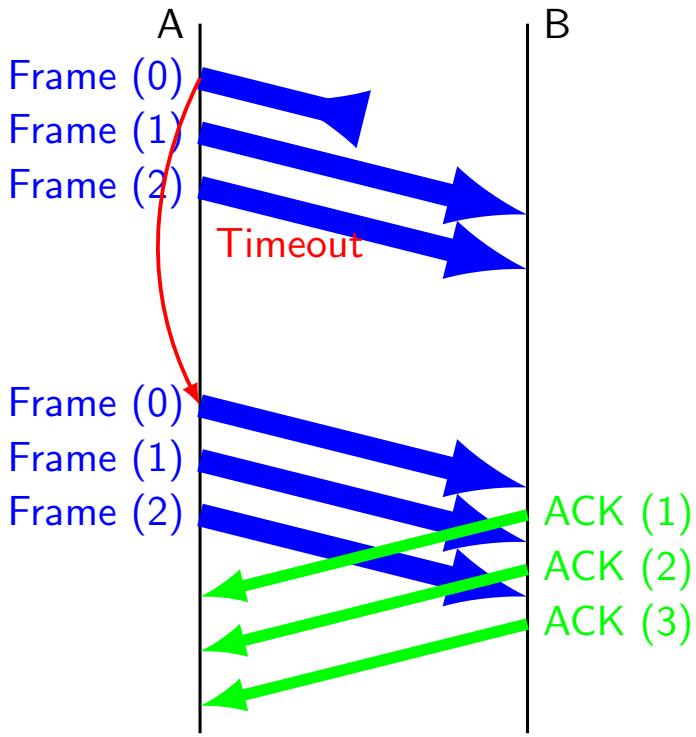
Go-Back-N

- Enhance performances of Send-and-Wait protocol
  - Ability to send one or many frames without receiving an acknowledgement for the last transmitted frame
  - Frames and Acknowledgements are numbered
  - Acknowledgement number N acknowledges all frames that their number is little than N
    - Savings on the number of acknowledgements to be sent
  - The number of frames that the sender can send without receiving an ACK is limited
  - When a frame is lost, all next frames must be retransmitted

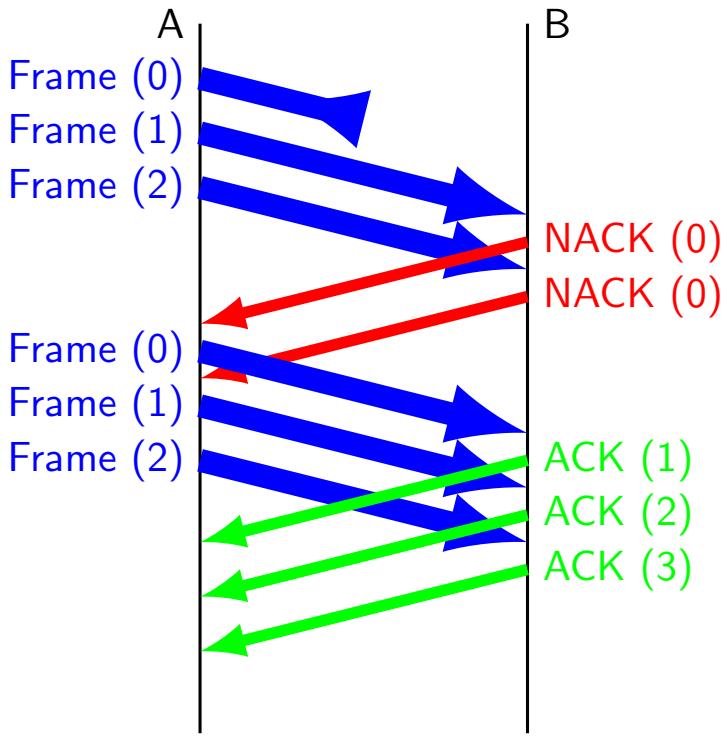
Go-Back-N



Go-Back-N



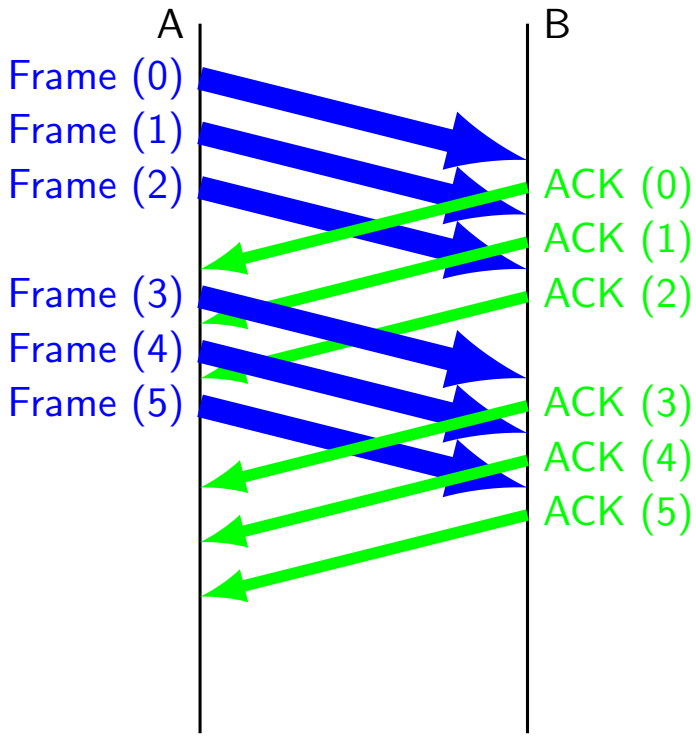
Go-Back-N with Negative Acknowledgement



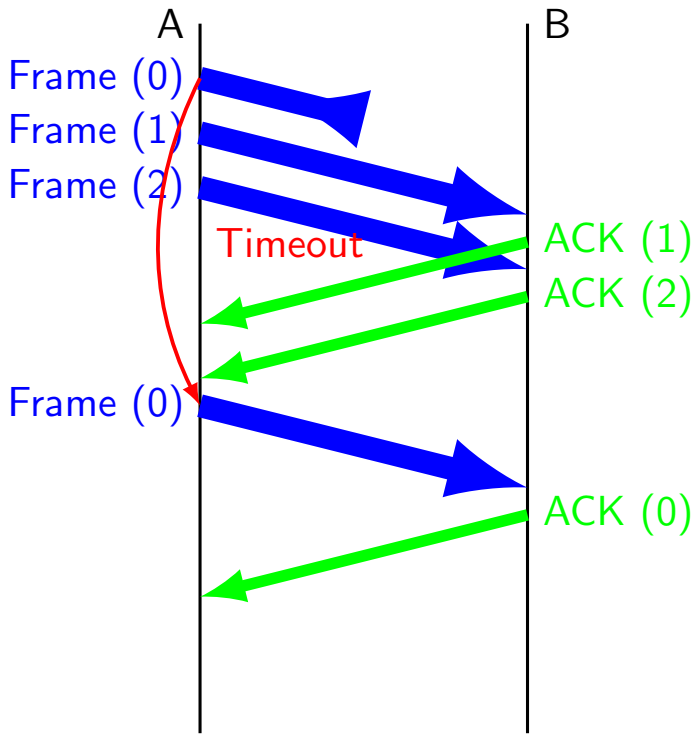
Selective-Repeat

- Enhance performances of Go-Back-N
  - Each frame is acknowledged with its proper ACK
  - When a frame is lost, only the lost frame will be retransmitted after timer expiration
  - Next frames will not be retransmitted

Selective-Repeat



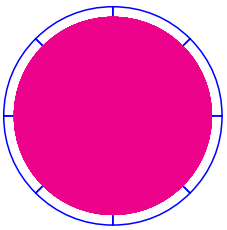
Selective-Repeat

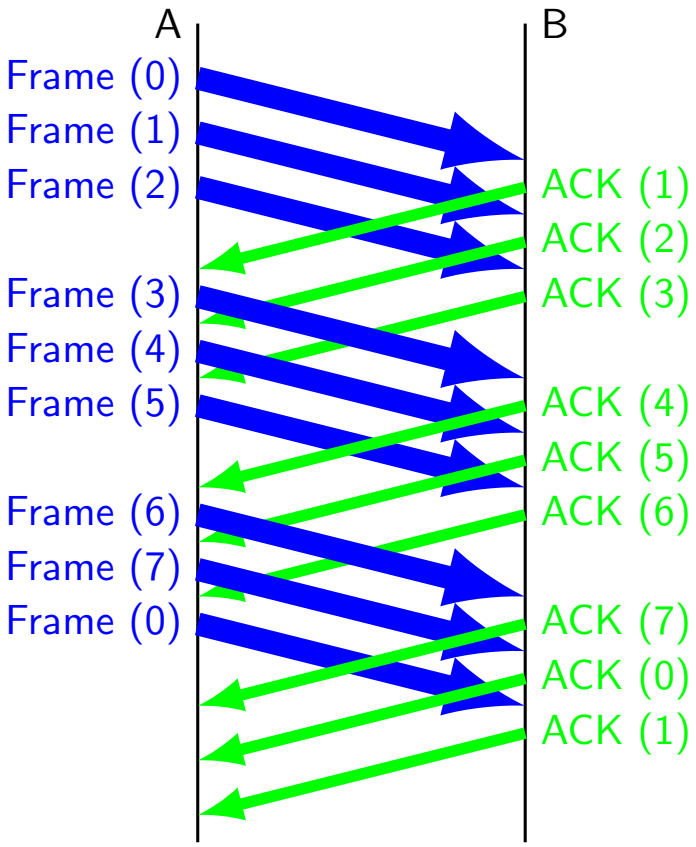


Flow Control

- How many frames can the source send without receiving acknowledgements from the receiver?
  - Bandwidth of the transmission channel
  - Ability of the receiver to handle transmitted frames
- Sliding Window Mechanism
  - The maximal number of transmitted frames and not yet acknowledged is limited by the size (width) of the window
  - Window Size (Width) may be
    - Statically fixed from the beginning
    - Static and negotiated between sender and receiver
    - Dynamic and negotiated between sender and receiver

Sliding Window





HDLC

- High-level Data Link Control
- HDLC is a Data-Link protocol designed by ISO
- HDLC provides a reliable connection oriented service

Frame Format

Frame Format

- Flag: 01111110
  - Frame Delimitation
  - What if data contains the sequence 01111110?
  - Bit Stuffing
    - Insertion of 0 after 5 successive 1 bits
    - Receiver discards every 0 coming after 5 successive 1 bits
      $01111110 \longrightarrow 011111010 \longrightarrow 01111110$
      $01111100 \longrightarrow 011111000 \longrightarrow 01111100$
    - Transparency with used encoding (ASCII, EBCDIC)

Frame Format

- Address (8 bits)
  - Point-to-point : we need two addresses
- Command (8 bits)
  - Different types of frames
- Information
  - Empty if it is a control frame
- FCS (16 bits)
  - Over entire frame except transparency bits and flags

FCS Generation

- At the sender the FCS is computed as the sum (xor) of the following three terms:
  - The remainder of the division (modulo 2) of $I(x) = x^k(x^{15} + x^{14} + \ldots + x + 1) by G(x)$
  - The remainder of the division (modulo 2) of $x^{16}M(x) by G(x)$
  - $x^{15} + x^{14} + \ldots + x + 1$
- The FCS is transmitted as a 16-bit sequence with higher order coefficient first, so the polynomial transmitted is: $x^{16}M(x) + FCS(x)$

Order of Transmission

- The elements of the frame should be transmitted as follows:
  - Opening Flag
  - Address field
  - Control field
  - Information field when present
  - Frame Check Sequence
  - Closing Flag
- Address and Control fields shall be transmitted least significant bit first
- FCS shall be transmitted higher coefficient bit first
- The order of bit transmission within the Information field is not specified by this standard

Frame Types

- 3 types of Frames
  - I : Information Frame
    - Data Transport
  - S : Supervisory Frame
    - Acknowledgement
  - U : Unnumbered Frame
    - Setup and Release of the Connection

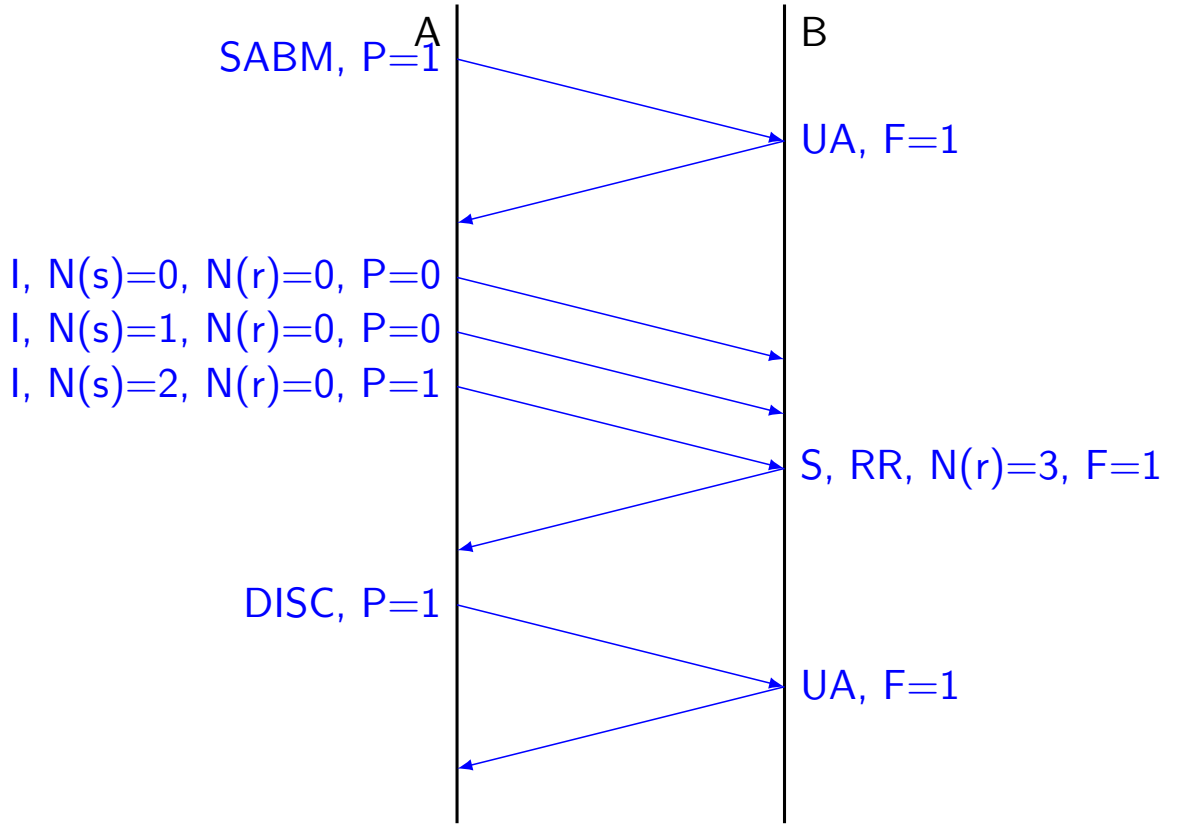
U Frame

- SABM(E)
  - (Set Asynchronous Balanced Mode (Extended)) :
  - Used to setup a connection, it cannot contain data (7 bits for Sequence Number in SABME)
- DISC (Disconnect) :
  - Ends a connection established with SABM(E)
- UA (Unnumbered Acknowledgement) :
  - Acknowledges SABM(E) and DISC frames
- DM (Disconnect Mode) :
  - Used to indicate the disconnection state of a station, it is used particularly as a negative response to SABM(E)
- FRMR (Frame Reject) :
  - Sent as response to a non conforming frame (reception of a corrupted command frame)

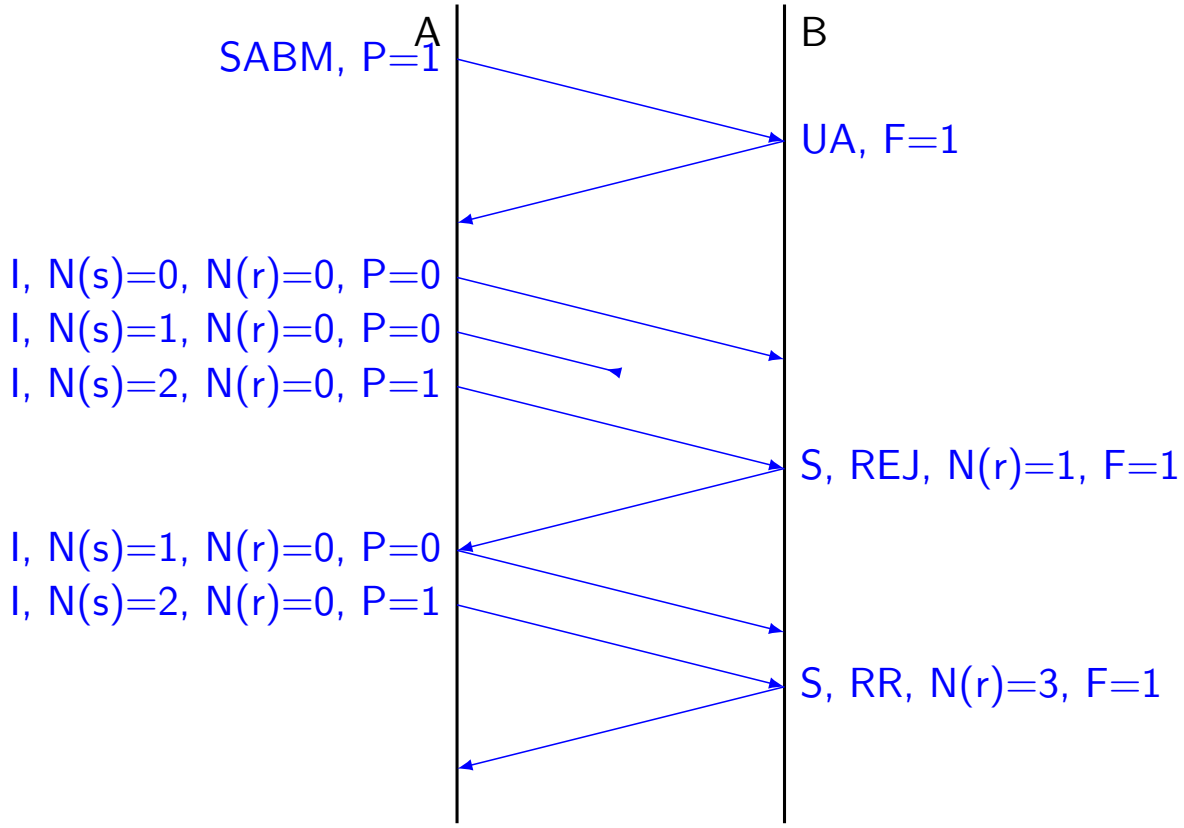
Control Field

		Control Field Bits							
Bit Order		1	2	3	4	5	6	7	8
I Frame		0	N(s)			P	N(r)		
S Frame	RR	1	0	0	0	P/F	N(r)		
	REJ	1	0	0	1	P/F	N(r)		
	RNR	1	0	1	0	P/F	N(r)		
	SREJ	1	0	1	1	P/F	N(r)		
U Frame	SABM	1	1	1	1	P	1	0	0
	DM	1	1	1	1	F	0	0	0
	DISC	1	1	0	0	P	0	1	0
	UA	1	1	0	0	F	1	1	0
	FRMR	1	1	1	0	F	0	0	1

HDLC


A
B
SABM, P=1
UA, F=1
I, N(s)=0, N(r)=0, P=0
I, N(s)=1, N(r)=0, P=0
I, N(s)=2, N(r)=0, P=1
S, RR, N(r)=3, F=1
DISC, P=1
UA, F=1

HDLC


A
B
SABM, P=1
UA, F=1
I, N(s)=0, N(r)=0, P=0
I, N(s)=1, N(r)=0, P=0
I, N(s)=2, N(r)=0, P=1
S, REJ, N(r)=1, F=1
I, N(s)=1, N(r)=0, P=0
I, N(s)=2, N(r)=0, P=1
S, RR, N(r)=3, F=1