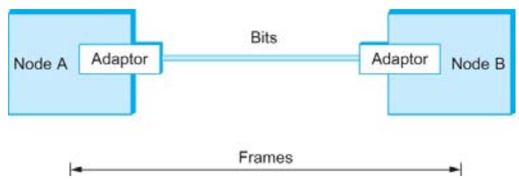
# Framing

Chapter 2

- We are focusing on packet-switched networks, which means that blocks of data (called *frames* at this level), not bit streams, are exchanged between nodes.
- It is the network adaptor that enables the nodes to exchange frames.




Bits flow between adaptors, frames between hosts

1

# Framing

Chapter 2

- When node A wishes to transmit a frame to node B, it tells its adaptor to transmit a frame from the node's memory. This results in a sequence of bits being sent over the link.
- The adaptor on node B then collects together the sequence of bits arriving on the link and deposits the corresponding frame in B's memory.
- Recognizing exactly what set of bits constitute a frame—that is, determining where the frame begins and ends—is the central challenge faced by the adaptor

2

## Framing

Chapter 2

- Byte-oriented Protocols
  - To view each frame as a collection of bytes (characters) rather than bits
  - BISYNC (Binary Synchronous Communication) Protocol
    - Developed by IBM (late 1960)
  - DDCMP (Digital Data Communication Protocol)
    - Used in DECNet

MK MORGAN KAUFMANN 3

## Framing

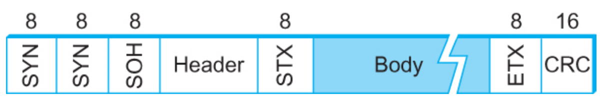
Chapter 2

- BISYNC – sentinel approach
  - Frames transmitted beginning with leftmost field
  - Beginning of a frame is denoted by sending a special SYN (synchronize) character
  - Data portion of the frame is contained between special sentinel character STX (start of text) and ETX (end of text)
  - SOH : Start of Header
  - DLE : Data Link Escape
    - Used to preceede a data portion that is equivalent to ETX
    - Used to precede a data portion that is equivalent to DLE
  - CRC: Cyclic Redundancy Check

MK MORGAN KAUFMANN 4

## Framing

Chapter 2




BISYNC Frame Format



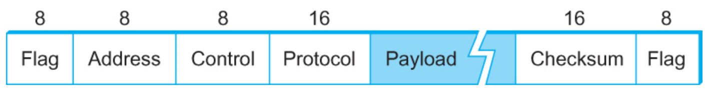
## Framing (point-to-point protocol)

Chapter 2

- Recent PPP which is commonly run over Internet links uses sentinel approach
  - Special start of text character denoted as Flag
    0 1 1 1 1 1 1 0
  - Address, control : default numbers
  - Protocol for demux : IP / IPX
  - Payload : negotiated (default:1500 bytes)
  - Checksum : for error detection
  - Several field sizes negotiated – Link control protocol (LCP)

## Framing






PPP Frame Format



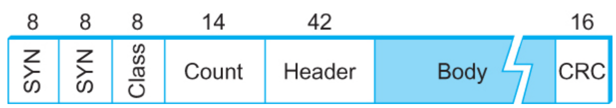
## Framing



- Byte-counting approach
  - DDCMP (Digital Data Communication Message Protocol)
  - *count* : how many bytes are contained in the frame body
  - If *count* is corrupted
    - Framing error
    - Usually results in back-to-back frames received in error

# Framing






DDCMP Frame Format



# Framing



- Bit-oriented Protocol
  - HDLC : High Level Data Link Control
    - Beginning and Ending Sequences
      0 1 1 1 1 1 1 0
    - Send 0 1 1 1 1 1 1 0 when idle


HDLC Frame Format

## Framing

Chapter 2

- HDLC Protocol – Sending Side
  - any time five consecutive 1's have been transmitted from the body of the message (i.e. excluding when the sender is trying to send the distinguished 01111110 begin/end sequence)
  - The sender inserts 0 before transmitting the next bit (bit stuffing)

MK MORGAN KAUFMANN 11

## Framing

Chapter 2

- HDLC Protocol - On the receiving side
  - Receive 5 consecutive 1's
    - Next bit 0 : Stuffed, so discard it, continue with data
    - Next bit 1 : Either End of the frame marker,
      Or Error introduced in the bitstream

        Look at the next bit after the $6^{th}$ 1
        If 0 ( 01111110 ) → End of the frame marker
        If 1 ( 01111111 ) → Error, discard the whole frame
            The receiver needs to wait for next 01111110 before it can start receiving again

MK MORGAN KAUFMANN 12

## Framing

Chapter 2

- Bit stuffing and Character stuffing
  - Frame size dependent on data sent
  - Not possible to make all frames the same size

MK MORGAN KAUFMANN 13

## Clock Based Framing (SONET)

Chapter 2

- Synchronous Optical Network
- Designed for phone company use
- Designed to multiplex several low-speed links on to one high-speed link
- STS-1 lowest SONET link (51.84 Mbps)
  - Frame is 9 rows of 90 bytes (810 bytes)
  - First 3 bytes of each row are overhead
  - First 2 bytes of the frame are a special bit pattern used for synchronization

MK MORGAN KAUFMANN 14

## Clock Based Framing (SONET)



- In general, SONET is extremely complex
- Overhead bytes are sent NRZ
- Payload bytes are XOR'd with a 127 bit sequence to ensure transitions
- Each SONET frame is 125 micro seconds
  - STS-1 (51.84 Mbps): 810 bytes
  - STS – 48 (2488.32 Mbps): 38,880 bytes



## Clock Based Framing (SONET)



- STS – N
  - Consist of N STS-1 frames
  - All of the STS – 1 frames are interleaved
    - Each STS -1 frame is received at the STS-1 rate
    - Reduces effect of burst noise

## Error Detection

Chapter 2

- Bit errors are introduced into frames
  - Because of electrical interference
  - Because of thermal noises
- Need a mechanism to
  - Detect any errors
  - Notify of or correct errors

MK MORGAN KAUFMANN 17

## Error Detection

Chapter 2

- Two approaches when the recipient detects an error
  - Notify the sender that the message was corrupted, so the sender can send again.
    - If the error is rare, then the retransmitted message will be error-free
  - Using some error correct detection and correction algorithm, the receiver reconstructs the message

MK MORGAN KAUFMANN 18

## Error Detection

Chapter 2

- Common techniques for detecting transmission error
  - CRC (Cyclic Redundancy Check)
    - Used in HDLC, DDCMP, CSMA/CD, Token Ring
  - Two Dimensional Parity (BISYNC)
  - Checksum (IP)



## Error Detection

Chapter 2

- Basic Idea of Error Detection
  - Add redundant information to a frame that can be used to determine if errors have been introduced
    - Extreme Case: Transmitting two complete copies of data
      - Identical → No error
      - Differ → Error
      - Poor Scheme? – not very efficient
        - n bit message, n bit redundant information
        - Error can go undetected
    - In general, we can provide strong error detection technique
      - k redundant bits, n bits message, k << n
      - In Ethernet, a frame carrying up to 12,000 bits of data requires only 32-bit CRC

# Error Detection

Chapter 2

- Extra bits are redundant
  - They add no new information to the message
  - Derived from the original message using some algorithm
  - Both the sender and receiver know the algorithm

| Sender | | Receiver | |
|---|---|---|---|
| m | r | m' | r' |

Receiver receives *m'* and *r'* computes *r* using *m'*

If the computed *r* matches the received *r'*, then message is assumed to be error free

MK 21

# Two-dimensional parity

Chapter 2

- Two-dimensional parity is exactly what the name suggests
- It is based on "simple" (one-dimensional) parity, which usually involves adding one extra bit to a 7-bit code to balance the number of 1s in the byte. For example one-dimensional parity is,
  - Odd parity sets the eighth bit to 1 if needed to give an odd number of 1s in the byte, and
  - Even parity sets the eighth bit to 1 if needed to give an even number of 1s in the byte

MK 22

## Two-dimensional parity

Chapter 2

- Two-dimensional parity does a similar calculation for each bit position across each of the bytes contained in the frame
- This results in an extra parity byte for the entire frame, in addition to a parity bit for each byte
- Two-dimensional parity catches all 1-, 2-, and 3-bit errors and most 4-bit errors
- In the following example, 42 bits of data and 14 bits of parity (redundant bits)

23

## Two-dimensional parity

Chapter 2

| | | Parity bits |
|---|---|---|
| Data | 0101001 | 1 |
| | 1101001 | 0 |
| | 1011110 | 1 |
| | 0001110 | 1 |
| | 0110100 | 1 |
| | 1011111 | 0 |
| Parity byte | 1111011 | 0 |

Two Dimensional Parity (using even parity)

24

## Internet Checksum Algorithm



- Not used at the link level
- Add up all the words that are transmitted and then transmit the result of that sum
  - The result is called the checksum
- The receiver performs the same calculation on the received data and compares the result with the received checksum
- If any transmitted data, including the checksum itself, is corrupted, then the results will not match, so the receiver knows that an error occurred



## Internet Checksum Algorithm



- Consider the data being checksummed as a sequence of 16-bit integers.
- Add them together using 16-bit ones complement arithmetic (explained next slide) and then take the ones complement of the result.
- That 16-bit number is the checksum
- Not a good detector of bit errors – however it is easy to implement in software

## Internet Checksum Algorithm



- In ones complement arithmetic, a negative integer −x is represented as the complement of x;
  - Each bit of x is inverted.
- When adding numbers in ones complement arithmetic, a carryout from the most significant bit needs to be added to the result.



## Internet Checksum Algorithm



- Consider, for example, the addition of −5 and −3 in ones complement arithmetic on 4-bit integers
  - +5 is 0101, so −5 is 1010; +3 is 0011, so −3 is 1100
- If we add 1010 and 1100 ignoring the carry, we get 0110
- In ones complement arithmetic, the fact that this operation caused a carry from the most significant bit causes us to increment the result, giving 0111, which is the ones complement representation of −8 (obtained by inverting the bits in 1000), as we would expect

## Cyclic Redundancy Check (CRC)

Chapter 2

- Reduce the number of extra bits and maximize protection
- Given a bit string 110001 we can associate a polynomial on a single variable *x* for it.
  $1*x^5+1*x^4+0*x^3+0*x^2+0*x^1+1*x^0 = x^5+x^4+1$ and the degree is 5.
  A *k*-bit frame has a maximum degree of *k*-1
- Let M(x) be a message polynomial and C(x) be a generator polynomial – pulled from a table.

MK 29

## Cyclic Redundancy Check (CRC)

Chapter 2

- Let M(x)/C(x) leave a remainder of 0.
- When M(x) is sent and M'(x) is received we have M'(x) = M(x)+E(x)
- The receiver computes M'(x)/C(x) and if the remainder is nonzero, then an error has occurred.
- The only thing the sender and the receiver should know is C(x).

MK 30

## Cyclic Redundancy Check (CRC)

Chapter 2

Polynomial Arithmetic Modulo 2

- Any polynomial B(x) can be divided by a divisor polynomial C(x) if B(x) is of higher degree than C(x).
- Any polynomial B(x) can be divided once by a divisor polynomial C(x) if B(x) is of the same degree as C(x).
- The remainder obtained when B(x) is divided by C(x) is obtained by subtracting C(x) from B(x).
- To subtract C(x) from B(x), we simply perform the exclusive-OR (XOR) operation on each pair of matching coefficients.

MORGAN KAUFMANN 31

## Cyclic Redundancy Check (CRC)

Chapter 2

- Let M(x) be a frame with *m* bits and let the generator polynomial have less than *m* bits say equal to *k*.
- Let *r* be the degree of C(x) where r = k-1
- Append *r* zero bits to the low-order end of the frame, so it now contains *m*+*r* bits and corresponds to the polynomial $x^r M(x)$.

If $M(x) = x^5+x^4+1$ and $C(x) = x^3+x^2+1 \rightarrow r=3$

Then $x^r M(x) = x^8+x^7+x^3$

MORGAN KAUFMANN 32

## Cyclic Redundancy Check (CRC)

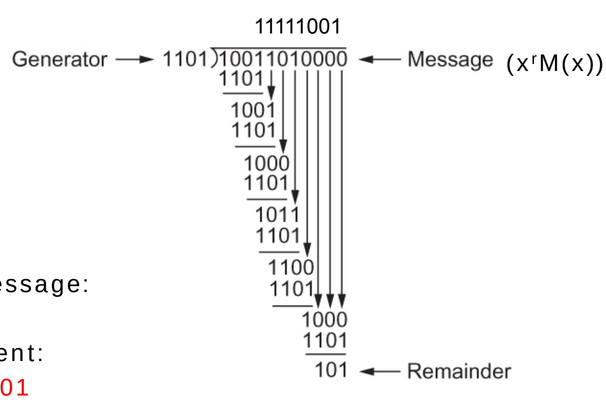
Chapter 2

- Divide the bit string corresponding to $x^r M(x)$ by the bit string corresponding to C(x) using modulo 2 division.
- Subtract the remainder (which is always *r* or fewer bits) from the string corresponding to $x^r M(x)$ using modulo 2 subtraction (addition and subtraction are the same in modulo 2).
- The result is the checksummed frame to be transmitted. Call it polynomial M'(x).



## Cyclic Redundancy Check (CRC)

Chapter 2




Original Message:
10011010
Message sent:
10011010101

CRC Calculation using Polynomial Long Division

## Cyclic Redundancy Check (CRC)

Chapter 2

- Properties of Generator Polynomial
  - Let P(x) represent what the sender sent and P(x) + E(x) is the received string. A 1 in E(x) represents that in the corresponding position in P(x) the bit is flipped.
  - We know that P(x)/C(x) leaves a remainder of 0, but if E(x)/C(x) leaves a remainder of 0, then either E(x) = 0 or C(x) is factor of E(x).
  - When C(x) is a factor of E(x) we have problem; errors go unnoticed.
  - If there is a single bit error then $E(x) = x^i$, where *i* determines the bit in error. If C(x) contains two or more terms it will never divide E(x), so all single bit errors will be detected.

MK MORGAN KAUFMANN 35

## Cyclic Redundancy Check (CRC)

Chapter 2

- Properties of Generator Polynomial
  - In general, it is possible to prove that the following types of errors can be detected by a C(x) with degree r (book uses k here) with the stated properties
    - All single-bit errors, as long as the $x^r$ and $x^0$ terms have nonzero coefficients.
    - All double-bit errors, as long as C(x) has a factor with at least three terms.
    - Any odd number of errors, as long as C(x) contains the factor (x+1).
    - Any “burst” error (i.e., sequence of consecutive error bits) for which the length of the burst is less than *r* bits. (Most burst errors of larger than *r* bits can also be detected.)

MK MORGAN KAUFMANN 36

## Cyclic Redundancy Check (CRC)

Chapter 2

- Six generator polynomials that have become international standards are:
  - CRC-8 = $x^8+x^2+x+1$
  - CRC-10 = $x^{10}+x^9+x^5+x^4+x+1$
  - CRC-12 = $x^{12}+x^{11}+x^3+x^2+x+1$
  - CRC-16 = $x^{16}+x^{15}+x^2+1$
  - CRC-CCITT = $x^{16}+x^{12}+x^5+1$
  - CRC-32 = $x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$

37