Chapter 2 Getting Connected

• When connecting two nodes with one link, we need to address four fundamental problems in the data link layer
  o Framing – delineating the sequence of bits transmitted over the link into frames that can be delivered to the end hosts
  o Error detection – detecting transmission errors and taking the appropriate action
  o Reliable delivery - making a link appear reliable even though it corrupts frames from time to time.
  o Media access control - mediating access to a link when the link is shared by multiple hosts

• Framing – determining where the frame begins and ends
  o Byte-counting approach: DDCMP
    ▪ Used in DEC’s DECNet
    ▪ A byte-oriented protocol – each frame is viewed as a collection of bytes (characters) rather than bits
    ▪ Uses special SYN character (i.e., the sentinel character) to indicate where the frame starts
    ▪ The COUNT field specifies the number of bytes in the frame’s body
      ▪ If the COUNT field is corrupted, the end of the frame would not be correctly detected
      ▪ The CRC field can be used to determine that the frame is bad
• Sentinel-based approach: HDLC
  ▪ Developed by IBM, standardized by ISO
  ▪ A bit-oriented protocol - a frame is viewed as a collection of bits
  ▪ The special bit sequence 01111110 (known as sentinel) denotes the beginning and the end of a frame
  ▪ The bit sequence 01111110 may appear in the body of a frame → use bit stuffing to solve the problem
    • Sender inserts a 0 if it sees 5 consecutive 1’s
    • When receiver sees 5 consecutive 1’s:
      o If next bit is 0, remove it.
      o If next two bits are 10: end of frame;
      o If next two bits are 11: an error has occurred, discard the frame
  ▪ Error detection
    o Bit errors are sometimes introduced into frames due to electrical interference or thermal noise
    o To allow the receiver to detect bit errors, the sender adds redundant bits to a frame
      ▪ Redundant bits are derived from the original message using some well-defined algorithm f
      ▪ Sender sends M (original message) and R (redundant bits), where R=f(M)
      ▪ Receiver gets M’ and R’ and checks if f(M’)=R’. If yes, no error detected; otherwise, error detected
    o Internet Checksum Algorithm
      ▪ Used by IP, TCP, UDP
Consider the data being checksummed as a sequence of 16-bit integers. Add them up using ones complement arithmetic and then take the ones complement of the result. That 16-bit number is the checksum.

- Pros: use only 16 redundant bits, easy to implement
- Cons: relatively weak protection against errors (compared to CRC)

**Cyclic Redundancy Check (CRC)**

- Represent an m-bit message as an m-1 degree polynomial
  - E.g., message=10011010 corresponds to \( M(x)=x^7+x^4+x^3+x^1 \)
- Sender and receiver agree on a divisor polynomial \( C(x) \) of degree \( k \). The last term of \( C(x) \) must be 1
  - E.g. \( C(x)=x^3+x^2+1, \ k=3 \)
- Sender appends \( k \) redundant bits to the end of the message such that the polynomial represented by the complete message is exactly divisible by \( C(x) \).
- Receiver divides the received message by \( C(x) \), if remainder is not 0, then an error has occurred.

- How to compute the \( k \) redundant bits?
  - Multiply \( M(x) \) by \( x^k \); that is, add \( k \) zeros at the end of the message. The resulting message is \( T(x) \).
  - Divide \( T(x) \) by \( C(x) \) using modulo 2 division.
  - Subtract the remainder from \( T(x) \). The result is the frame to be transmitted.
- How to select \( C(x) \)?
  - Select \( C(x) \) so that it is very unlikely to divide evenly into a message that has errors introduced into it
- It can be proved that $C(x)$ of degree $k$ can detect
  - All single-bit errors, as long as the $x^k$ and $x^0$ terms have nonzero coefficients
  - All double-bit errors, as long as $C(x)$ contains 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 errored bits) for which the length of the burst is less than $k$ bits.
  - Most burst errors of length greater than $k$ bits.