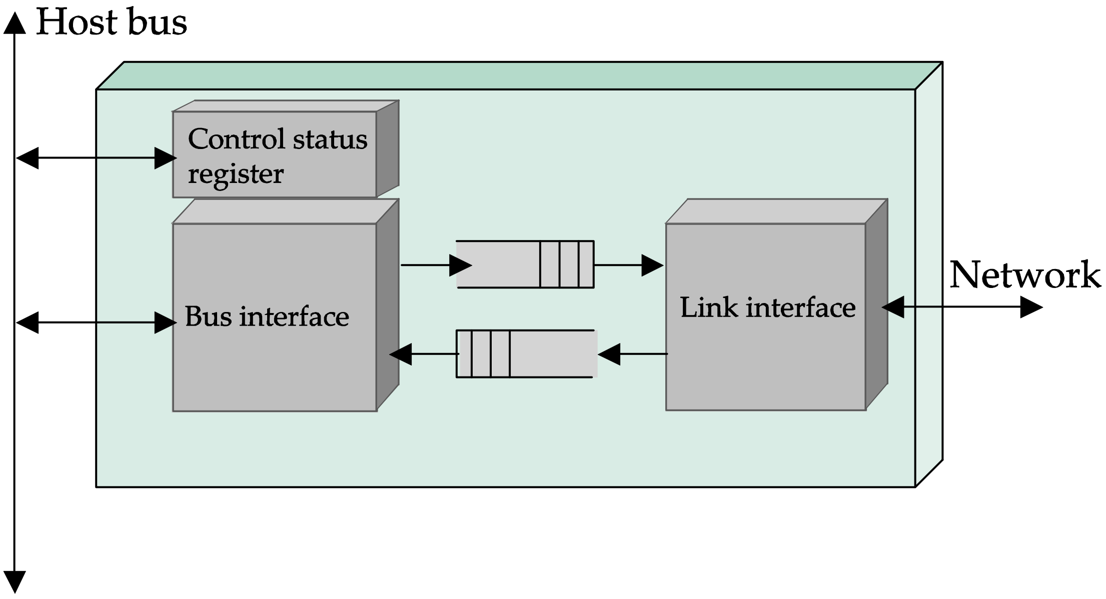
Chapter 2 Direct Link Networks

Network adaptor

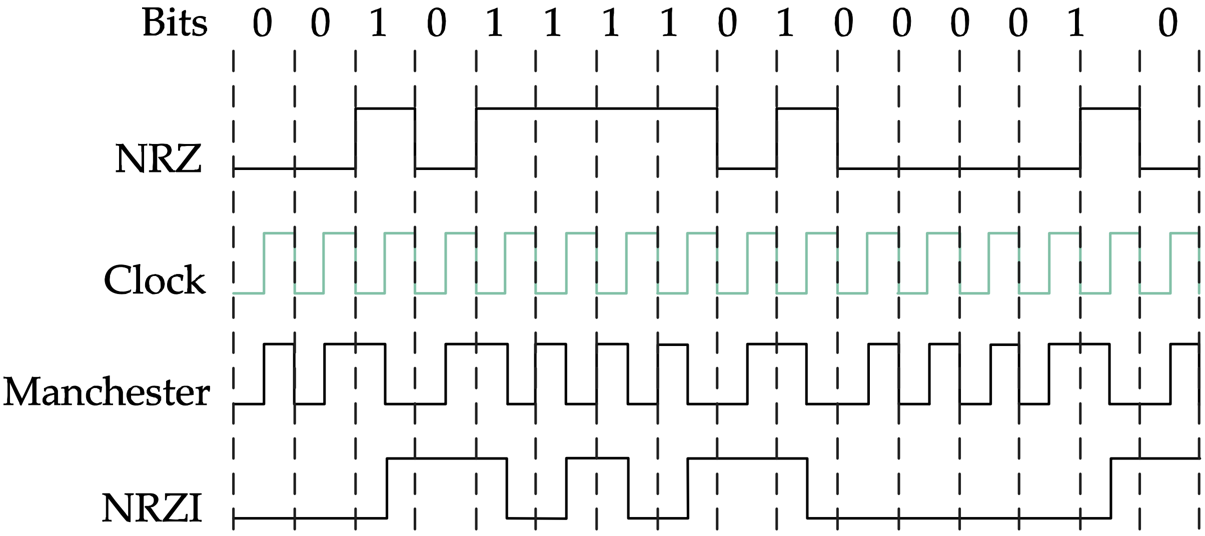
- Connect a node to a link
- Implement nearly all the networking functionality, including encoding, framing, error detection, reliable data transfer, and media access control
    - Link interface varies as link varies
    - Bus interface tends to be similar
    - CSR is typically located at some address in the memory, and is readable and writable from the CPU
    - Adaptor driver writes to CSR and reads CSR
- Data is transferred between the adaptor and the host memory via DMA or programmed I/O



Encoding

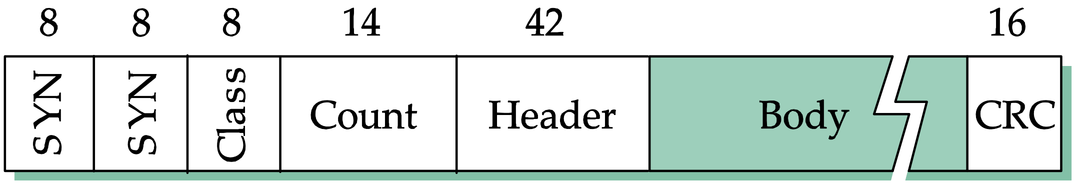
- Encode binary data into signals that the link can carry
- NRZ (Nonreturn to zero): high signal for bit 1 and low signal for bit 0
    - Long sequence of 1's and 0's may cause baseline wander and make receiver clock recovery harder
    - NRZI (Nonreturn to zero inverted): make a transition from the current signal to encode 1 and stay at the current signal to encode 0
        - Long string of 0s may still exist

- Manchester Encoding: XOR the clock with NRZ-encoded data – 50% efficiency
- 4B/5B encoding: every 4-bit of actual data are encoded in a 5bit code
    - The 5-bit code has at most one leading 0s and at most two trailing 0s
    - The 5-bit code is transmitted via NRZI encoding
    - 80% efficiency

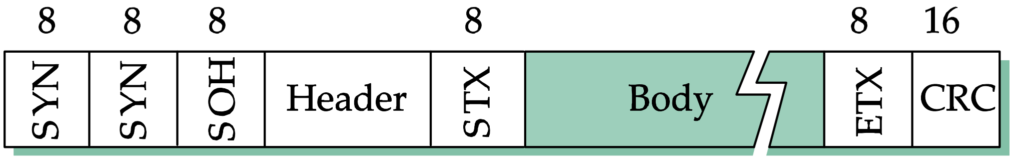


Framing

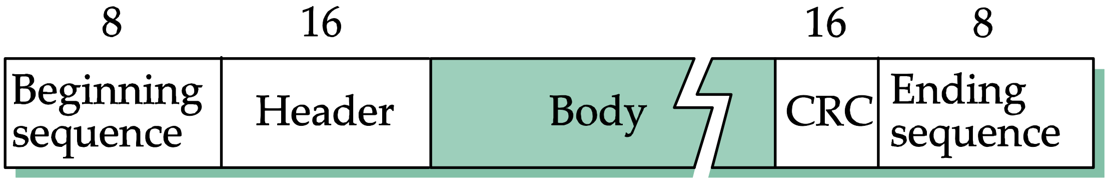
- Determining where the frame begins and ends is a challenging problem since frames (packet switching) are exchanged between nodes
- Byte-counting approach (DDCMP) – e.g. DDCMP frame



- Sentinel-based approach – character stuffing (e.g. BISYNC frame format uses DLE (data link escape))



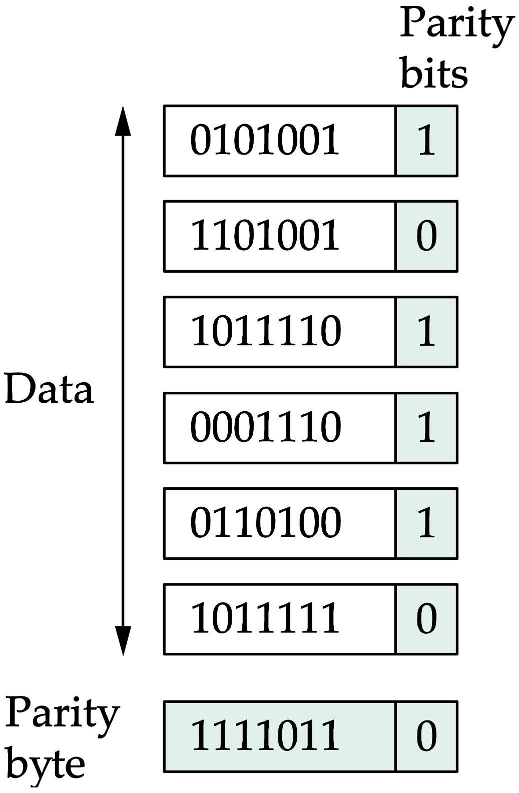
- Bit stuffing – e.g. HDLC frame employs the special bit sequence 01111110



- How bit stuffing in HDLC protocol works?
- Example: Show the bit sequence after bit stuffing: 110101111101011111101011111110
- Example: Show the original bit sequence after the stuffed bits are removed: 11010111110101111100101111110110

Error detection

- Basic idea: add redundant bits to a frame
- Two-dimensional parity



0101001	1
1101001	0
1011110	1
0001110	1
0110100	1
1011111	0
1111011	0

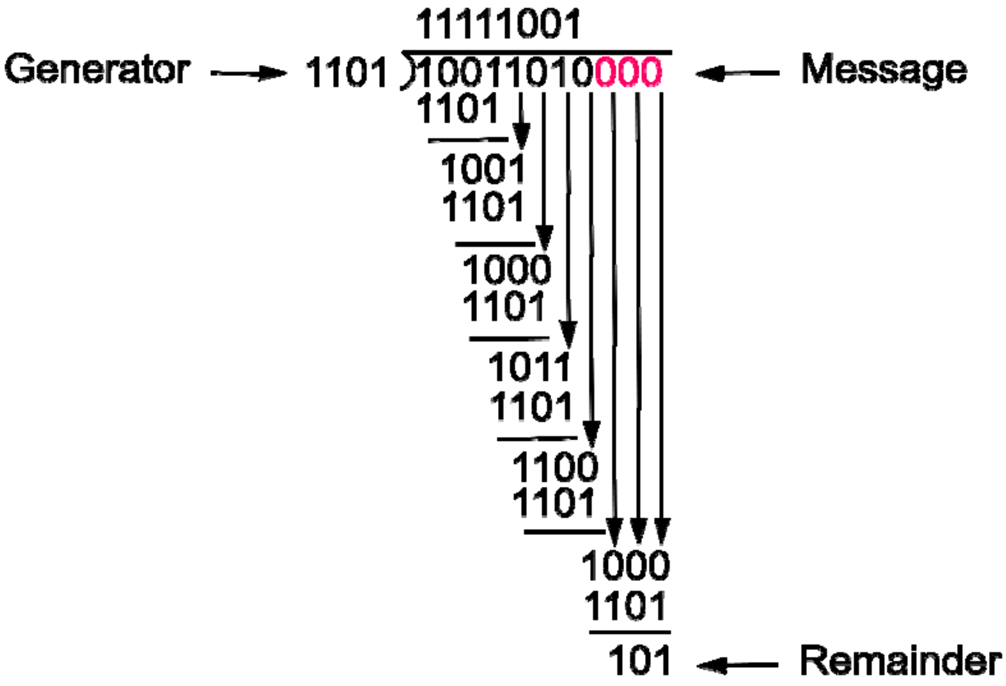
- Internet checksum algorithm – used by the Internet protocol
  - Take the input data as a sequence of 16-bit integers
  - Add them together using 16-bit ones complement arithmetic
  - Take the ones complement of the result as the checksum
  - Example:

    A protocol uses 1's complement of the sum of all the 8-bit bytes in the segment for its checksum. Suppose the bit sequence of a segment from the sender has the format 10100010 11000110 01011011 xxxxxxxx, where xxxxxxxx is the checksum. What is the checksum byte? How does the receiver detect errors?

Answer: *Checksum: 00111011*

Computer the 1's complement sum over all the bytes, includingthe checksum. If the result is 11111111, the check succeeds

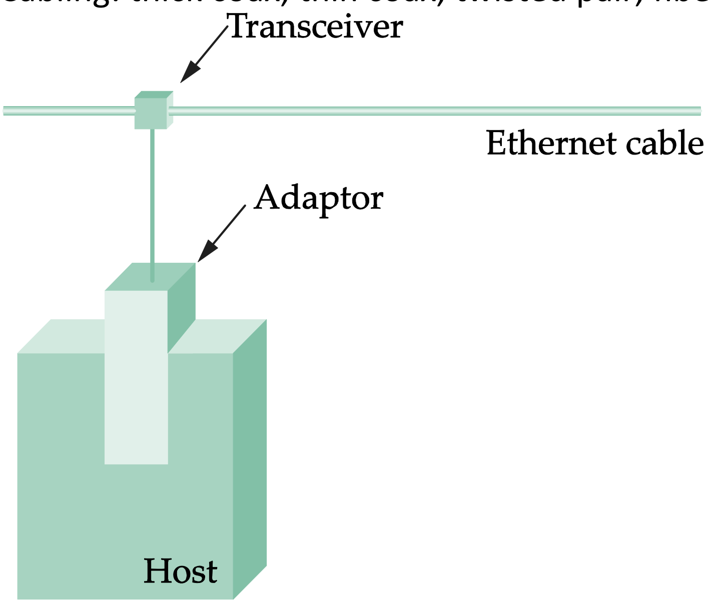
- Cyclic Redundancy Check – based on field theory, treat data as the coefficients of a polynomial, easy implementation in hardware based on shift registers
  - Add *k* bits of redundant data to an *n*-bit message -- want *k* << *n* , e.g., *k* = 32 and *n* = 12,000 (1500 bytes)
  - Represent *n*-bit message as *n*-1 degree polynomial -- e.g., MSG=10011010 as $M(x) = x^7 + x^4 + x^3 + x^1$
  - Let *k* be the degree of some divisor polynomial -- e.g., $C(x) = x^3 + x^2 + 1$
  - Transmit polynomial *P*(*x*) that is evenly divisible by *C*(*x*)
    - shift left *k* bits, i.e., $M(x)x^k$
    - subtract remainder of $M(x)x^k$ / $C(x)$ from $M(x)x^k$
  - Receiver polynomial *P*(*x*) + *E*(*x*)
    - *E*(*x*) = 0 implies no errors
  - Divide (*P*(*x*) + *E*(*x*)) by *C*(*x*); remainder zero if:
    - *E*(*x*) was zero (no error), or
    - *E*(*x*) is exactly divisible by *C*(*x*)
  - Example



    - Choice of *C(x)*
        - Want to ensure C(x) doesn't divide E(x). We can detect
            - All single-bit errors if C(x) has at least 2 terms
            - All double-bit errors if C(x) doesn't divide $x^j + 1$
                - $X^{15} + x^{14} + 1$ doesn't divide $x^j + 1$ for any j below 32768
            - Any odd number of errors if C(x) contains the factor x+1
            - Any "burst" error of length less than or equal to k bits
            - Most burst errors of length greater than k bits

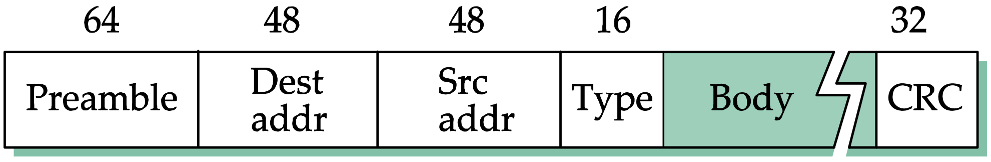
Ethernet (IEEE 802.3)

- Physical properties
    - Cabling: thick coax, thin coax, twisted pair, fiber



    - Speeds: 10Mbps, 100Mbps, 1Gbps, 10Gbps
    - Devices: repeaters (at most four), hubs (multiway repeater, star topology), switches
    - All hosts are in the same collision domain when connecting via hubs and repeaters

- Frame format (802.3)



- Ethernet addresses
  - Each Ethernet adaptor has a unique 6-byte Ethernet address
  - Broadcast address: all 1s
  - Multicast address: first bit set to 1
- Ethernet adaptor receives all frames and accepts
  - frames addressed to its own address
  - frames addressed to the broadcast address
  - frames addressed to a multicast address, if programmed to listen to that address
  - all frames, if in promiscuous mode
- Transmitter algorithm: Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
  - See slides
- Why an Ethernet frame must be at least 64 bytes long?
  - The magic number: 51.2 microsecond
- Ethernet performance affected by cable length, packet length, amount of traffic.

Examples:

1. Consider a CSMA/CD network running at 10 Mbps over 2-km cable with no repeaters. The signal speed in the cable is 200,000 km/sec. Suppose a station starts transmitting a frame of size 1K bytes at time T.

   (a) Can it happen that the station detects a collision at time T+7 micro seconds if there was no collision detected between time T and T+7 microseconds? Why?

   YES, RTT = 20 microseconds

   (b) Can it happen that the station detects a collision at time T+16 microseconds, if there was no collision detected between time T and T+16 microseconds? Why?

   YES

   (c) Can it happen that the station detects a collision at time T+29 microseconds, if there was no collision detected between time T and T+29 microseconds? Why?

NO. There will be no collision.

2. In a version of Slotted Aloha, the frame transmission time is 1 ms and the slot length is 0.5 ms. Frames can arrive for transmission at any time, but are transmitted only on slot boundaries.
(a) What is the length of the “vulnerable period" for the protocol at hand? The vulnerable period refers to the time around the transmission period of a frame, during which if transmission of another frame begins, there will be a collision.

Solution: 1.5ms

(b) How does the efficiency of this protocol compare with that of Pure Aloha? Better or worse? Why?

Solution: For Pure Aloha, the vulnerable period is 2 ms and for Slotted Aloha it is 1 ms. Hence the efficiency of this protocol is in between that of Pure Aloha and Slotted Aloha.

Lecture on Sep 28:

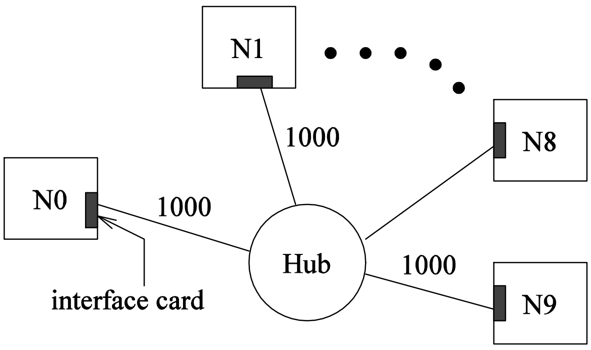
Review Questions:

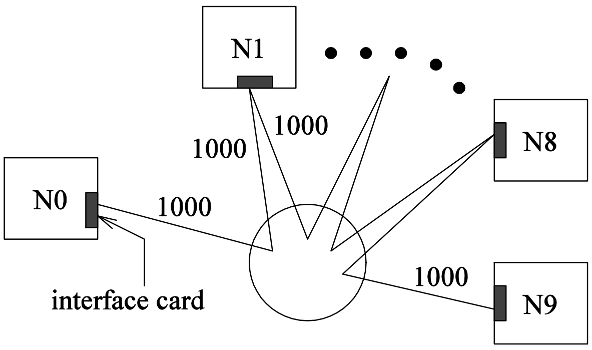
1. How does CSMA/CD protocol work?
2. Why a 48-bit jam signal is needed?
3. Why minimum fame size is imposed?

Examples:

1. In a CSMA/CD Network when can a station be certain that it has seized the channel, i.e., no other station would interfere with its transmission?
After RTT time.

2. Consider a 10 Mbps CSMA/CD network interconnecting 10 computers. Assume that the speed of propagation of a signal in a cable is 2 *10^8 m/s. The following figures show two possible ways of interconnecting them.





(a)The figure on the left shows a network with a hub. Each computer is connected to the hub with a cable of length 1000 m. Calculate the minimum frame size that can be supported so that CSMA/CD protocol will function correctly.

The distance between two farthest computers = 2000 m
End to end propagation delay = 10microseconds
Worst case collision detection time = 20microseconds
Minimum frame size = 200 bits = 25 bytes

(b) The figure on the right shows a network without a hub but the computers remain in the same locations. A single cable is strung between the computers as shown above. The cable starts at computer N0, runs via the location where the hub was, then onto computers N1, N2, …, N9 in turn. The cable terminates at computer N9. What is the minimum frame size in this network?

The distance between two farthest computers =1000 + 8X2000 + 1000 = 18000 m
End to end propagation delay = 90 microseconds
Worst case collision detection time = 180microseconds
Minimum frame size = 1800 bits = 225 bytes