Chapter 4
Local Area network

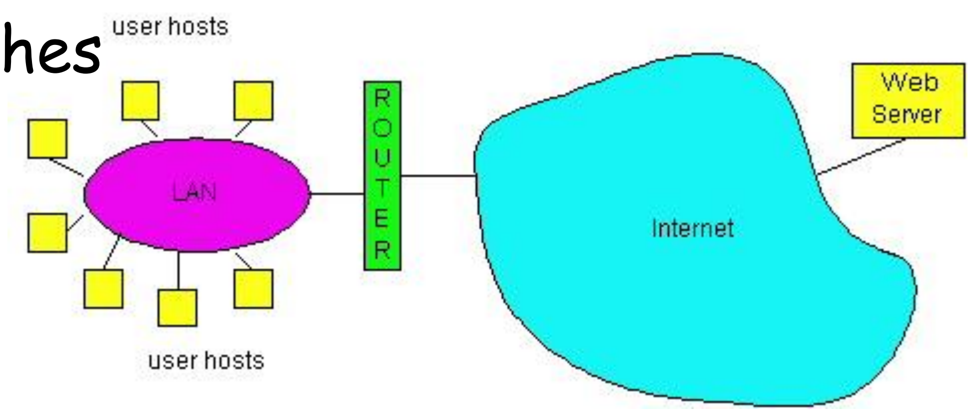
LAN technologies

Data link layer so far:

- services, error detection/correction, multiple access

Next: LAN technologies

- LAN model
- addressing
- Ethernet
- hubs, bridges, switches



Keypoints and Difficulties

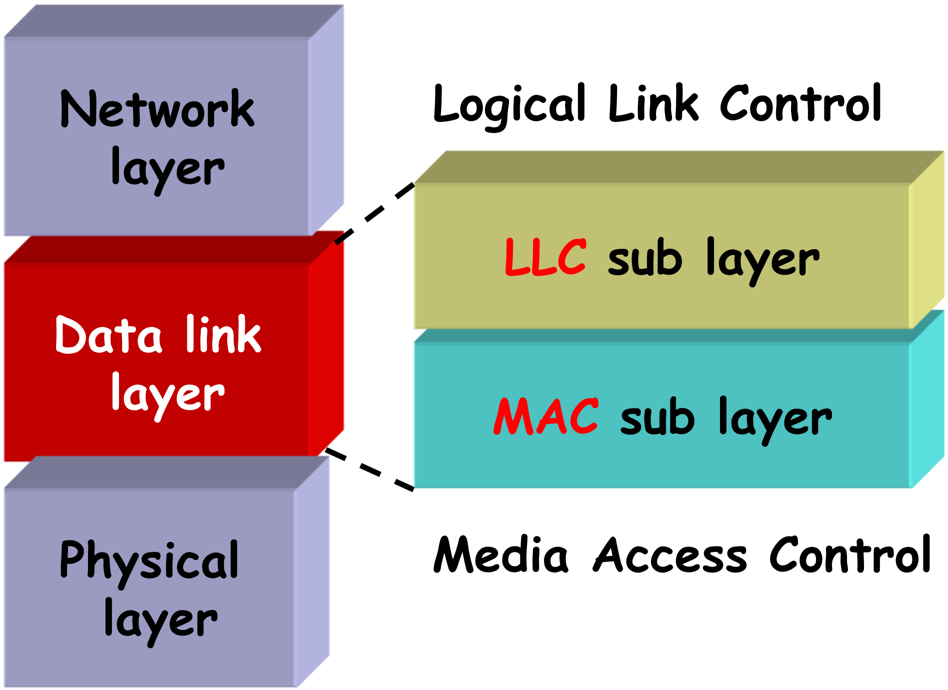
Keypoints:

- LAN model
- Ethernet
- Hubs, bridges, switches

Difficulties:

- The minimum frame length
- The exponential Backoff algorithm

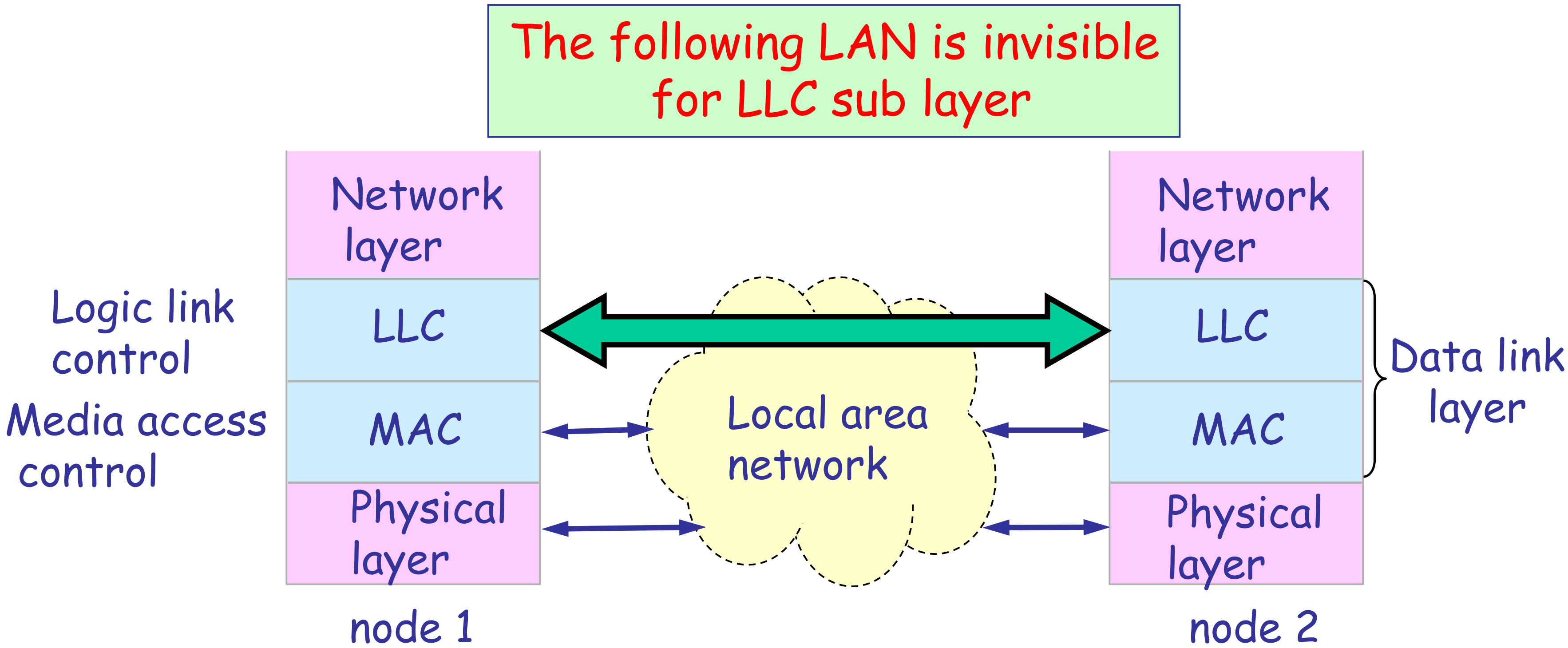
LAN model



Provide the connection environment to the upper level

Providing media access to the lower layer

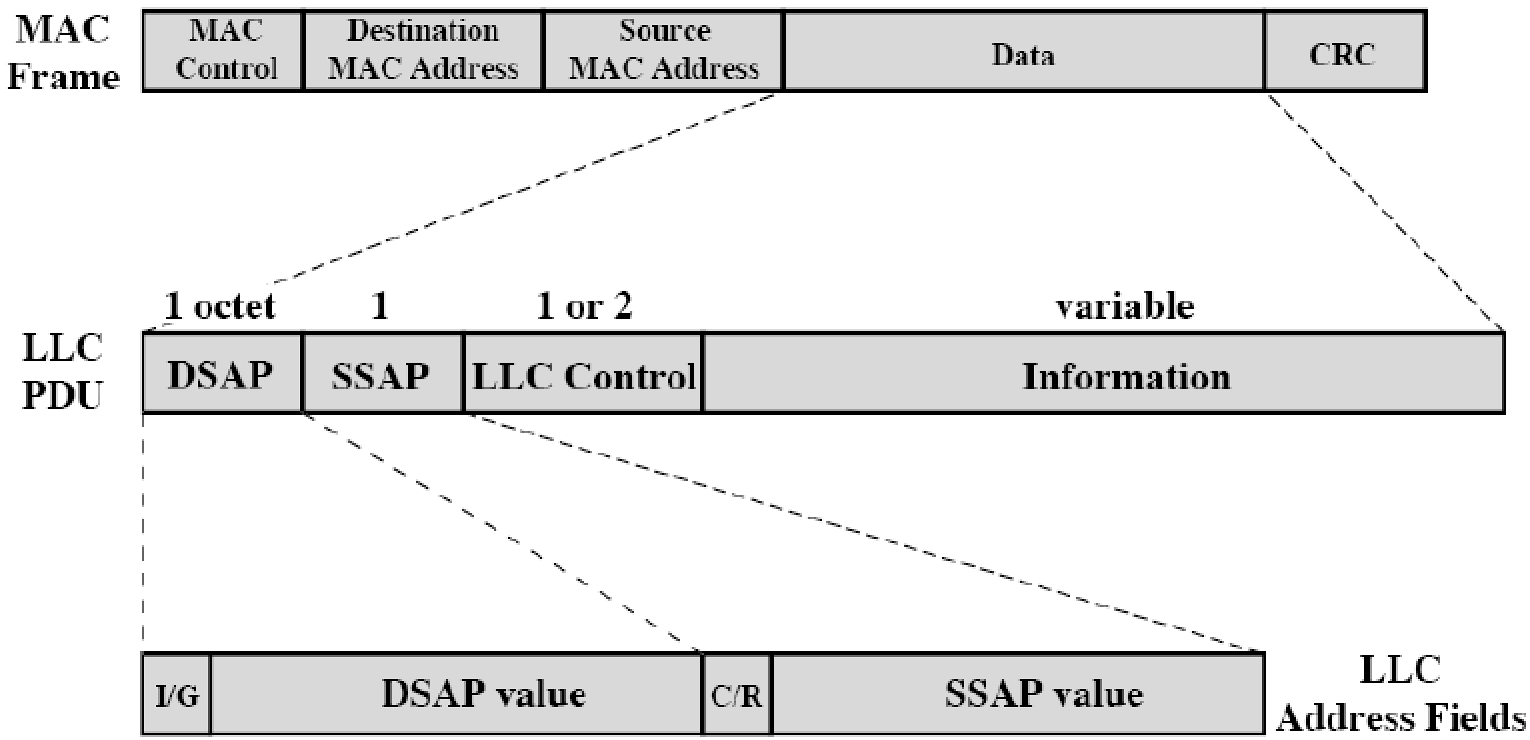
LAN model



For the same LLC, several MAC options may be provided.

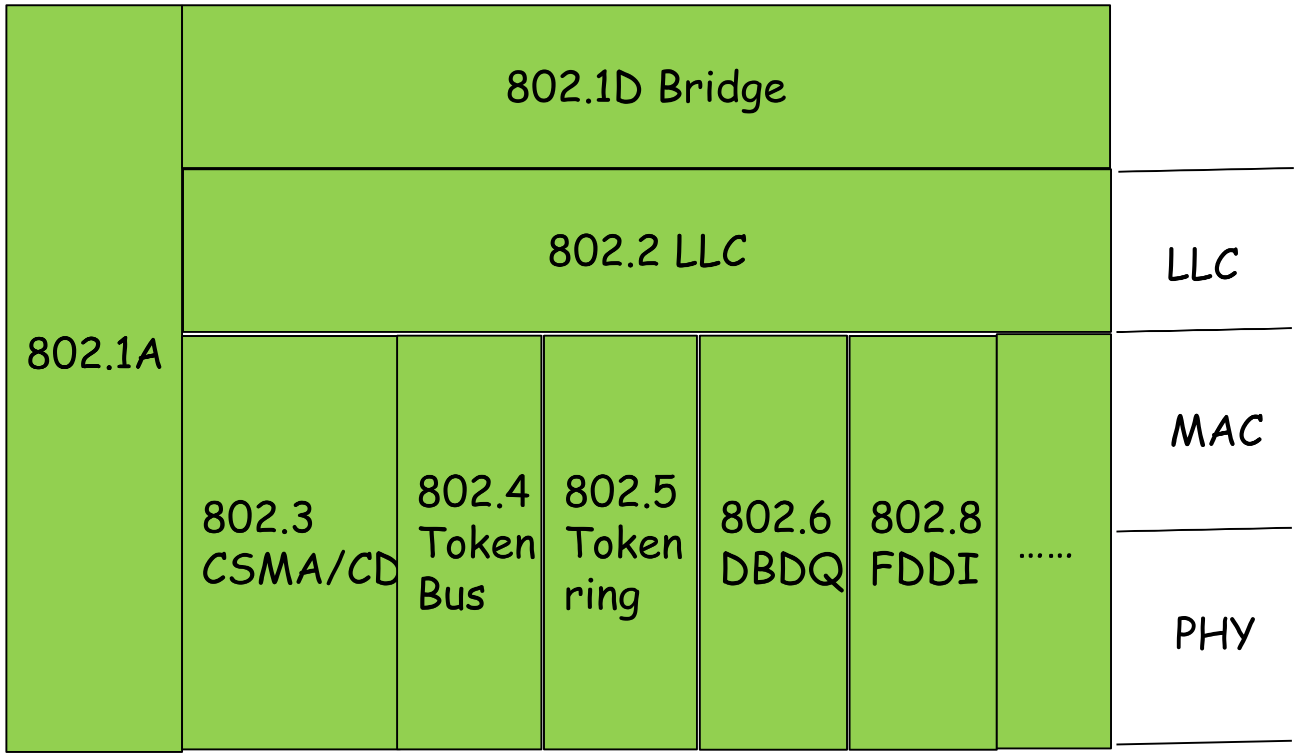
LLC and MAC

MAC Frame Format



I/G = individual/group
C/R = command/response
DSAP = destination service access point
SSAP = source service access point

IEEE 802 working group



LAN Addresses

32-bit IP address:

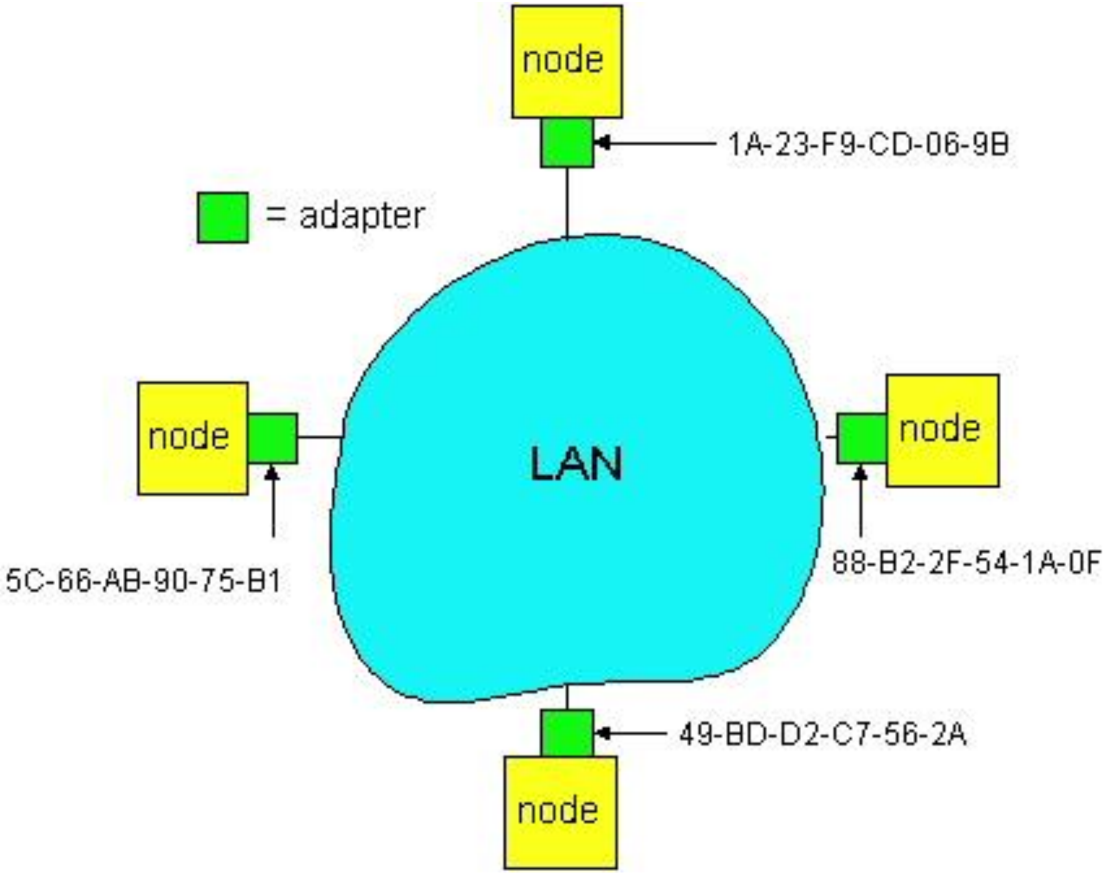
- *network-layer* address
- used to get datagram to destination network

LAN (or MAC or physical) address:

- used to get datagram from one interface to another physically-connected interface (same network)
- 48 bit MAC address (for most LANs) burned in the adapter ROM

LAN Addresses

Each adapter on LAN has unique LAN address



LAN Address (more)

- MAC address allocation administered by IEEE
- manufacturer buys portion of MAC address space (to assure uniqueness)
- Analogy:

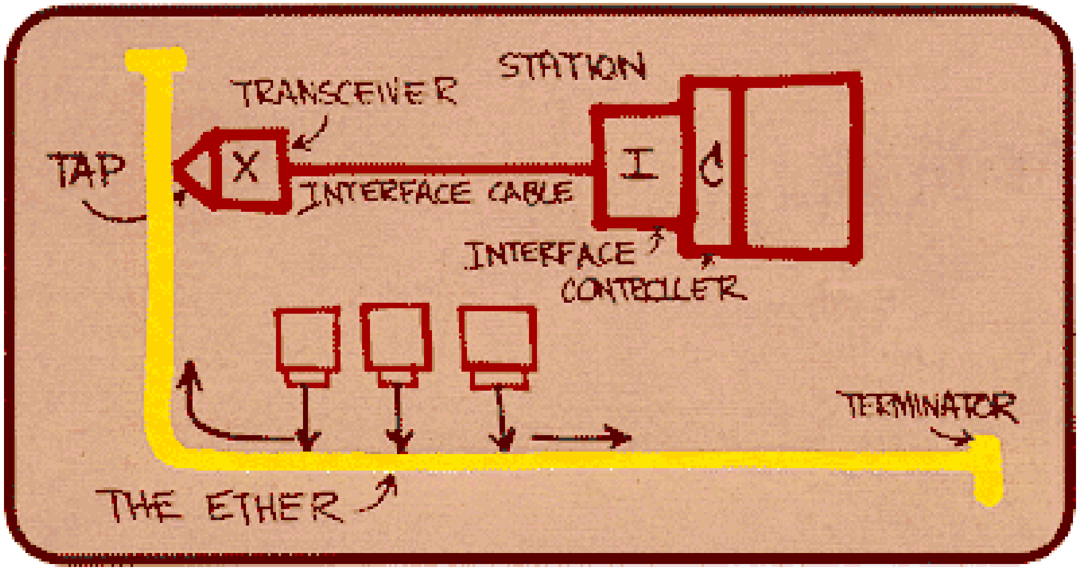
  (a) MAC address: like Social Security Number

  (b) IP address: like postal address
- MAC flat address => portability
  - can move LAN card from one LAN to another
- IP hierarchical address NOT portable
  - depends on network to which one attaches

Ethernet

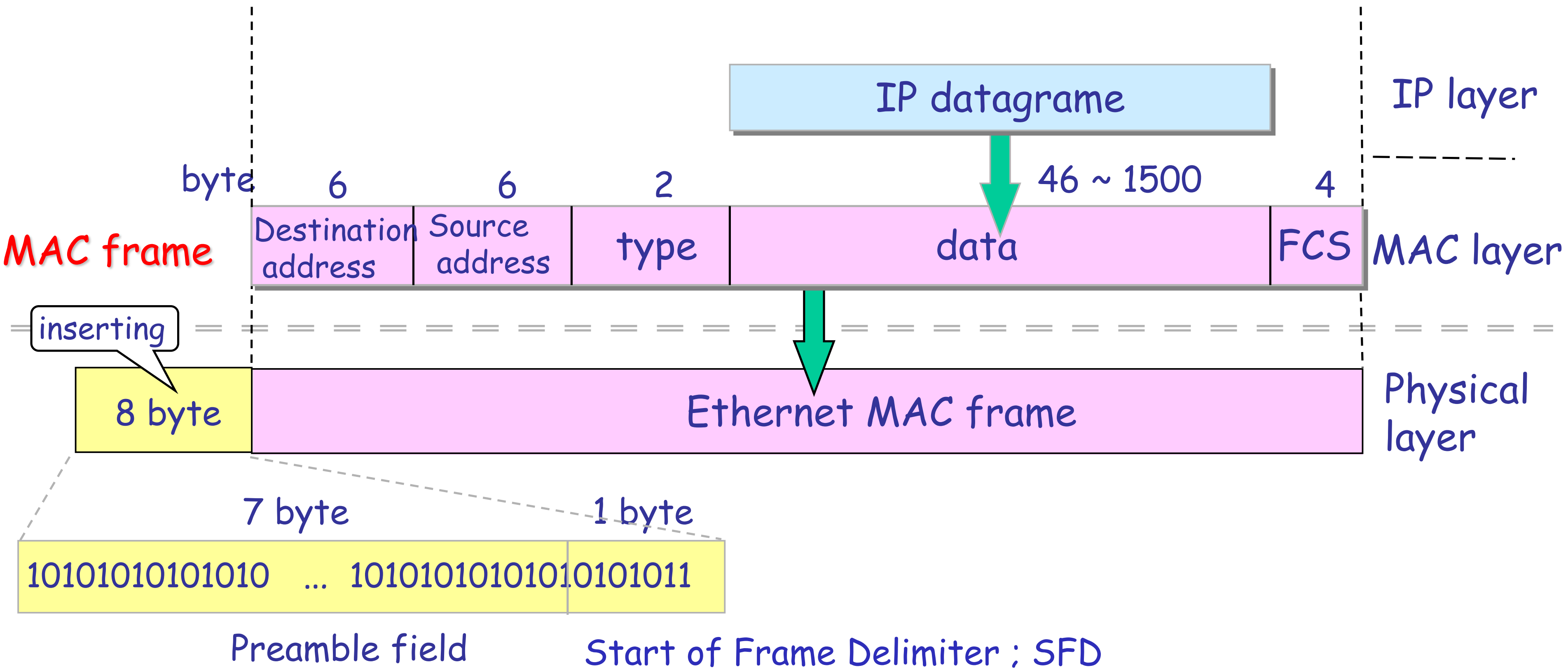
"dominant" LAN technology:

- first wildey used LAN technology
- Simpler, cheaper than token LANs and ATM
- Kept up with speed race: 10, 100, 1000 Mbps,……



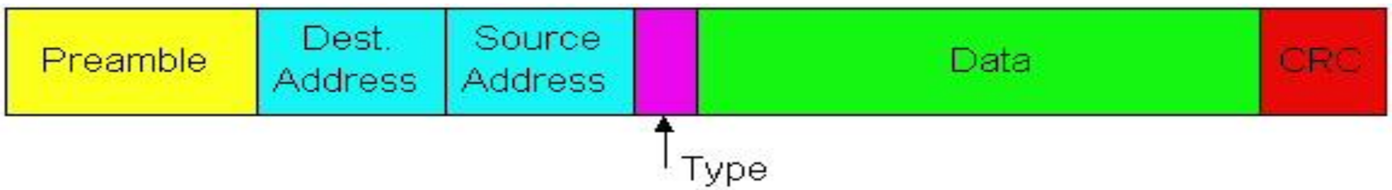
Metcalfe's Etheret sketch

Ethernet Frame Structure



Ethernet Frame Structure

Sending adapter encapsulates IP datagram (or other network layer protocol packet) in Ethernet frame

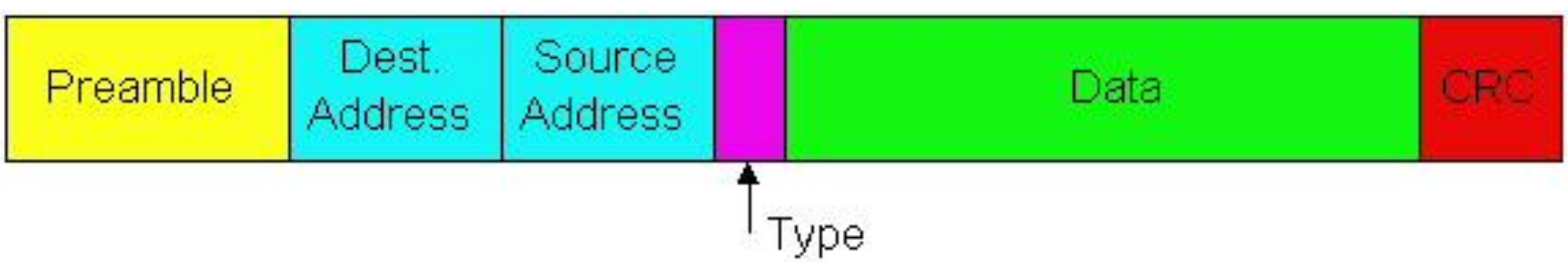


Preamble:

- 7 bytes with pattern 10101010 followed by one byte with pattern 10101011
- used to synchronize receiver, sender clock rates

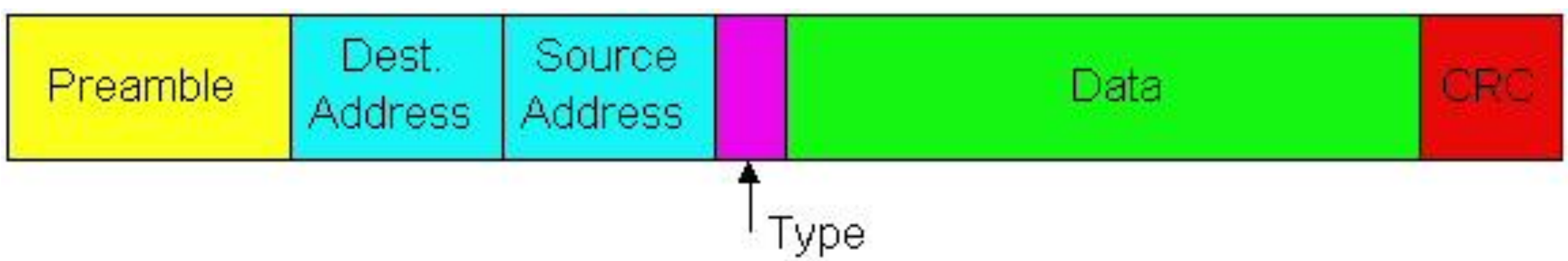
Ethernet Frame Structure (more)

- Addresses: 6 bytes, frame is received by all adapters on a LAN and dropped if address does not match
- Type: 2 bytes, indicates the higher layer protocol, mostly IP, but others may be supported such as Novell IPX and AppleTalk
- CRC: 4 bytes, checked at receiver, if error is detected, the frame is simply dropped



Ethernet Frame Structure (more)

- Data: 46~1500 bytes
- Minimum frame length: 64 bytes, why? (contention period 2τ is 51.2 μs for IEEE 802.3, R=10Mbps)
- Maximum frame length: 1518 bytes, why?

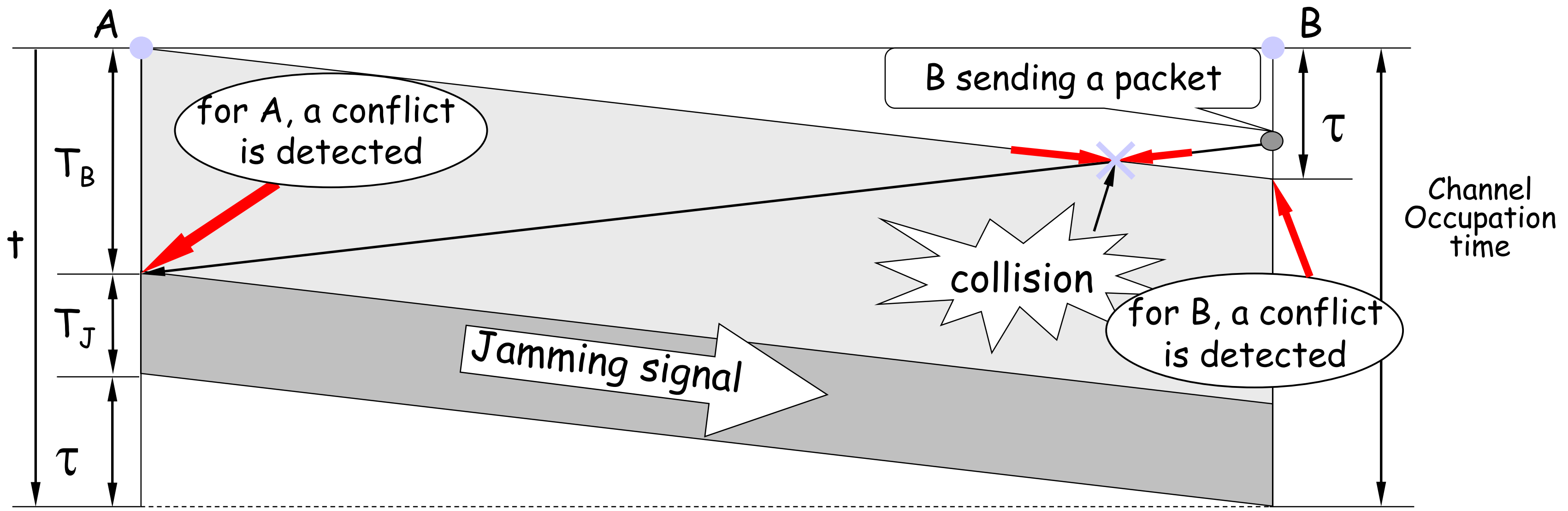


Ethernet: uses CSMA/CD

```
A: sense channel, if idle
   then {
         transmit and monitor the channel;
         If detect another transmission
           then {
              abort and send jam signal;
              update # collisions;
              delay as required by exponential backoff algorithm;
              goto A
              }
          else {done with the frame; set collisions to zero}
      }
   else {wait until ongoing transmission is over and goto A}
```

Ethernet's CSMA/CD (more)

Jam Signal: make sure all other transmitters are aware of collision; 48 bits;



Ethernet's CSMA/CD (more)

Exponential Backoff:

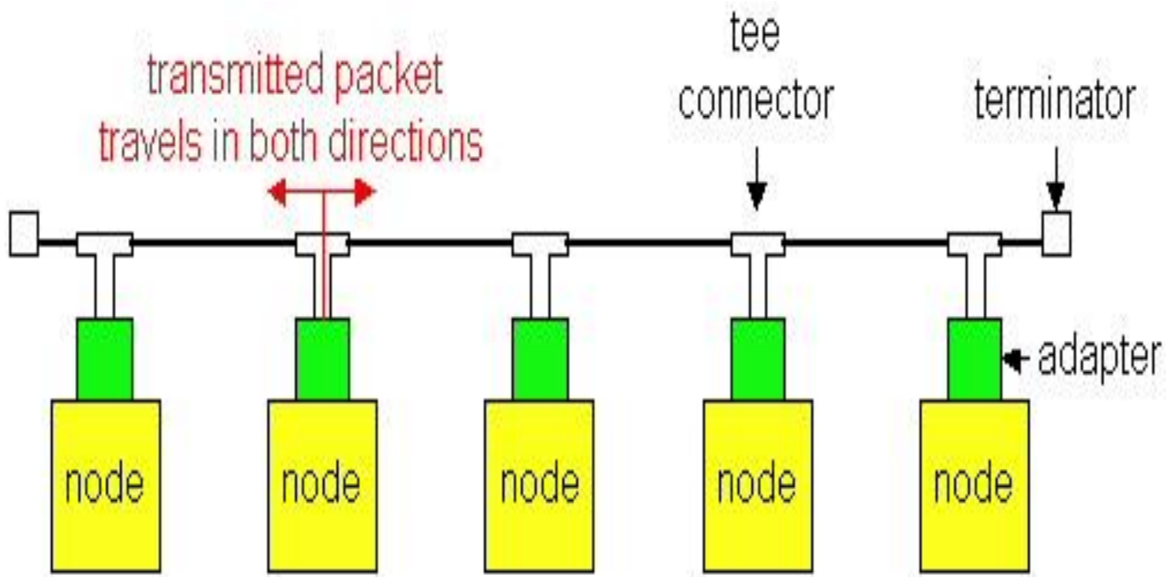
- *Goal*: adapt retransmission attemtps to estimated current load
  - heavy load: random wait will be longer
- first collision: choose K from {0,1}; delay is K x 512 bit transmission times (contention period: 2τ)
- after second collision: choose K from {0,1,2,3}…
- after ten or more collisions, choose K from {0,1,2,3,4,…,1023}

Exercise

- In CSMA/CD, after the fifth collision, what is the probability that a node chooses K=4? The result K=4 corresponds to a delay of how many seconds on a 10Mbps Ethernet?

Ethernet Technologies: 10Base2

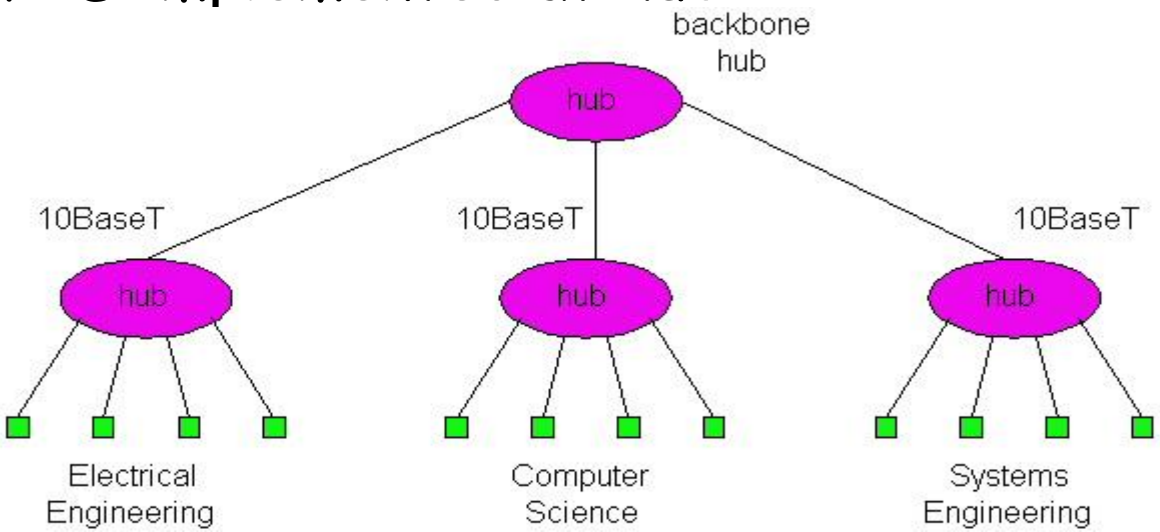
- 10: 10Mbps; 2: under 200 meters max cable length
- thin coaxial cable in a bus topology



- repeaters used to connect up to multiple segments
- repeater repeats bits it hears on one interface to its other interfaces: physical layer device only!

10BaseT and 100BaseT

- 10/100 Mbps rate; latter called "fast ethernet"
- T stands for Twisted Pair
- Hub to which nodes are connected by twisted pair, thus "star topology"
- CSMA/CD implemented at hub



10BaseT and 100BaseT (more)

- Max distance from node to Hub is 100 meters
- Hub can disconnect "jabbering" adapter
- Hub can gather monitoring information, statistics for display to LAN administrators

Gbit Ethernet

- use standard Ethernet frame format
- allows for point-to-point links and shared broadcast channels
- in shared mode, CSMA/CD is used; short distances between nodes to be efficient
- uses hubs, called here "Buffered Distributors"
- Full-Duplex at 1 Gbps for point-to-point links

Token Passing: IEEE802.5 standard

- 4 Mbps
- max token holding time: 10 ms, limiting frame length

SD	AC	FC

SD	AC	FC	dest addr	src addr	data	checksum	ED	FS

- SD, ED mark start, end of packet
- AC: access control byte:
  - token bit: value 0 means token can be seized, value 1 means data follows FC
  - priority bits: priority of packet
  - reservation bits: station can write these bits to prevent stations with lower priority packet from seizing token after token becomes free

Token Passing: IEEE802.5 standard

- FC: frame control used for monitoring and maintenance
- source, destination address: 48 bit physical address, as in Ethernet
- data: packet from network layer
- checksum: CRC
- FS: frame status: set by dest., read by sender
  - set to indicate destination up, frame copied OK from ring
  - DLC-level ACKing

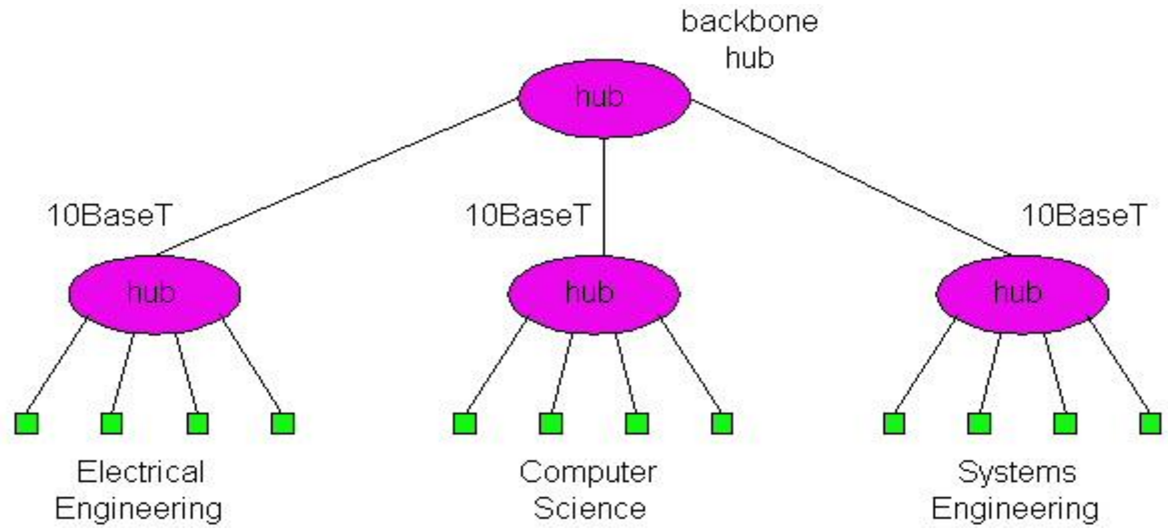
Interconnecting LANs

Q: Why not just one big LAN?

- Limited amount of supportable traffic: on single LAN, all stations must share bandwidth
- limited length: 802.3 specifies maximum cable length
- large "collision domain" (can collide with many stations)
- limited number of stations: 802.5 have token passing delays at each station

Hubs

- Physical Layer devices: essentially repeaters operating at bit levels: repeat received bits on one interface to all other interfaces
- Hubs can be arranged in a hierarchy (or multi-tier design), with backbone hub at its top



Hubs (more)

- Each connected LAN referred to as LAN **segment**
- Hubs do not isolate collision domains: node may collide with any node residing at any segment in LAN
- Hub Advantages:
  - simple, inexpensive device
  - Multi-tier provides graceful degradation: portions of the LAN continue to operate if one hub malfunctions
  - extends maximum distance between node pairs (100m per Hub)

Hub limitations

- single collision domain results in no increase in max throughput
  - multi-tier throughput same as single segment throughput
- individual LAN restrictions pose limits on number of nodes in same collision domain and on total allowed geographical coverage
- cannot connect different Ethernet types (e.g., 10BaseT and 100baseT)

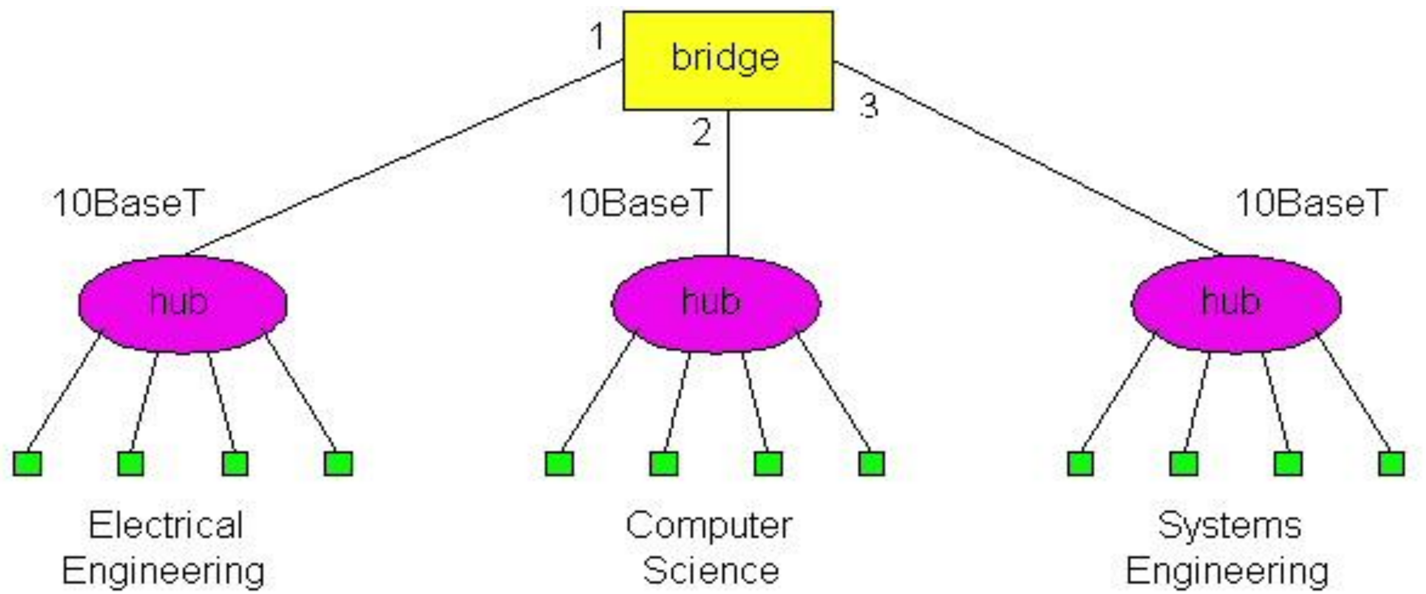
Bridges

- Link Layer devices: operate on Ethernet frames, examining frame header and selectively forwarding frame based on its destination
- Bridge isolates collision domains since it buffers frames
- When frame is to be forwarded on segment, bridge uses CSMA/CD to access segment and transmit

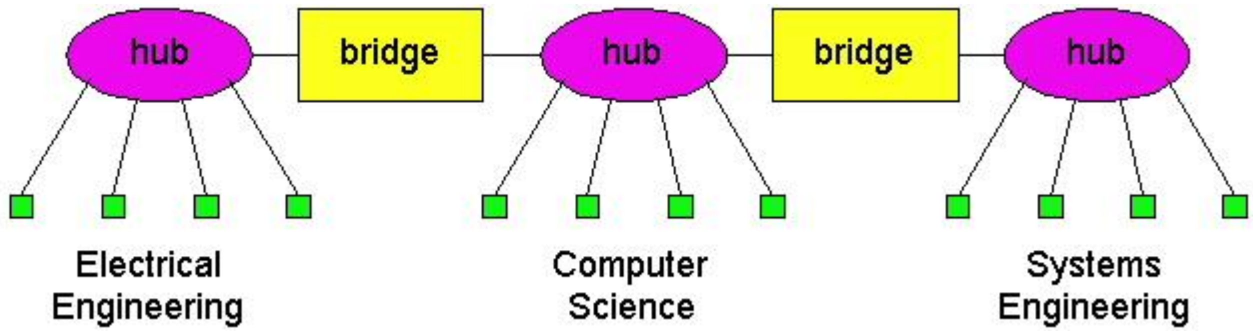
Bridges (more)

- Bridge advantages:
  - Isolates collision domains resulting in higher total max throughput, and does not limit the number of nodes nor geographical coverage
  - Can connect different type Ethernet since it is a store and forward device
  - Transparent: no need for any change to hosts LAN adapters

Backbone Bridge



Interconnection Without Backbone



- Not recommended for two reasons:
  - single point of failure at Computer Science hub
  - all traffic between EE and SE must path over CS segment

Bridges: frame filtering, forwarding

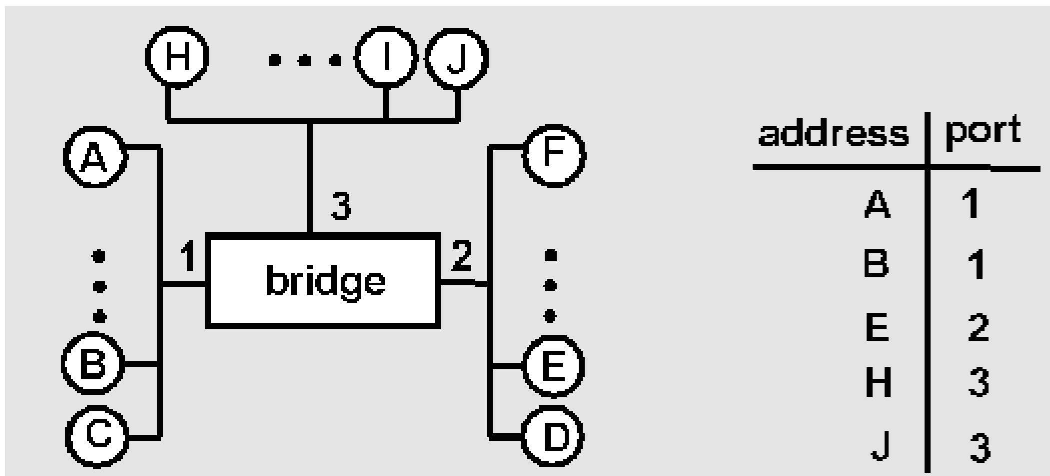
- bridges filter packets
  - same-LAN -segment frames not forwarded onto other LAN segments
- forwarding:
  - how to know which LAN segment on which to forward frame?
  - looks like a routing problem (more shortly!)

Bridge Filtering

- bridges *learn* which hosts can be reached through which interfaces: maintain filtering tables
  - when frame received, bridge "learns" location of sender: incoming LAN segment
  - records sender location in filtering table
- filtering table entry:
  - (Node LAN Address, Bridge Interface, Time Stamp)
  - stale entries in Filtering Table dropped (TTL can be 60 minutes)

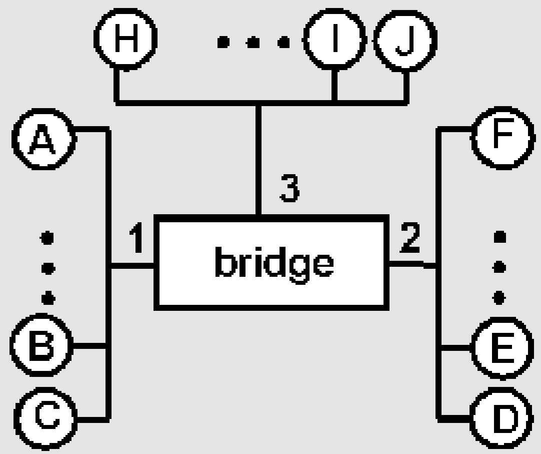
Bridge Learning: example

Suppose C sends frame to D and D replies back with frame to C



- C sends frame, bridge has no info about D, so floods to both LANs
  - bridge notes that C is on port 1
  - frame ignored on upper LAN
  - frame received by D

Bridge Learning: example



address	port
A	1
B	1
E	2
H	3
J	3

- D generates reply to C, sends
  - bridge sees frame from D
  - bridge notes that D is on interface 2
  - bridge knows C on interface 1, so *selectively* forwards frame out via interface 1

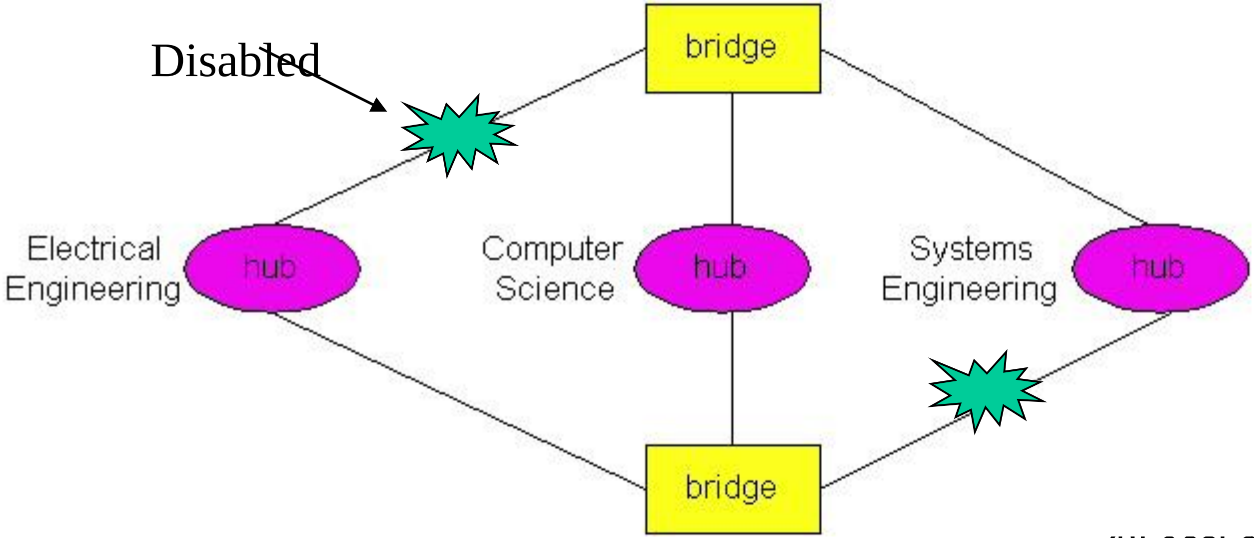
Bridge Filtering

- filtering procedure:

```
if destination is on LAN on which frame was received
    then drop the frame
    else { lookup filtering table
           if entry found for destination
             then forward the frame on interface indicated;
             else flood;    /* forward on all but the interface
               on                                which the frame
               arrived*/
         }
```

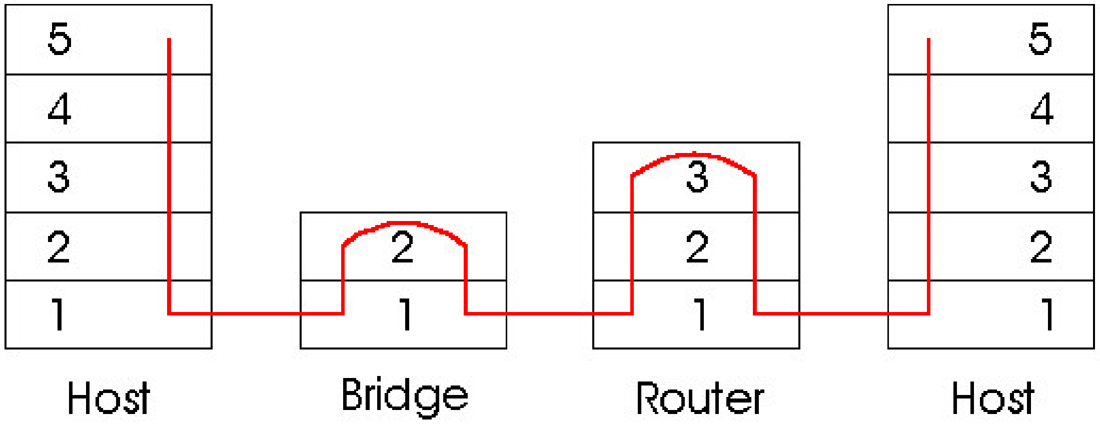
Bridges Spanning Tree

- for increased reliability, desirable to have redundant, alternate paths from source to dest
- with multiple simultaneous paths, cycles result - bridges may multiply and forward frame forever
- solution: organize bridges in a spanning tree by disabling subset of interfaces



Bridges vs. Routers

- both store-and-forward devices
  - routers: network layer devices (examine network layer headers)
  - bridges are Link Layer devices
- routers maintain routing tables, implement routing algorithms
- bridges maintain filtering tables, implement filtering, learning and spanning tree algorithms



Routers vs. Bridges

Bridges + and -

+ Bridge operation is simpler requiring less processing bandwidth
- Topologies are restricted with bridges: a spanning tree must be built to avoid cycles
- Bridges do not offer protection from broadcast storms (endless broadcasting by a host will be forwarded by a bridge)

Routers vs. Bridges

Routers + and -

\+ arbitrary topologies can be supported, cycling is limited by TTL counters (and good routing protocols)

\+ provide firewall protection against broadcast storms

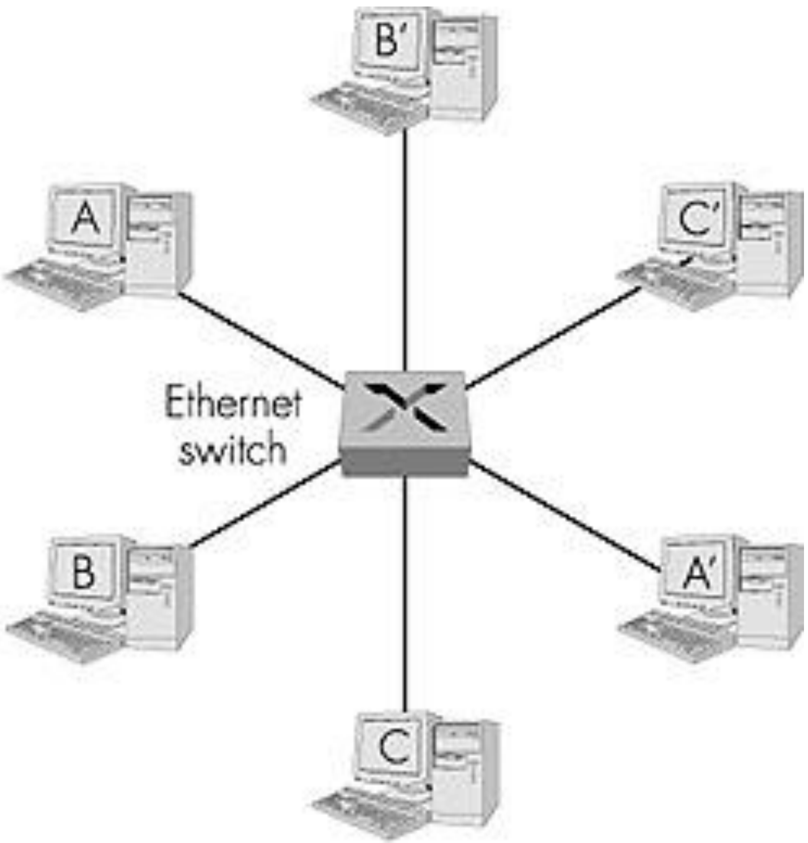
\- require IP address configuration (not plug and play)

\- require higher processing bandwidth

- bridges do well in small (few hundred hosts) while routers used in large networks (thousands of hosts)

Ethernet Switches

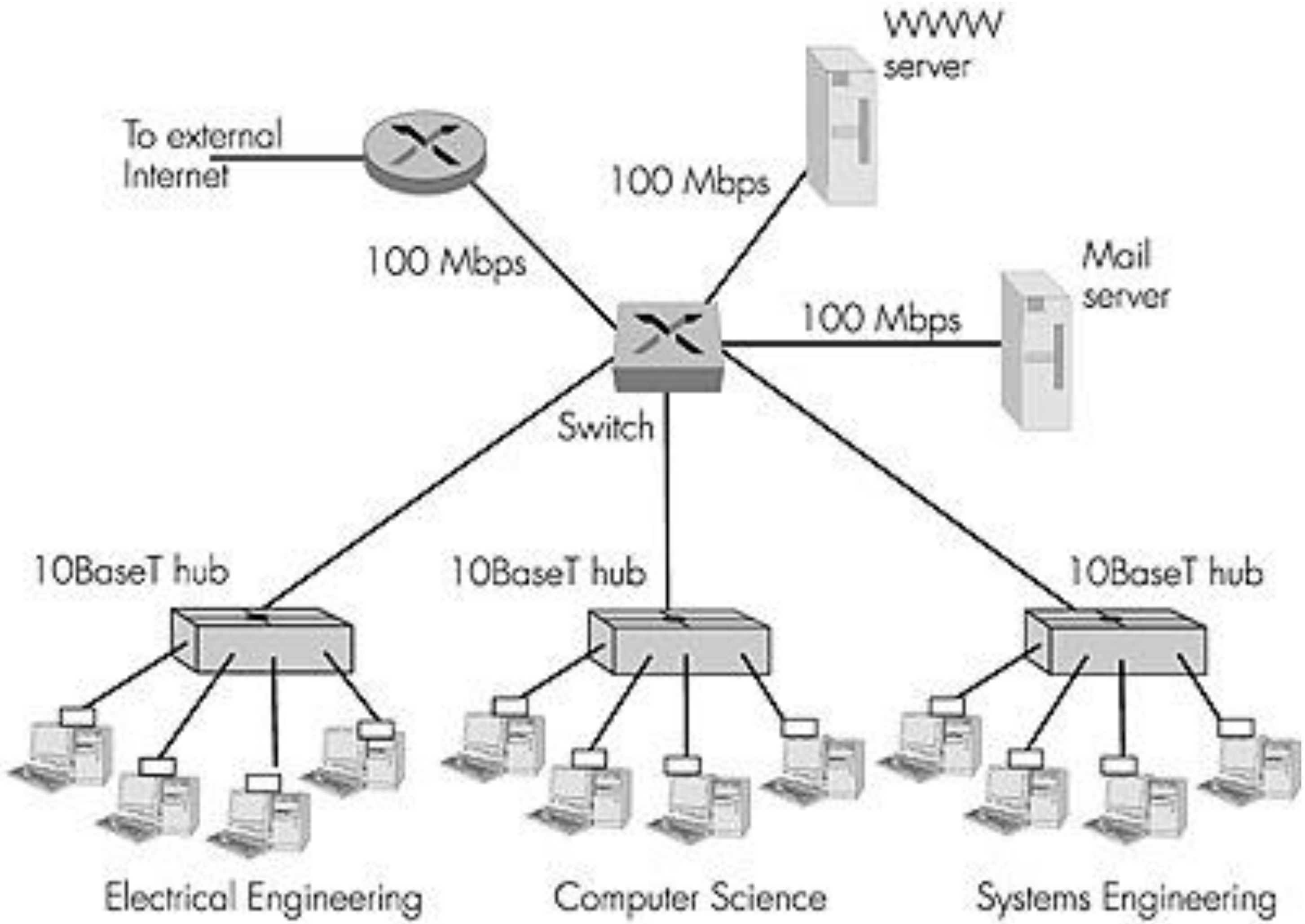
- layer 2 (frame) forwarding, filtering using LAN addresses
- Switching: A-to-B and A'-to-B' simultaneously, no collisions
- large number of interfaces
- often: individual hosts, star-connected into switch
  - Ethernet, but no collisions!



Ethernet Switches

- cut-through switching: frame forwarded from input to output port without awaiting for assembly of entire frame
  - slight reduction in latency
- combinations of shared/dedicated, 10/100/1000 Mbps interfaces

Ethernet Switches (more)



Chapter 4:Local area network Summary

- principles behind data link layer services:
  - error detection, correction
  - sharing a broadcast channel: multiple access
  - link layer addressing
- various link layer technologies
  - LAN model
  - Ethernet
  - hubs, bridges, switches