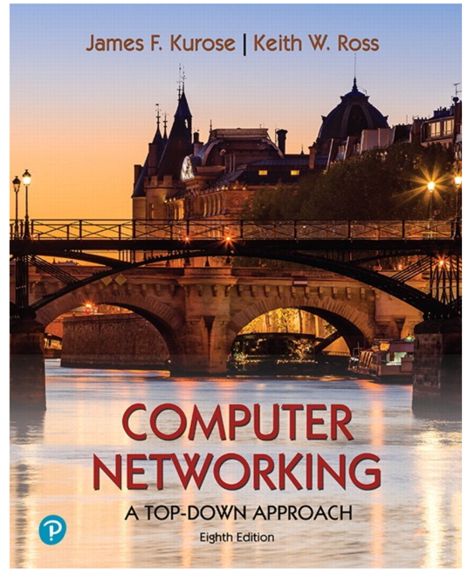
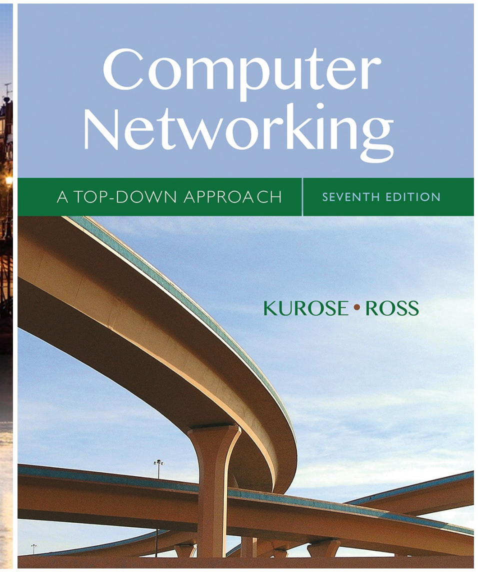
CS 655
Computer Networks

Abraham Matta
Computer Science
Boston University

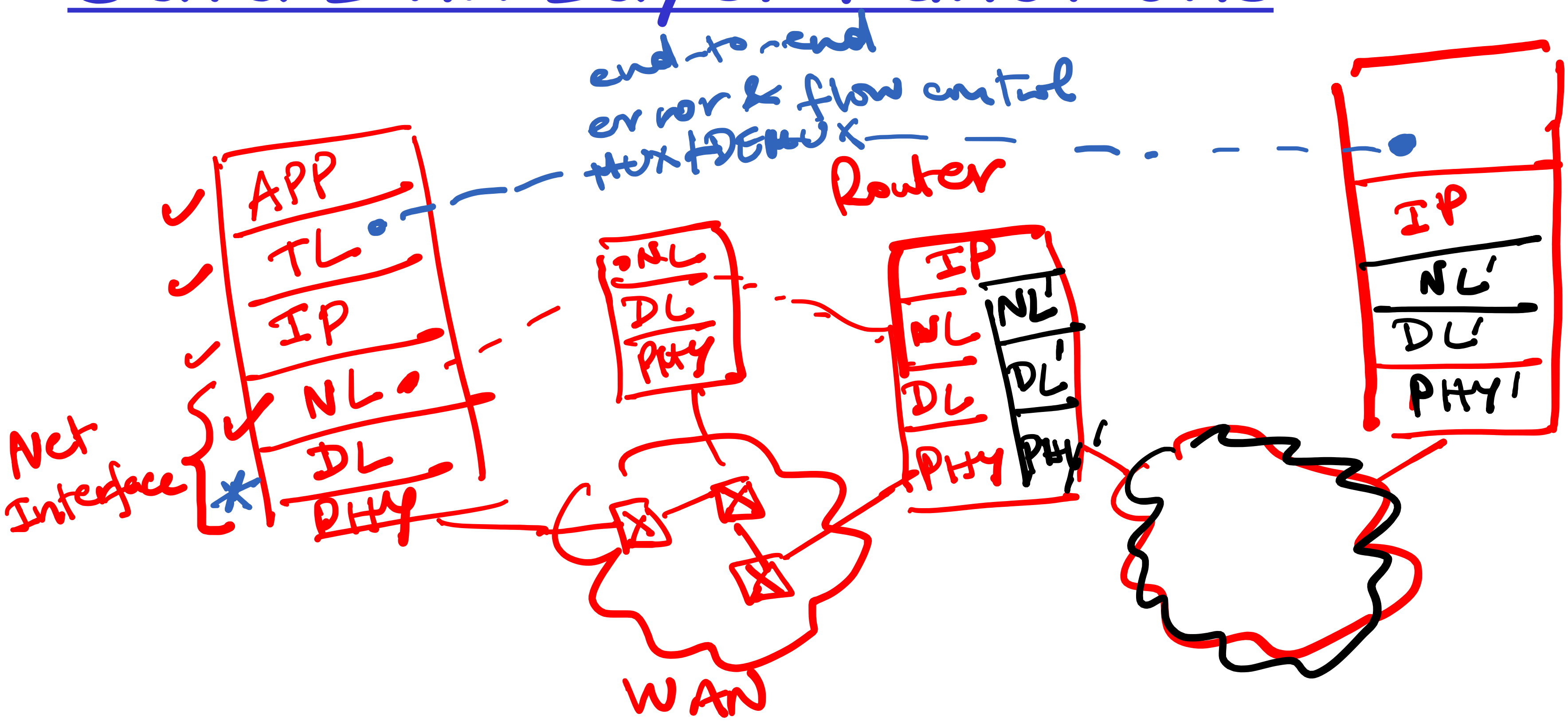
Chapter 6
Network Interface
(focus on Data Link Layer)





Computer Networking: A Top-Down Approach, 8th edition. Jim Kurose, Keith Ross. Pearson.
7th edition is OK too!

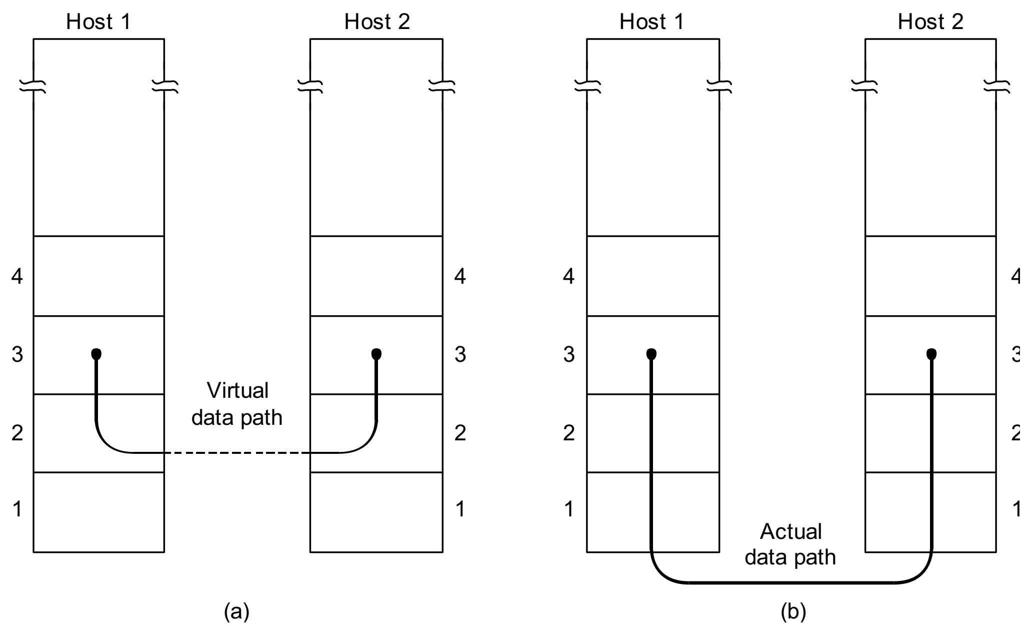
Data Link Layer Functions



DL on a single physical link
(dedicated or shared)

Data Link Layer Functions

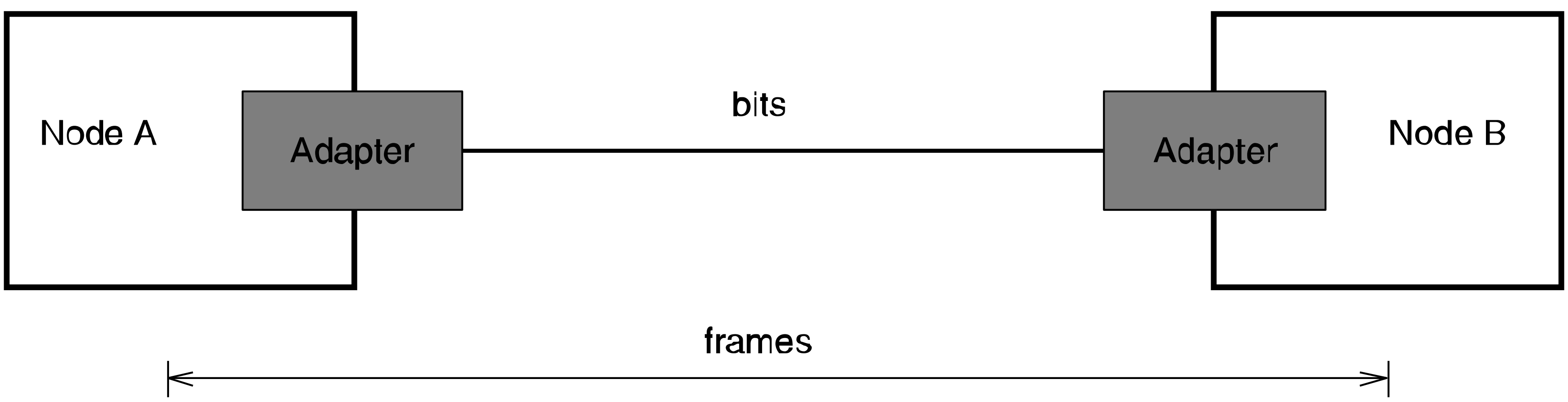
- Framing
- Error detection (checksum)
- Error correction (reliable delivery, e.g. by retransmission)
- Flow control
- Multiplexing / demultiplexing
- MAC (Medium Access Control for shared links)



- Physical Layer provides Data Link Layer with unreliable bit pipe (bits corrupted due to noise, attenuation, etc.)
- Data Link Layer provides Network Layer with (reliable) frames

Framing

- Problem: Breaking sequence of bits into a frame
  - Must determine first and last bit of the frame
  - Typically implemented by network adaptor
  - Adaptor fetches (deposits) frames out of (into) host memory



Bit-Oriented Framing

0111 1110
opening flag

(a) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

0111 1110
closing flag

(b) 0 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 0 0 1 0

sender inserts an extra '0'

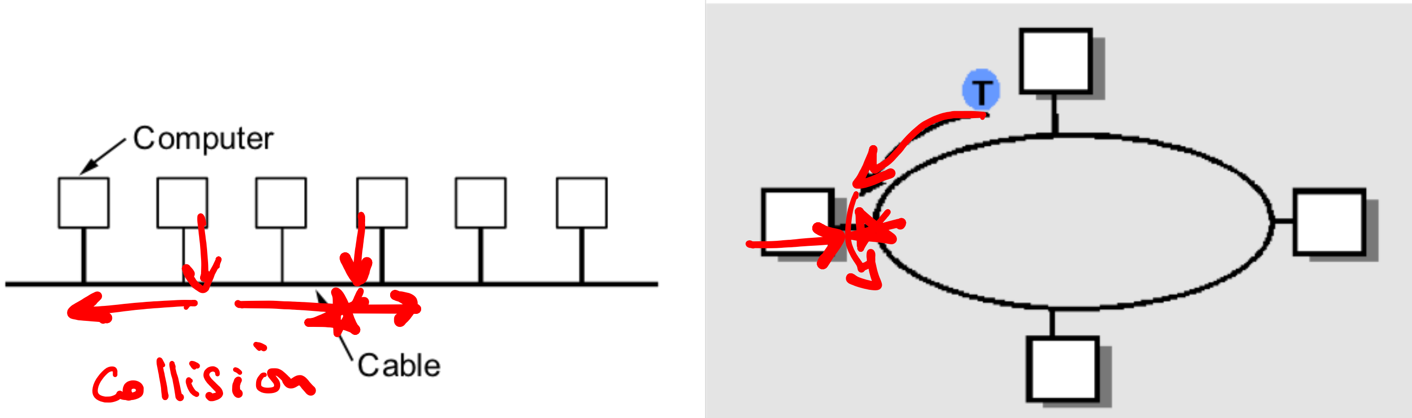
Stuffed bits

receiver removes that extra '0'

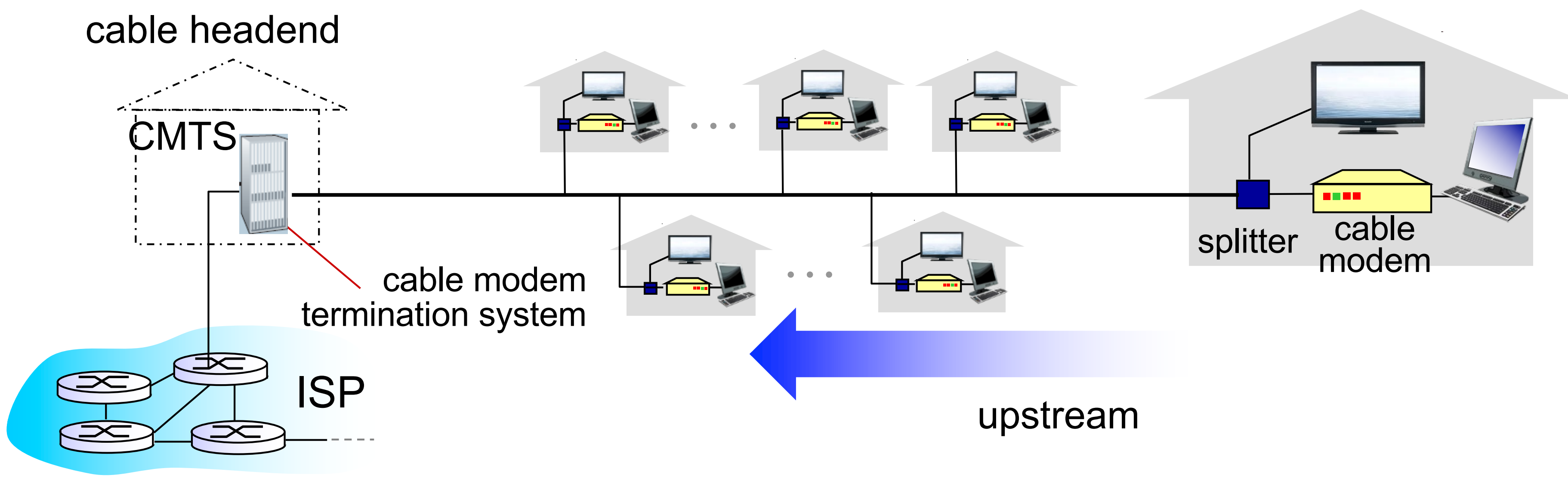
(c) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

- Encapsulates the frame with a special bit pattern (flag), e.g. 01111110
- Problem: flag might appear in the data portion of the frame
- Solution: Bit stuffing is used for "data transparency"

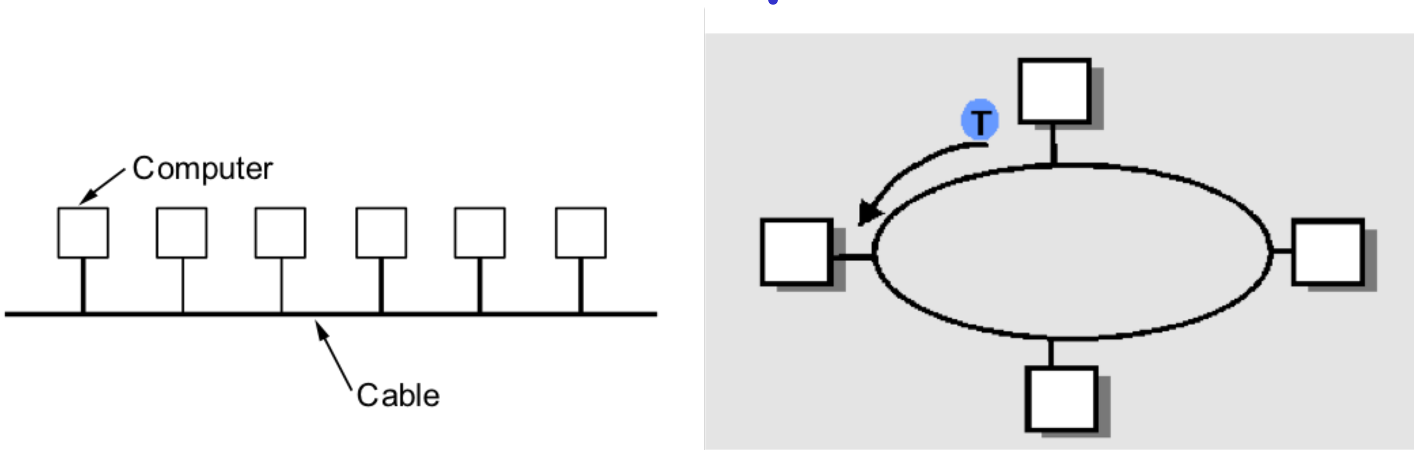
Shared LANs (Multiple-Access Links)



(a) (b)



Shared LANs (Multiple-Access Links)

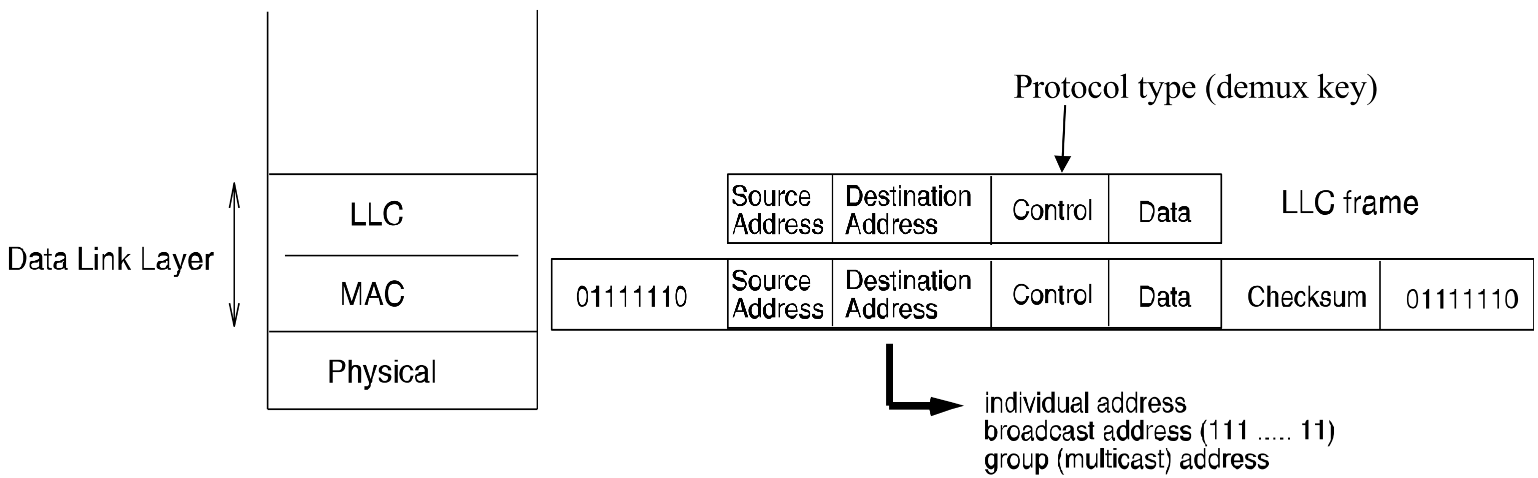


(a) (b)

- Single shared communication link, e.g. shared (old-fashioned) Ethernet, wireless LAN, upstream HFC (cable Internet access network), …
- Two or more simultaneous transmissions by nodes may collide
- Problem: how to share this link
- Solution: distributed algorithm which determines when each node can transmit

Data Link Layer in Shared LANs

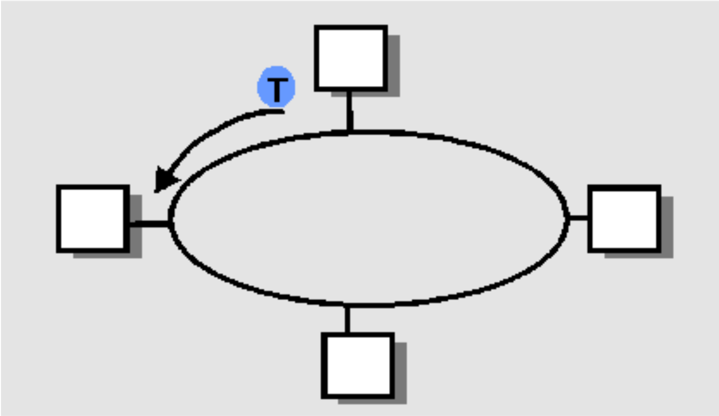
- Two sublayers:
  - MAC (Medium Access Control) sublayer; implements a distributed algorithm to control access to the shared medium. May vary depending on LAN type
  - LLC (Logical Link Control) sublayer; common to all types of LANs. Generally used in connectionless mode unless BER is high



- Framing and error detection are done by the lower MAC sublayer

Multiple Access Protocols

- Random access protocols; nodes contend for channel, collisions (overlapping transmissions) can occur.
  - E.g. Carrier Sense Multiple Access with Collision Detection (CSMA/CD): used in (old-fashioned) Ethernet bus network, half-duplex link, or cable Internet access network (DOCSIS)
- Controlled access protocols; nodes reserve or are assigned channel, no collisions
  - E.g. TDM, FDM, Token Passing (used in token ring network)



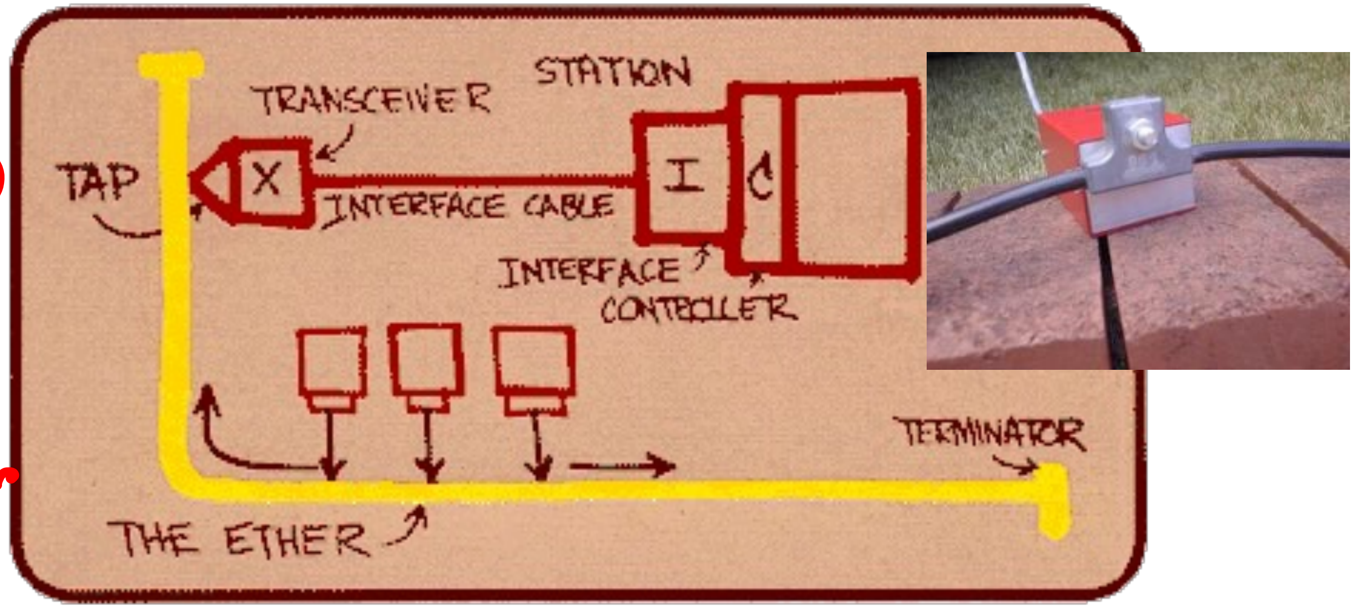
CSMA/CD

Metcalfe's Ethernet sketch

Carrier Sense

Collision Detection

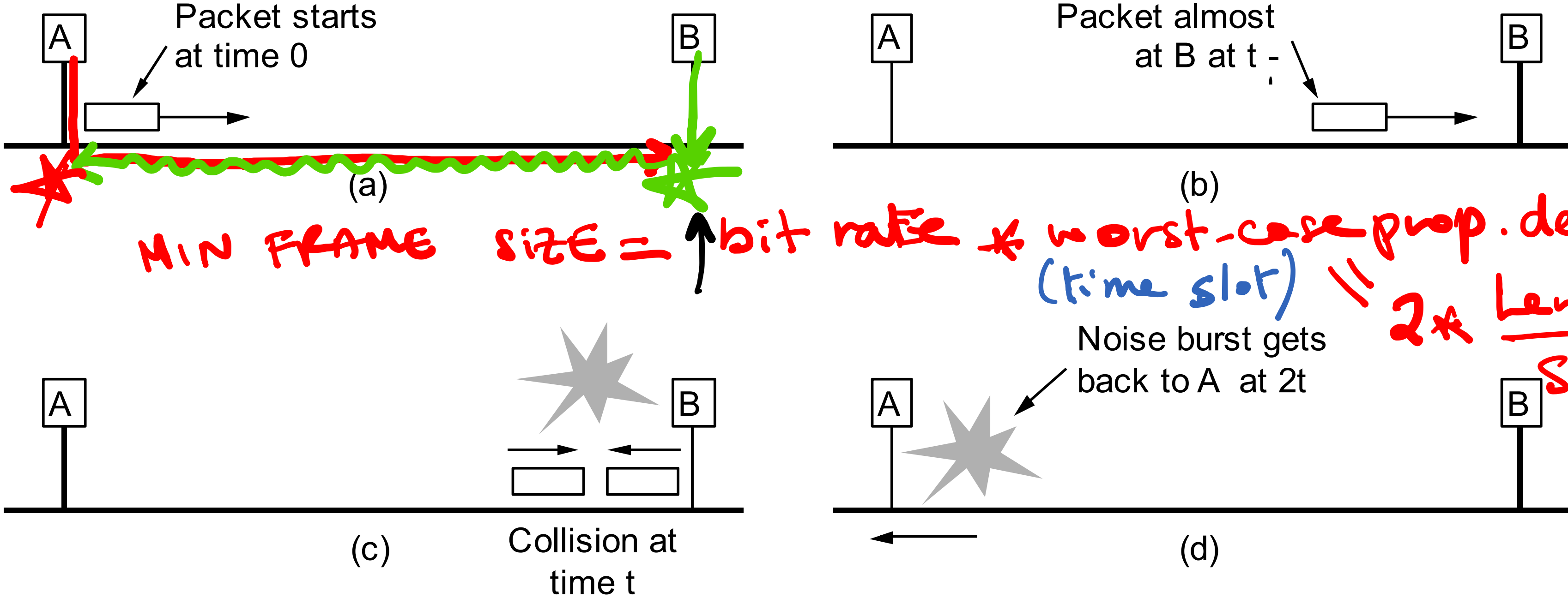
LBT | LWT



- Basic rule: listen before talking (carrier sense) and listen while talking (for collision detection)
- If channel is idle, node can transmit
- If channel is busy, node waits random time and tries later
- While transmitting, if collision is detected, node stops transmitting and waits a random time (i.e. backs off) before it tries to retransmit
- CSMA/CD is not deterministic
- Works well for lightly loaded networks (30% utilization is about max)

CSMA/CD (cont'd)

max frame size
min frame size



MIN FRAME SIZE = bit rate * worst-case prop. delay (time slot) = 2* Length / SOL

- Time required to reliably detect a collision = worst-case round trip propagation delay
- This imposes a minimum frame size (512 bits for 10Mbps, 2500m)
- Performance depends on bit rate and cable length

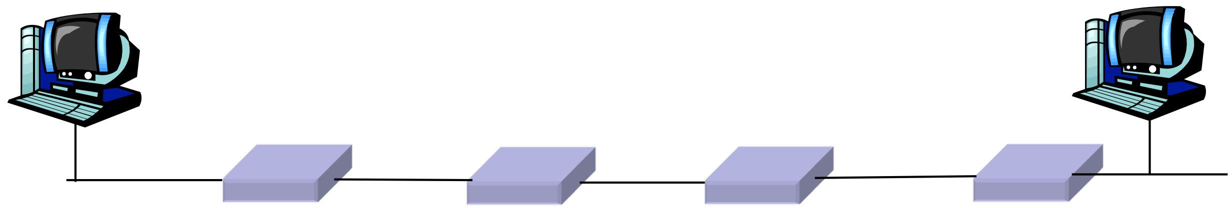
Exponential Backoff

- *Goal*: adapt retransmission attempts to estimated current load
  - heavy load: random wait will be longer
- first collision: choose K from {0,1}; delay is K· 512 bit transmission times
- after second collision: choose K from {0,1,2,3}... #i

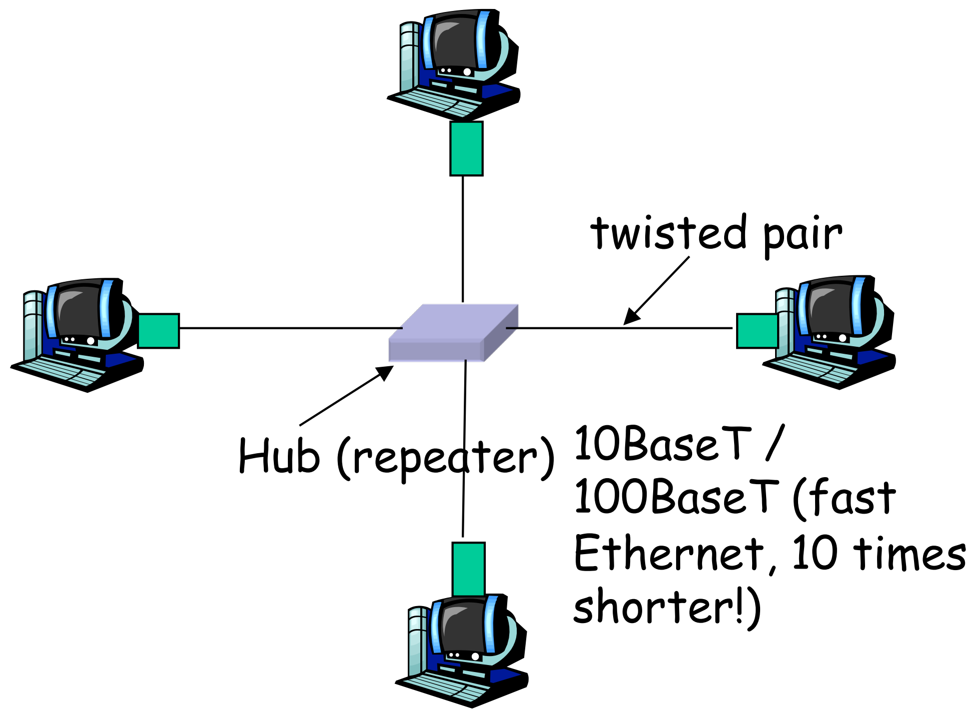
  $\{0, 1, \ldots, 2^i - 1\}$

- after ten collisions, choose K from {0,1,2,3,4,…,1023}

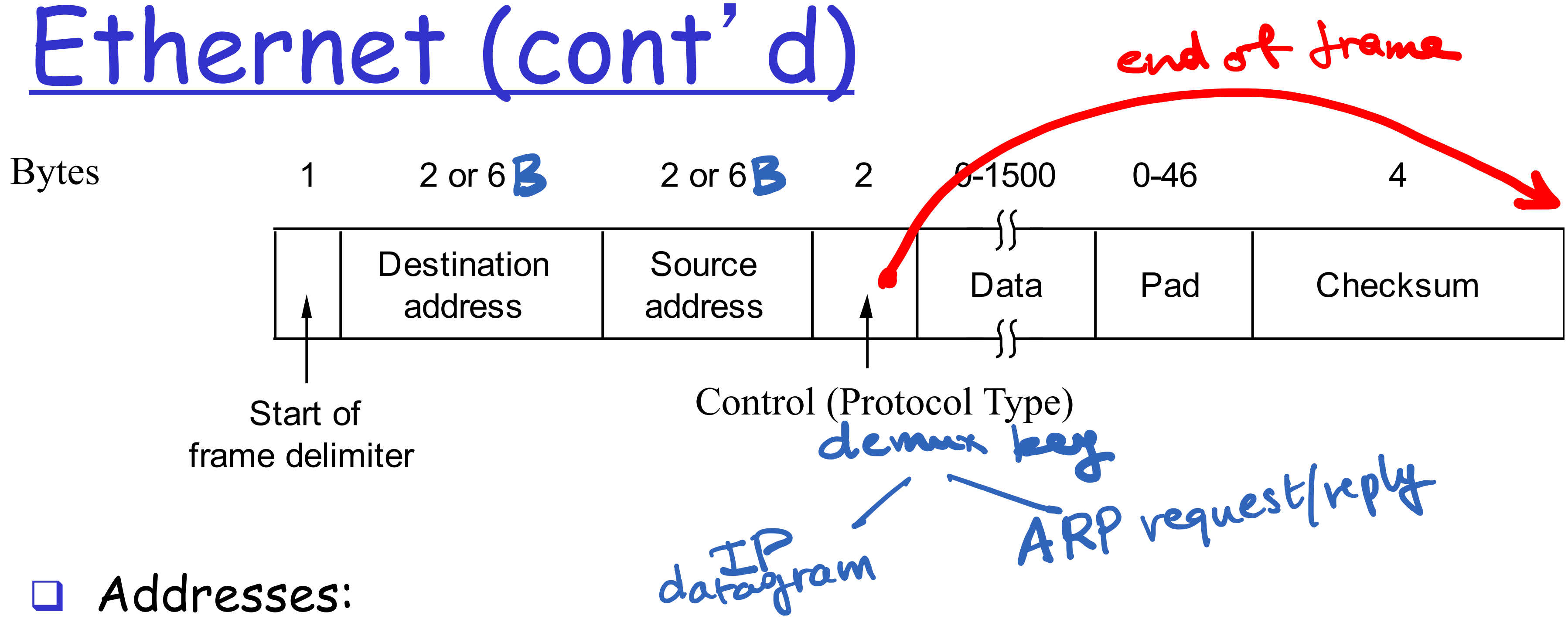
Ethernet



- Uses CSMA/CD
- IEEE 802.3 standard
- Classical Ethernet
  - 10Mbps coaxial cable
  - maximum segment of 500m
  - transceiver taps at least 2.5m apart
  - connect multiple segments with repeaters
  - no more than 4 repeaters between any pair of nodes (2500m total)
  - maximum of 100 hosts per segment
  - also called 10Base5



Ethernet (cont’d)



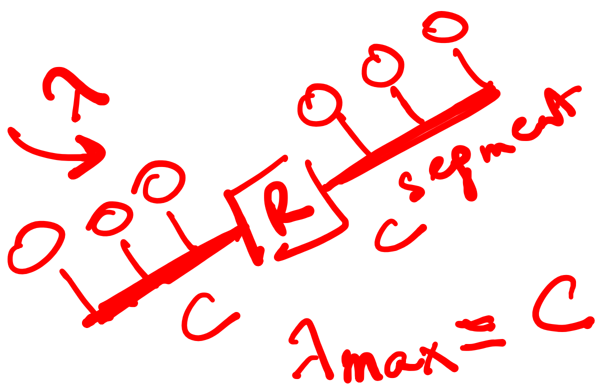
- Addresses:
  - Unique, 48-bit unicast address assigned to each adaptor (IEEE and vendor assigned)
  - Example: 8:0:2b:e4:b1:2
  - Broadcast: all 1s
  - Multicast: first (high-order) bit is 1

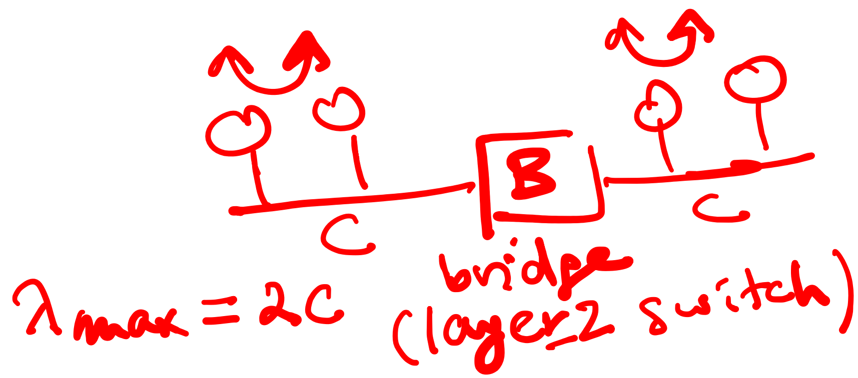
Ethernet (cont'd)

- Adaptor receives all (error-free) frames; it accepts (passes to host):
  - Frames addressed to its own unicast address
  - Frames addressed to the broadcast address
  - Frames to any multicast (group) address it has been programmed to accept
  - All frames when in promiscuous mode

Bridges and Extended LANs

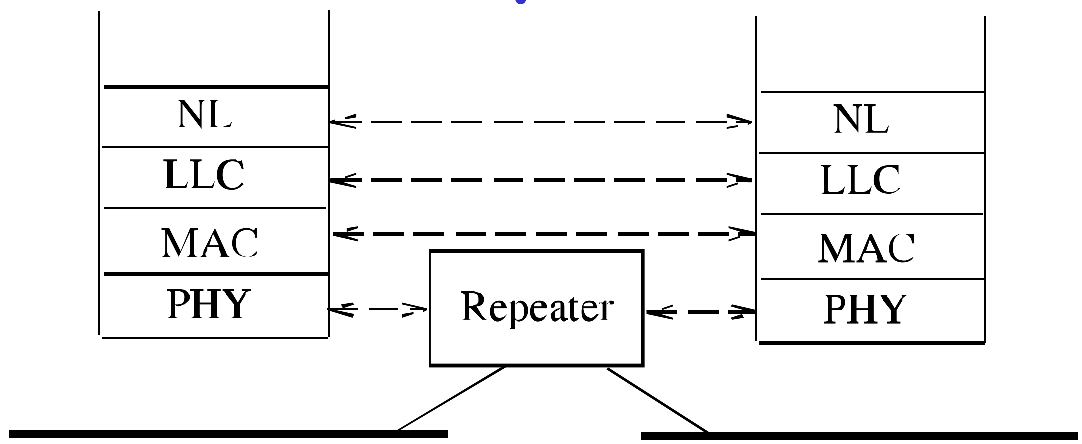
- LANs can support limited amount of traffic (workload): on a single LAN, all computers must share capacity
- LANs have distance limitations (e.g., 2500m Ethernet)





- **Solution:** connect two or more LANs with a repeater (hub) or bridge (layer-2 switch)

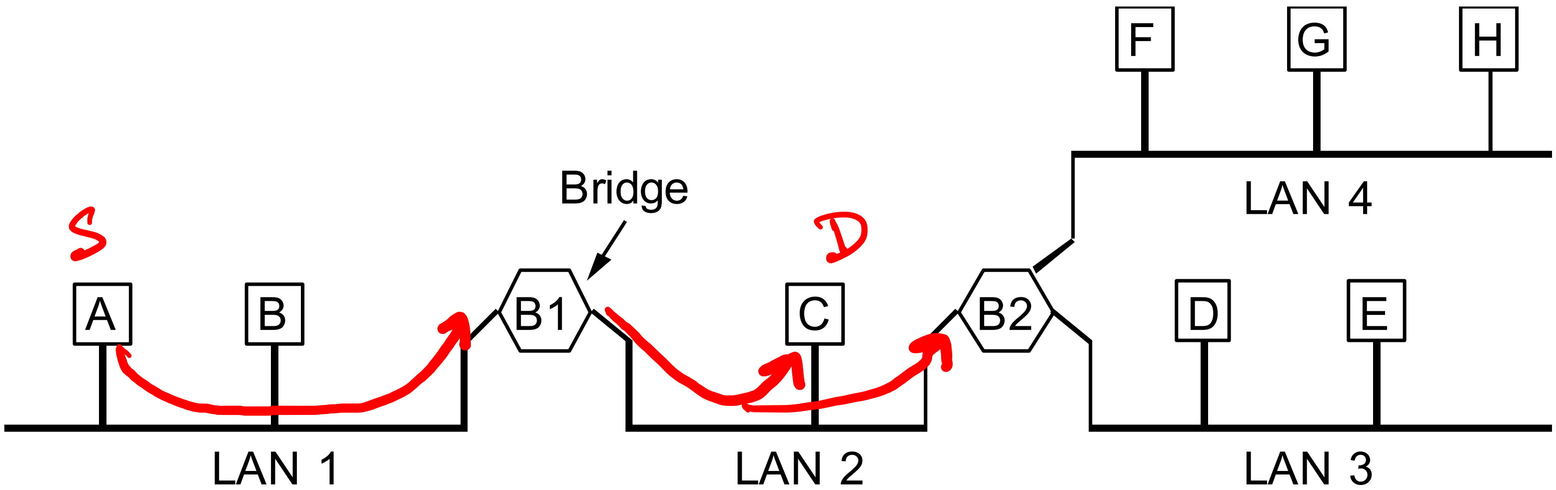
Bridges versus Repeaters



Repeater:

- copies (amplifies, regenerates) bits between LAN segments
- no storage of frames
- physical-level (only) interconnection of LANs
- solves only the distance problem, but not the workload problem: each LAN segment will have to carry the total traffic / workload coming from all users

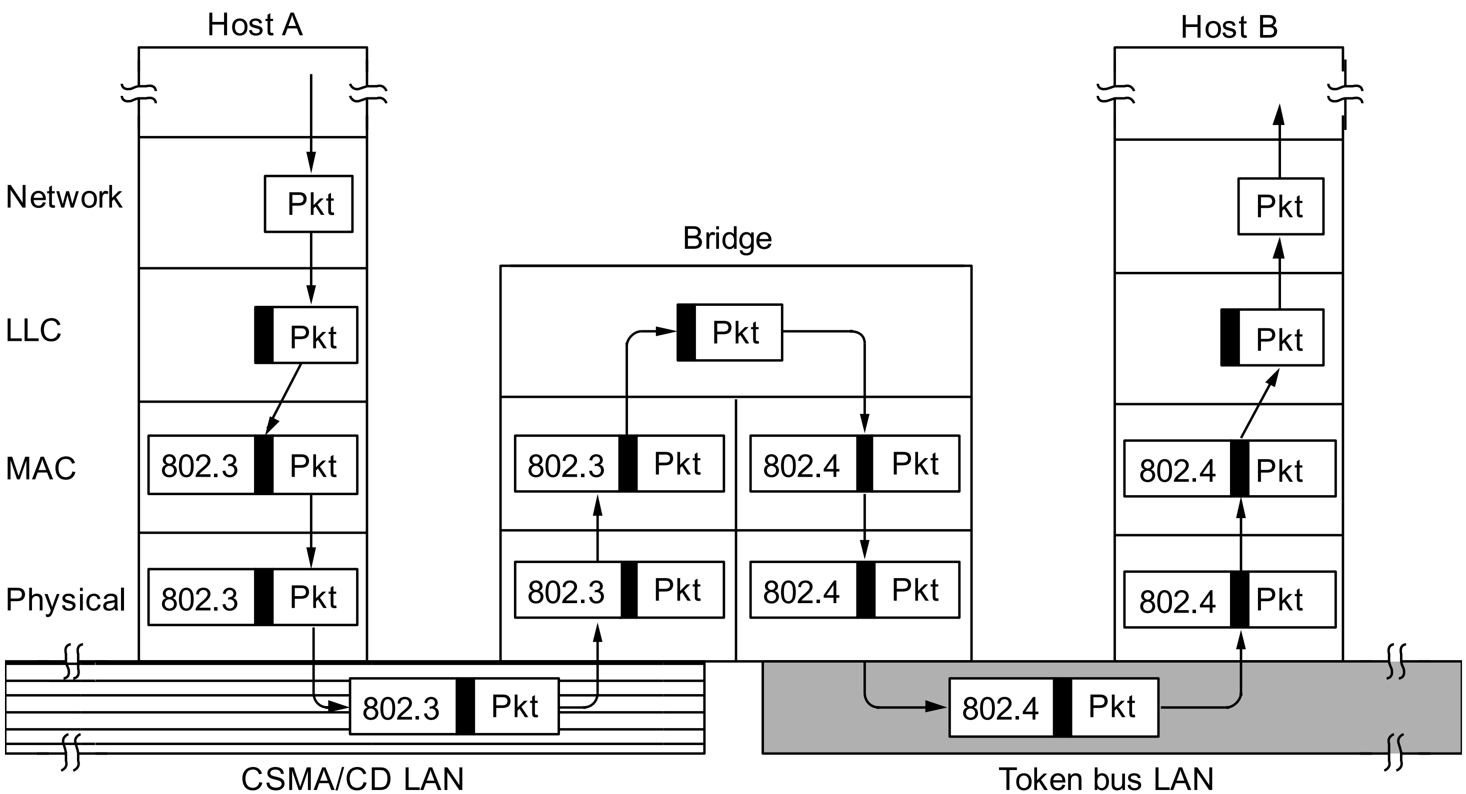
Bridges versus Repeaters (cont'd)



Bridge:

- receives, stores, forward (when appropriate) frames between LANs
- forwarded frames are error-free
- demand is reduced on each LAN segment: total workload can be greater than the capacity of individual segments
- solves both distance and workload problems

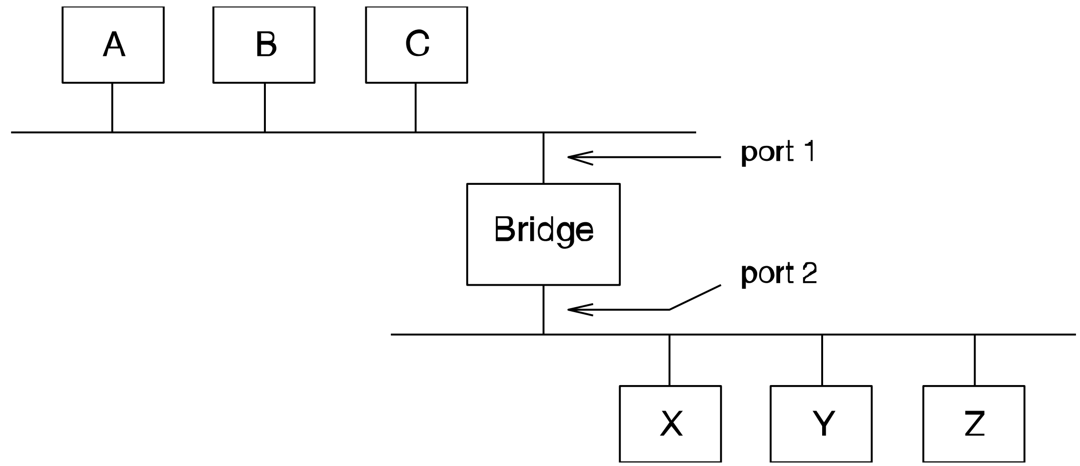
Bridged LAN



- Bridge has two layers of protocol stack: physical and link-level

Transparent (Spanning-Tree) Bridges

- routing of frames is transparent to hosts
- bridges maintain routing information / tables and make routing decisions
- routing table at a bridge lists for each destination host what is the output port



Host (MAC address)	Port
A	1
B	1
C	1
X	2
Y	2
Z	2

Frame Forwarding/Filtering

- When a bridge receives a frame, it looks up its routing table with the destination address in the header of the frame
- If the output port is the same as the input port, the bridge discards the frame
- Otherwise, the bridge forwards the frame to the specified output port

Bridge (self-)Learning

- Bridge ``observes'' traffic and ``learns'' which computers are reachable via each port based on source address
- Table is an optimization; need not be complete
- bridge receives every frame transmitted on every attached LAN (operates in promiscuous mode)
- bridge stores for each frame
  - MAC address of sender
  - port (incoming LAN segment) on which frame was received
- for each frame received on any port: lookup destination MAC address in table
  - if not found, flood onto all other attached LANs
  - if found, forward only out to specified LAN
- forwarding entry deleted if not refreshed