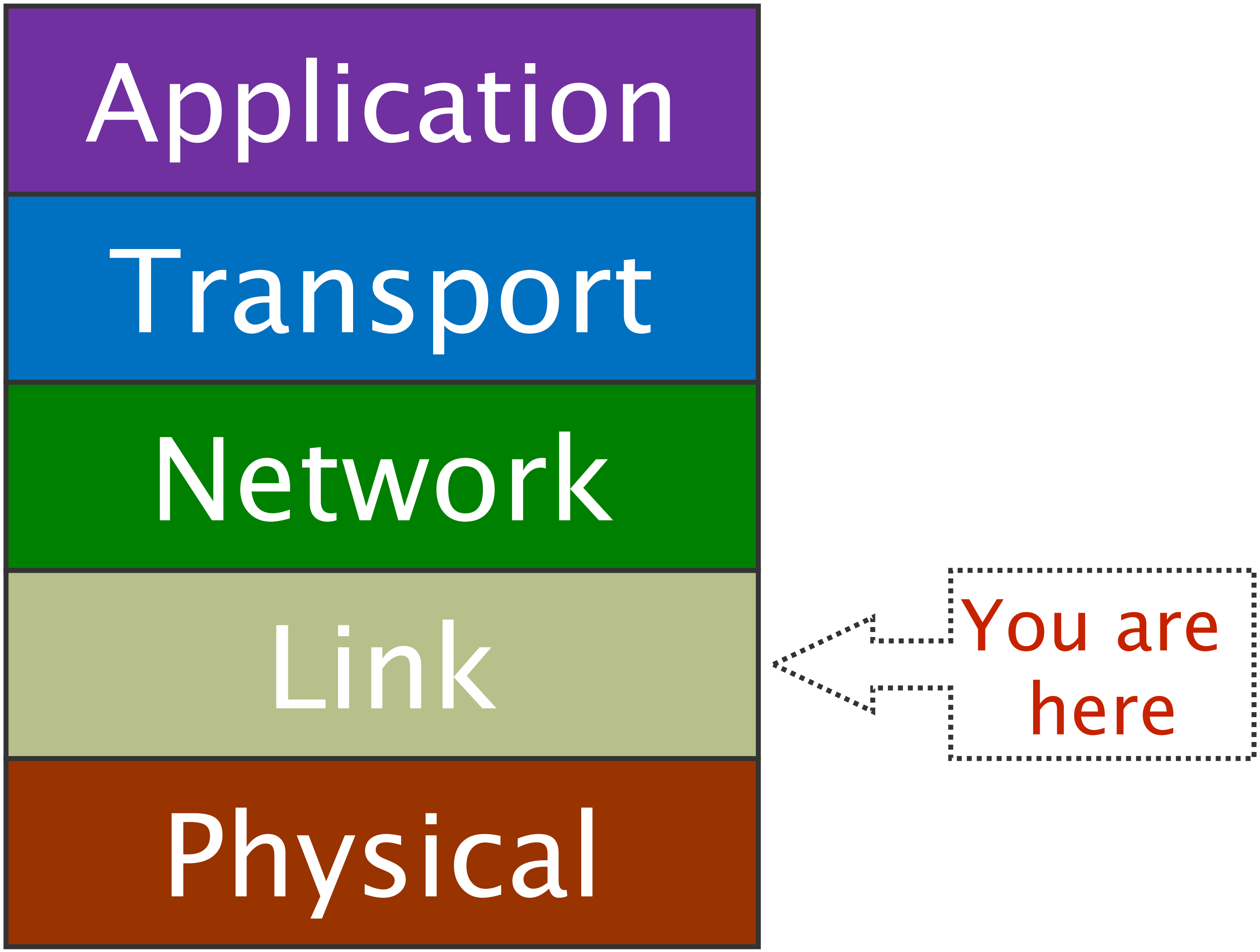
CS2105

An *Awesome* Introduction to Computer Networks

Lecture 8: The Link Layer, Part I

NUS National University of Singapore
Department of Computer Science
School of Computing


Application
Transport
Network
Link
Physical
You are here

Lectures 8&9: The Link Layer

After the next 2 classes, you are expected to understand:

- the role of link layer and the services it could provide.
- how parity and CRC scheme work.
- different methods for accessing shared medium.
- how ARP allows a host to discover the MAC addresses of other nodes in the same subnet.
- the role of switches in interconnecting subnets in a LAN.

L9

Lecture 8: Roadmap

6.1 Introduction to the Link Layer

6.2 Error Detection and Correction

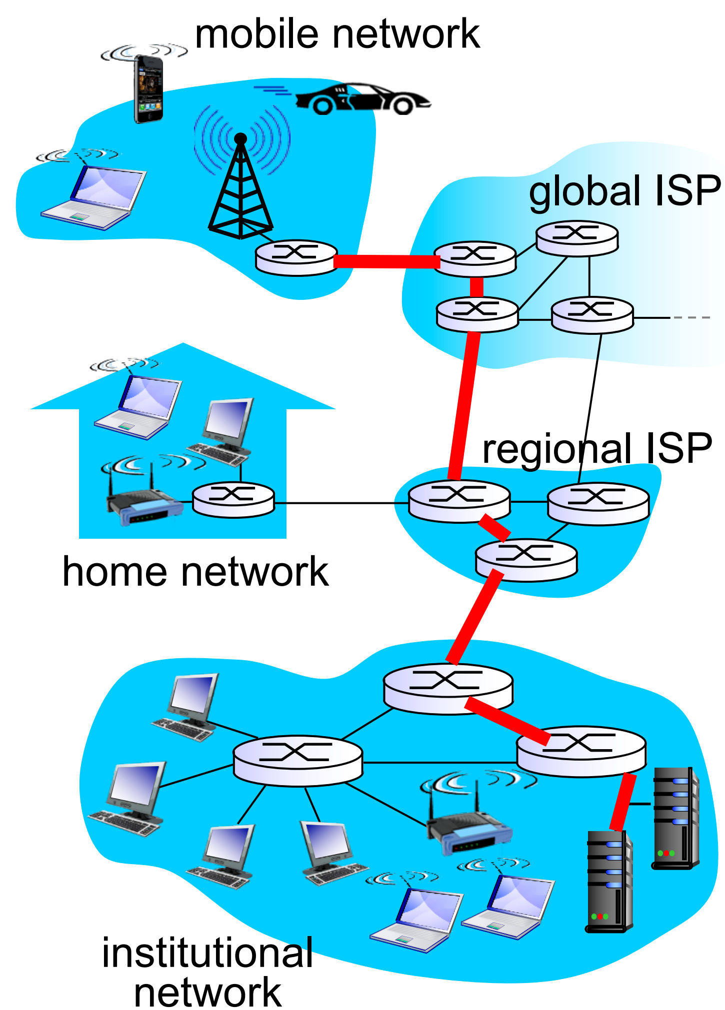
6.3 Multiple Access Links and Protocols

6.4 Switched Local Area Networks

Kurose Textbook, Chapter 6
(Some slides are taken from the book)

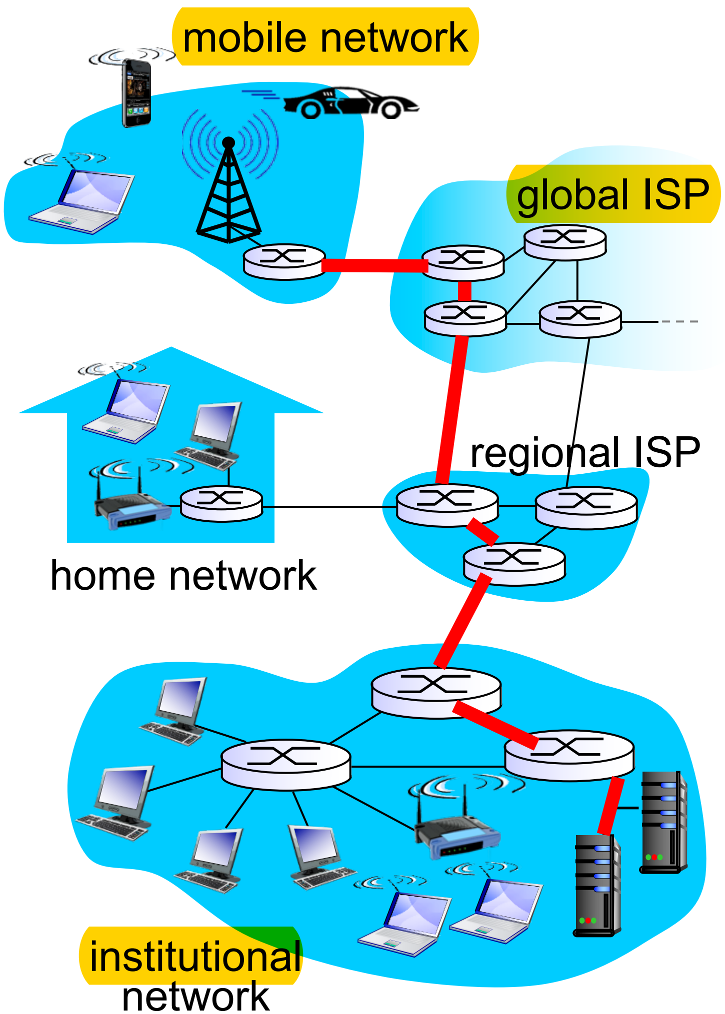
Link Layer: Introduction (1/2)

- Network layer provides communication service between any two hosts.
- An IP datagram may travel through multiple routers and links before it reaches destination.



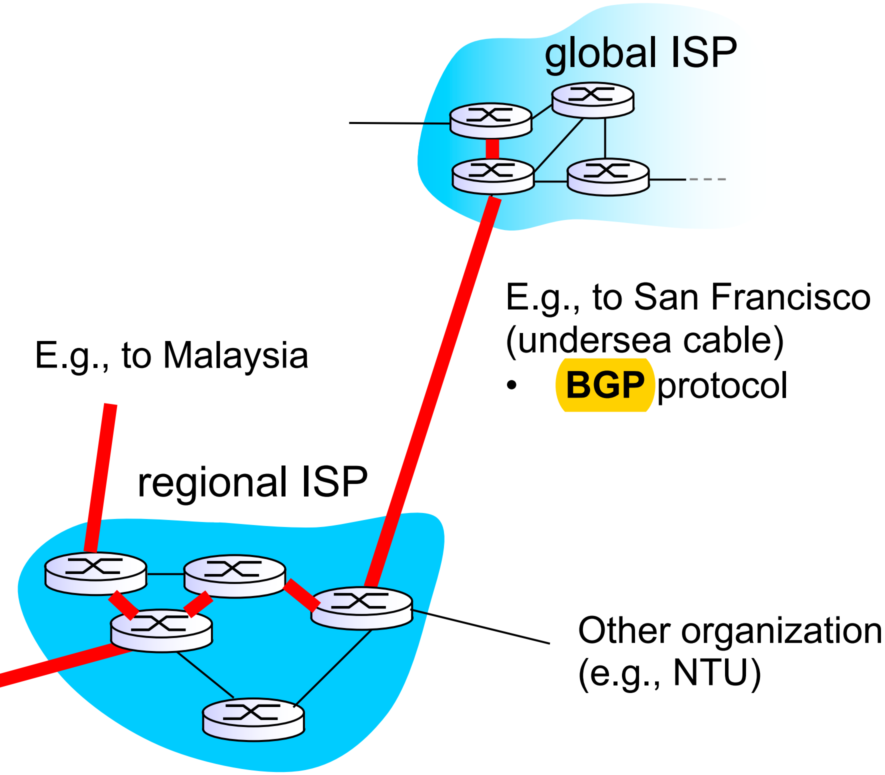
Link Layer: Introduction (2/2)

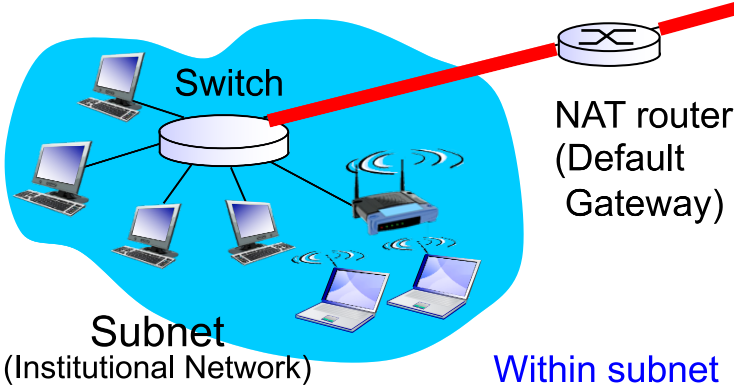
- Link layer sends datagram between adjacent nodes (hosts or routers) over a single link.
  - IP datagrams are encapsulated in link-layer frames for transmission.
  - Different link-layer protocols may be used on different links.
    - Each protocol may provide a different set of services.



Routing: Big Picture

Hub or Switch = "  "





- **BGP** protocol

DHCP protocol provides:
- IP address, e.g., 192.168.0.x/24
- Subnet mask, e.g., 255.255.255.0
- IP of DNS server
- IP of Default Gateway (e.g.: 192.168.0.1)

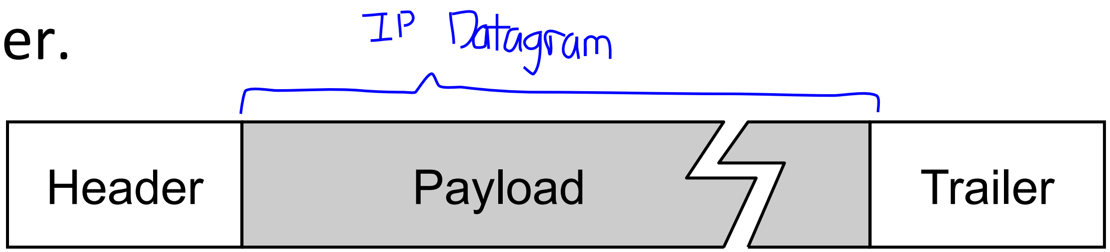
Which link/path to choose?

Intra-AS routing
- **RIP, OSPF** protocols
- Distributed algo.
- Build routing table

Within subnet
- **ARP** protocol

Possible Link Layer Services (1/2)

- Framing
  - Encapsulate datagram into frame, adding header and trailer.



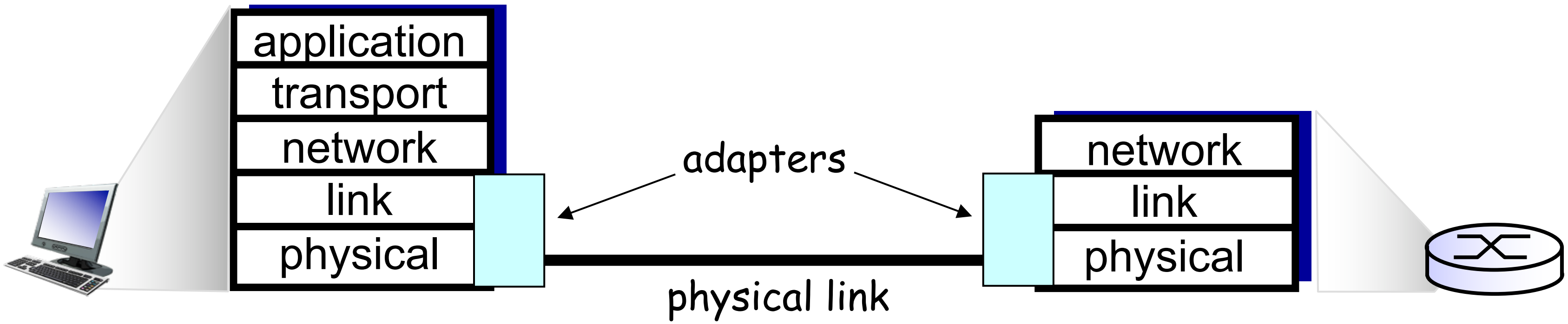
- Link access control
  - When multiple nodes *share* a single link, need to coordinate which nodes can send frames at a certain point of time.

humans at a cocktail party (shared air)

Possible Link Layer Services (2/2)

- Reliable delivery
  - Seldom used on low bit-error link (e.g., fibre) but often used on error-prone links (e.g., wireless link).
- Error detection
  - Errors are usually caused by signal attenuation or noise.
  - Receiver detects presence of errors.
    - *may signal sender for retransmission or simply drops frame*
- Error correction
  - Receiver identifies and corrects bit error(s) without resorting to retransmission.

Link Layer Implementation



- Link layer is implemented in "adapter" (aka NIC) or on a chip.
  - E.g., Ethernet card/chipset, 802.11 card
- Adapters are semi-autonomous, implementing both link & physical layers.

Lectures 8&9: Roadmap

6.1 Introduction to the Link Layer

6.2 Error Detection and Correction

- 6.2.1 Parity Checks
- 6.2.3 Cyclic Redundancy Check (CRC)

6.3 Multiple Access Links and Protocols

6.4 Switched Local Area Networks

Error Detection and Correction

- Popular error detection schemes:
  - Checksum (used in TCP/UDP/IP)
  - Parity Checking
  - CRC (commonly used in link layer)
- Error detection schemes are not 100% reliable!
  - may miss some errors, but rarely.
  - larger error detection and correction (EDC) field yields better detection (and even correction).

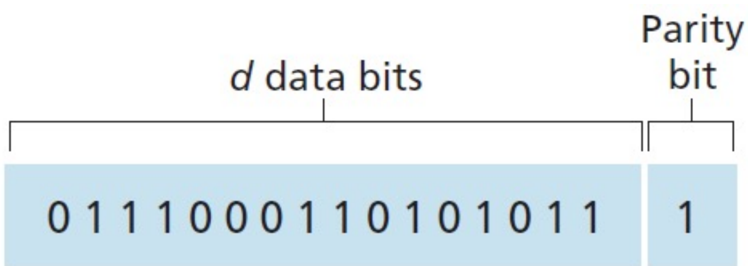
Tradeoff - the better the error detection / correction scheme is, the higher the overhead will be

Parity Checking

2d bit parity has a much higher overhead in terms of space
- requires 9 more extra bits for the same 15 bit data
as compared to single bit parity only needing 1

Single bit parity

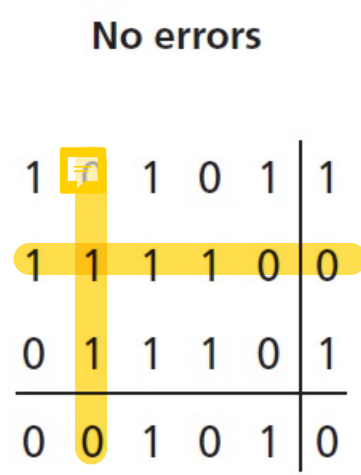
- can detect single bit errors in data.



This will fail when 2 bits flip
- since their effects will be cancelled out

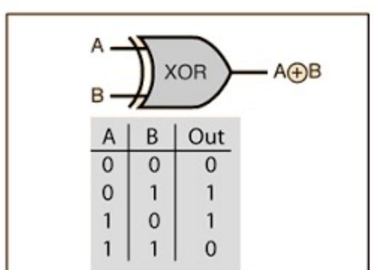
Two-dimensional bit parity

- can detect and correct single bit errors in data.
- can detect any two-bit error in data.



Cyclic Redundancy Check (CRC)

- Powerful error-detection coding that is widely used in practice (e.g., Ethernet, Wi-Fi)
  - D: data bits, viewed as a binary number.
  - G: generator of $r+1$ bits, agreed by sender and receiver beforehand.
  - R: will generate CRC of r bits.



Example: $r = 3$

```
1001 ) 101110000
       1001
       ----
         10
         1001
         ----
           1100
           1001
           ----
            1010
            1001
            ----
             011
```

G

D

R

Cyclic Redundancy Check (CRC)

- CRC calculation is done in bit-wise XOR operation without carry or borrow.
- Sender sends (D, R)

  101110011

- Receiver knows G, divides (D, R) by G.
  - If non-zero remainder: error is detected!

Example: $r = 3$

```
1001 ) 101110000
       1001
       ----
        1010
        1001
        ----
         1100
         1001
         ----
          1010
          1001
          ----
           011
```

G

D

R

Lectures 8&9: Roadmap

6.1 Introduction to the Link Layer

6.2 Error Detection and Correction

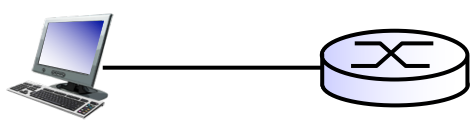
6.3 Multiple Access Links and Protocols

- 6.3.1 Channel Partitioning Protocols
- 6.3.2 Random Access Protocols
- 6.3.3 Taking-Turns Protocols

6.4 Switched Local Area Networks

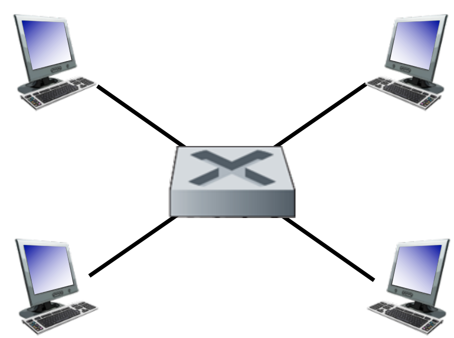
Two Types of Network Links

- **Type 1: point-to-point link**
  - A sender and a receiver connected by a dedicated link
  - Example protocols: Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP)
    - No need for multiple access control



A host connects to router through a dedicated link

RJ45

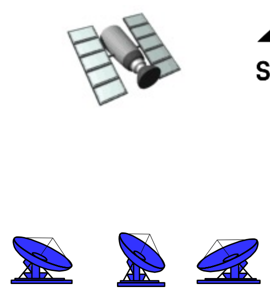


A point-to-point link between Ethernet switch and a host

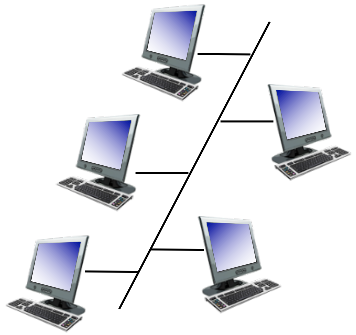
Two Types of Network Links

- **Type 2: broadcast link** (shared medium)
  - Multiple nodes connected to a shared broadcast channel.
  - When a node transmits a frame, the channel broadcasts the frame and each other node receives a copy.

802.11 Wi-Fi



Satellite



Ethernet with bus topology

Multiple Access Protocols

- In a broadcast channel, if two or more nodes transmit simultaneously
  - Every node receives multiple frames at the same time ➜ frames *collide* at nodes and none would be correctly read.
- Multiple Access Protocol
  - distributed algorithm that determines how nodes share channel, i.e. when a node can transmit.
  - However, coordination about channel sharing must use channel itself!
    - *no out-of-band channel signaling*

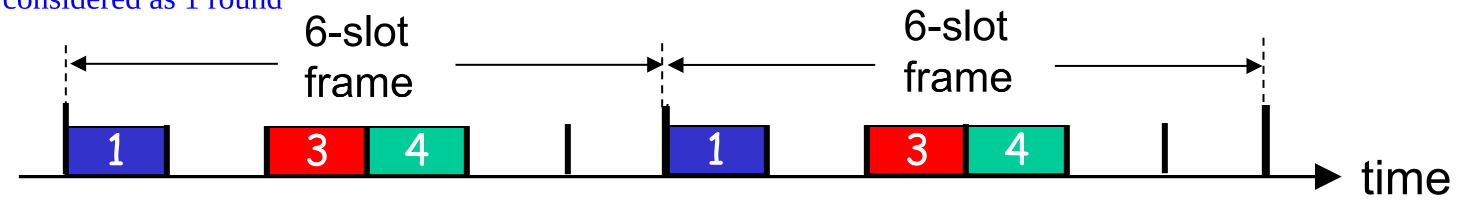
Multiple Access Protocols

- Multiple access protocols can be categorized into three broad classes:
  - **Channel partitioning**
    - divide channel into fixed, smaller "pieces" (e.g., time slots, frequency).
    - allocate piece to node for exclusive use.
  - **"Taking turns"**
    - nodes take turns to transmit.
  - **Random Access**
    - channel is not divided, collisions are possible.
    - "recover" from collisions.

Channel Partitioning Protocols

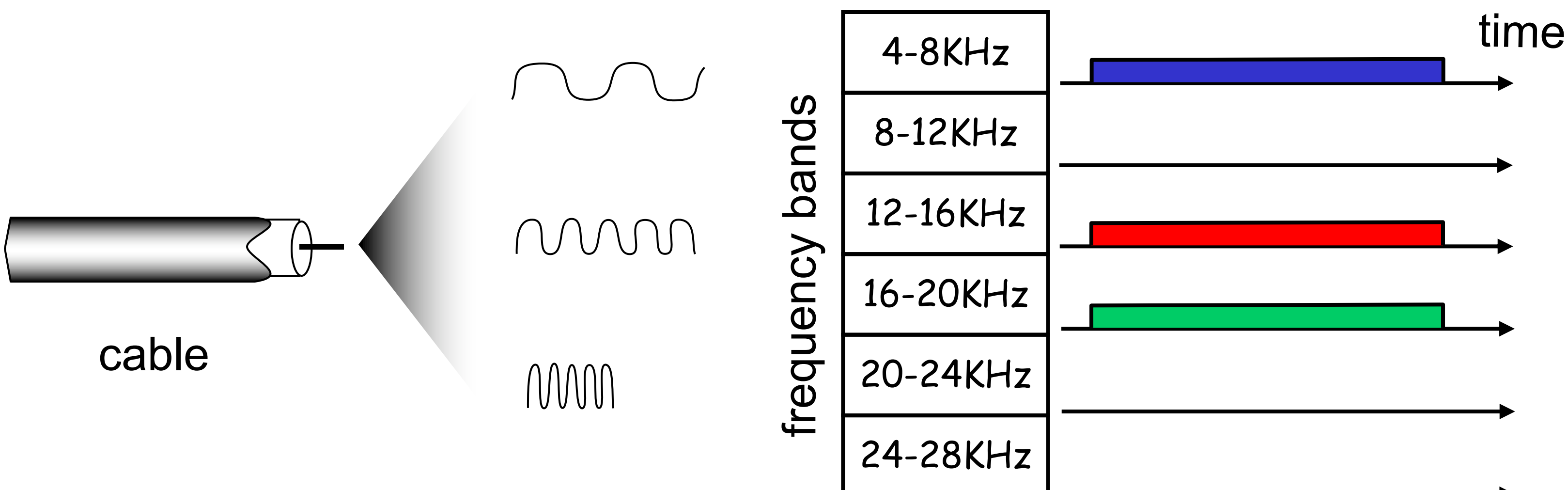
- TDMA (time division multiple access)
  - Access to channel in "rounds".
  - Each node gets fixed length slot (length = frame transmission time) in each round.
  - Unused slots go idle.
  - Example: 6 nodes sharing a link, 1, 3, 4 have frames, slots 2, 5, 6 are idle.

this is considered as 1 round



Channel Partitioning Protocols

- FDMA (frequency division multiple access)
  - Channel spectrum is divided into frequency bands.
  - Each node is assigned a fixed frequency band.
  - Unused transmission time in frequency bands go idle.
  - Example: 6 nodes, 1, 3, 4 have frames, frequency bands 2, 5, 6 are idle.



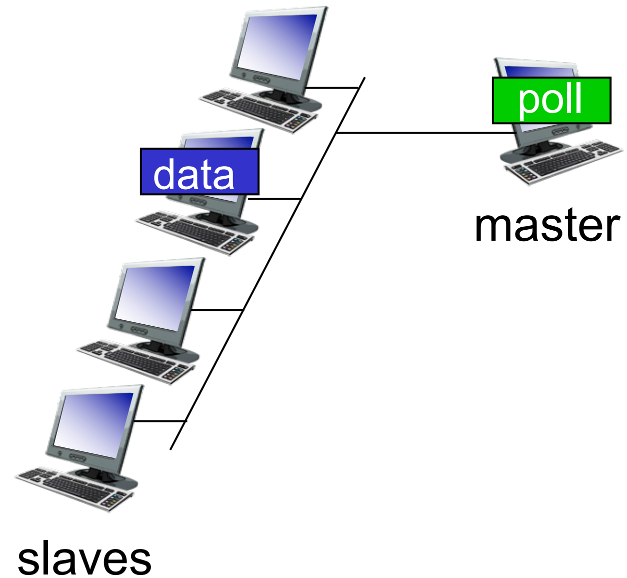
Multiple Access Protocols

- Multiple access protocols can be categorized into three broad classes:
  - Channel partitioning
    - divide channel into fixed, smaller "pieces" (e.g., time slots, frequency).
    - allocate piece to node for exclusive use.
  - **"Taking turns"**
    - nodes take turns to transmit.
  - Random Access
    - channel is not divided, collisions are possible.
    - "recover" from collisions.

"Taking Turns" Protocols

Polling:

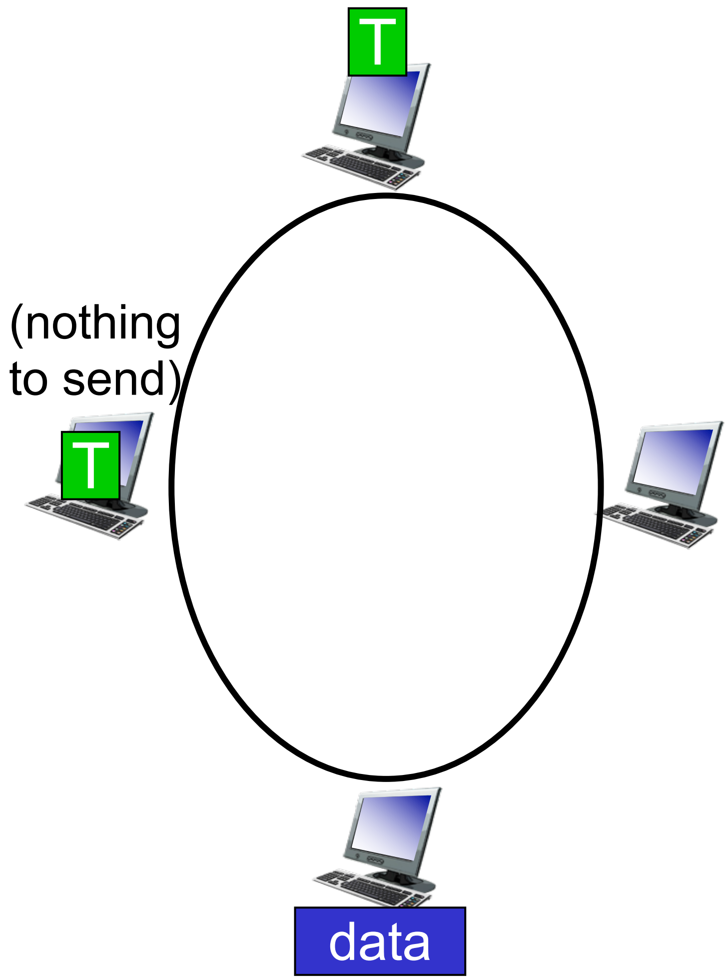
- master node "invites" slave nodes to transmit in turn.
- concerns:
  - polling overhead
  - single point of failure (master node)



"Taking Turns" Protocols

Token passing:

- control token is passed from one node to next sequentially.
- concerns:
  - token overhead
  - single point of failure (token)



Multiple Access Protocols

- Multiple access protocols can be categorized into three broad classes:
  - Channel partitioning
    - divide channel into smaller "pieces" (e.g., time slots, frequency).
    - allocate piece to node for exclusive use.
  - "Taking turns"
    - nodes take turns to transmit.
  - **Random Access**
    - channel is not divided, collisions are possible.
    - "recover" from collisions.

Random Access Protocols

- When node has packet to send
  - no *a priori* coordination among nodes
  - two or more transmitting nodes ➜ "collision"
- Random access protocols specify:
  - how to detect collisions
  - how to recover from collisions (e.g., via delayed retransmissions)
- We will skip the mathematical formulas on the efficiency of random access protocols.

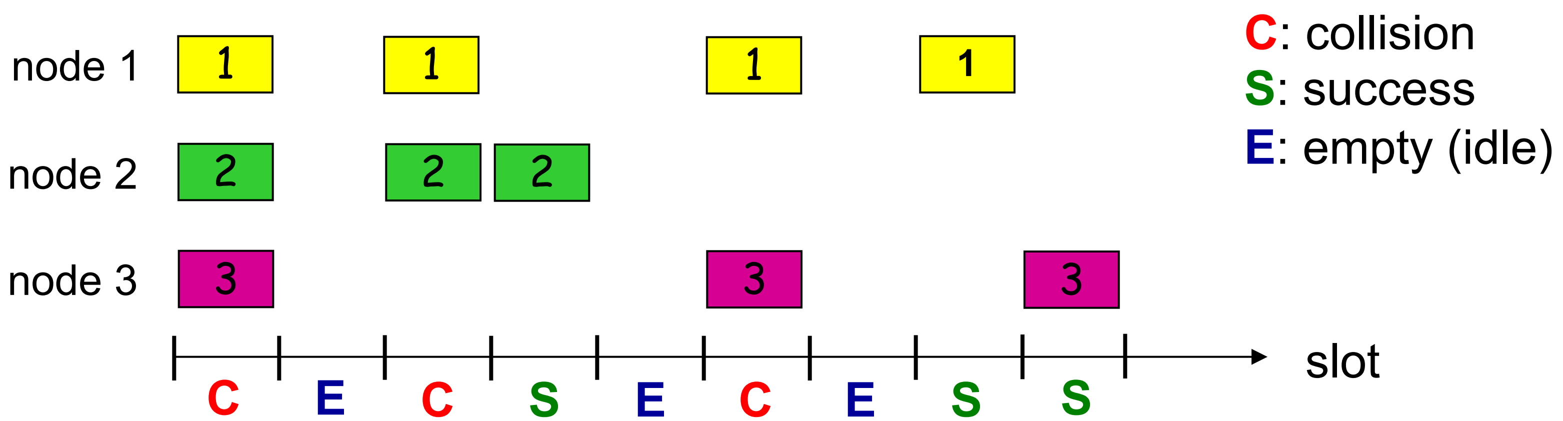
Slotted ALOHA

Assumptions:

- All frames are of equal size.
- Time is divided into slots of equal length (length = time to transmit 1 frame).
- Nodes start to transmit only at the beginning of a slot.

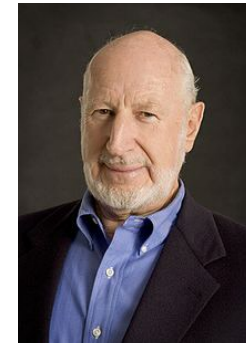
Operations:

- Listens to the channel while transmitting (**collision detection**).
- *if collision happens:* node retransmits a frame in each subsequent slot with probability p until success.



A Little Side Note

Figure 1 *ALOHA TCU 1971*

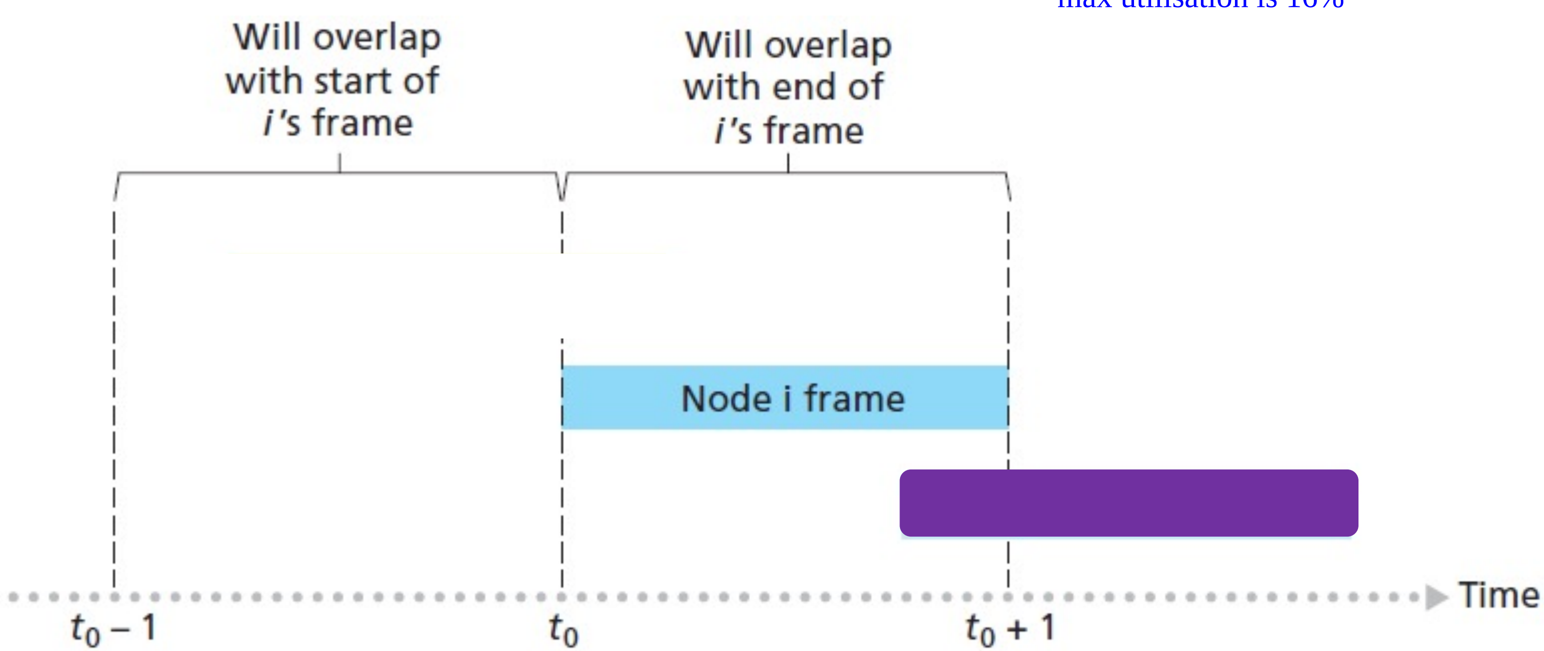


- Q: Why is it called ALOHA?
- A: The **ALOHAnet**, also known as the ALOHA System, or simply ALOHA, was a pioneering computer networking system developed – maybe you can guess it – at the University of Hawaii.
- Norman Abramson was the leader of the team.
- The idea was to use a radio network to connect Oahu and the other Hawaiian islands together. ALOHA made use of one, shared, inbound channel, and thus requiring a novel ***multiple access protocol***.

Pure (unslotted) ALOHA

- Even simpler: no slot, no synchronization
  - When there is a fresh frame: transmit immediately
  - Chance of collision increases:
    - frame sent at t_0 collides with other frames sent in $(t_0 - 1, t_0 + 1)$

max utilisation is 16%



Carrier Sense Multiple Access

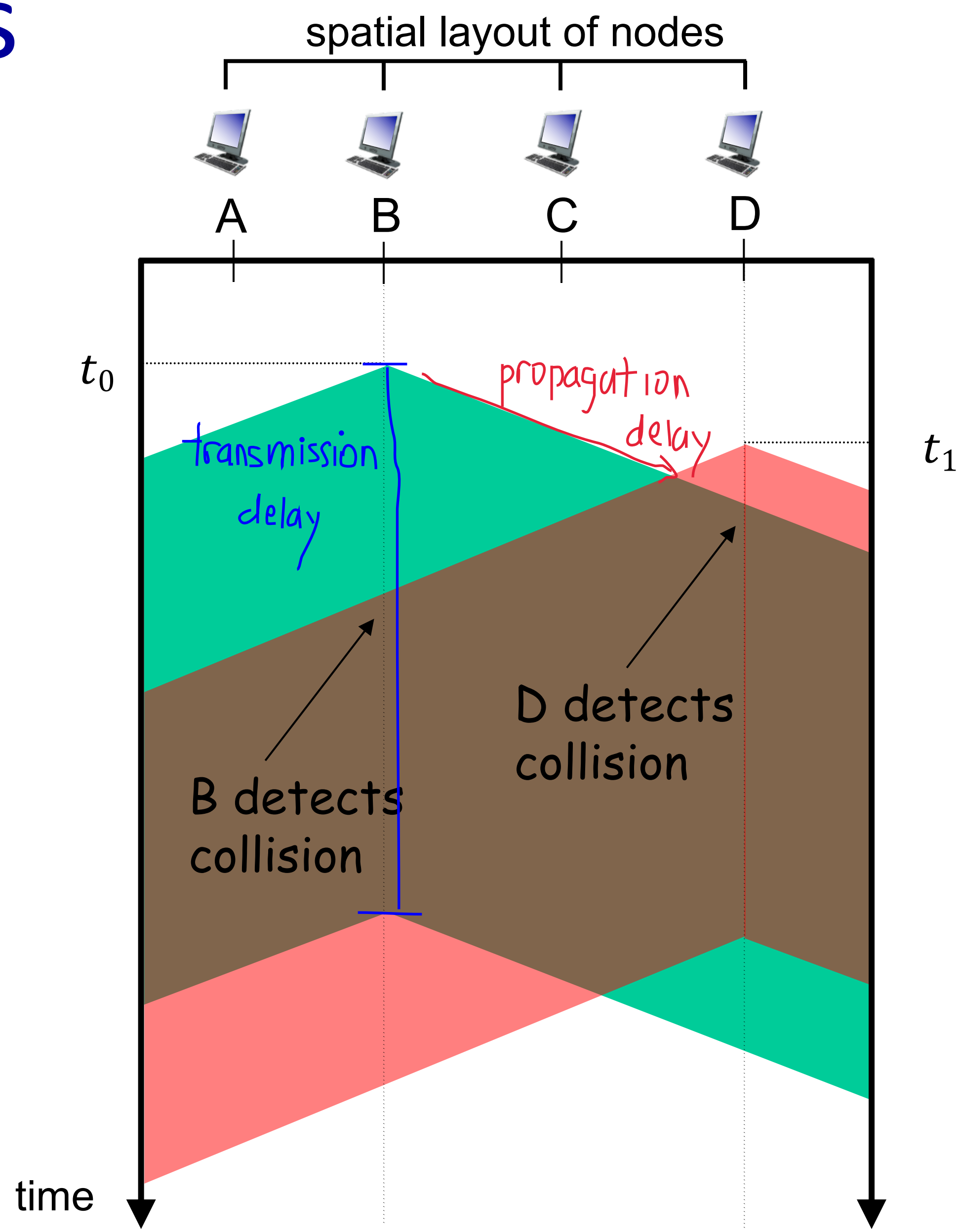
- CSMA (carrier sense multiple access)
  - Sense the channel before transmission:
    - if channel is sensed idle, transmit frame
    - if channel sensed busy, defer transmission

- Human analogy: don’t interrupt others!

- Q: Will collision ever happen in CSMA?
  - collisions may still exist, e.g., when two nodes sense the channel idle at the same time and both start transmission.

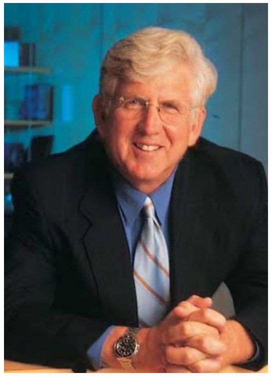
CSMA Collisions

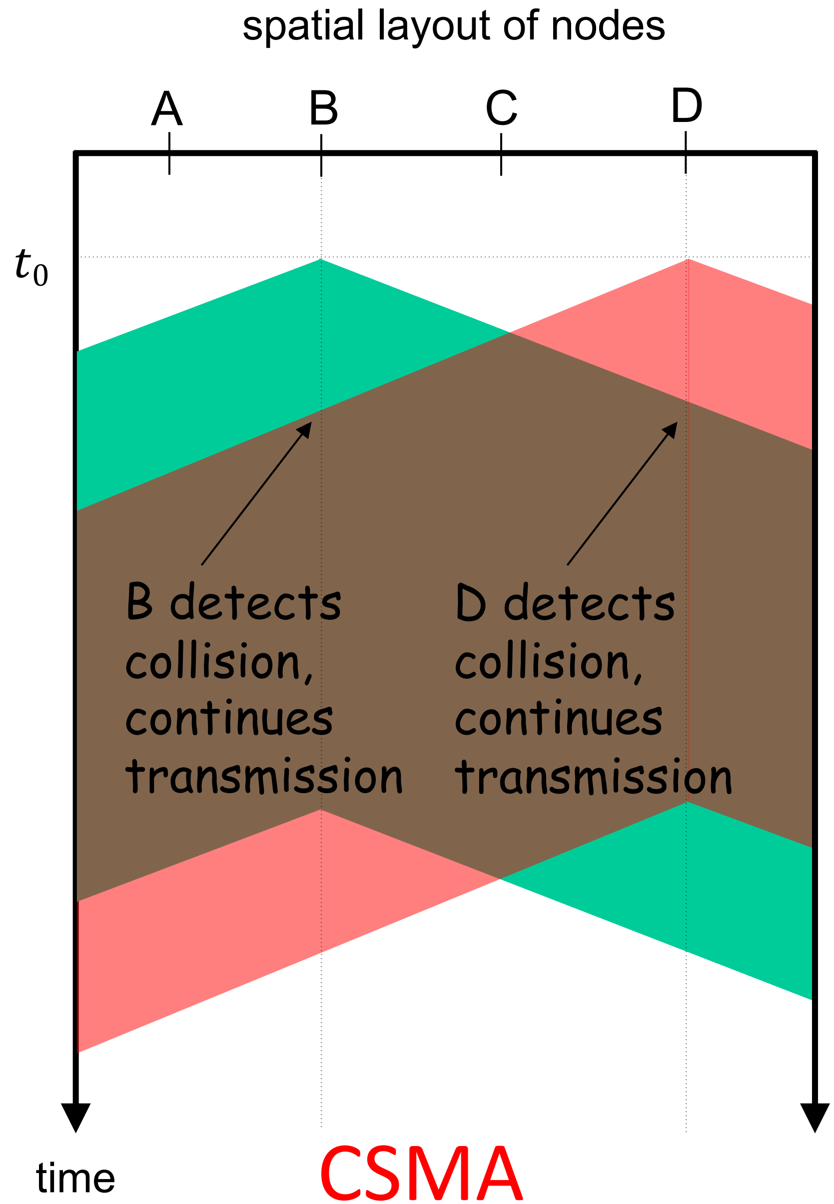
- Collisions can still occur:
  - propagation delay means two nodes may not hear each other's transmission immediately.



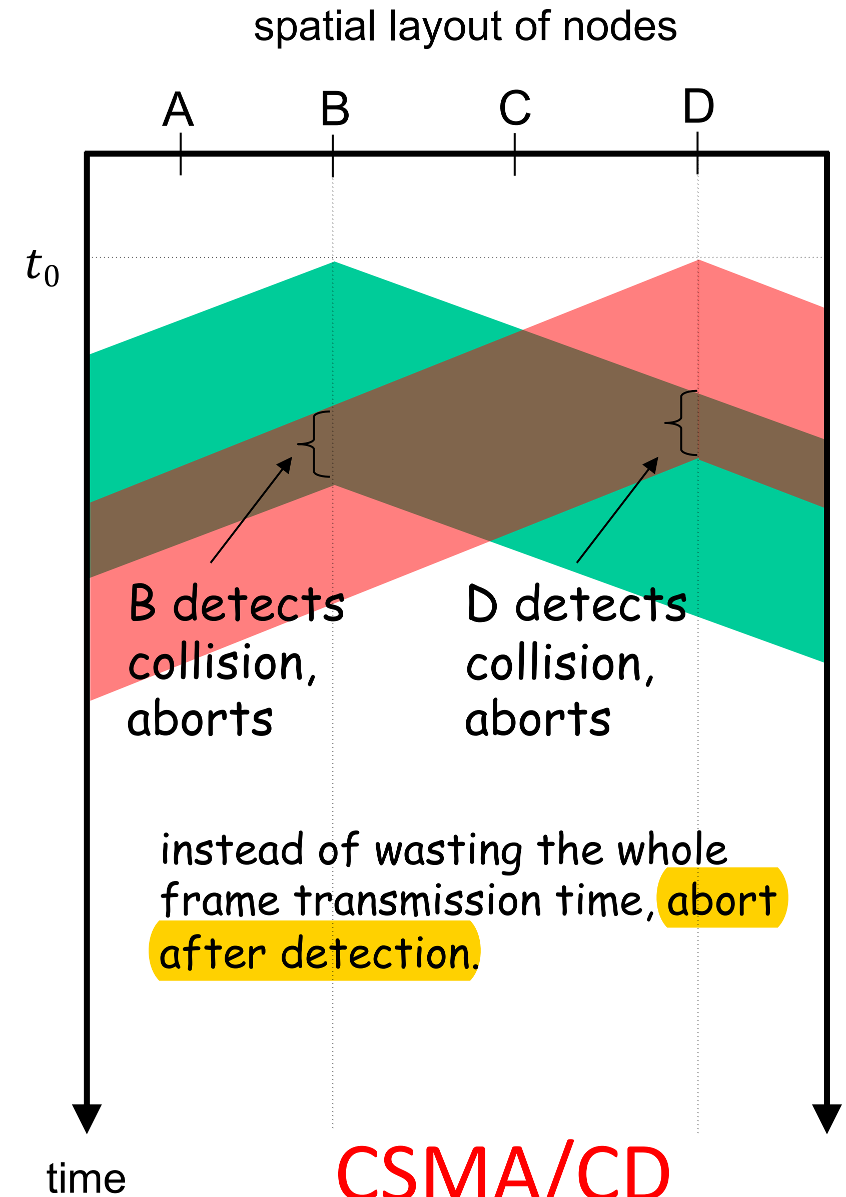
CSMA/CD (Collision Detection)

- CSMA/CD
  - Carrier sensing & deferral as in CSMA
  - When collision is detected, transmission is aborted (reducing channel wastage).
  - Retransmit after a random amount of time.
    - *An example algorithm will be given in the next lecture*
  - CSMA/CD is the underlying method of the early Ethernet, invented by Bob Metcalfe.





CSMA



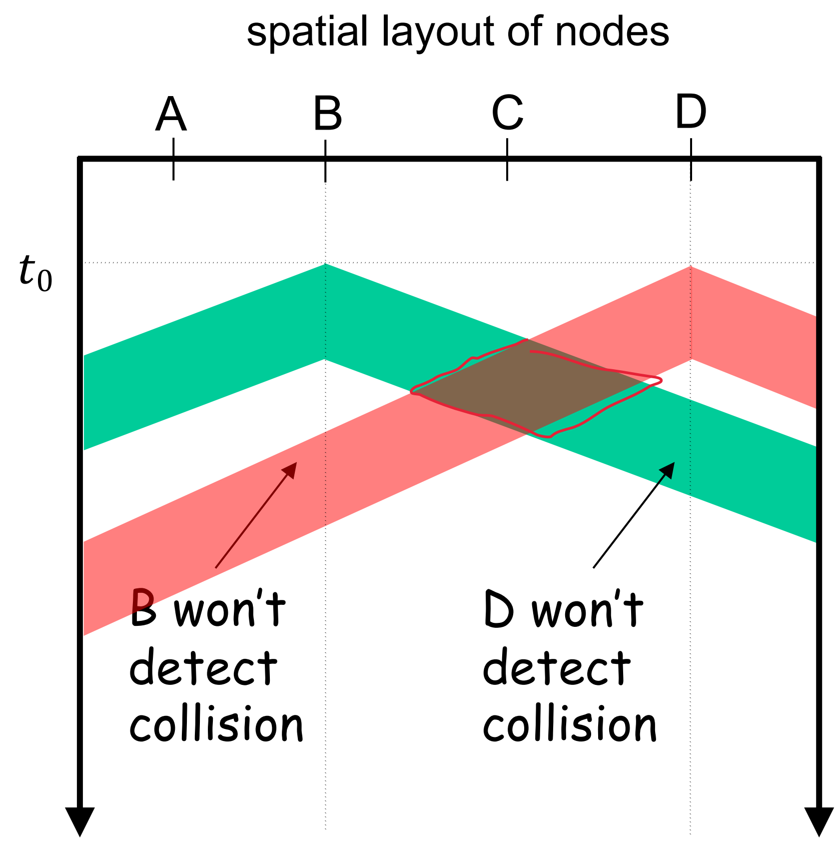
instead of wasting the whole frame transmission time, abort after detection.

CSMA/CD

Minimum Frame Size

- What if the frame size is too small?
  - Collision happens but may not be detected by sending nodes.
    - No retransmission!

- For example, Ethernet requires a minimum frame size of 64 bytes.

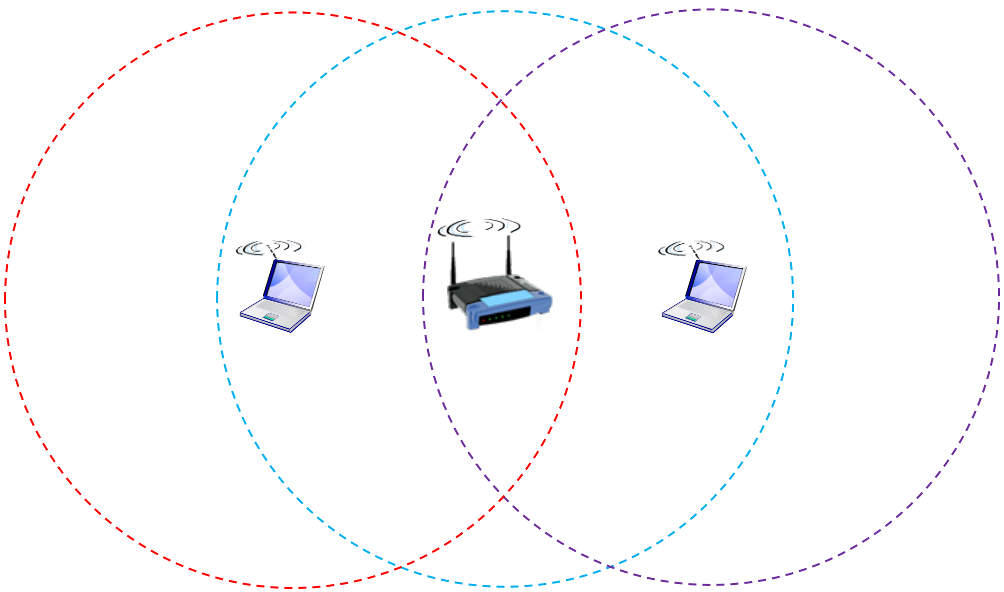


A Little Side Note

- **Q:** Why was early Ethernet using CSMA/CD? Nowadays Ethernet is mostly point-to-point, e.g., directly from a computer to a switch, so no need for multiple access.
- **A:** What we use today is called switched Ethernet. Switches are cheap and we connect every computer in a star-topology to a switch.
- In the early days, Ethernet was using a shared coaxial cable. Computers were connected to this one, long cable with vampire taps ☺.

CSMA/CA (Collision Avoidance)

- Collision detection is easy in wired LANs, but difficult in wireless LANs. For example,



Hidden node problem (two laptops cannot detect each other)

- 802.11 (Wi-Fi) uses CSMA/CA protocol instead.
  - Receiver needs to return ACK if a frame is received OK.

Lecture 8: Summary

- Channel partitioning
  - Divide channel by time, used in GSM
  - Divide channel by frequency, commonly used in radio, satellite systems
- Taking turns
  - polling from central site, used in Bluetooth
  - token passing, used in FDDI and token ring
- Random access
  - CSMA/CD used in Ethernet
  - CSMA/CA used in 802.11 Wi-Fi