Chapter 3: The Link Layer

Our goals:

- understand principles behind data link layer services:
  - framing
  - error detection, correction
  - reliable data transfer, flow control
  - sharing a broadcast channel: multiple access
  - link layer addressing

Overview:

- link layer services
- framing
- error detection, correction
- reliable data transfer
- multiple access protocols and LANs
- link layer addressing

Keypoints and Difficulties

Keypoints:

- Four framing methods
- CRC
- reliable data transfer
- multiple access protocols
- link layer addressing

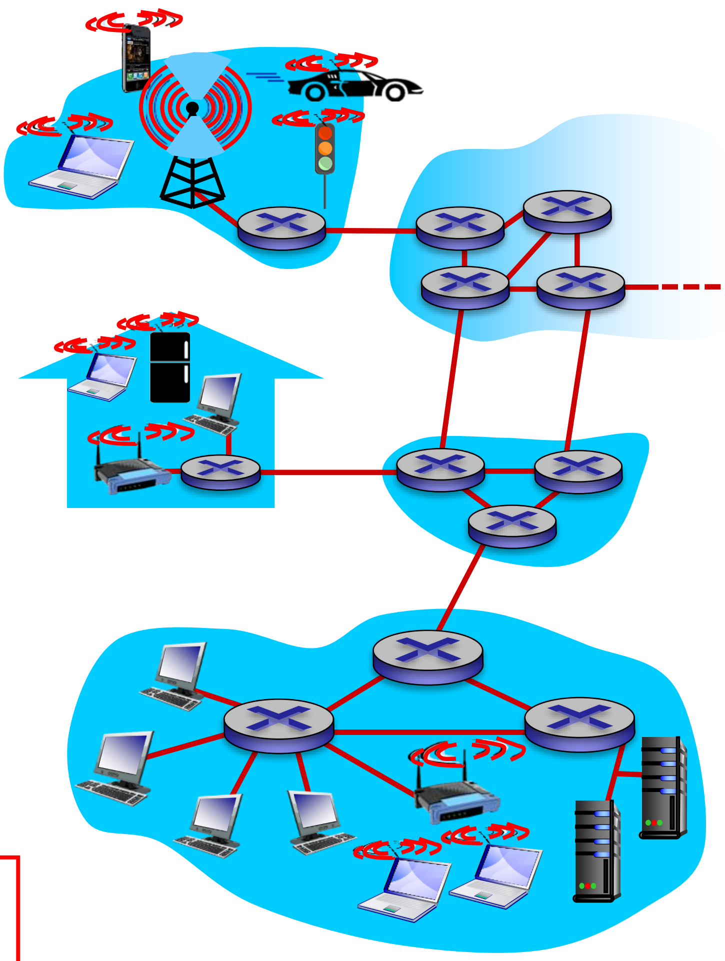
Difficulties:

- CRC
- Flow control
- Sliding-window protocol
- CSMA/CD

Link layer: Introduction

terminology:

- hosts and routers: nodes
- communication channels that connect adjacent nodes along communication path: links
  - wired links
  - wireless links
  - LANs
- layer-2 packet: frame, encapsulates datagram



data-link layer has responsibility of transferring datagram from one node to *physically adjacent* node over a link

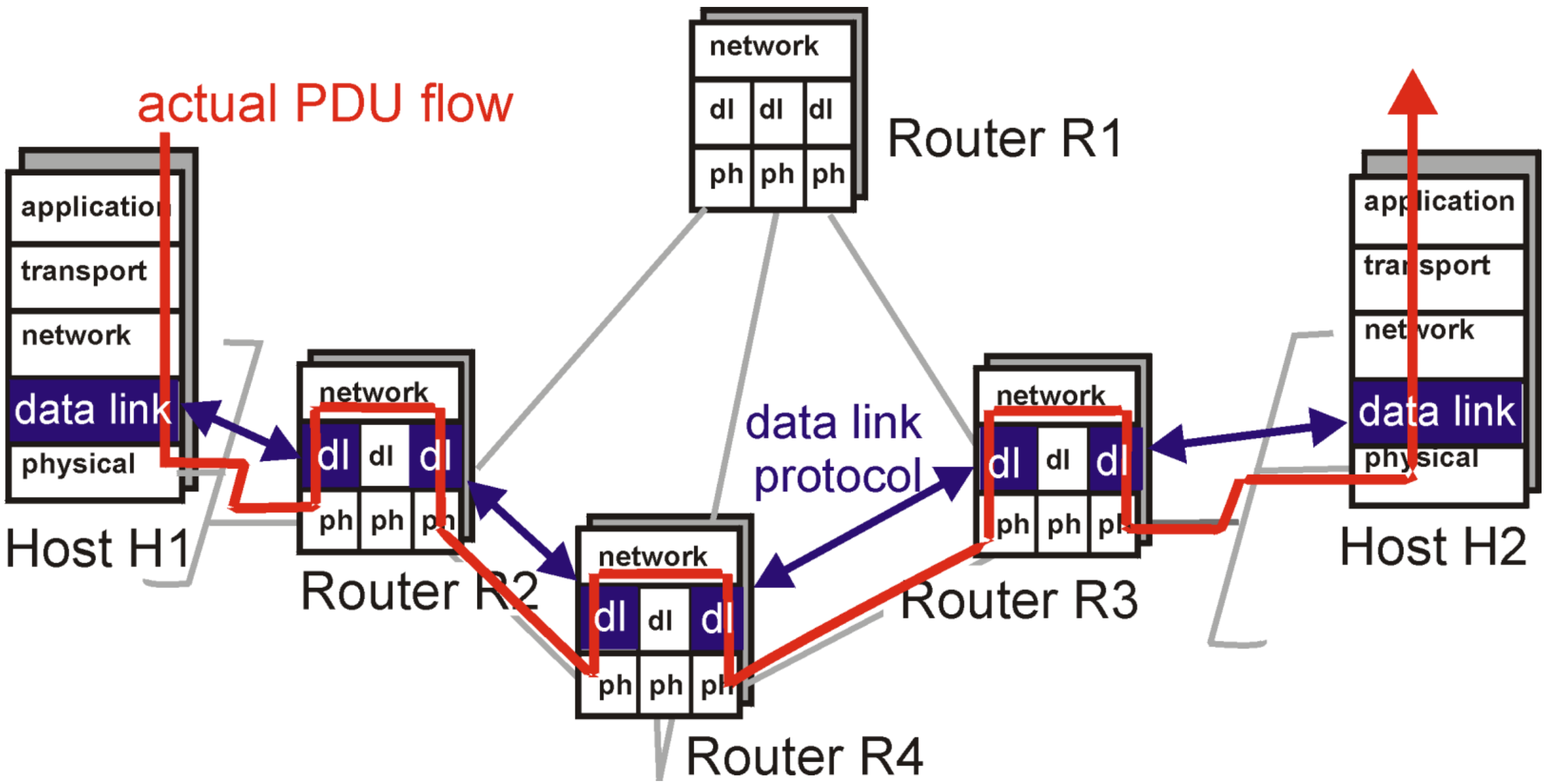
Link layer: context

- datagram transferred by different link protocols over different links:
  - e.g., Ethernet on first link, frame relay on intermediate links, 802.11 on last link
- each link protocol provides different services
  - e.g., may or may not provide rdt over link

transportation analogy:

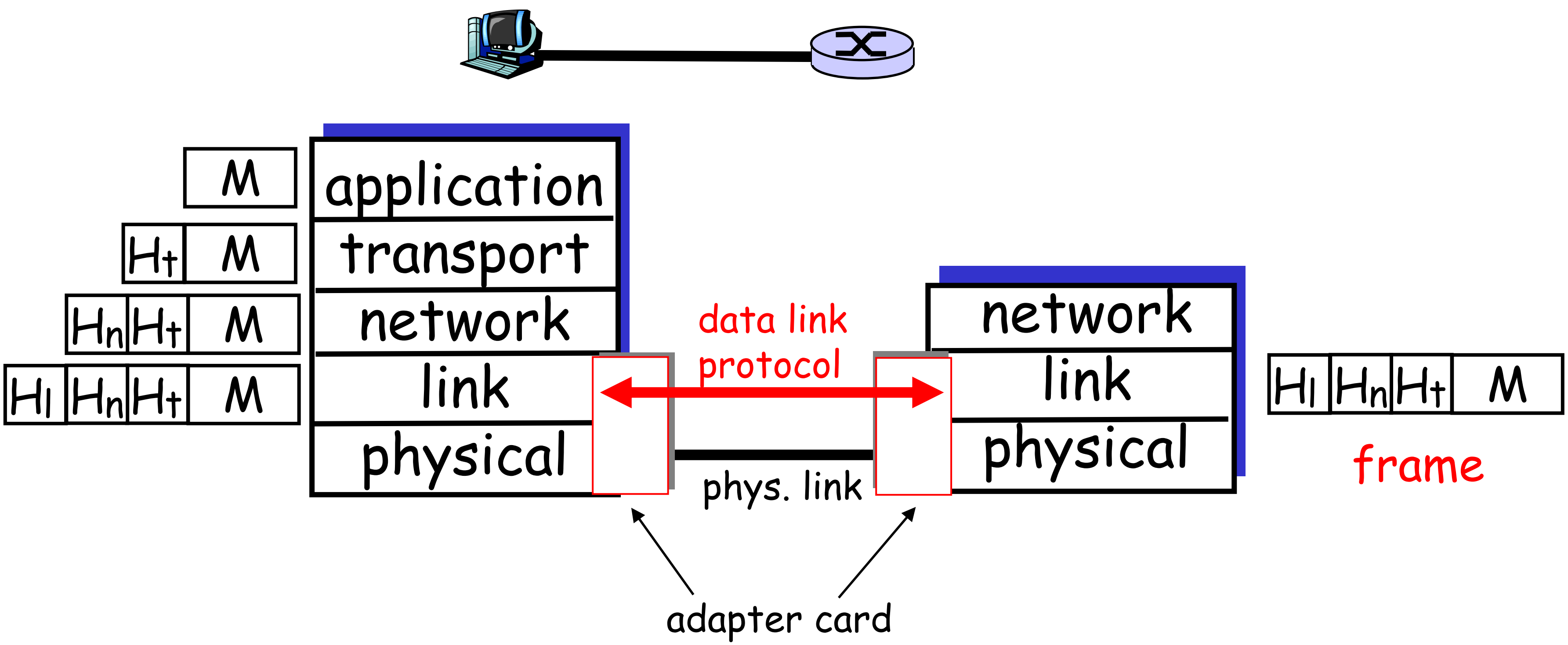
- trip from Princeton to Lausanne
  - car: Princeton to JFK
  - plane: JFK to Geneva
  - train: Geneva to Lausanne
- tourist = datagram
- transport segment = communication link
- transportation mode = link layer protocol
- travel agent = routing algorithm

Link Layer: setting the context



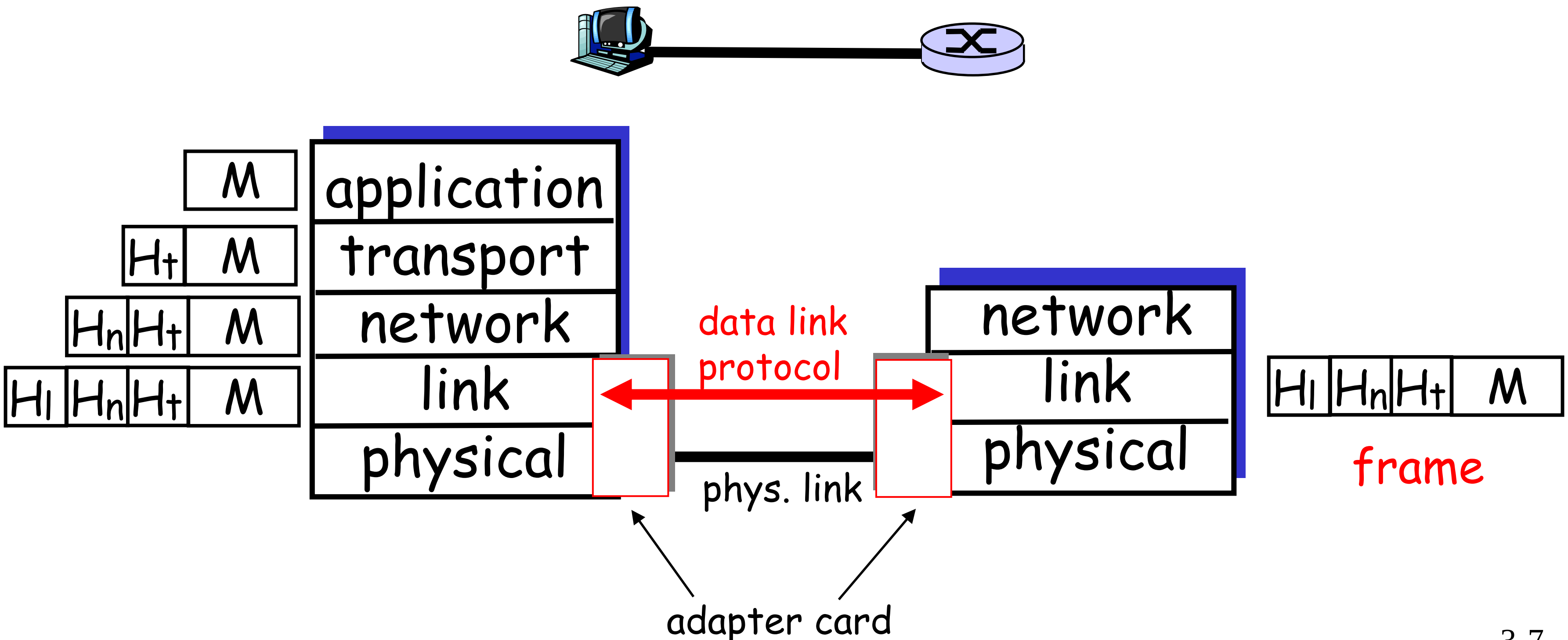
Link Layer: setting the context

- two *physically connected* devices:
  - host-router, router-router, host-host
- unit of data: *frame*



Link Layer: Implementation

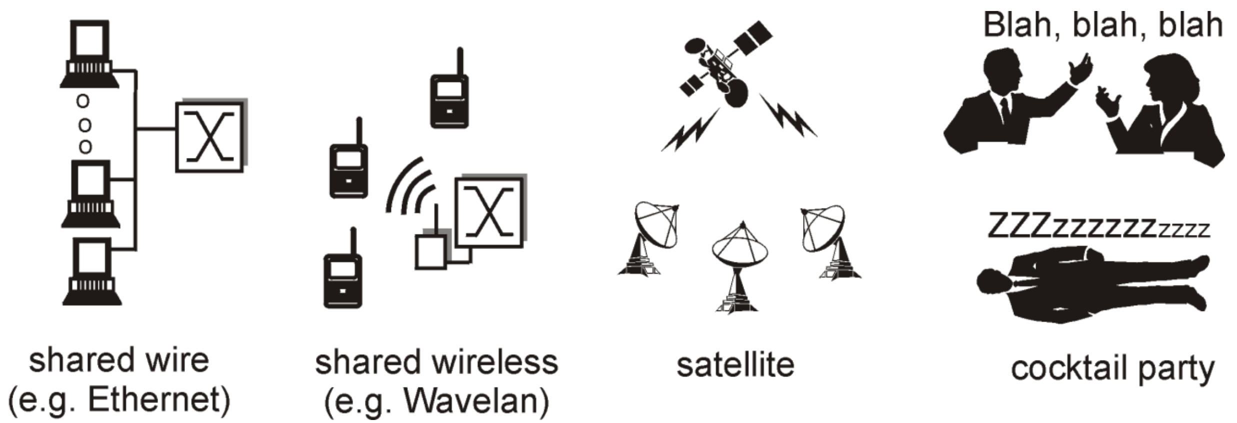
- implemented in "adapter"
  - e.g., PCMCIA card, Ethernet card
  - typically includes: RAM, DSP chips, host bus interface, and link interface



Multiple Access Links and Protocols

Three types of "links":

- point-to-point (single wire, e.g. PPP, SLIP)
- broadcast (shared wire or medium; e.g, Ethernet, Wavelan, etc.)



- switched (e.g., switched Ethernet, ATM etc)

Link Layer Services

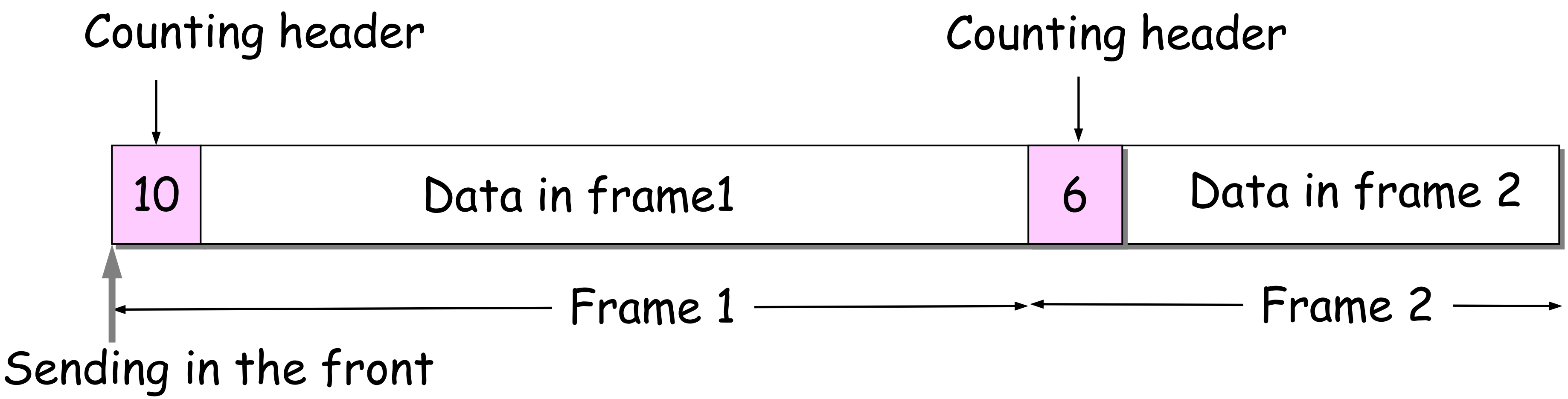
- Framing, link access:
  - encapsulate datagram into frame, adding header, trailer
  - implement channel access if shared medium,
  - 'physical addresses' used in frame headers to identify source, dest
- Reliable delivery between two physically connected devices:
  - Reliable data transfer protocol
  - seldom used on low bit error link (fiber, some twisted pair)
  - wireless links: high error rates

Link Layer Services (more)

- Flow Control:
  - pacing between sender and receivers
- *Error Detection*:
  - errors caused by signal attenuation, noise.
  - receiver detects presence of errors:
    - signals sender for retransmission or drops frame
- Error Correction:
  - receiver identifies *and corrects* bit error(s) without resorting to retransmission

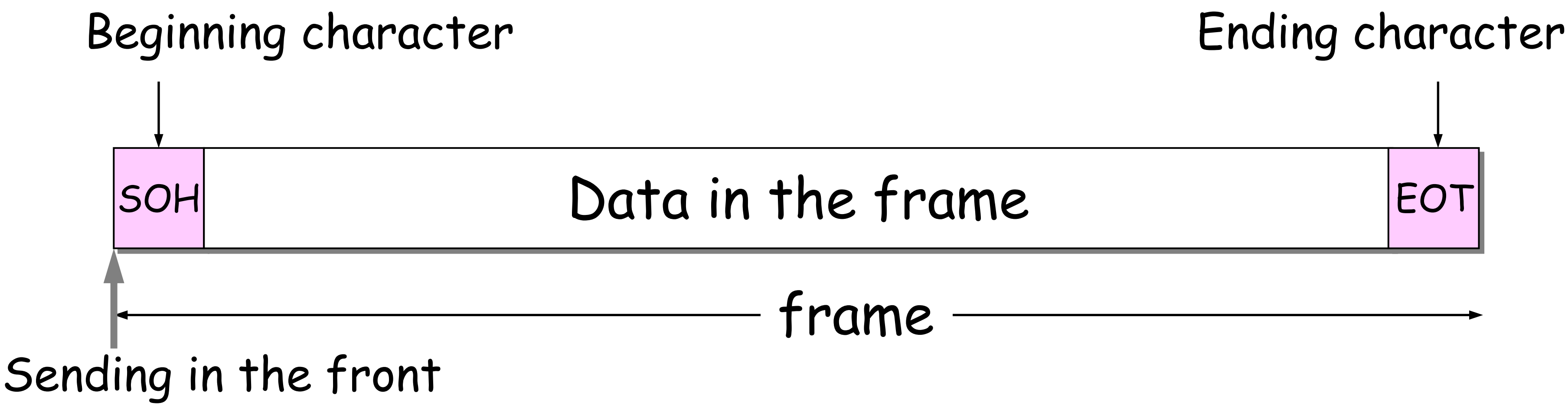
Framing

- Character count method :
  - encapsulate datagram into frame, adding header (character number)



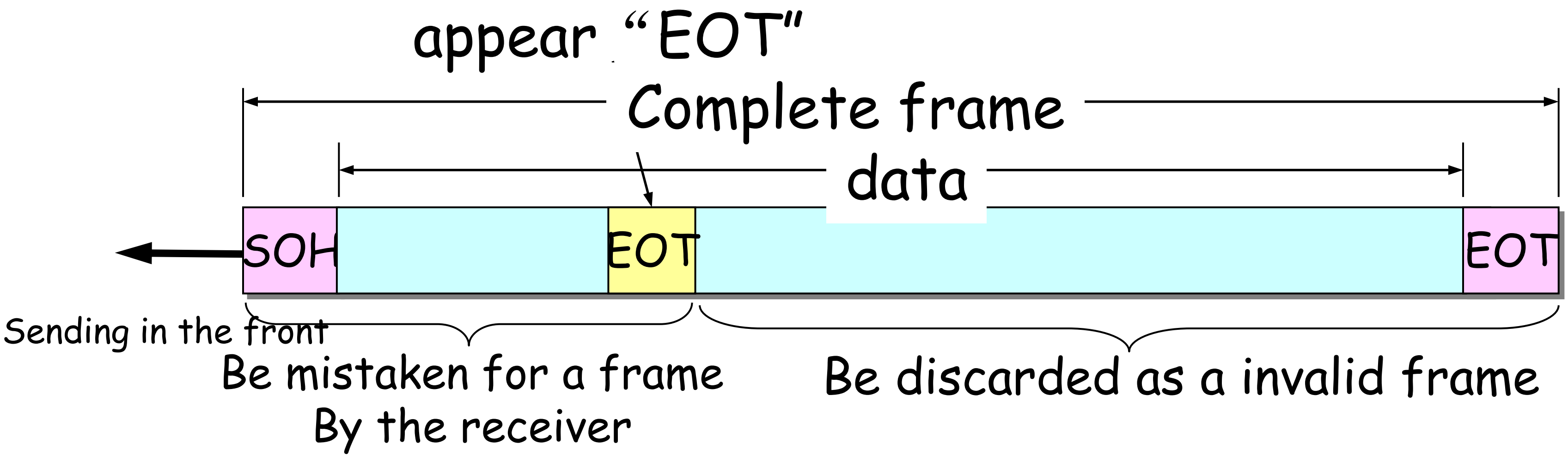
Framing

- First and tail bound method based on character:
  - encapsulate datagram into frame, adding header, trailer (character)



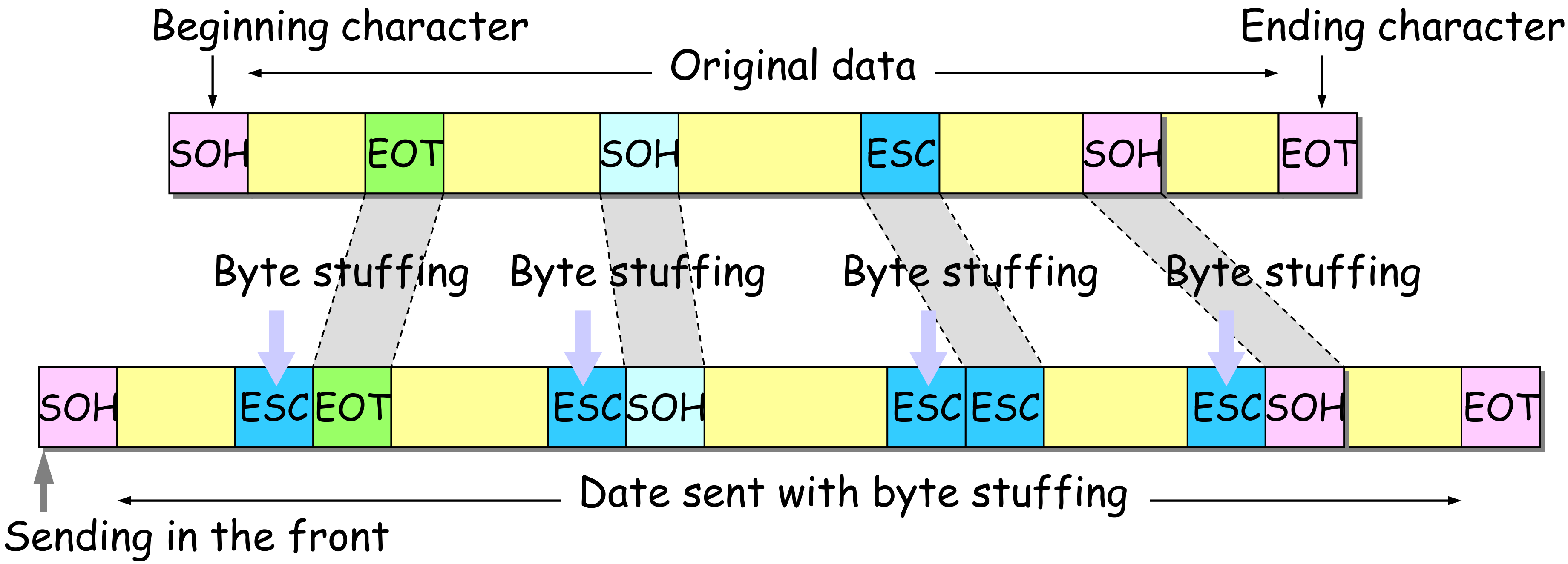
Framing

- First and tail bound method based on character:
  - encapsulate datagram into frame, adding header, trailer (character)



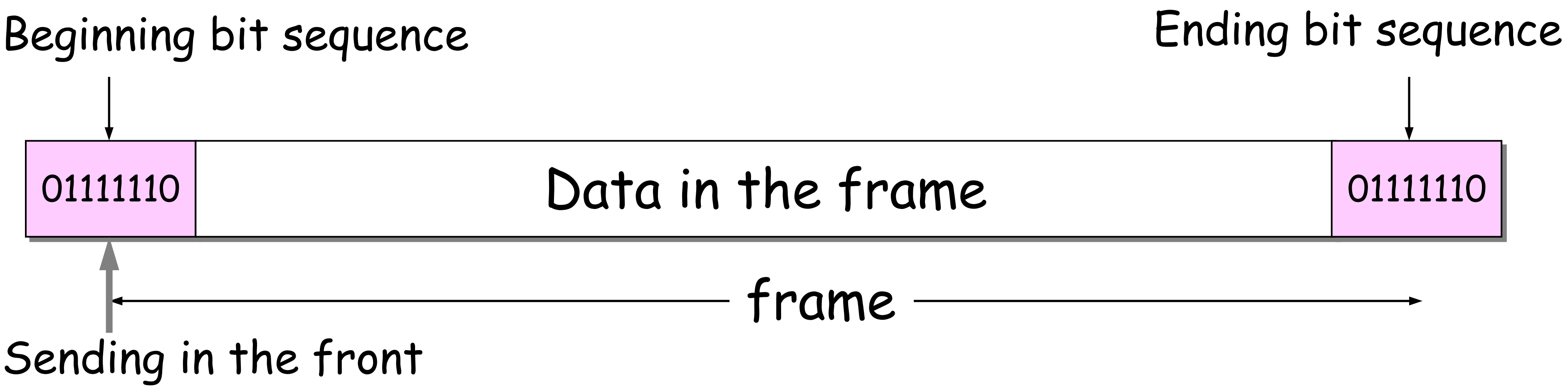
Framing

- First and tail bound method based on character:
  - Inserting/ stuffing a Escape character before the special character in the data part



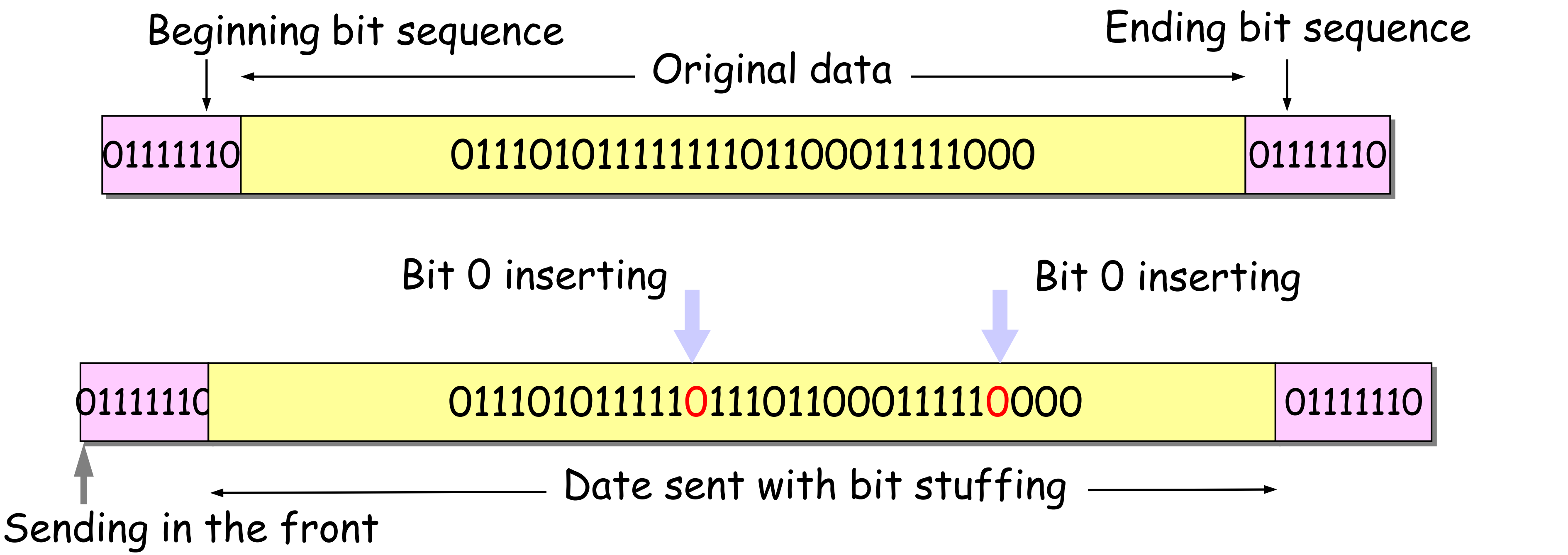
Framing

- First and tail bound method based on bit:
  - encapsulate datagram into frame, adding header, trailer (bit sequence)



Framing

- First and tail bound method based on bit:
  - Inserting a bit "0" after successive five bits "0" in the transmitter; vice versa



Framing

- Physical layer coding violation method:
  - encapsulate datagram into frame without stuffing
  - Only be used in the networks with redundancy coding technology in the physical layer
- For example (IEEE 802.11 with Manchester code):
  - Bit 1 with level jump mode from high to low
  - Bit 0 with level jump mode from low to high
  - Level jump modes from high to high or from low to low can be used for beginning and ending of a frame

Exercise-1

1. HDLC protocol sets the bit stream 01111100011111110 after framing as (   )

A. 01111100000111111010

B.0111110001111101011111110

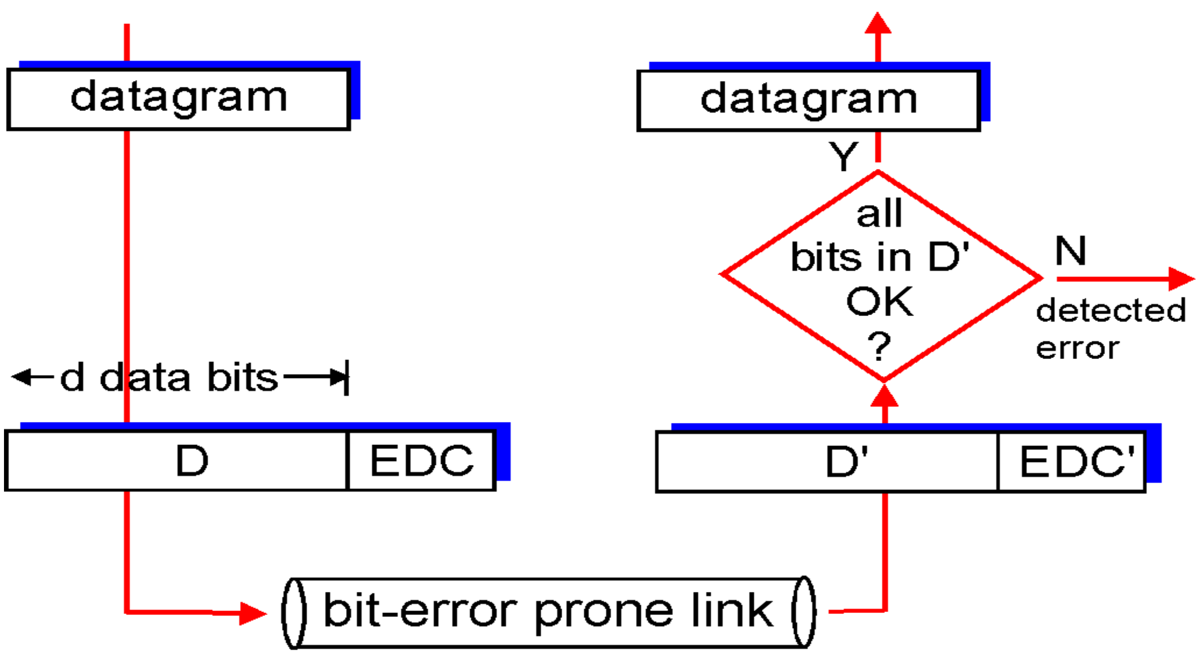
C.01111100011111010

D.0111110001111111001111101

Error Detection

EDC= Error Detection and Correction bits (redundancy)
D = Data protected by error checking, may include header fields

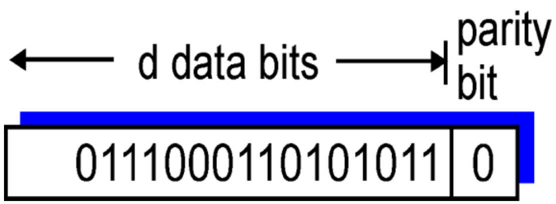
- Error detection not 100% reliable!
  - protocol may miss some errors, but rarely
  - larger EDC field yields better detection and correction



Parity Checking

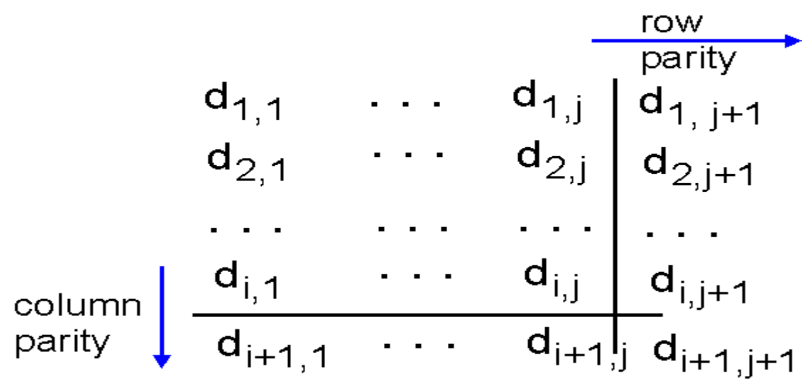
Single Bit Parity:

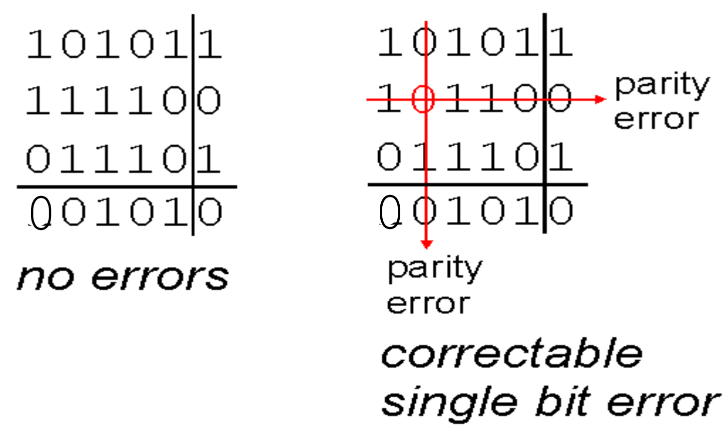
Detect single bit errors



Two Dimensional Bit Parity:

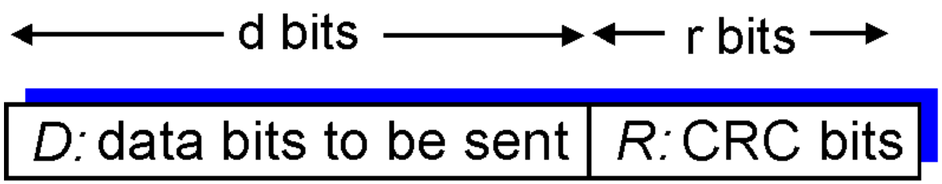
Detect *and correct* single bit errors





Checksumming: Cyclic Redundancy Check

- view data bits, D, as a binary number
- choose r+1 bit pattern (generator), G
- goal: choose r CRC bits, R, such that
  - <D,R> exactly divisible by G (modulo 2)
  - receiver knows G, divides <D,R> by G. If non-zero remainder: error detected!
  - can detect all burst errors less than r+1 bits
- widely used in practice (ATM, HDCL)



bit pattern

$D * 2^r$ XOR R

mathematical formula

CRC Example

Want:

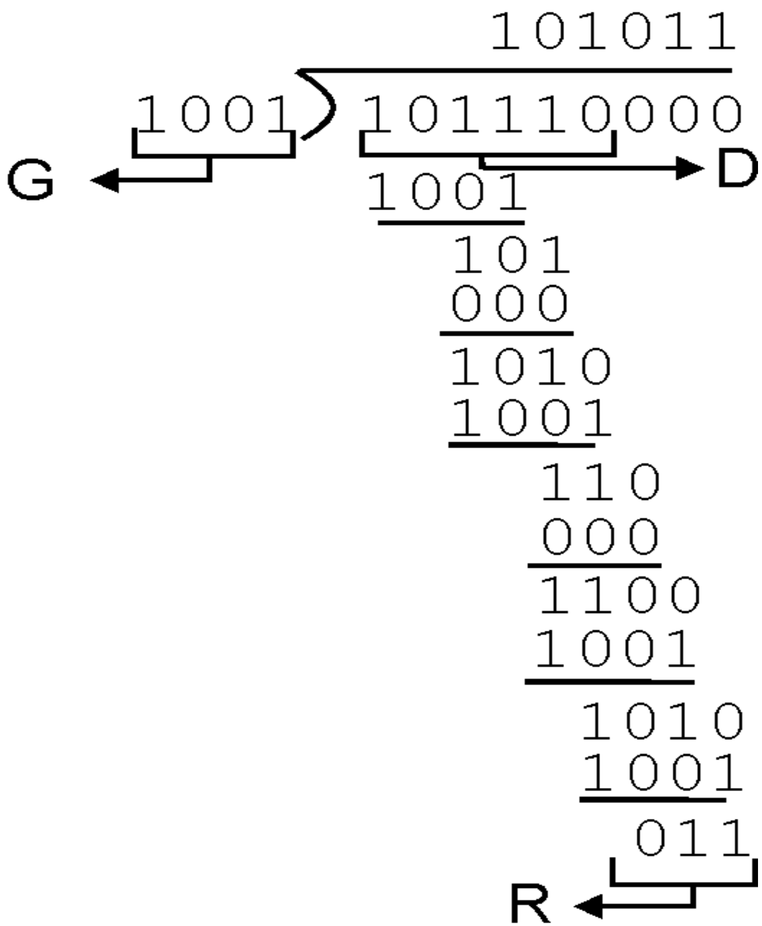
$D\cdot 2r$ XOR $R = nG$

equivalently:

$D\cdot 2r = nG$ XOR R

equivalently:

if we divide $D\cdot 2r$ by G, want reminder R



$$R = \text{remainder}\left[\frac{D\cdot 2r}{G}\right]$$

CRC well-known generator

- CRC-12: $x^{12} + x^{11} + x^{3} + x^{2} + x^{1} + 1$
- CRC-16 : $x^{16} + x^{15} + x^{2} + 1$
- CRC-CCITT : $x^{16} + x^{12} + x^{5} + 1$
- CRC-32: $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x^{1} + 1$

CCITT: Consultative Committee on International Telegraphy and Telephone

ITU-T: International Telecommunications Union – Telecommunications Standardization Sector

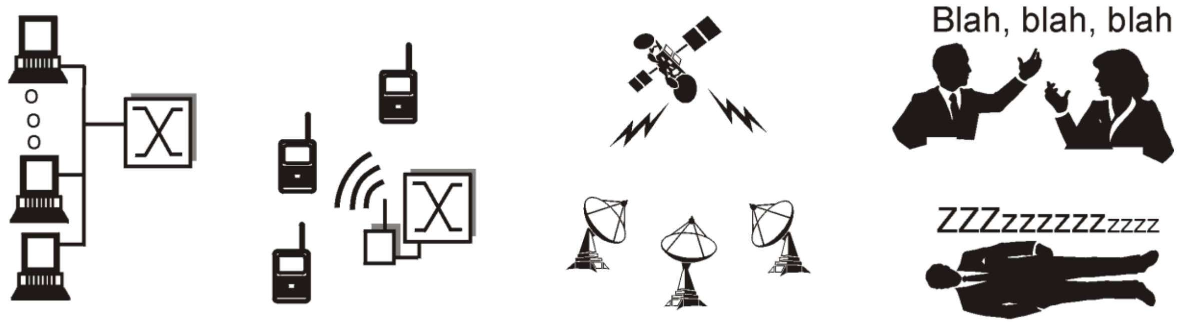
Exercise-2

1. If the information received by an Ethernet adapter is 101101001 and the generator is $G(x) = x^3+x^2+1$, judge whether the transmission has bit error?

Multiple Access Links and Protocols

Three types of "links":

- point-to-point (single wire, e.g. PPP, SLIP)
- broadcast (shared wire or medium; e.g, Ethernet, Wavelan, etc.)



shared wire (e.g. Ethernet)

shared wireless (e.g. Wavelan)

satellite

cocktail party

- switched (e.g., switched Ethernet, ATM etc)

Multiple Access protocols

- single shared communication channel
- two or more simultaneous transmissions by nodes: interference
  - collision if node receives two or more signals at the same time
  - only one node can send successfully at a time
- *multiple access protocol:*
  - distributed algorithm that determines how nodes share channel, i.e., determine when node can transmit
  - communication about channel sharing must use channel itself!
  - what to look for in multiple access protocols:
    - synchronous or asynchronous
    - information needed about other stations
    - robustness (e.g., to channel errors)
    - performance

Multiple Access protocols

- claim: humans use multiple access protocols all the time
- class can "guess" multiple access protocols
  - multiaccess protocol 1:
  - multiaccess protocol 2:
  - multiaccess protocol 3:
  - multiaccess protocol 4:

MAC Protocols: a taxonomy

Three broad classes:

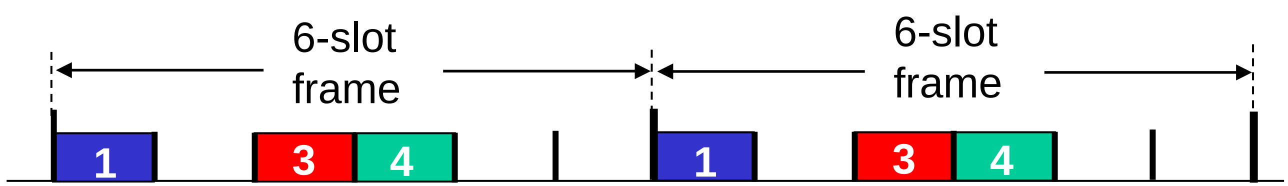
- Channel Partitioning
  - divide channel into smaller "pieces" (time slots, frequency)
  - allocate piece to node for exclusive use
- Random Access
  - allow collisions
  - "recover" from collisions
- **"Taking turns"**
  - tightly coordinate shared access to avoid collisions

Goal: efficient, fair, simple, decentralized

Channel Partitioning MAC protocols: TDMA

TDMA: time division multiple access

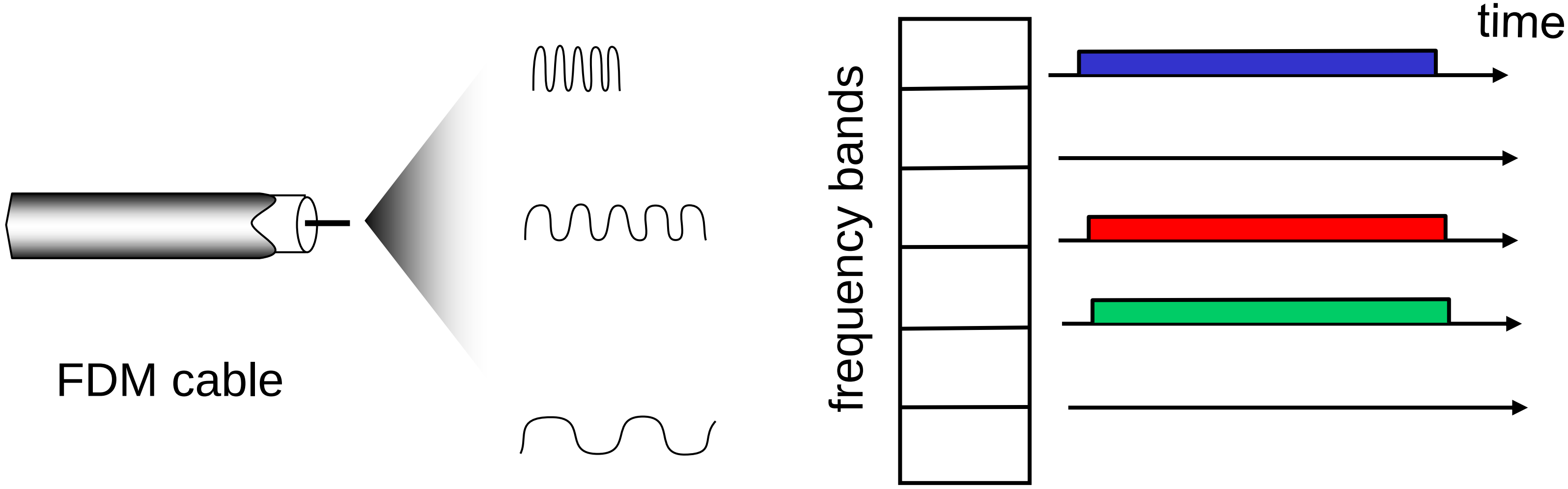
- access to channel in "rounds"
- each station gets fixed length slot (length = pkt trans time) in each round
- unused slots go idle
- example: 6-station LAN, 1,3,4 have pkt, slots 2,5,6 idle



Channel Partitioning MAC protocols: FDMA

FDMA: frequency division multiple access

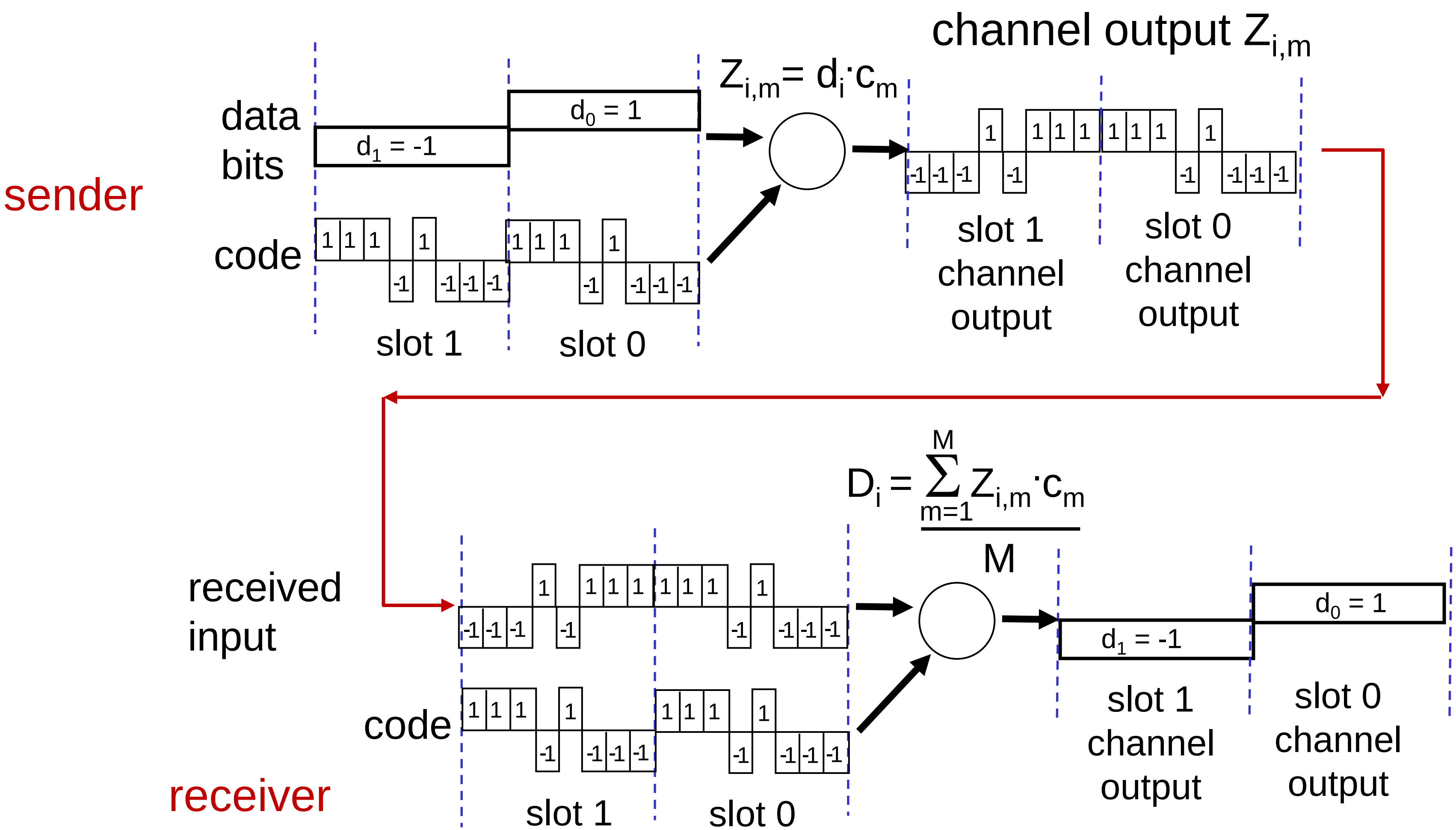
- channel spectrum divided into frequency bands
- each station assigned fixed frequency band
- unused transmission time in frequency bands go idle
- example: 6-station LAN, 1,3,4 have pkt, frequency bands 2,5,6 idle



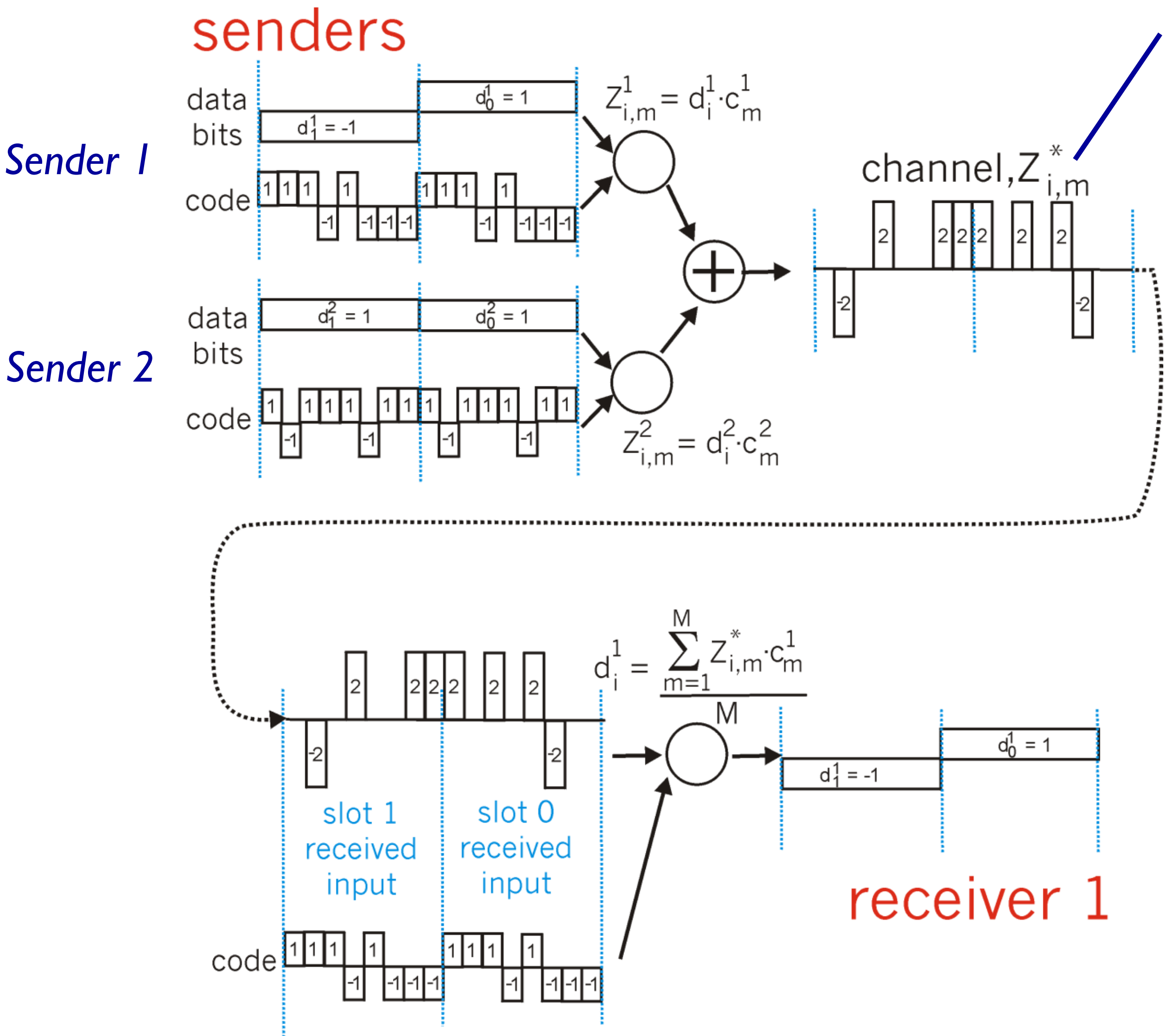
Code Division Multiple Access (CDMA)

- unique “code” assigned to each user; i.e., code set partitioning
  - all users share same frequency, but each user has own “chipping” sequence (i.e., code) to encode data
  - allows multiple users to “coexist” and transmit simultaneously with minimal interference (if codes are “orthogonal”)
- *encoded signal* = (original data) X (chipping sequence)
- *decoding:* inner-product of encoded signal and chipping sequence

CDMA encode/decode



CDMA: two-sender interference



channel sums together transmissions by sender 1 and 2

using same code as sender 1, receiver recovers sender 1's original data from summed channel data!

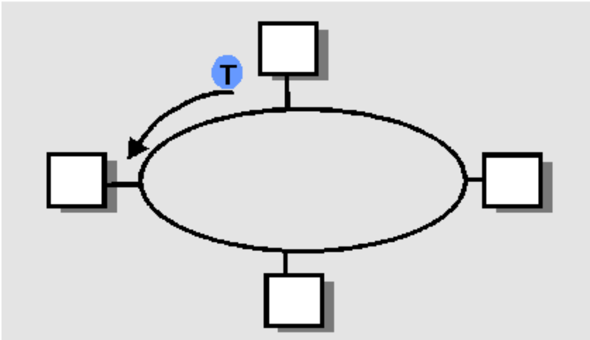
"Taking Turns" MAC protocols

Polling:

- master node "invites" slave nodes to transmit in turn
- Request to Send, Clear to Send msgs
- concerns:
  - polling overhead
  - latency
  - single point of failure (master)

Token passing:

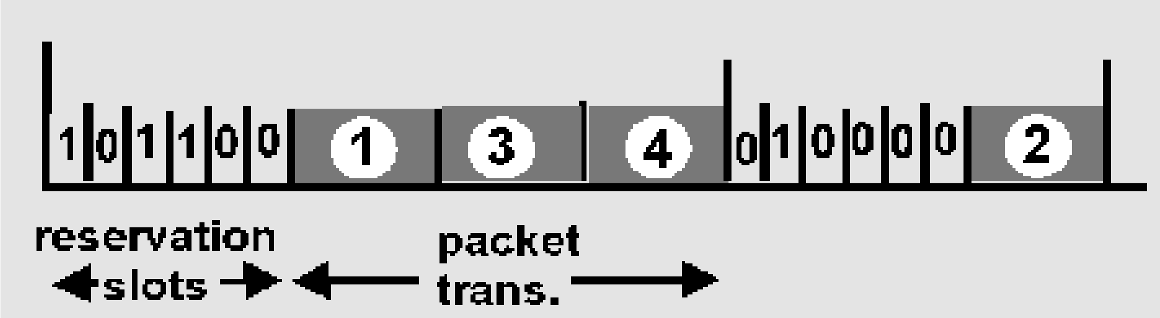
- control **token** passed from one node to next sequentially.
- token message
- concerns:
  - token overhead
  - latency
  - single point of failure (token)



Reservation-based protocols

Distributed Polling:

- time divided into slots
- begins with N short reservation slots
  - reservation slot time equal to channel end-end propagation delay
  - station with message to send posts reservation
  - reservation seen by all stations
- after reservation slots, message transmissions ordered by known priority

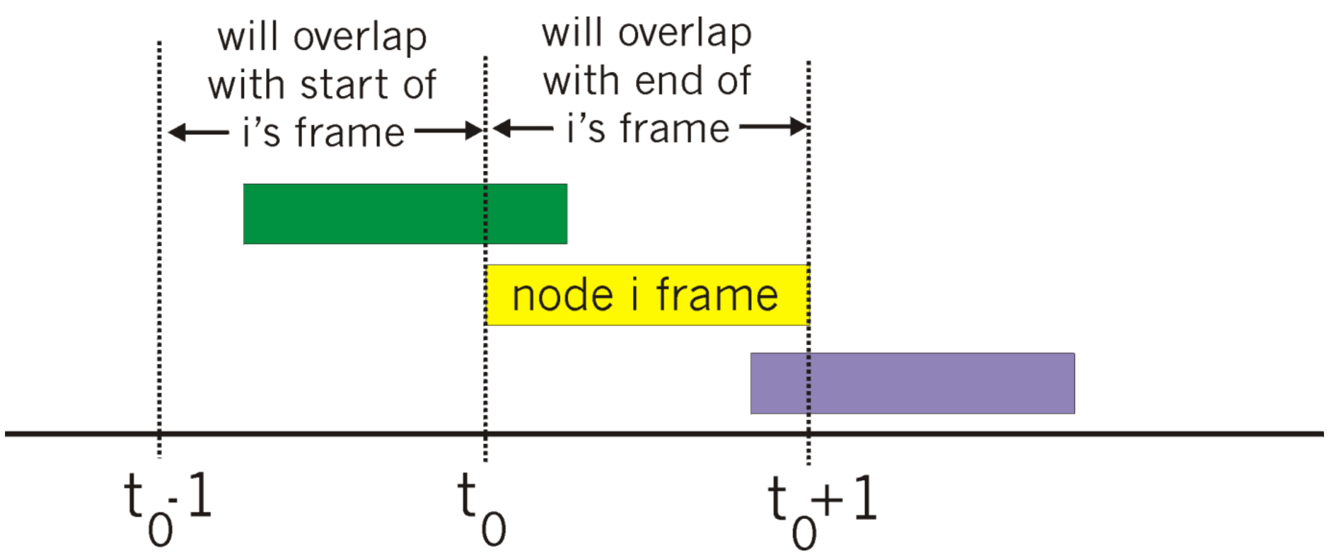


Random Access protocols

- When node has packet to send
  - transmit at full channel data rate R.
  - no *a priori* coordination among nodes
- two or more trasnmitting nodes -> "collision",
- random access MAC protocol specifies:
  - how to detect collisions
  - how to recover from collisions (e.g., via delayed retransmissions)
- Examples of random access MAC protocols:
  - ALOHA
  - slotted ALOHA
  - CSMA and CSMA/CD

Pure ALOHA

- unslotted Aloha: simpler, no synchronization
- pkt needs transmission:
  - send without awaiting for beginning of slot
- collision probability increases:
  - pkt sent at t_0 collide with other pkts sent in $[t_0-1, t_0+1]$



Pure Aloha (cont.)

P(success by given node) = P(node transmits) $\cdot$

P(no other node transmits in $[p_0-1,p_0]$ $\cdot$

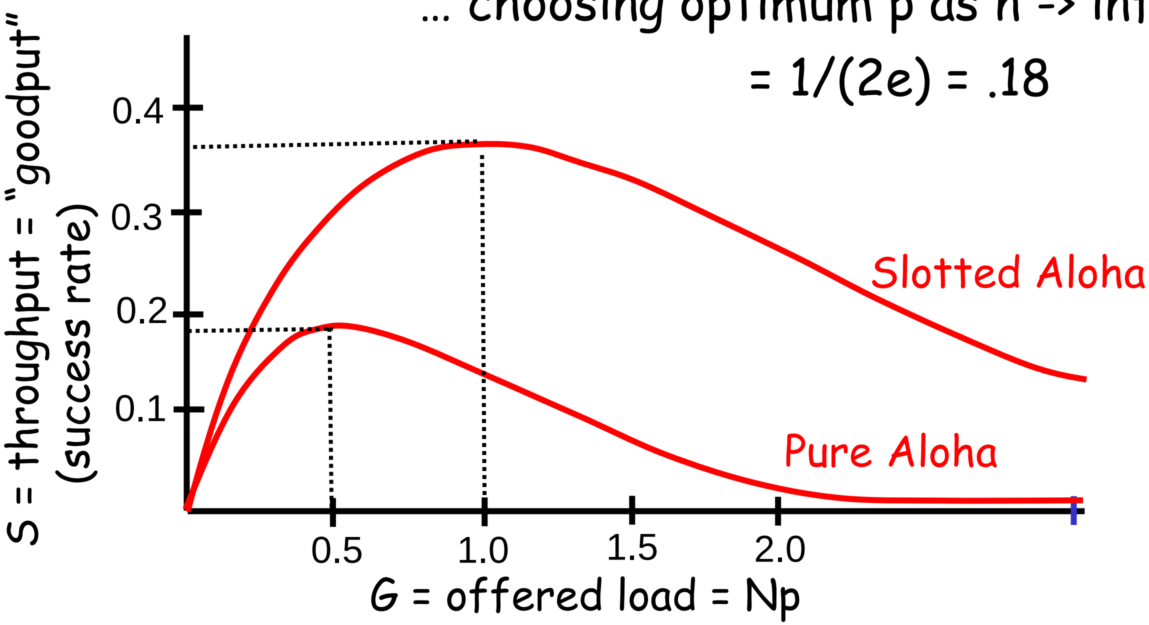
P(no other node transmits in $[p_0-1,p_0]$

$= p \cdot (1-p)^{N-1} \cdot (1-p)^{N-1}$

$= p \cdot (1-p)^{2(N-1)}$

… choosing optimum p as n -> infty ...

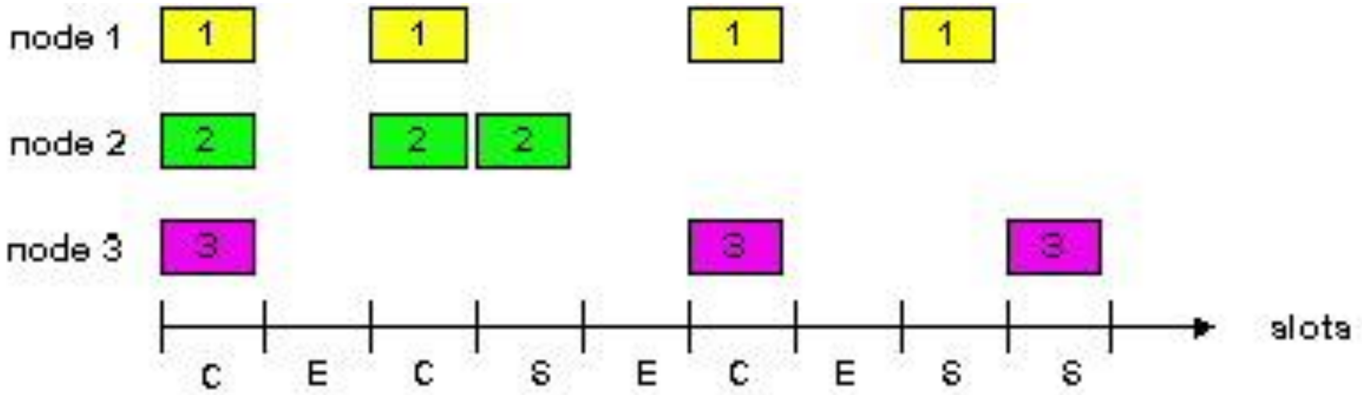
= 1/(2e) = .18



protocol constrains effective channel throughput!

Slotted Aloha

- time is divided into equal size slots (= pkt trans. time)
- node with new arriving pkt: transmit at beginning of next slot
- if collision: retransmit pkt in future slots with probability p, until successful.



Success (S), Collision (C), Empty (E) slots

Slotted Aloha efficiency

Q: what is max fraction slots successful?

A: Suppose N stations have packets to send

- each transmits in slot with probability p
- prob. successful transmission S is:

by single node: $S = p\,(1-p)^{(N-1)}$

by any of N nodes

S = Prob (only one transmits)

$= N\,p\,(1-p)^{(N-1)}$

… choosing optimum p as n -> infty …

$= 1/e = .37$ *as N -> infty*

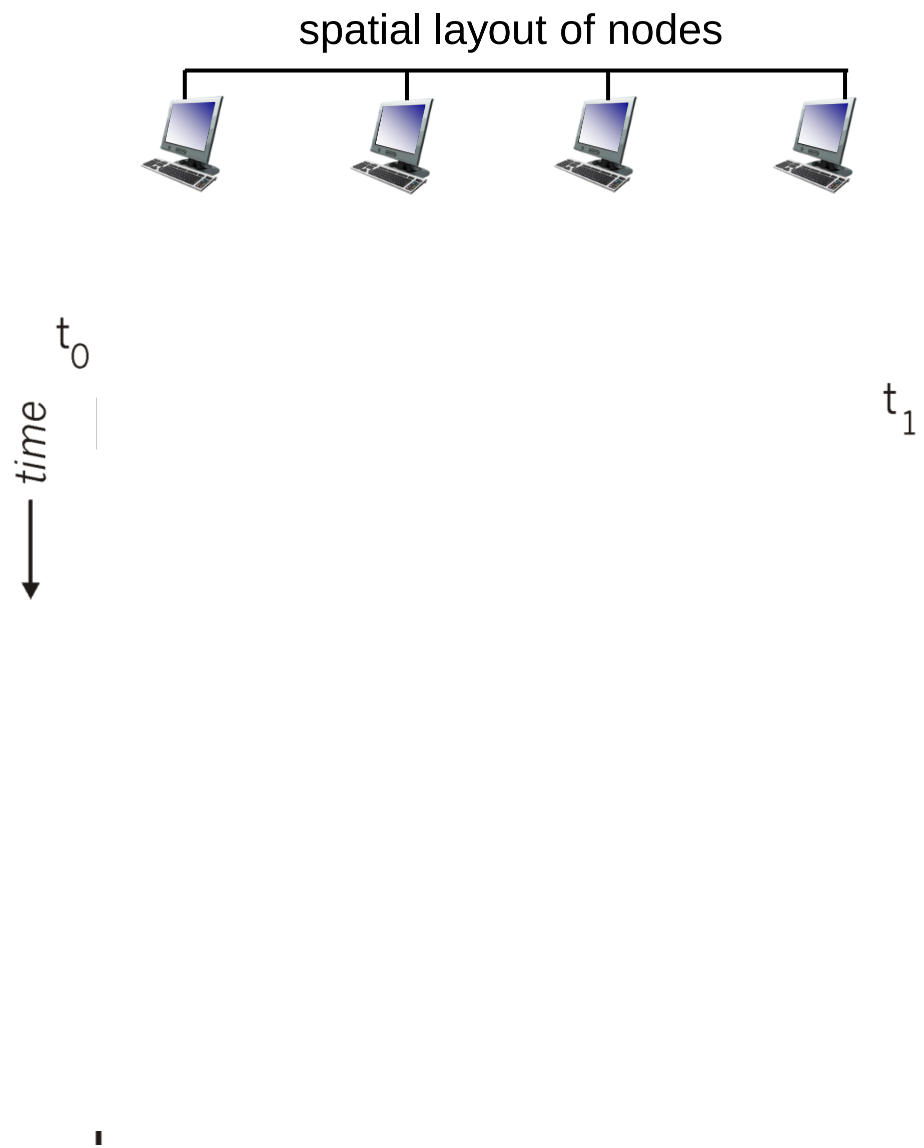
At best: channel use for useful transmissions 37% of time!

CSMA: Carrier Sense Multiple Access)

CSMA: listen before transmit:

- If channel sensed idle: transmit entire frame
- If channel sensed busy, defer transmission
  - Persistent CSMA: retry immediately with probability p when channel becomes idle (may cause instability)
  - Non-persistent CSMA: retry after random interval
- human analogy: don't interrupt others!

CSMA collisions



collisions *can* occur:

propagation delay means two nodes may not year hear each other's transmission

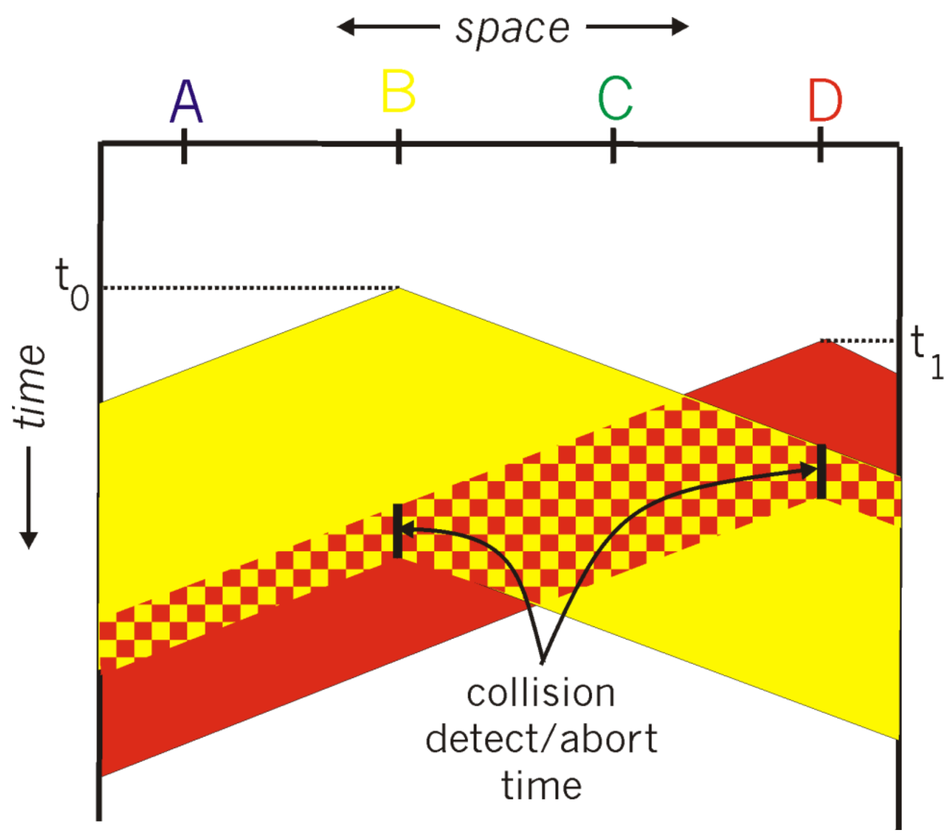
collision:

entire packet transmission time wasted

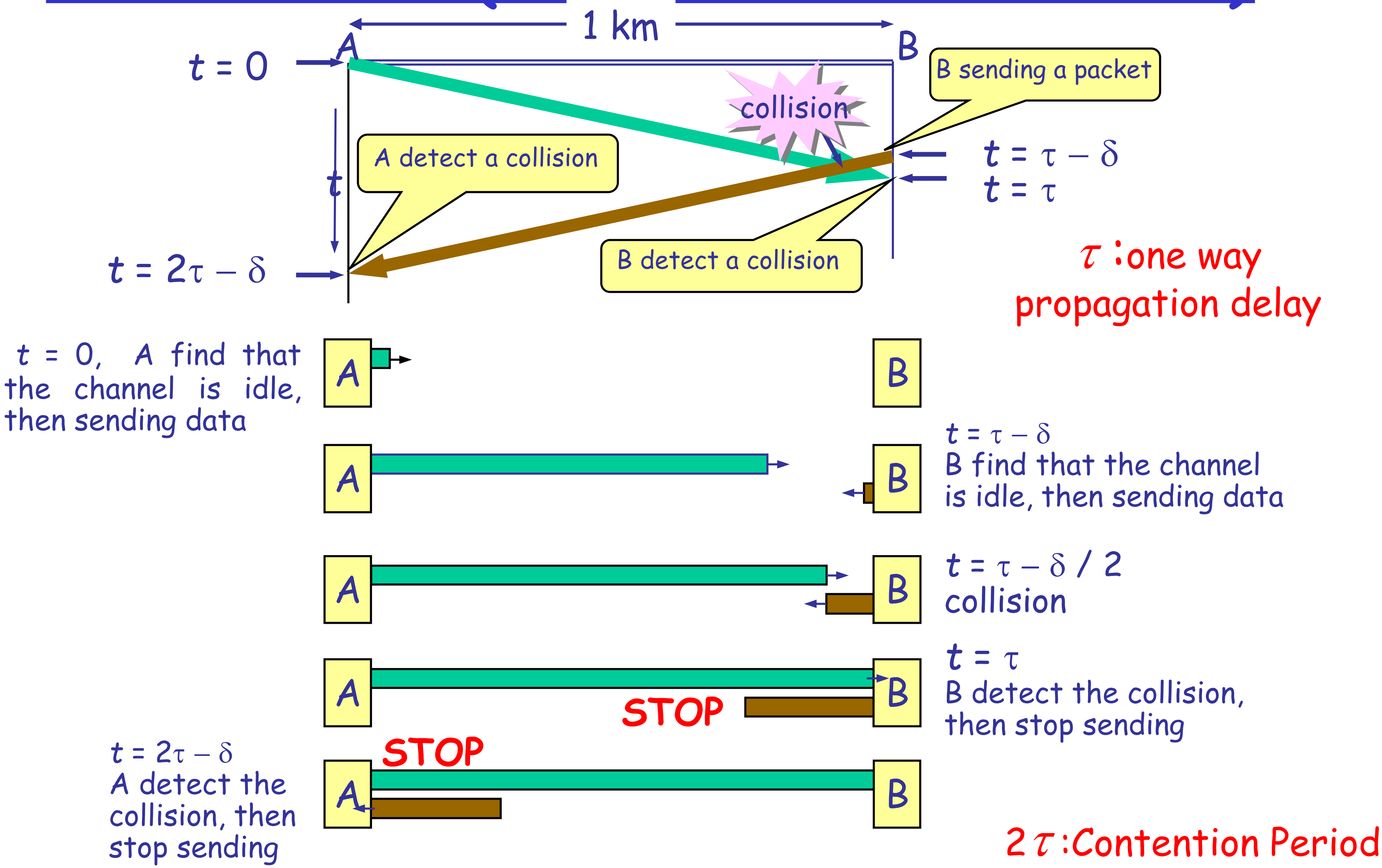
note:

role of distance and propagation delay in determining collision prob.

CSMA/CD collision detection



CSMA/CD (Collision Detection)



CSMA/CD (Collision Detection)

CSMA/CD: carrier sensing, deferral as in CSMA
- collisions *detected* within short time
- colliding transmissions aborted, reducing channel wastage
- persistent or non-persistent retransmission

- collision detection:
  - easy in wired LANs: measure signal strengths, compare transmitted, received signals
  - difficult in wireless LANs: receiver shut off while transmitting
- human analogy: the polite conversationalist

CSMA/CD efficiency

- T_{prop} = max prop delay between 2 nodes in LAN
- t_{trans} = time to transmit max-size frame

$$efficiency = \frac{1}{1 + 5t_{prop}/t_{trans}}$$

- efficiency goes to 1
  - as t_{prop} goes to 0
  - as t_{trans} goes to infinity
- better performance than ALOHA: and simple, cheap, decentralized!

Summary of MAC protocols

- What do you do with a shared media?
  - Channel Partitioning, by time, frequency or code
    - Time Division,Code Division, Frequency Division
  - Random partitioning (dynamic),
    - ALOHA, S-ALOHA, CSMA, CSMA/CD
    - carrier sensing: easy in some technoligies (wire), hard in others (wireless)
    - CSMA/CD used in Ethernet
  - Taking Turns
    - polling from a central cite, token passing

Summary of MAC protocols

channel partitioning MAC protocols:

- share channel efficiently at high load
- inefficient at low load: delay in channel access, 1/N bandwidth allocated even if only 1 active node!

Random access MAC protocols

- efficient at low load: single node can fully utilize channel
- high load: collision overhead

"taking turns" protocols

look for best of both worlds!

Exercises-4

- A LAN adopts CSMA/CD protocol to realize the media access control. The data transmission rate is 10Mbps, the distance between host A and host B is 2km, and the signal propagation speed is 200000km/s. If there is a conflict when two hosts send data, how long will it take from the time when they start sending data to the time when both hosts detect the conflict? (What is the minimum and maximum duration?)

Chapter 3: Summary

- principles behind data link layer services:
  - framing
  - error detection, correction
  - reliable data transfer
  - sharing a broadcast channel: multiple access
- Next, various link layer technologies
  - LAN Model
  - Ethernet
  - WLAN

Homework

- P319-322
  P9,11,17,22
- P537
  P5