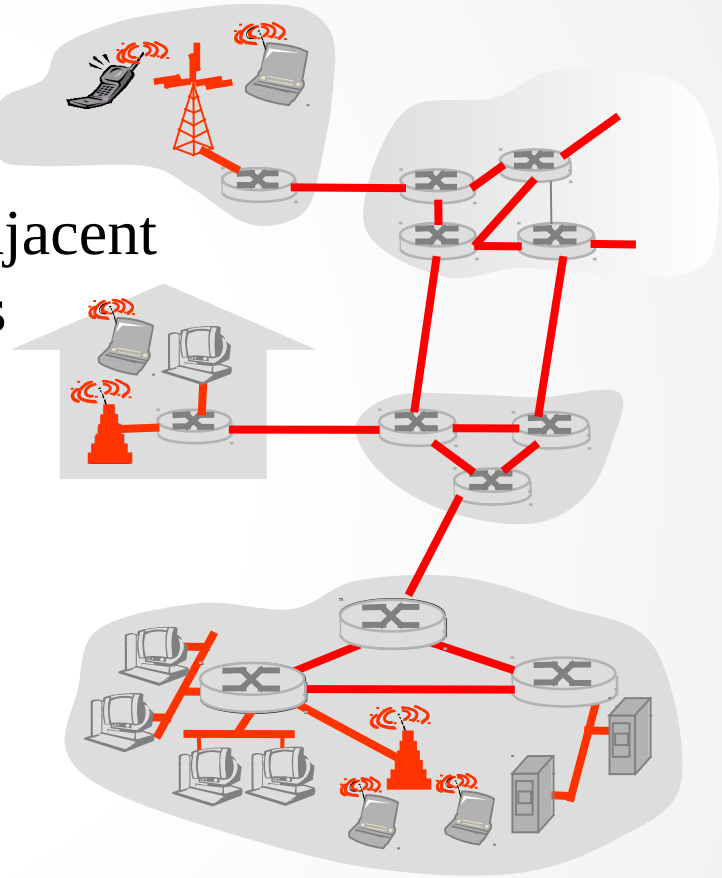
Data Link Layer

Manas Ranjan Lenka
School of Computer Engineering,
KIIT University

Link Layer: Introduction

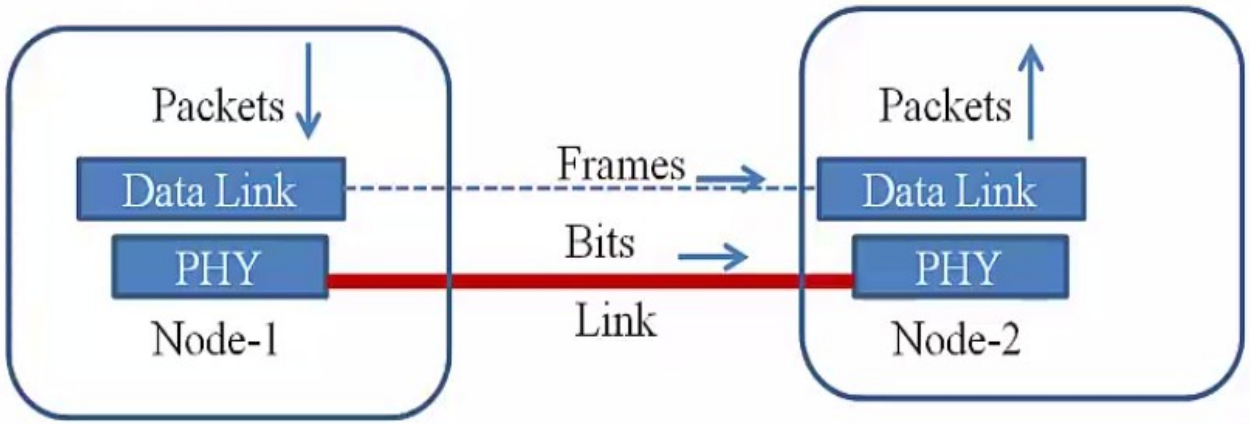
- hosts and routers are nodes
- communication channels that connect adjacent nodes along communication path are links
  - wired links
  - wireless links
- layer-2 packet is a frame, encapsulates datagram



Responsibility :
Transferring datagram from one node to physically adjacent node over a link

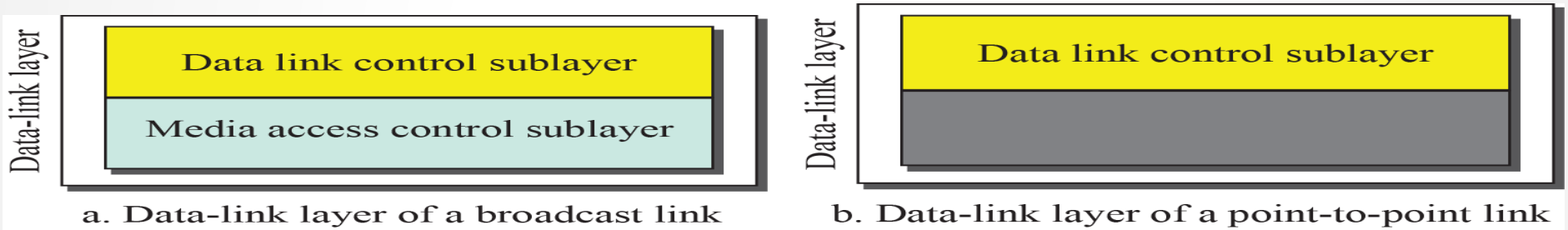
Data-Link Layer

- Frame-by-Frame next-hop delivery
  - Frame: Block of data exchanged at link layer
- Uses services of PHY layer (which delivers bits) to deliver frames



Link Layer Protocols

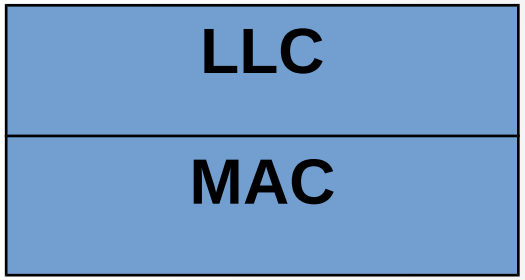
- Link could be point-to-point or broadcast
  – Broadcast: Many nodes connected to same communication channel (e.g. wireless)



- Protocol:
  – Define format of frames to be exchanged over the link
  – In response to frames, action to be taken by nodes
  – Examples: Ethernet, Token-Ring, WiFi, PPP etc

Link Layer Services

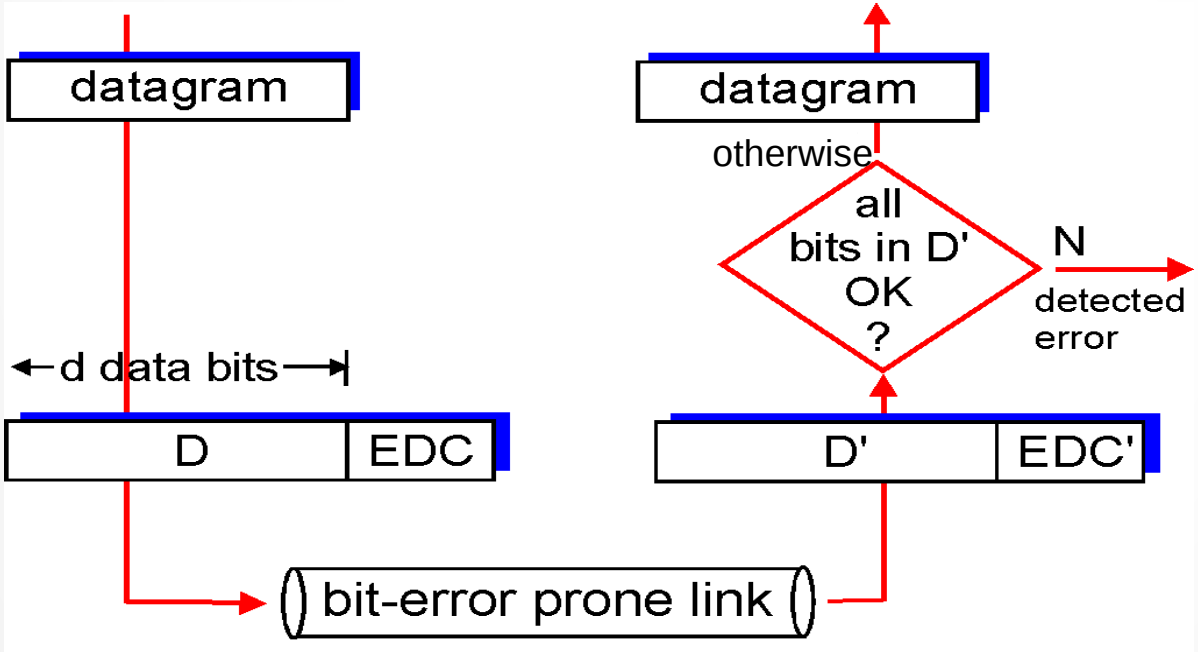
- Logical Link Control (LLC): Interface between Network layer and MAC sub-layer
  - Error Detection
  - Error Recovery (optional)
  - Flow Control (optional)



- Media Access Control (MAC): Controls access to physical media (Broadcast Channels)
  - Framing
- Switching (Interconnecting LANs)

Error Detection

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



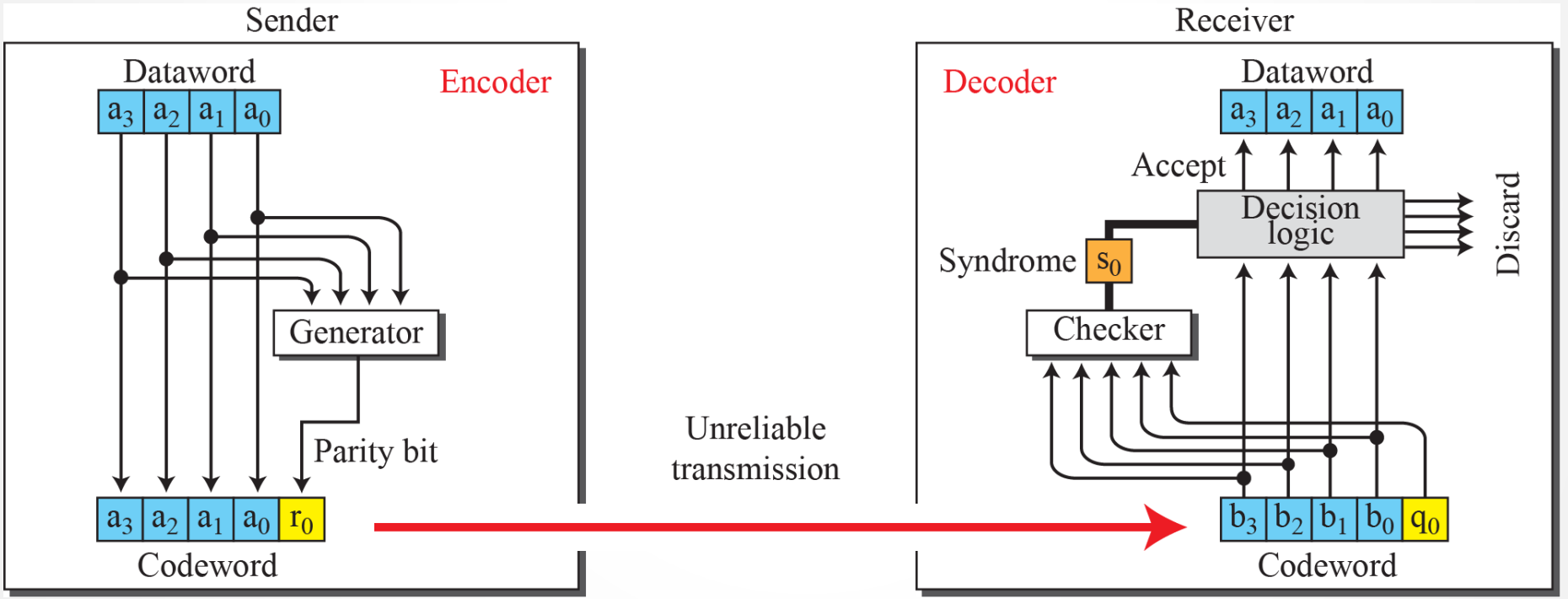
Single Parity Bit

The list of datawords and codewords with Even Parity.

Datawords	Codewords	*Datawords*	Codewords
0000	00000	1000	10001
0001	00011	1001	10010
0010	00101	1010	10100
0011	00110	1011	10111
0100	01001	1100	11000
0101	01010	1101	11011
0110	01100	1110	11101
0111	01111	1111	11110

Single Parity Bit

Encoder and decoder for simple parity-check code

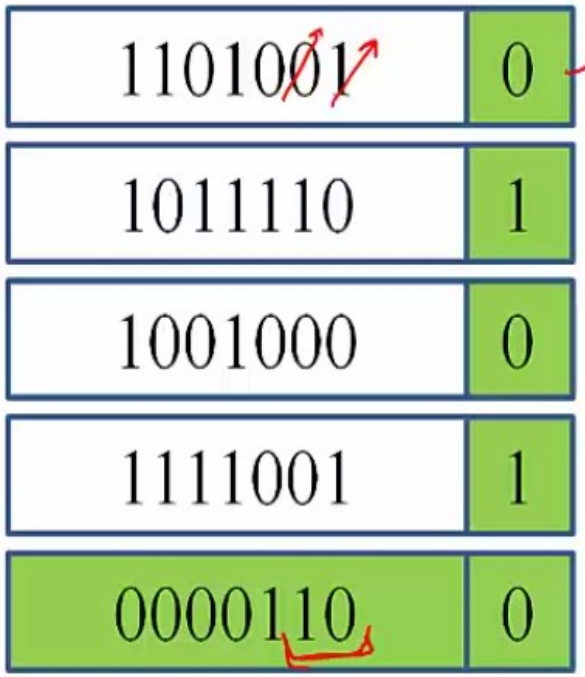


Single Parity Bit : Example

Let us look at some transmission scenarios. Assume the sender sends the dataword 1011. The codeword created from this dataword is 10111, which is sent to the receiver. We examine five cases:

1. No error occurs; the received codeword is 10111. The syndrome is 0. The dataword 1011 is created.
2. One single-bit error changes a_1. The received codeword is 10**0**11. The syndrome is 1. No dataword is created.
3. One single-bit error changes r_0. The received codeword is 1011**0**. The syndrome is 1. No dataword is created. Note that although none of the dataword bits are corrupted, no dataword is created because the code is not sophisticated enough to show the position of the corrupted bit.
4. An error changes r_0 and a second error changes a_3. The received codeword is **0**011**0**. The syndrome is 0. The dataword 0011 is created at the receiver. Note that here the dataword is wrongly created due to the syndrome value. The simple parity-check decoder cannot detect an even number of errors. The errors cancel each other out and give the syndrome a value of 0.
5. Three bits—a_3, a_2, and a_1—are changed by errors. The received codeword is **010**11. The syndrome is 1. The dataword is not created. This shows that the simple parity check, guaranteed to detect one single error, can also find any odd number of errors.

Two Dimensional Parity



- Used by BISYNC protocol for ASCII characters
- "N + 8" bits of redundancy for "N" ASCII characters (character is 7 bits)
- Catches all 1, 2, 3 bit errors and most 4 bit errors

Two Dimensional Parity Bit : Example

In the previous given example let us look at some transmission scenarios.

1. The 1st row data has been received as 1101000 and all other bits remain un-altered. Then w.r.to 2-dimensional parity the parity bit in the first row and the parity bit in the first column must be 1 instead of the received value 0. Hence the error is detected correctly. Also the cross section of these row and column (which is in error) gives the exact bit which is incorrect.

2.The 1st row data has been received as 1101010 and all other bits remain un-altered. In this case, it could able to detect the error but not able to correct these two-bit error.

Checksum

- Not very strong in detecting errors
  – Pair of single-bit errors, one which increments a word, other decrements a word by same amount

- Why is it used still in Transport/Network Layer?
  – Very easy to implement in software
  – Majority of errors picked by CRC at link-level (implemented in hardware)

Cyclic Redundancy Check (CRC)

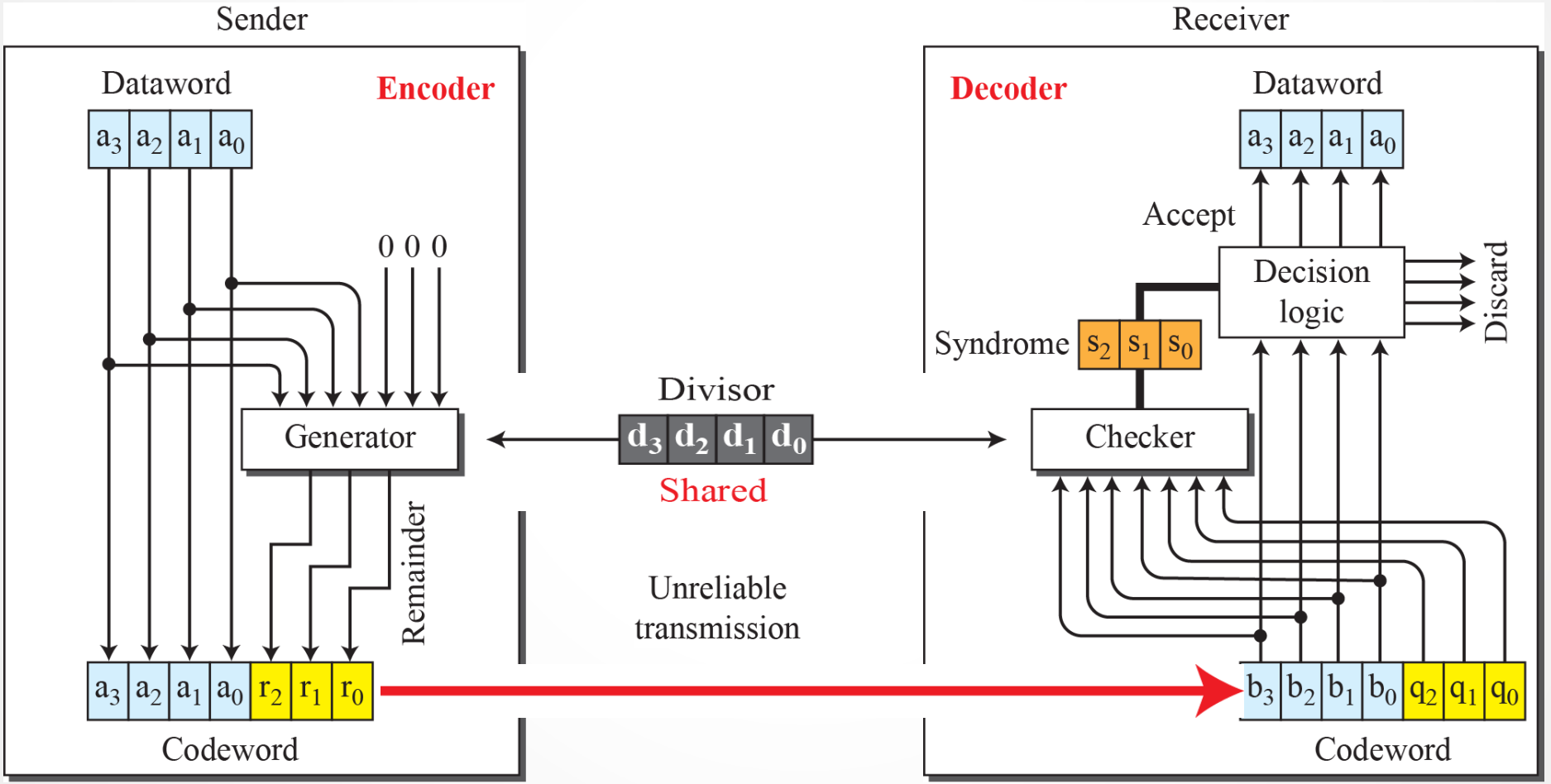
- Used by many link-level protocols:
  - Ethernet, 802.11, Token-Ring, HDLC
- Uses powerful math based on finite fields
- Background: Polynomial Arithmetic

Cyclic Redundancy Check (CRC)

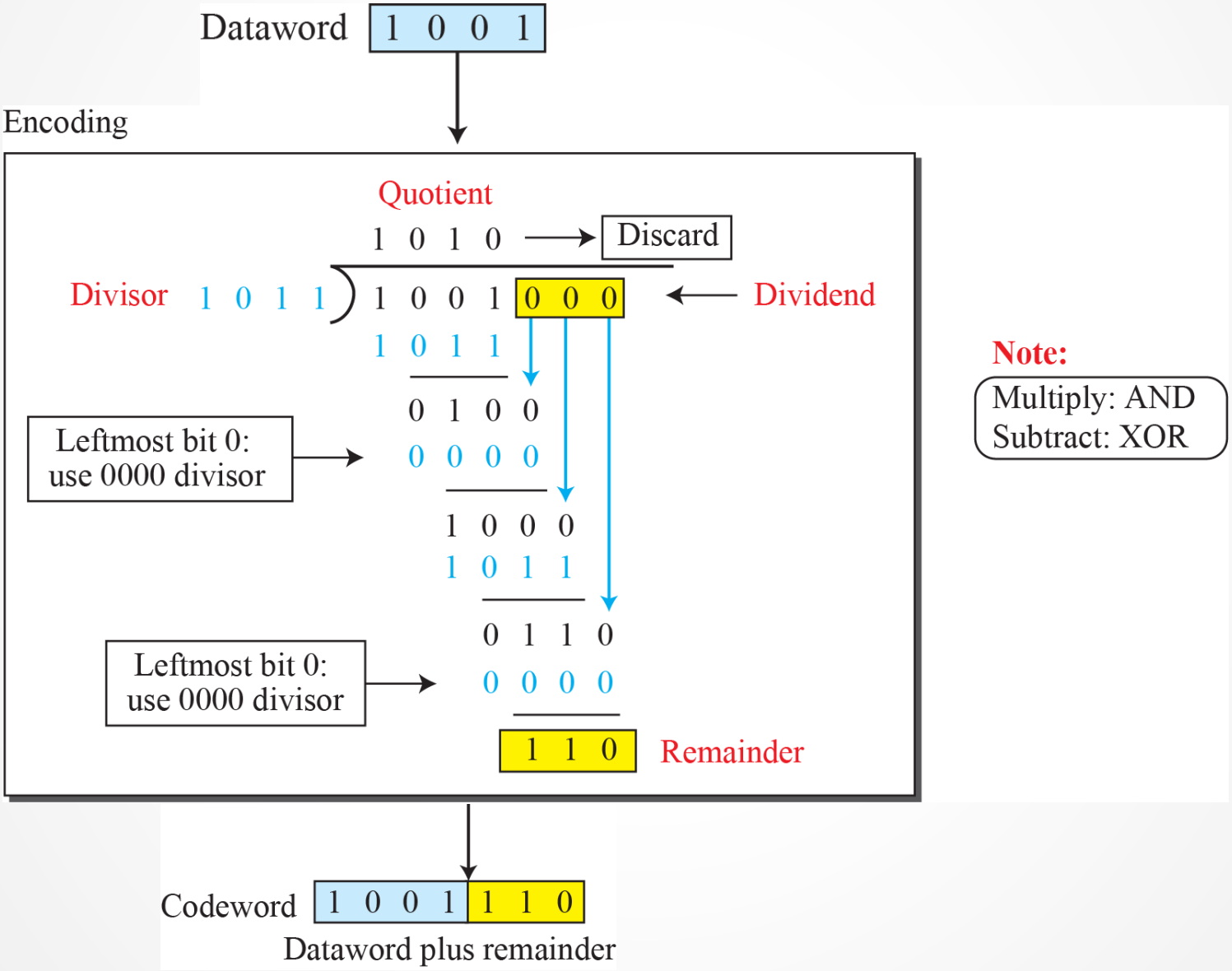
- Message polynomial M(x): m bit message represented with a polynomial of degree “m-1”;
  - 11000101 = $x^7 + x^6 + x^2 + 1$
- Sender and receiver agree on a divisor polynomial C(x) of degree k
  - k: Number of redundancy bit
  - E.g. $C(x) = x^3 + x^2 + 1$ (degree k = 3)
  - Choice of C(x) significantly effects error detection and is derived carefully based on observed error patterns
  - Ethernet uses CRC of 32 bits, HDLC use 16 bits
  - Ethernet:

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

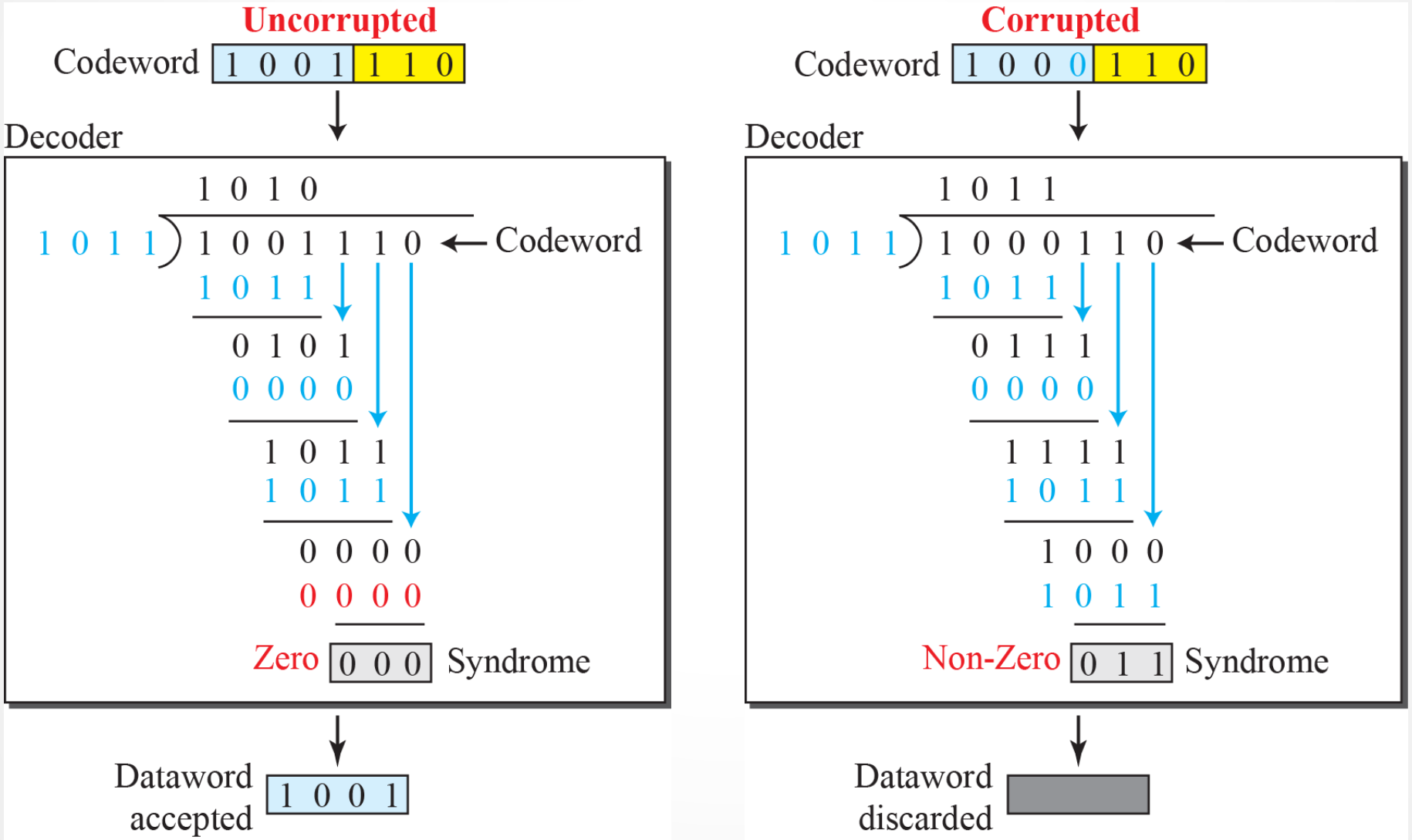
Cyclic Redundancy Check (CRC)



Cyclic Redundancy Check (CRC)



Cyclic Redundancy Check (CRC)



Cyclic Redundancy Check (CRC)

- Requirement :

A Generator must have the follwing 2 properties

  - The Pattern should have at least 2 bits.
  - Rightmost and leftmost bits should be both ones.

- Capabilities :
  - Single-bit errors : All qualified generators can detect any single bit error
  - Burst errors : Assume Length of burst error is L bits and r is the length of remainder.
    1. All burst error of size L <= r are detected
    2. All burst error of size L = r+1 are detected with probability 1- (0.5)^(r-1)
    3. All burst error of size L > r+1 are detected with probability 1- (0.5)^r

Error Control

- After Detection:
  - Drop Frame
    - Higher layers (e.g TCP) will recover or few losses dont hurt applications (e.g. audio)
  - Recover Frame
    - **Error Correction:** Frame carries enough information to correct errors. This is known as “forward error correction”
    - **Retransmission:** Receiver signals sender on error, sender retransmits the frame. This is known as “backward error correction”

Error correction vs Retransmission

- Error correction requires more redundant bits per frame than error detection
  - Redundancy bits are sent all the time (every frame)

- Retransmission requires another copy to be transmitted
  - Copy sent only on error

- Error correction useful when
  - Error rate if high (e.g. wireless)
  - Cost (e.g. latency) of retransmission is too high (e.g. satellite link)

Hamming Distance

- Hamming distance signifies the number of bits flipped among two given codes. For ex.

Hamming distance between 101011 and 111010 is 2

101011
111010

010001

Error correction using Hamming Distance

- At Sender: How to find no. Of redundant bits (r) for data bits (d) ?
  - value of 'r' is derived from 'd' data bits as follows
    - total number of bits = d+r
    - r must be able to indicate at least d+r+1 different value
    - Of these, one value means no error, and remaining d+r values indicate error location of error in each of d+r locations.
    - So, d+r+1 states must be distinguishable by r bits, and r bits can Indicates 2^r states.
    - Hence, $2^r >= d+r+1$ to detect, and correct all single bit error
    - For example, if d is 7, then the smallest value of r that satisfies the above relation is 4. So the total bits, which are to be transmitted is 11 bits (d+r = 7+4 =11)

Error correction using Hamming Distance

- Basic approach for error detection by using Hamming code is as follows:
  - To each group of m information bits, k parity bits are added to form (m+k) bit
  - Location of each of the (m+k) digits is assigned a decimal value.
  - The k parity bits are placed in positions 1, 2, ..., 2^{k-1} positions.
  - K parity checks are performed on selected digits of each codeword.
  - At the receiving end the parity bits are recalculated and Syndrome is generated
    - If the Syndrome contains all 0s, no error
    - If the Syndrome contains only one bit set to 1, then error occured in one of the 4 check bits hence no correction needed
    - If the Syndrome contains more than one bit set to 1, then numerical value of syndrome indicates the postion of the bit in error

Error correction using Hamming Distance : Example

An 8-bit byte with binary value 00111001 is to be encoded using an even-parity Hamming code. What is the binary value after encoding? The codeword received at the other end is 101101001111 then find the position of the error.

Answer: How many check bits? 4

Bit position	12	11	10	9	8	7	6	5	4	3	2	1
Bit number	1100	1011	1010	1001	1000	0111	0110	0101	0100	0011	0010	0001
Data bit	D8	D7	D6	D5		D4	D3	D2		D1		
Check bit					C8				C4		C2	C1

C1 is a parity check on every data bit whose position is xxx1
C2 is a parity check on every data bit whose position is xx1x
C4 is a parity check on every data bit whose position is x1xx
C8 is a parity check on every data bit whose position is 1xxx

$$C1 = 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 = 1$$
$$C2 = 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 = 1$$
$$C4 = 0 \oplus 0 \oplus 1 \oplus 0 = 1$$
$$C8 = 1 \oplus 1 \oplus 0 \oplus 0 = 0$$

Bit position	12	11	10	9	8	7	6	5	4	3	2	1
Position number	1100	1011	1010	1001	1000	0111	0110	0101	0100	0011	0010	0001
Data bit	D8	D7	D6	D5		D4	D3	D2		D1		
Check bit					C8				C4		C2	C1
Word stored as	0	0	1	1	0	1	0	0	1	1	1	1

Error correction using Hamming Distance : Example

Let us verify that this scheme works with an example. Assume that the 8-bit input word is 00111001, with data bit D1 in the rightmost position. The calculations are as follows:

$$C1 = 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 = 1$$
$$C2 = 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 = 1$$
$$C4 = 0 \oplus 0 \oplus 1 \oplus 0 = 1$$
$$C8 = 1 \oplus 1 \oplus 0 \oplus 0 = 0$$

Suppose now that data bit 3 sustains an error and is changed from 0 to 1. When the check bits are recalculated, we have

$$C1 = 1 \oplus 0 \oplus 1 \oplus 1 \oplus 0 = 1$$
$$C2 = 1 \oplus 1 \oplus 1 \oplus 1 \oplus 0 = 0$$
$$C4 = 0 \oplus 1 \oplus 1 \oplus 0 = 0$$
$$C8 = 1 \oplus 1 \oplus 0 \oplus 0 = 0$$

When the new check bits are compared with the old check bits, the syndrome word is formed:

	C8	C4	C2	C1
	0	1	1	1
$\oplus$	0	0	0	1
	0	1	1	0

The result is 0110, indicating that bit position 6, which contains data bit 3, is in error.

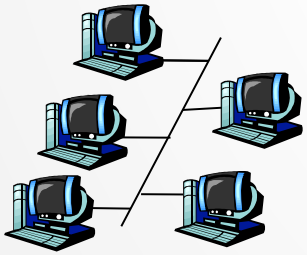
Increased Word length for Error correction

	Single-Error Correction		Single-Error Correction/ Double-Error Detection	
Data Bits	Check Bits	% Increase	Check Bits	% Increase
8	4	50	5	62.5
16	5	31.25	6	37.5
32	6	18.75	7	21.875
64	7	10.94	8	12.5
128	8	6.25	9	7.03
256	9	3.52	10	3.91

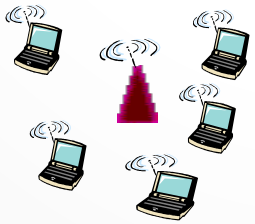
Multiple Access Links and Protocols

Two types of “links”:

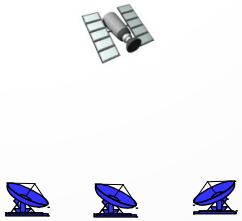
- point-to-point
  - PPP for dial-up access
  - point-to-point link between Ethernet switch and host
- broadcast (shared wire or medium)
  - Cable Ethernet
  - 802.11 wireless LAN



shared wire (e.g., cabled Ethernet)



shared RF (e.g., 802.11 WiFi)



shared RF (satellite)

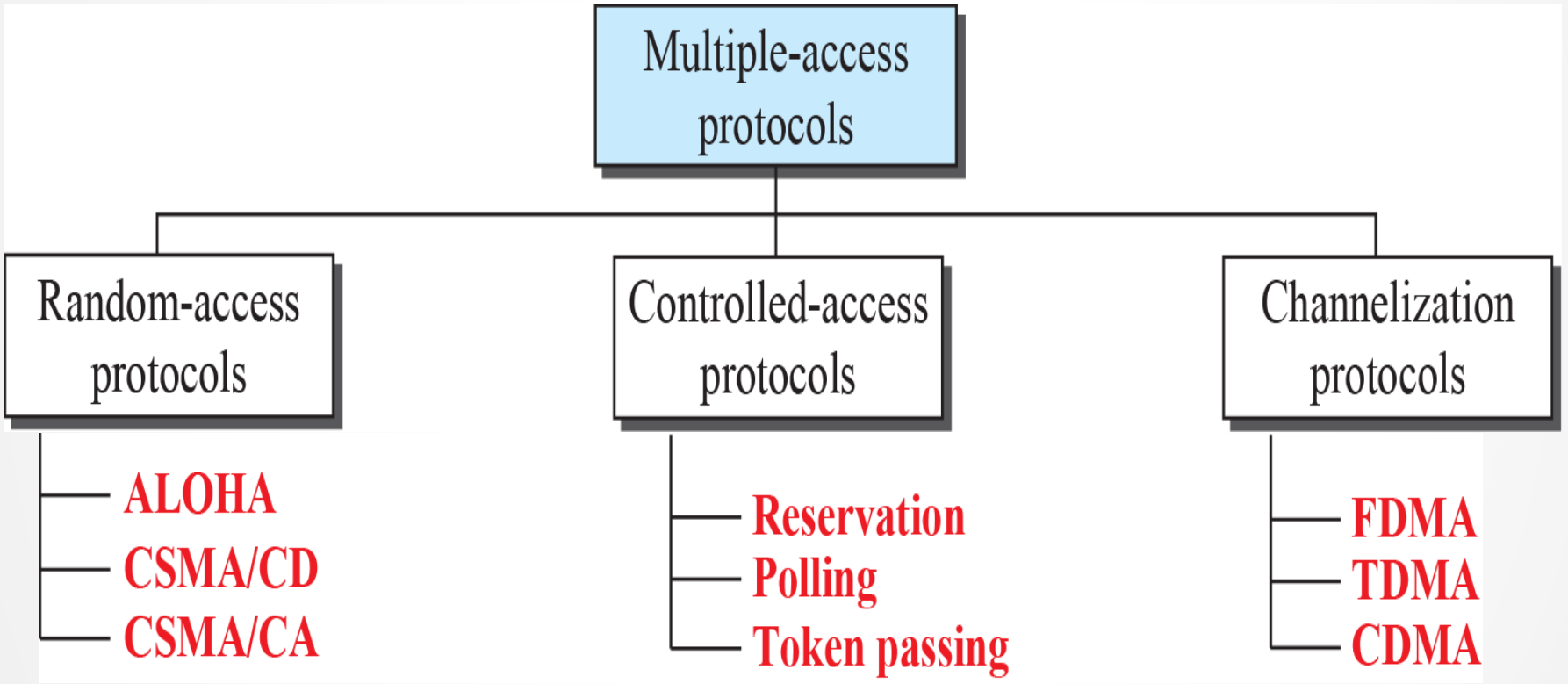
humans at a cocktail party (shared air, acoustical)

Media Access Control (MAC)

- Two or more nodes simultaneous transmits -> interference (collision)

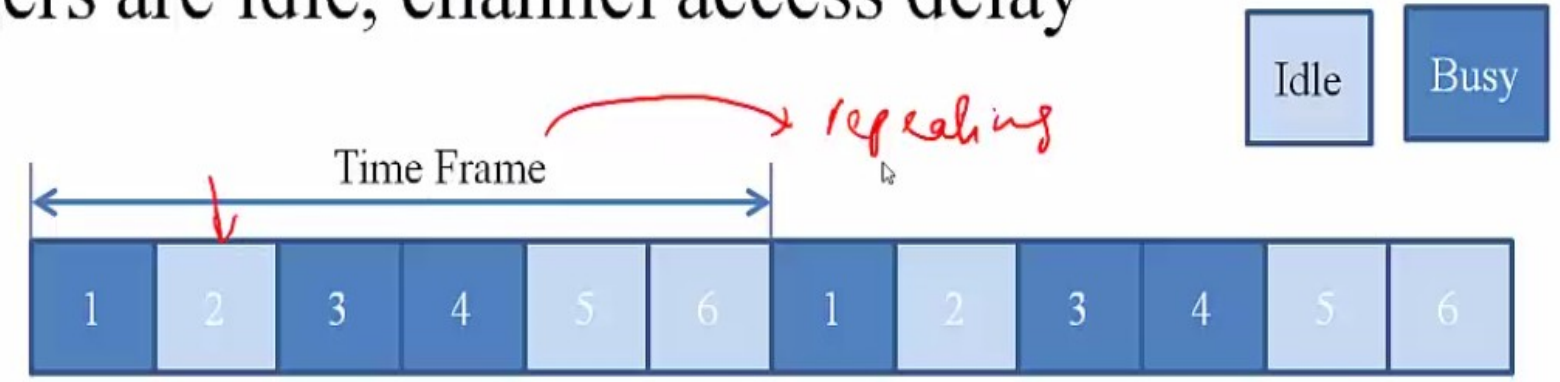
- MAC: Protocol that determines how nodes share channel among themselves
  - – Determine when a node can transmit
  - – Communication about channel sharing must use channel itself!

MAC Protocols



Time Division Multiplexing

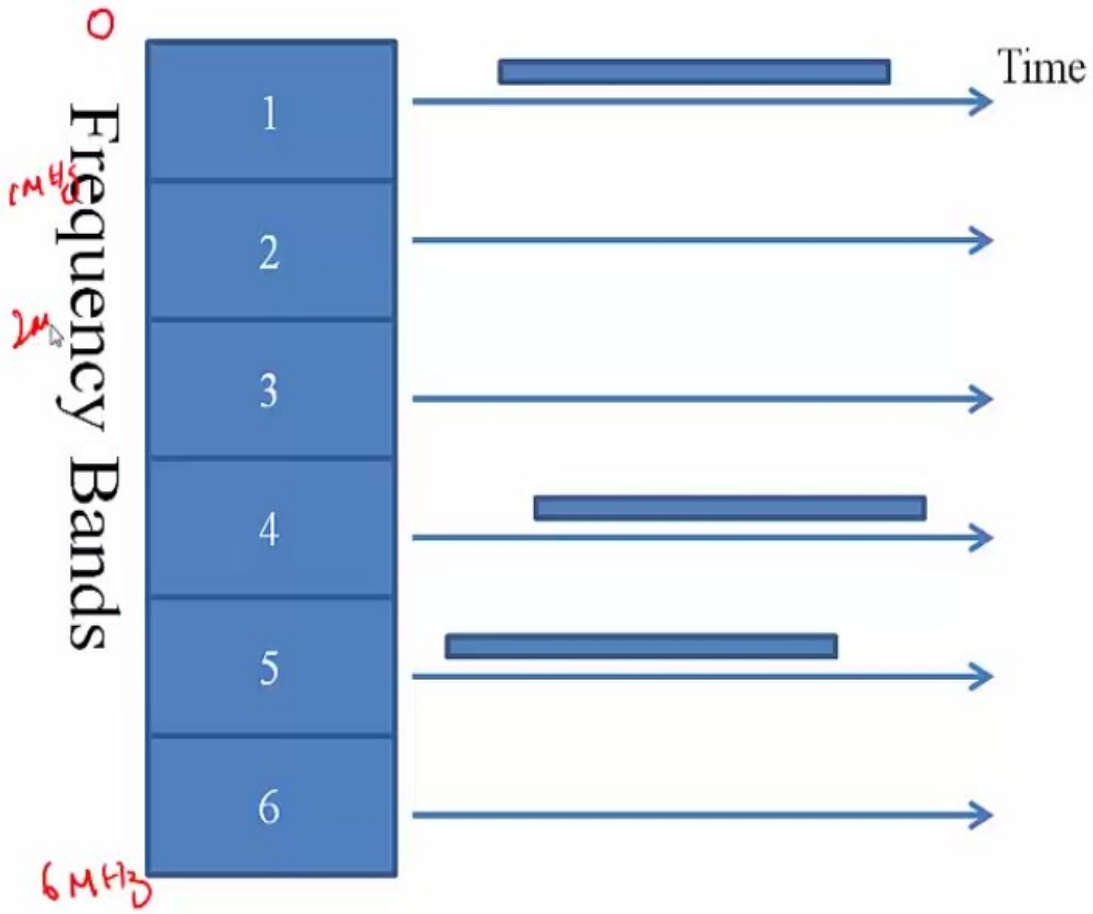
- Allocate couples different time slots → Time Division Multiplexing (TDM)
- Time divided into time frames. Time frames divided into N time slots. Each sender allocated one time slot.
- Disadvantage: Sender limited to R/N even when other senders are idle, channel access delay



Frequency Division Multiplexing

- Move couples to different rooms →Frequency Division Multiplexing (FDM)
- Spectrum divided into frequency bands
  - Sender/Receivers tune in to assigned frequency band
  - If there are N senders, each sender gets R/N bandwidth
- Disadvantages:
  - A sender limited to R/N even when other senders are idle
  - Sender-Receiver channel coordination

Frequency Division Multiplexing



Code Division Multiplexing

- Ask couples to speak in different languages → Code Division Multiple Access (CDMA)
- Each sender is assigned a different code
  - Sender can transmit in the entire frequency band all the time,
  - With N senders, achievable rate is still R/N
- Same problem as with previous protocols

Random Access Protocols

- Polite Speaker: Listen. If its quiet, start talking.

If this clashes with others, backoff and try again.

- Sender transmits at full rate. If two or more transmit at same time -> Collision

- Specify:
  - How to detect collisions?
  - How to recover from collisions?
- Disadvantages:
  - High load leads to too many collisions and wastage of resources

Controlled Access Protocols

- Quickly poll to see who wants to talk, give time slots to only speakers

- Channel partitioning MAC protocols: efficient and fair at high load, inefficient at low load

- Random access MAC protocols: efficient at low load, inefficient at high load

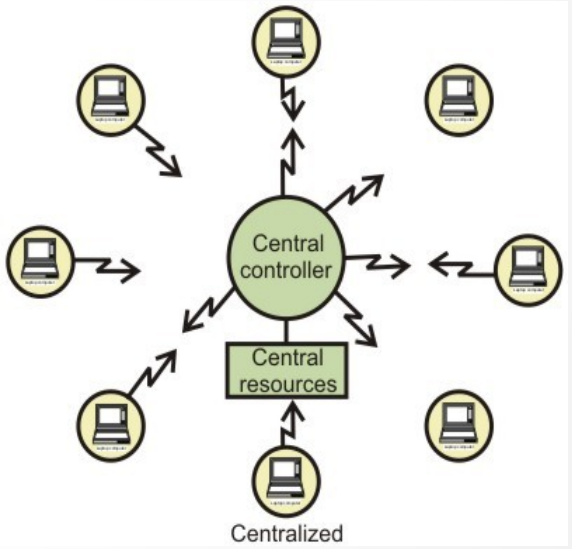
- Controlled Access protocols: Make the best of both worlds!

Polling (Centralized)

A central coordinator polls nodes in a round robin fashion

- Advantages:
  - – eliminates the collisions and empty slots that plague random access protocols.
  - – achieve a much higher efficiency

- Disadvantages:
  - – protocol introduces a polling delay
  - – Single point of failure (coordinator)

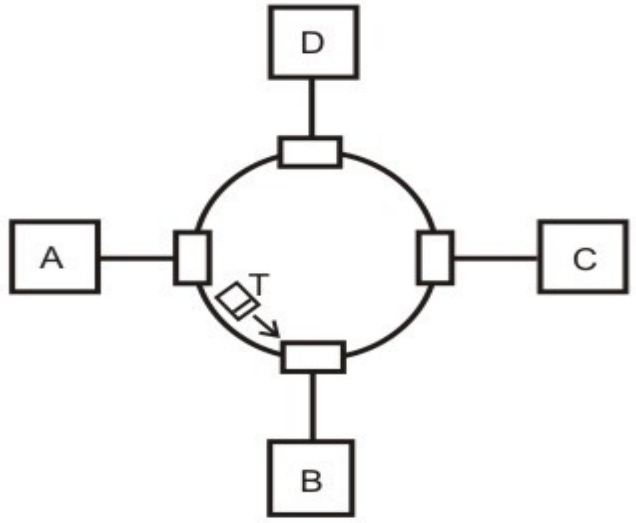


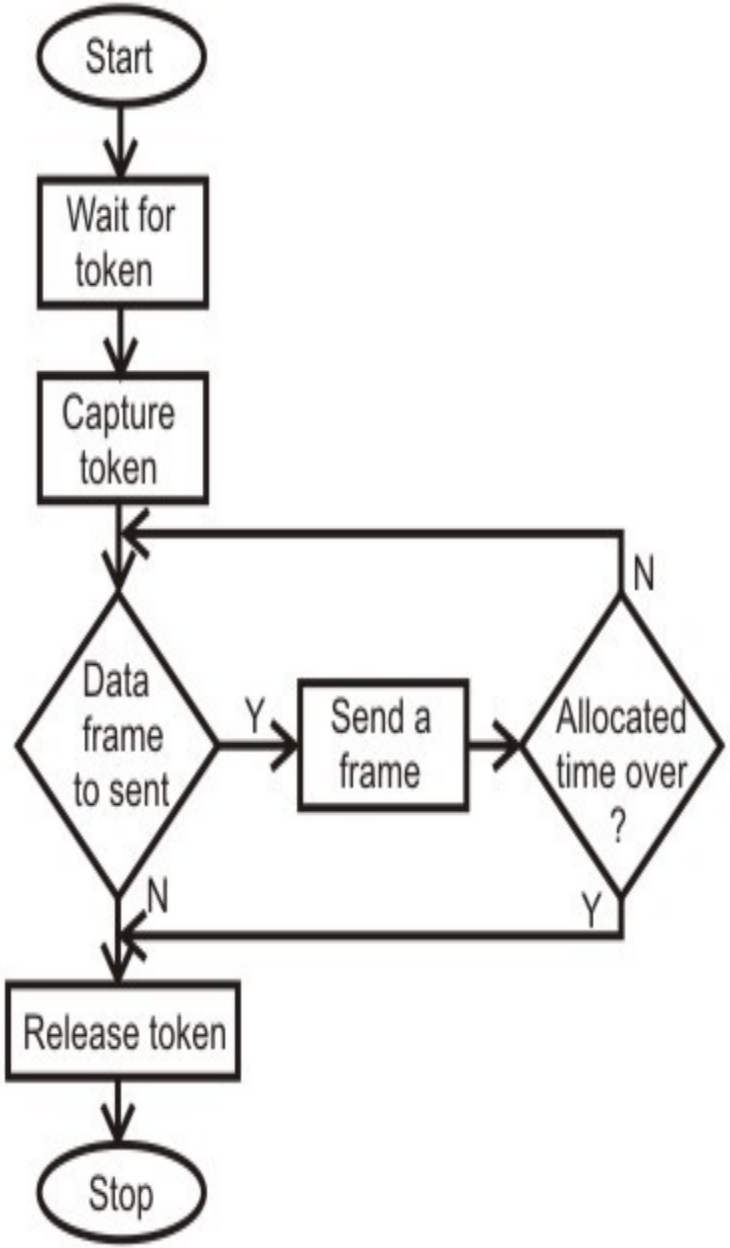
802.15 and Bluetooth protocol uses polling technique

Token Passing (Decentralized)

Control token passed from one node to next in certain order

- Advantage
  - – Token passing is decentralized and highly efficient
- Disadvantage
  - – Token overhead
  - – Single point of failure (token)
  - – Failure of one node can crash the entire channel

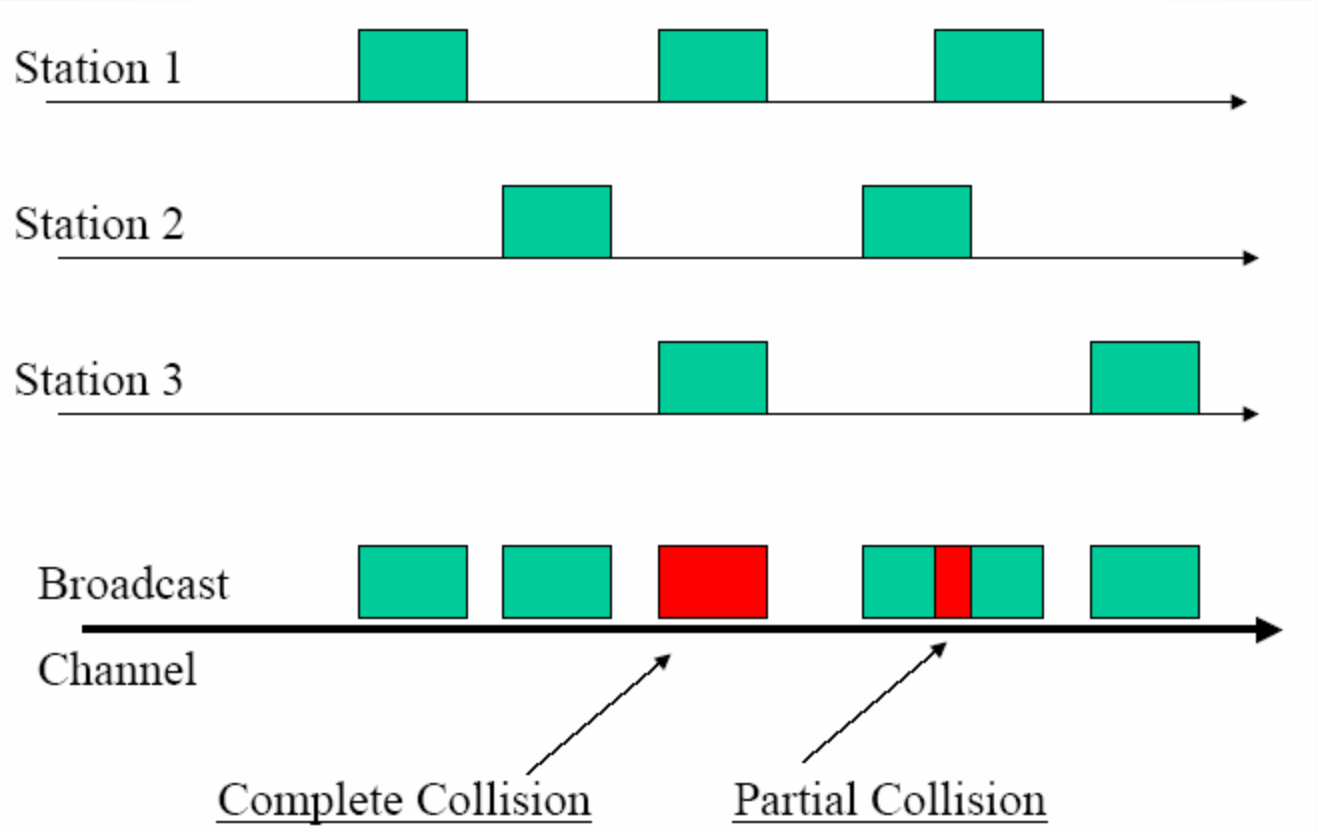




Usage

- TDMA with FDM: GSM, WiMAX, 3-4G
- CDMA: IS-95, CDMA2000, 3-4G
- Random Access: Ethernet, WiFi
- Polling: Bluetooth, 802.15
- Token Passing: Token Ring, FDDI

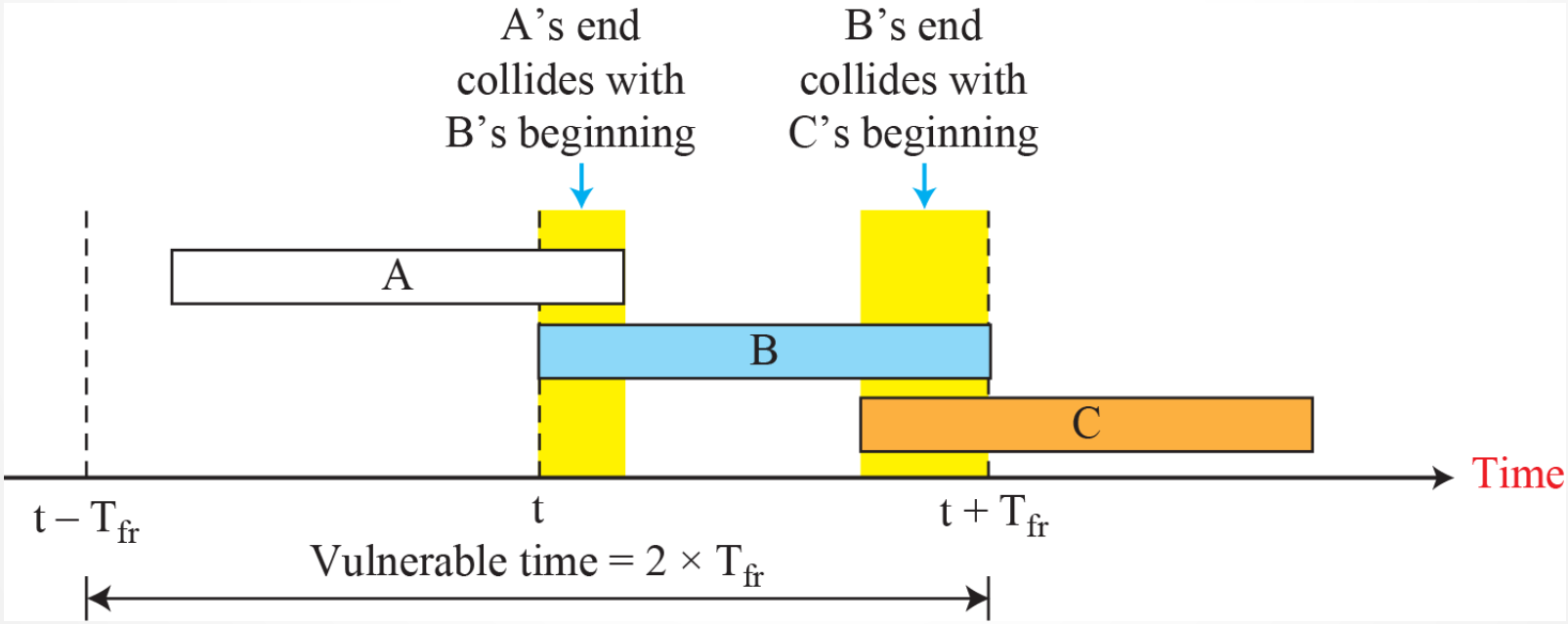
Pure ALOHA


Station 1
Station 2
Station 3
Broadcast
Channel
Complete Collision
Partial Collision

Vulnerable time for Pure ALOHA

- when frame first arrives transmit immediately
- collision probability:

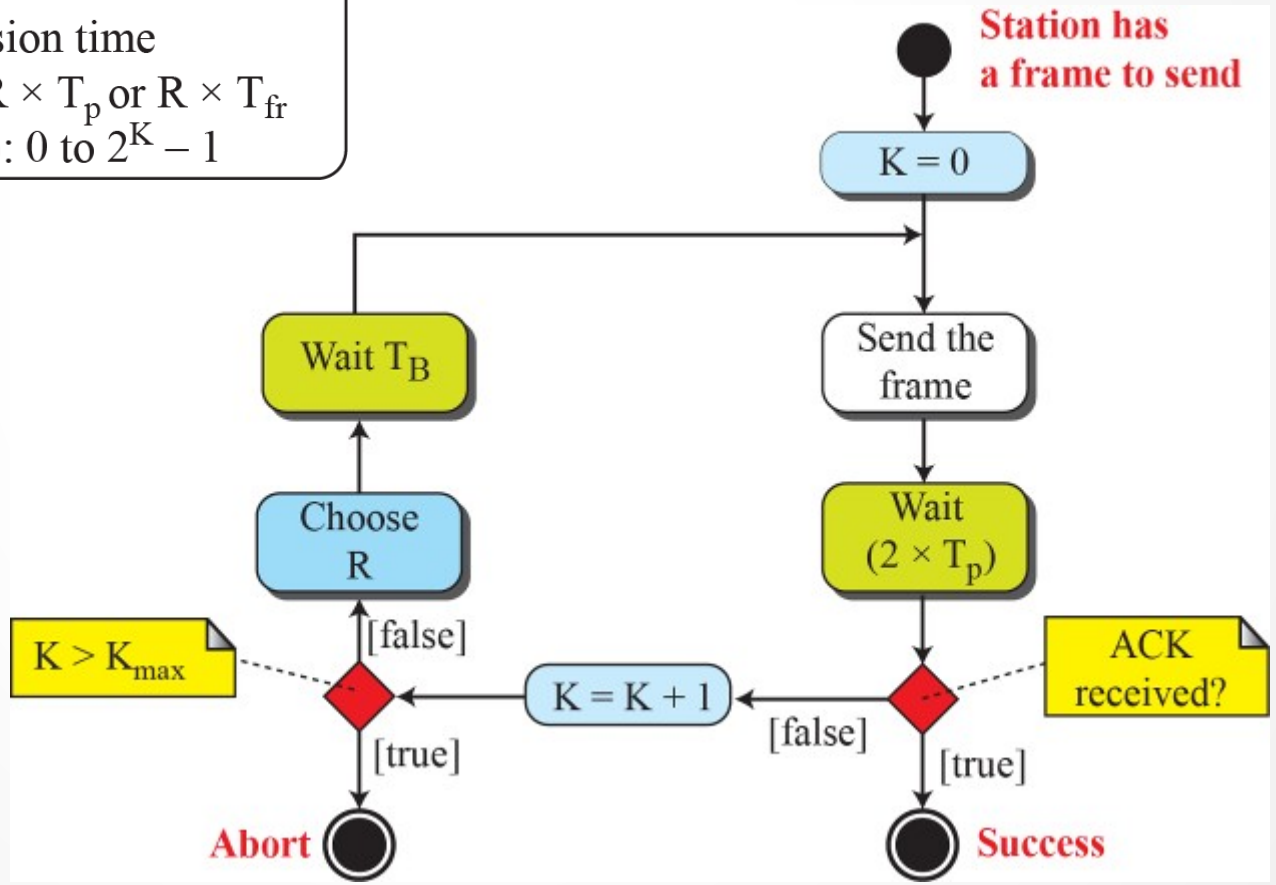
  frame sent at t collides with other frames sent in [t-T_{fr},t+T_{fr}]



Pure ALOHA

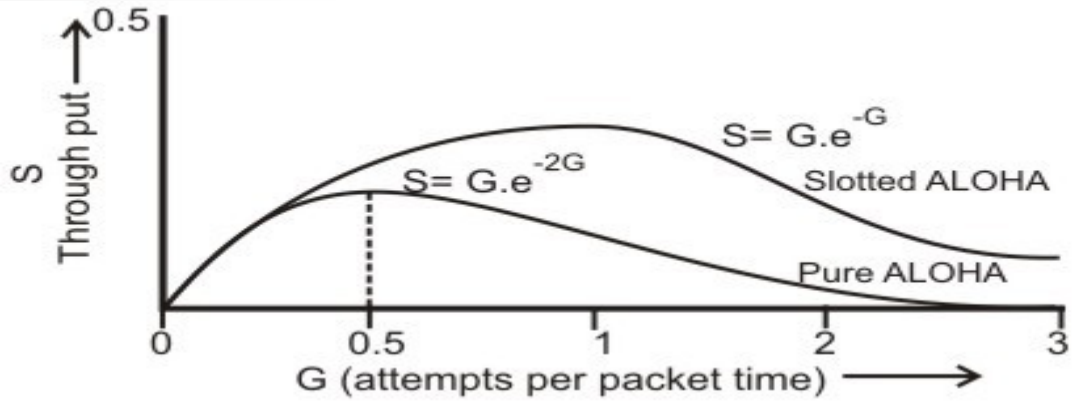
Legend

K : Number of attempts
T_p : Maximum propagation time
T_{fr}: Average transmission time
T_B: (Back-off time): $R \times T_p$ or $R \times T_{fr}$
R : (Random number): 0 to $2^K - 1$



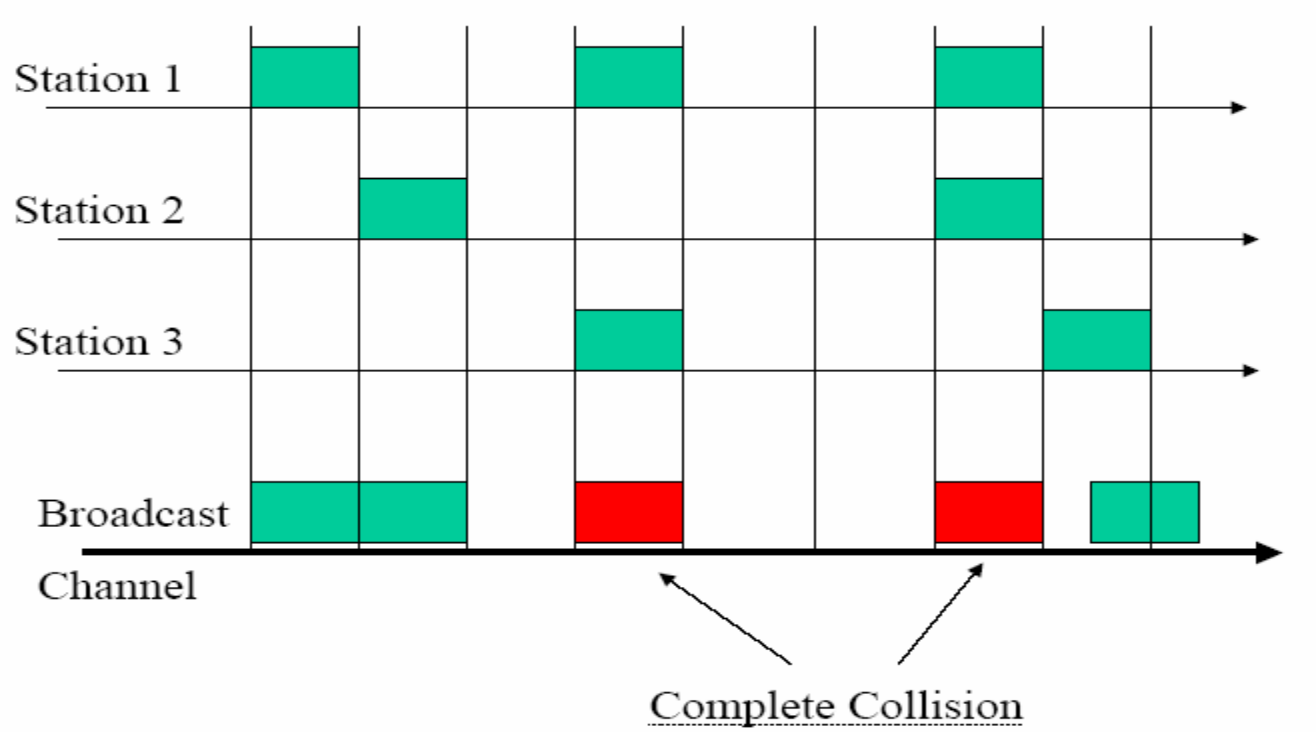
Efficiency of Pure ALOHA

- Frames are of equal length
- The channel utilization, expressed as throughput S, in terms of the offered load G is given by $S=Ge^{-2G}$
- Based on this, the best channel utilization of 18% can be obtained
- At smaller offered load, channel capacity is underused and at higher offered load too many collisions occur reducing the throughput.



Slotted ALOHA

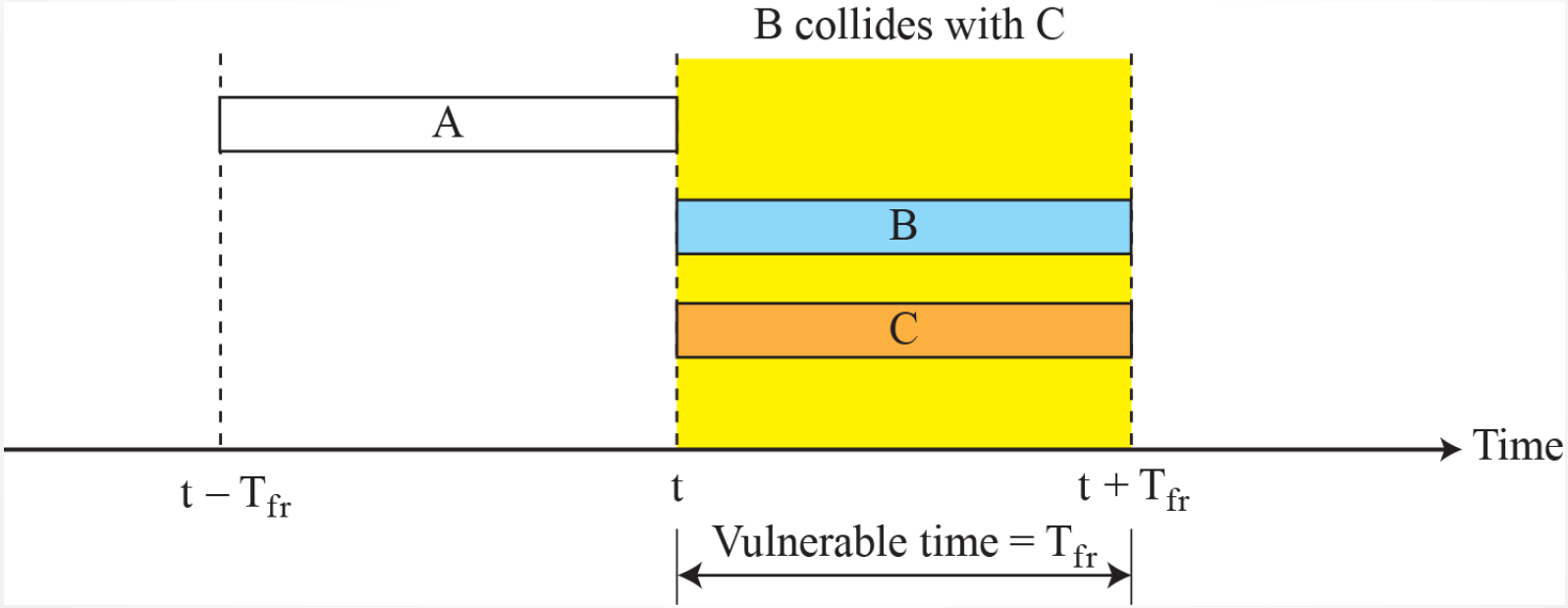
- time divided into equal size slots (time to transmit 1 frame)
- Nodes can transmit frames only at beginning of slots
- Vulnerable period reduced by half



Vulnerable time for Slotted ALOHA

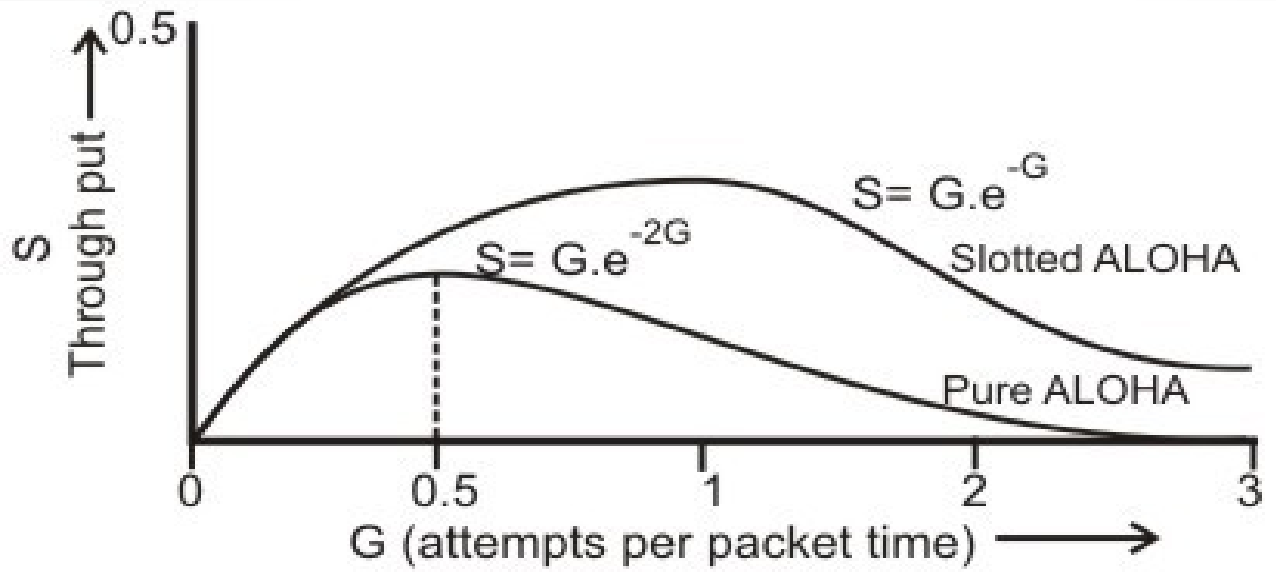
- when frame first arrives it has to wait for the beginning of a slot
- collision probability :

  frame sent at t collides with other frames sent in $[t, t+T_{fr}]$



Efficiency of Slotted ALOHA

- The reduction in the vulnerable period from $2T_{fr}$ to T_{fr} improves efficiency by reducing the probability of collision
- This gives a maximum throughput of 37% at 100 percent of offered load



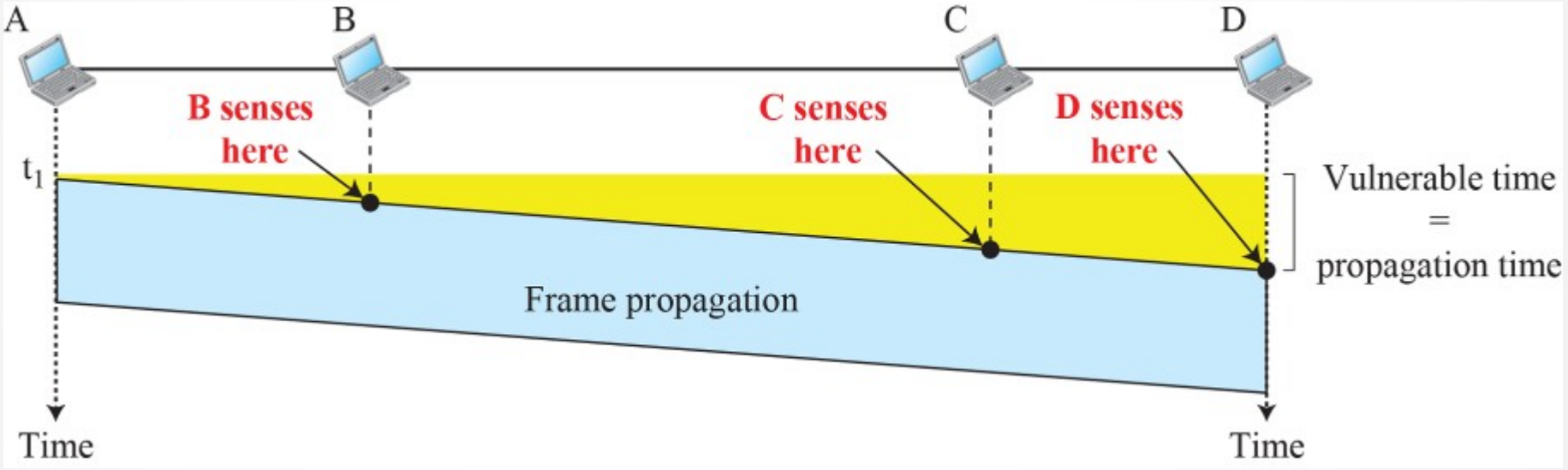
CSMA

- poor efficiency of ALOHA : Transmissions without care or concern for channel state

- In this scheme, ‘Listen before Talk’ – Carrier Sense
- If a node has a frame to send, listen to channel first
  - – If busy, don’t send frame --- don’t disrupt ongoing transmission
  - – If idle, send frame

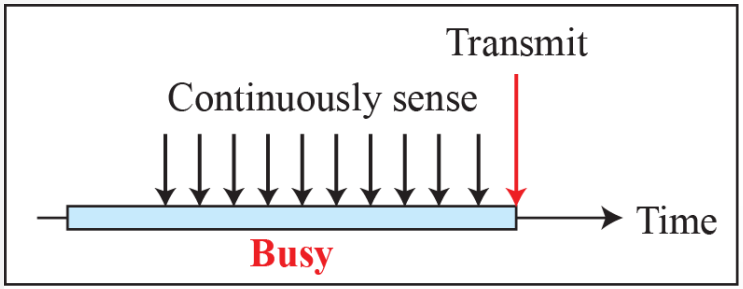
- Two categories: persistent and non-persistent

Vulnerable time for CSMA

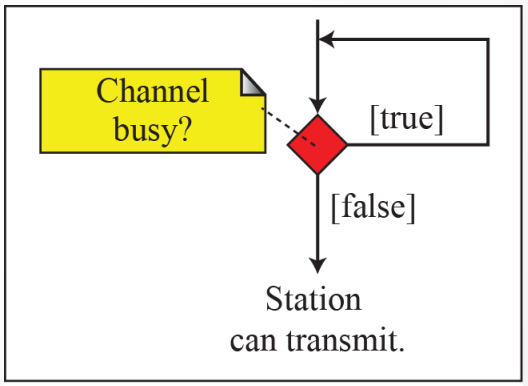


1-Persistent CSMA

- Employed by Ethernet
- If a node has a frame to send:
  - If channel busy, wait till it becomes idle, then transmit
  - If channel idle, transmit
  - If collision, wait a random amount of time and start over
- Better than Aloha



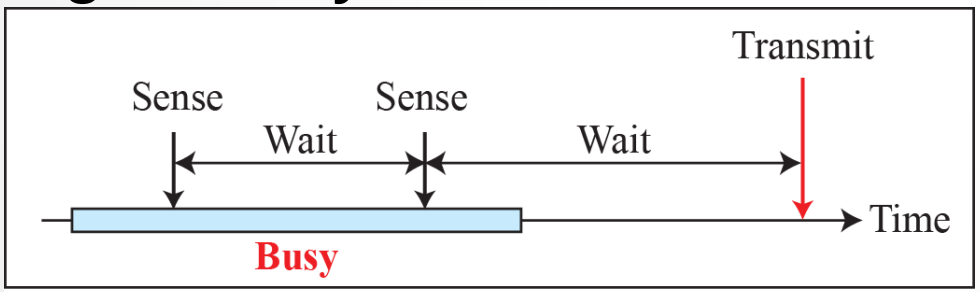
a. 1-persistent



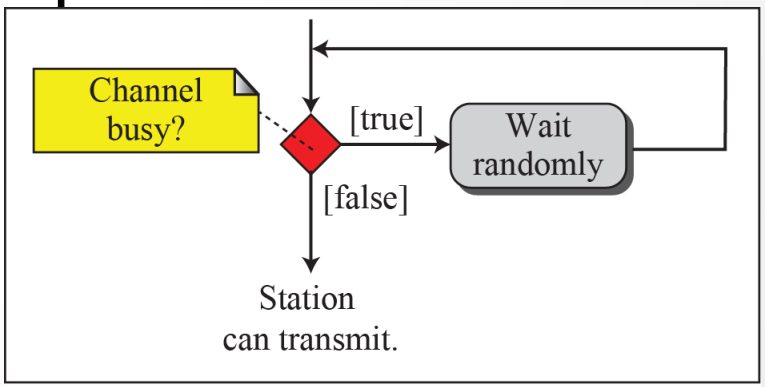
a. 1-persistent

Non Persistent CSMA

- Used in 802.15.4 (Zigbee/Sensor technology)
- If a node has a frame to send:
  - If channel busy, do not sense anymore. Wait a random amount of time and try again
  - If channel idle, transmit
  - If collision, wait a random amount of time and start over
- Better channel utilization than 1-persistent but longer delays



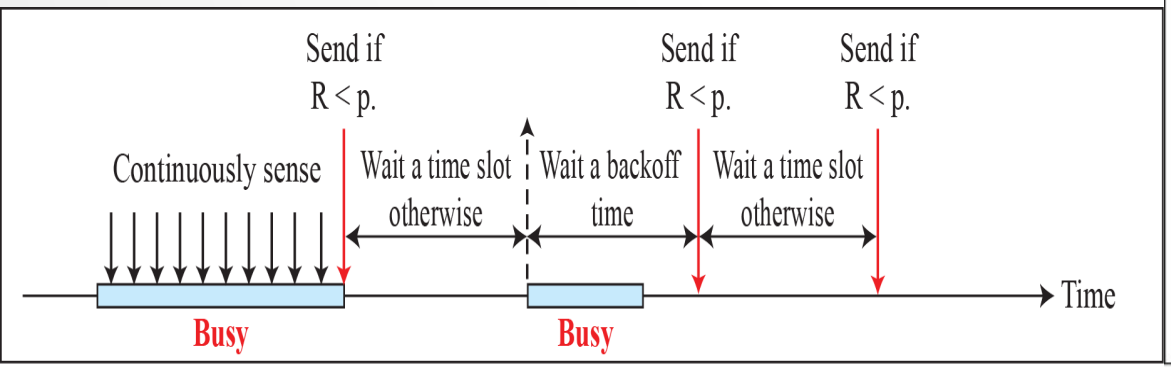
b. Nonpersistent



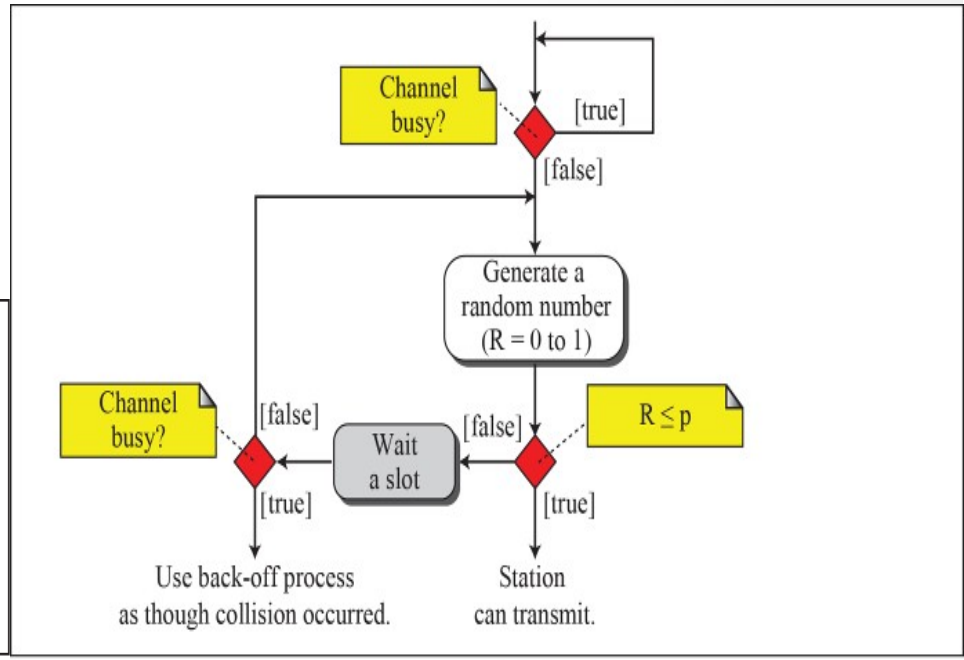
b. Nonpersistent

P-persistent CSMA

- Employed by 802.11 (WiFi)
- If a node has a frame to send:
  - If channel idle, transmit with probability p (defer to next slot with probability q=1-p). Repeat till frame sent or channel busy due to another transmission
  - If channel busy, wait till idle. Repeat above.
  - If collision, wait a random time and try again
- Good Tradeoff between non-persistent and 1-persistent



c. *p*-persistent



c. *p*-persistent

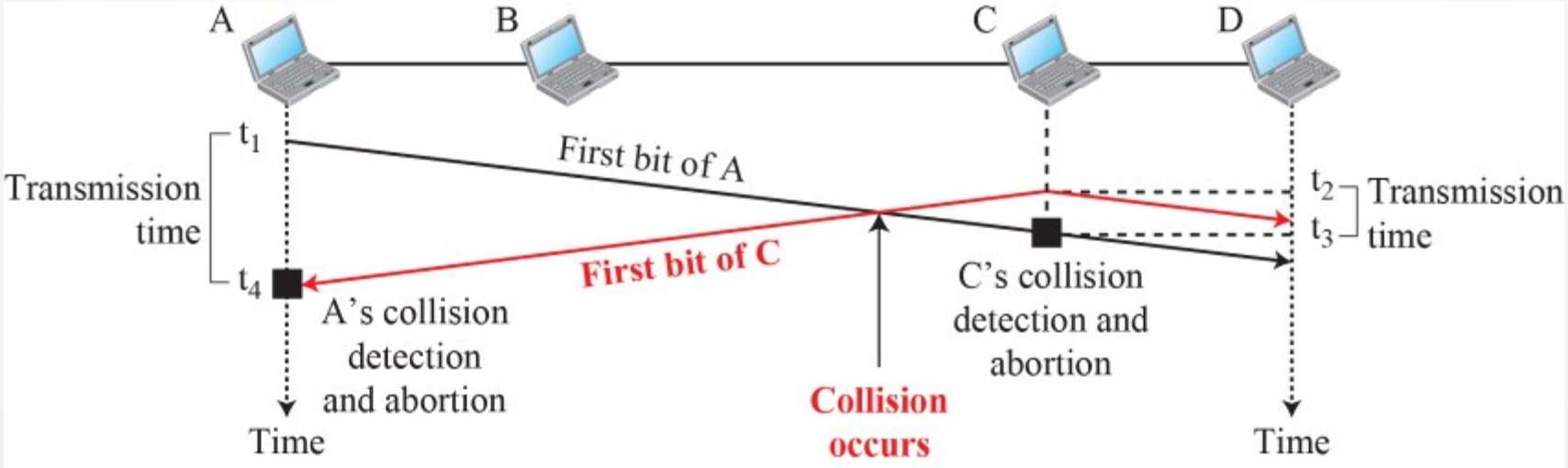
CSMA/CD

- refinement over the CSMA scheme used for Ethernet MAC

- CSMA/CD: Carrier Sense Multiple Access (1-persistent) with Collision Detection
  - Listen-While-Talk.
  - in CSMA, when two packets collide the channel remains unutilized for the entire duration of transmission time of both the packets
  - in CSMA/CD, If a collision is detected during transmission of a packet, the node immediately ceases transmission to reduce the wastage of channel capacity.

Collision Detection

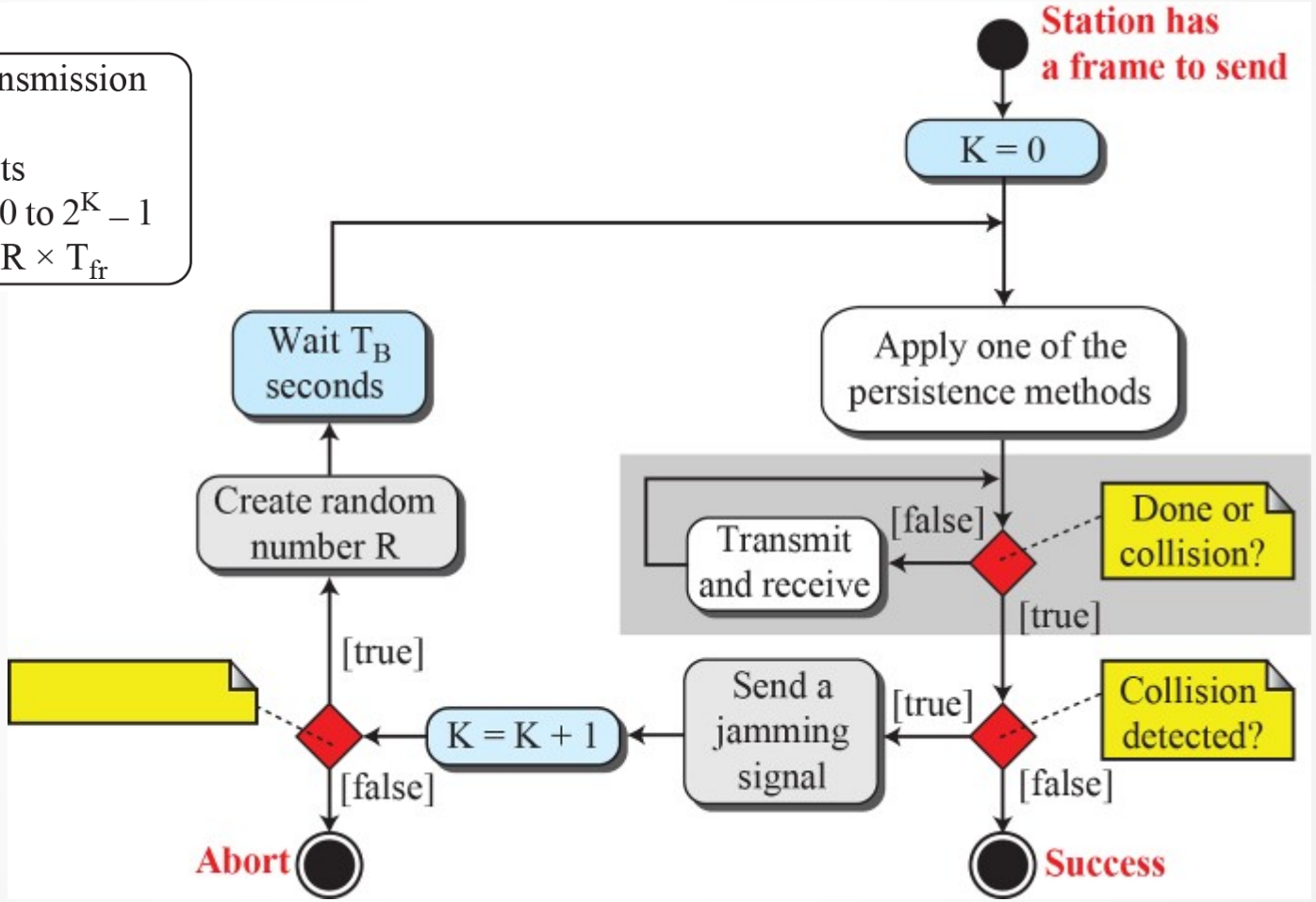
- Cases under which collision occurs?
  - – Two stations waiting for channel to become idle
  - – Two stations attempting transmission at same time on an idle channel
  - – Two stations attempting transmission at slightly different times on an idle channel



CSMA/CD

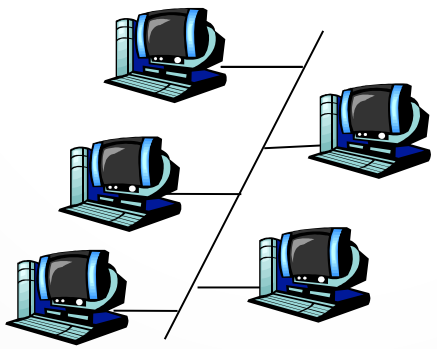
Legend

T_{fr}: Frame average transmission time
K : Number of attempts
R : (random number): 0 to $2^K - 1$
T_B: (Back-off time) = R × T_{fr}



Ethernet -- Overview

- Up to early 1990's: Ethernet uses Bus topology which is based on co-axial cable
  - Thicknet (10Base5)
  - Thinnet (10Base2)
- Media Access Control: CSMA/CD



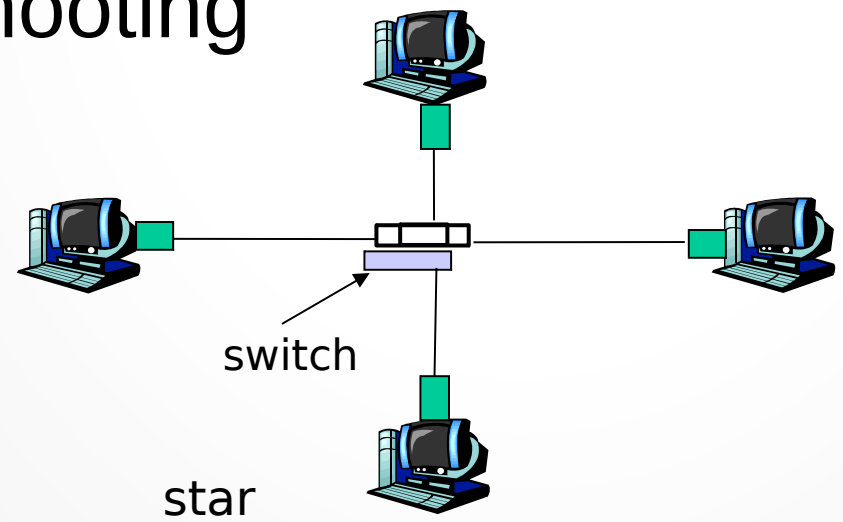
bus: coaxial cable

Problems with Bus Topology

- Co-axial cables were expensive
- Break/Fault in co-axial cable affects all nodes
- Adding/removing nodes disrupts the entire network
- Cabling Issues lead to star topology

Star Topology

- Connect via hub or switch
- 10BaseT (Standard Ethernet), 100BaseT (Fast Ethernet), 1000BaseT (Gigabit Ethernet)
  - Based on twisted pair cables
  - Low cost, reliable, easy management/ troubleshooting

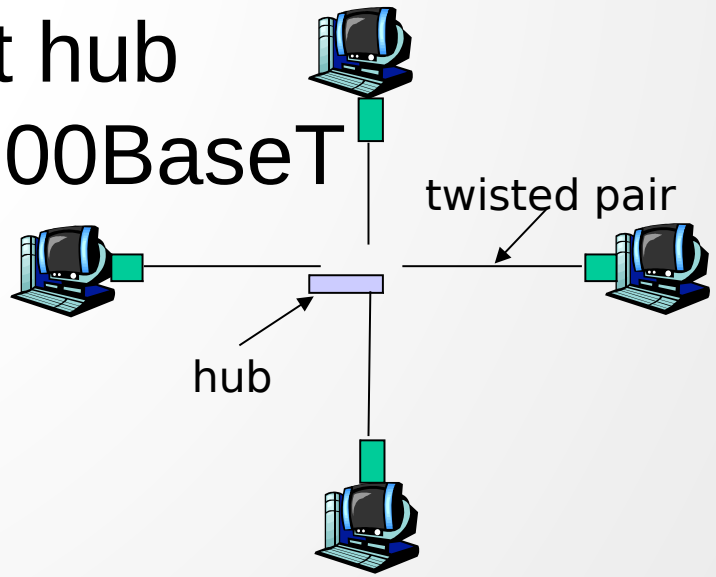


star

Hub

Physical layer (“dumb”) repeaters

- bits from one link sent out on all other links at same rate after boosting up the energy
- all nodes connected to hub can collide with one another
- No frame buffering
- No MAC protocol (CSMA/CD) at hub
- Cannot connect 10BaseT with 100BaseT

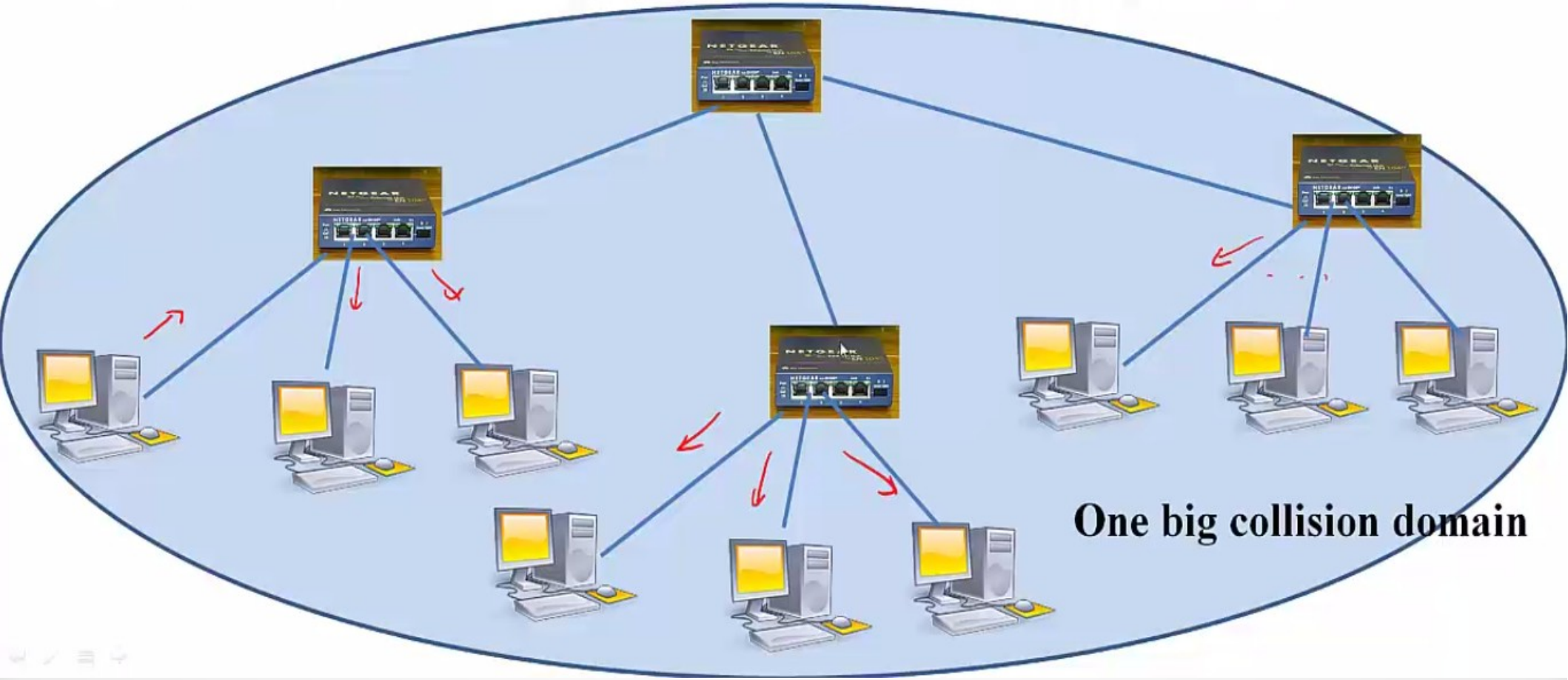


Layer-2 Switch

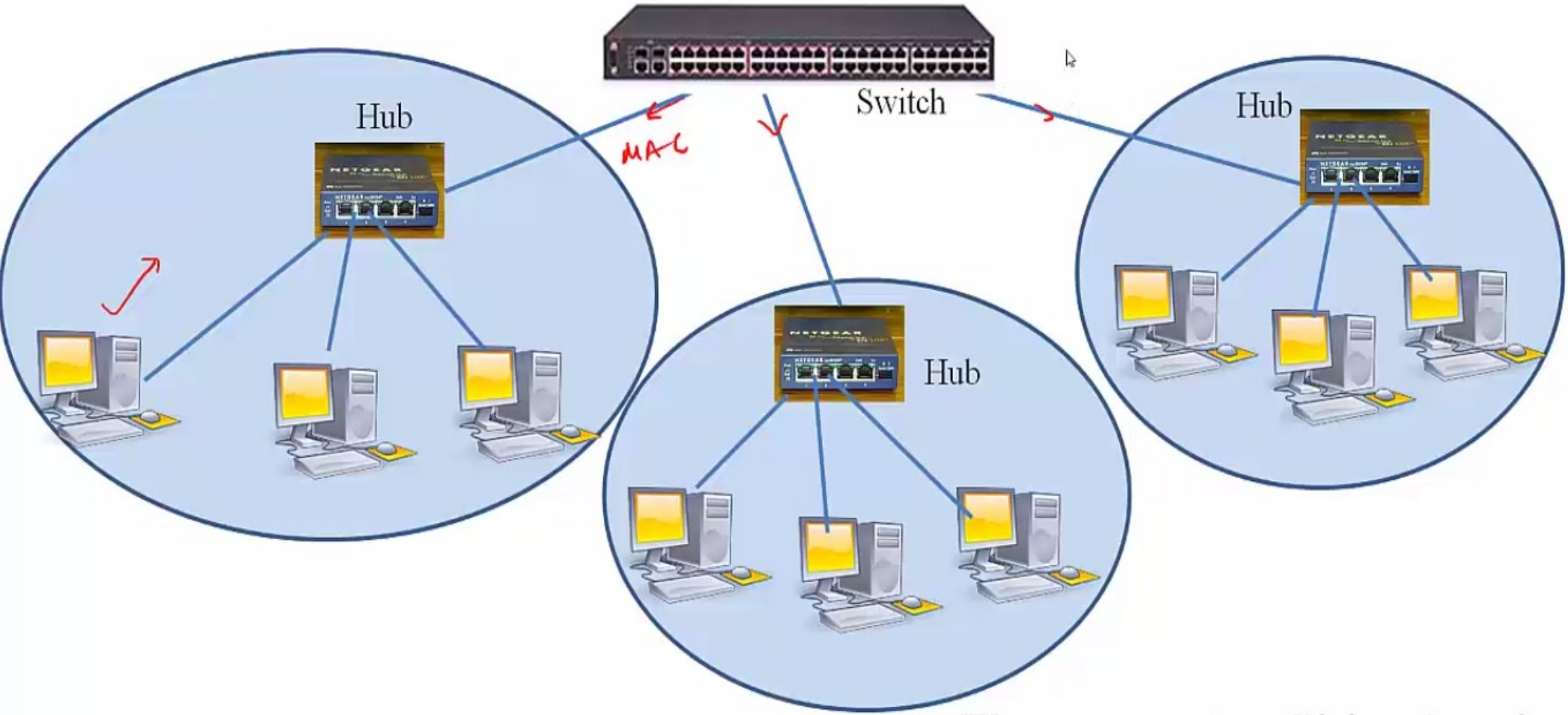
- link-layer device: smarter than hubs, take *active* role
- Also called Ethernet Bridge
- Mostly used configuration
- Transfers frames from an input to an output link
  - Runs MAC protocol on each interface
  - Buffer packets
  - Break up collision domains
  - Can switch speeds (10Mbps, 100Mbps)

Interconnecting Hubs

- Can increases reach
- Cannot connect 10BaseT with 100BaseT



Interconnection with Switch



Three separate collision domains

Switching

a. Original

Address	Port

b. After A sends a frame to D

Address	Port
71:2B:13:45:61:41	1

c. After D sends a frame to B

Address	Port
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4

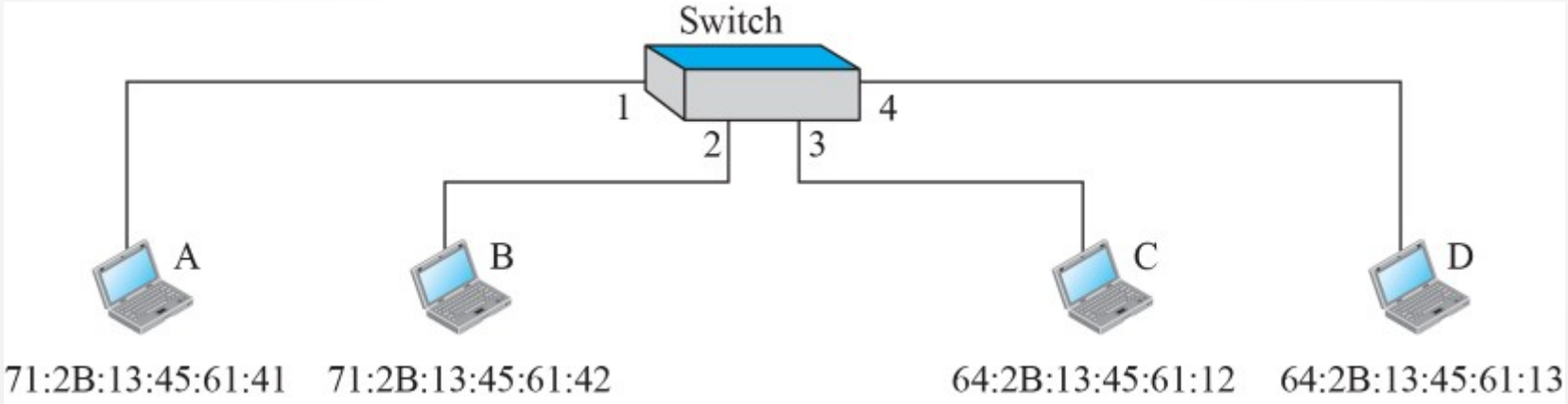
d. After B sends a frame to A

Address	Port
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4
71:2B:13:45:61:42	2

e. After C sends a frame to D

Address	Port
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4
71:2B:13:45:61:42	2
64:2B:13:45:61:12	3

Gradual building of Table



Switching

- Connectionless: No handshaking between sender and receiver

- Unreliable: Does not provide any means for recovering lost frames
  - If application needs reliability, it needs to employ TCP

Switching Algorithm

- If a frame received at bridge for destination D on port p
  - No entry for D in the table, forward on all ports except port p
  - If entry for D in forwarding table corresponds to p, drop frame
  - If entry for D in forwarding table corresponds to I != p, then forward on i

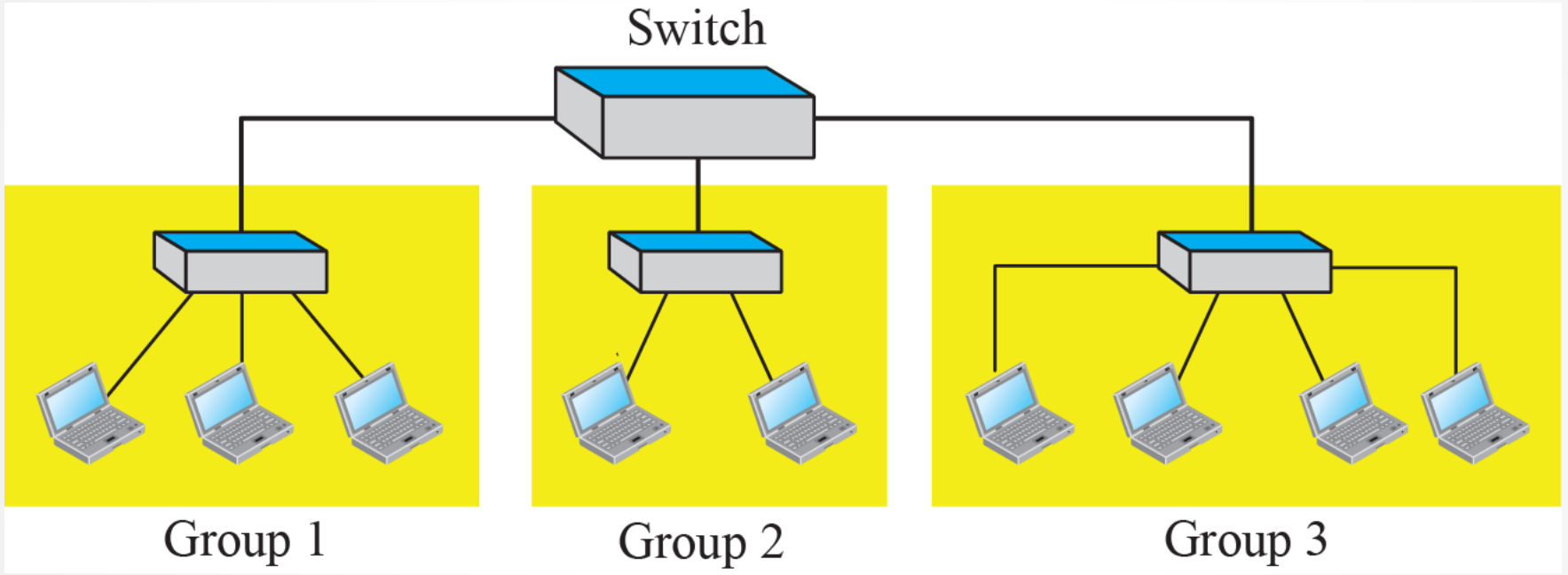
Virtual LANs (VLAN)

- A station is considered part of a LAN if it physically belongs to that LAN.

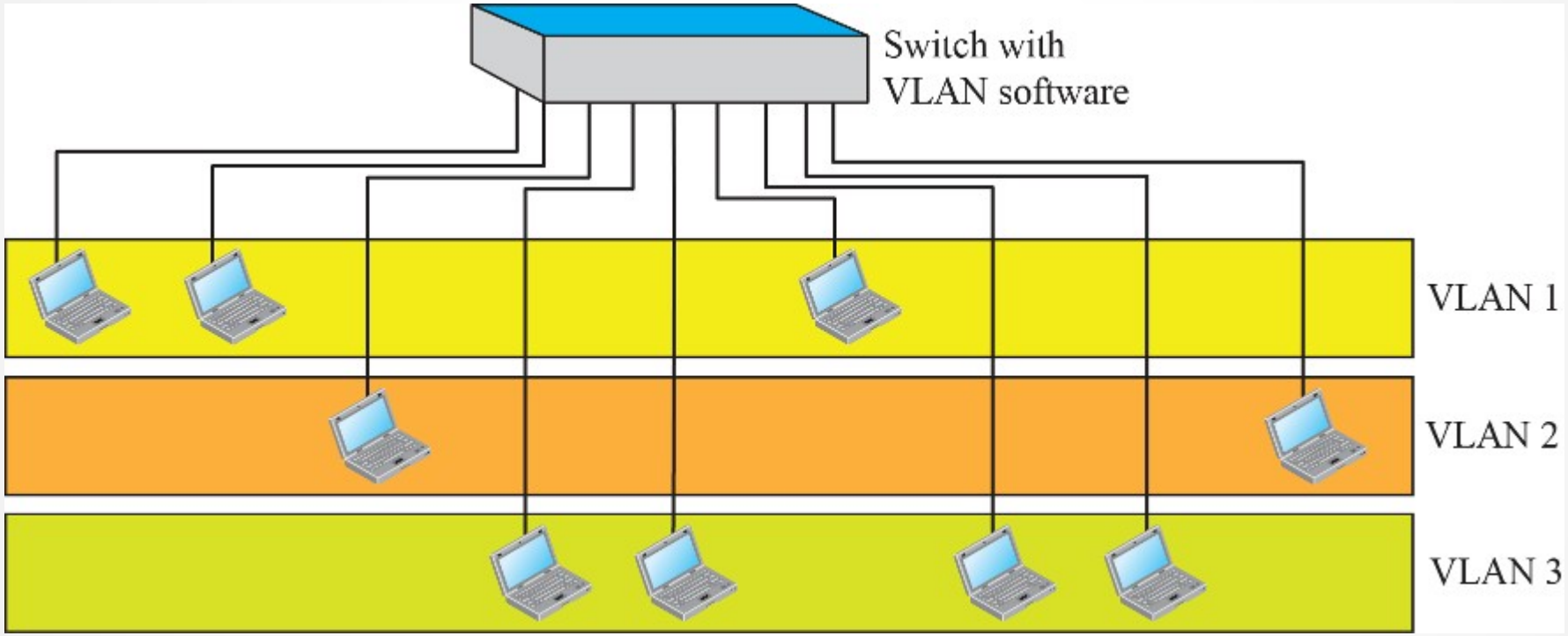
- What happens if we need a virtual connection between two stations belonging to two different physical LANs?

- We can roughly define a virtual local area network (VLAN) as a local area network configured by software, not by physical wiring.

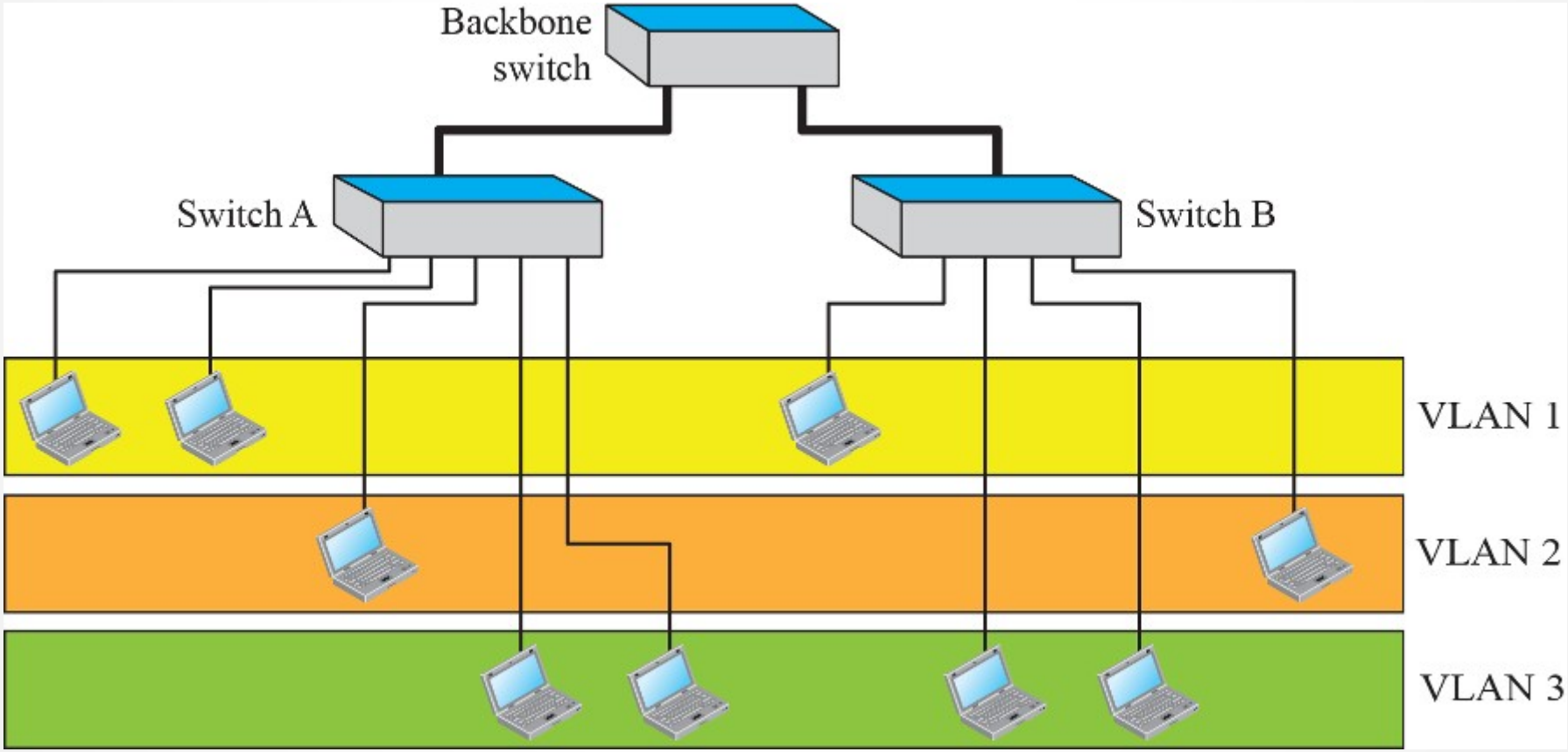
switch connecting multiple LANs



switch using VLAN software



Two switches in a backbone using VLAN software

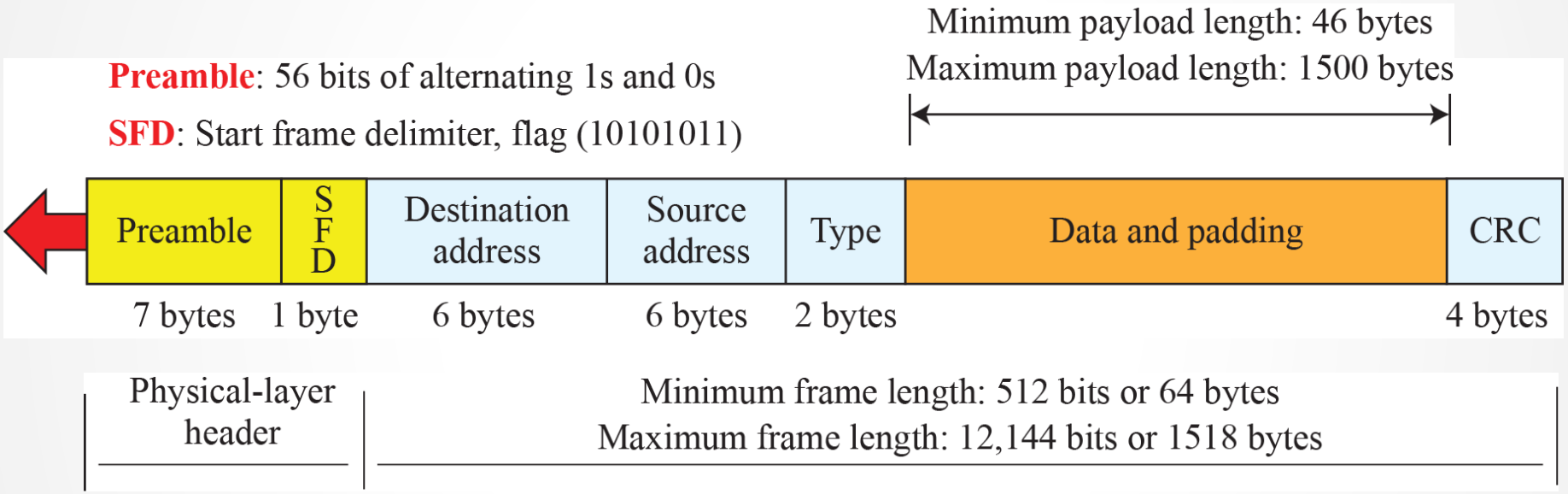


Ethernet Service

- Connectionless: No handshaking between sender and receiver

- Unreliable: Does not provide any means for recovering lost frames
  - If application needs reliability, it needs to employ TCP

Ethernet Frame Structure



Ethernet Frame Structure

- Preamble: Sequence of alternating 1's and 0's for synchronization
  - 10BaseT: Manchester encoding
- SFD: 10101011 (start frame delimiter)
- Source and Destination addresses: 48 bit MAC Address
- Type: Demultiplexing key – specifies which higher layer protocol the packet is intended
- Data: IP payload
  - Minimum 46 bytes and up to 1500 bytes
- CRC: Error Detection
- Inter Frame Gap: 96 bits (12 bytes)

Ethernet Address

- Unique address belonging to the adaptor
  - Each manufacturer allocated different prefix
  - E.g. Intel: C4-85-08 (C4-85-08-30-33-48)

- In normal mode, an adaptor passes up frames if
  - Addressed to it (Unicast)
  - Broadcast address (all 1’s)

Wireless Link Characteristics

- decreased signal strength: radio signal attenuates as it propagates through matter (path loss)
- interference from other sources: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone)
- multipath propagation: radio signal reflects off objects ground, arriving destination at slightly different times

Collision detection is easy in wired networks but difficult in wireless medium.

IEEE 802.11: multiple access

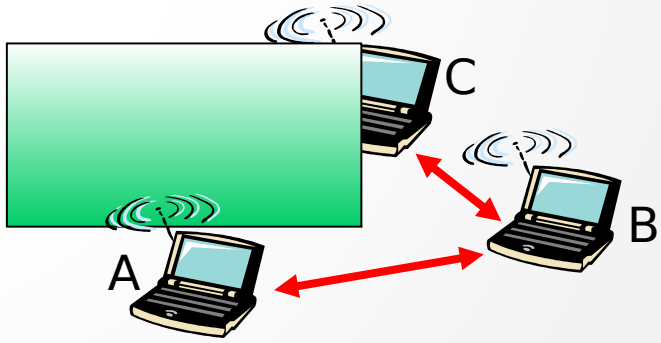
- avoid collisions: 2^+ nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
  - – don’t collide with ongoing transmission by other node
- 802.11: *no* collision detection!
  - – difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - – can’t sense all collisions in any case: hidden terminal, fading
  - – goal: *avoid collisions:* CSMA/C(ollision)A(voidance)

CSMA problems in wireless medium

- CSMA gives rise to hidden terminal and exposed terminal problems.

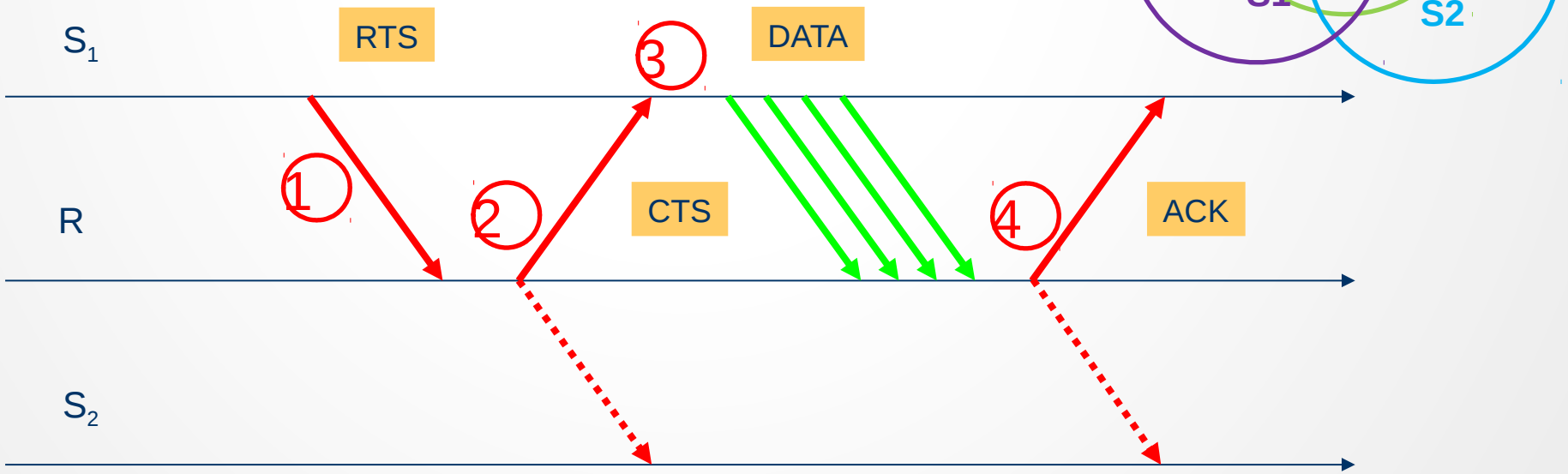
hidden terminal problem:
Other senders' information are hidden from the current sender, so that transmissions at the same receiver cause collisions.

- B, A hear each other
- B, C hear each other
- A, C can not hear each other means A, C unaware of their interference at B



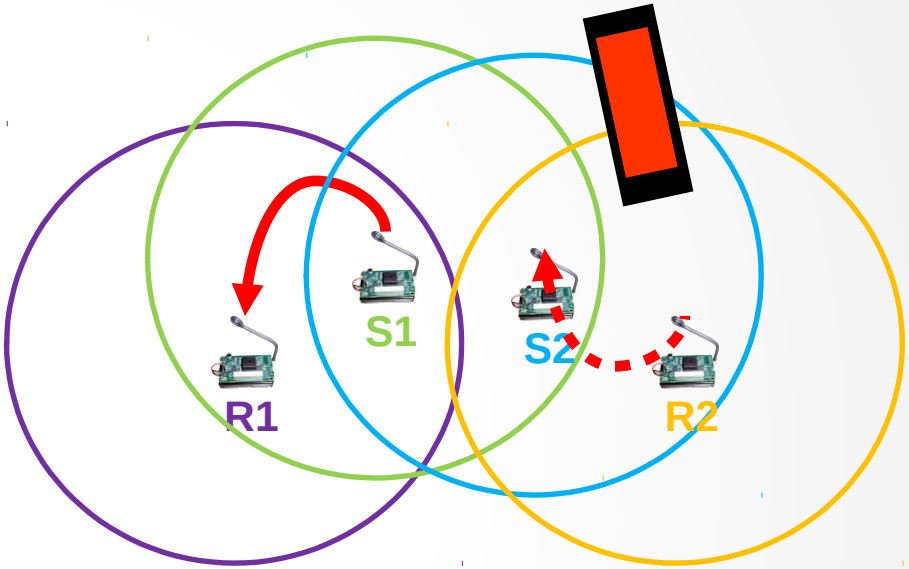
Resolving hidden terminal problem

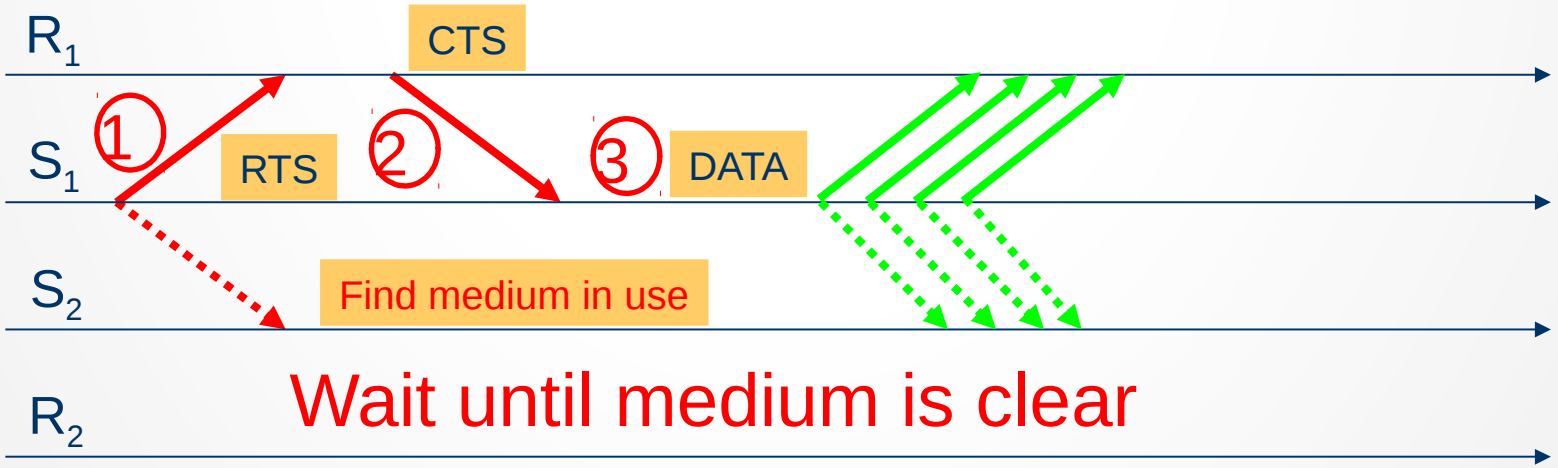
- Use of additional signaling packets.
  - Sender asks receiver whether it is able to receive a transmission - ***Request to Send (RTS)***
  - Receiver agrees, sends out a ***Clear to Send (CTS)***
  - Sender sends, receiver **Acknowledgements (ACKs)**



Exposed terminal problem

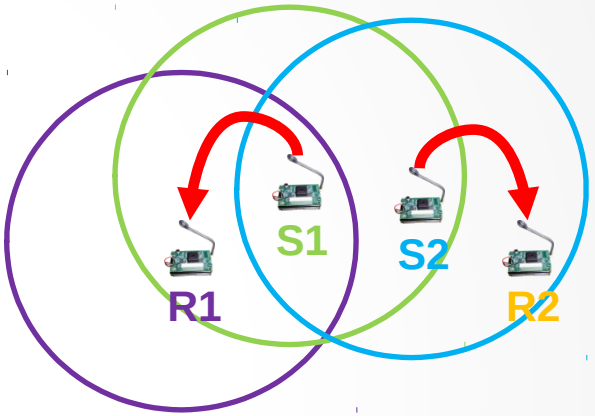
- The sender mistakenly think the medium is in use, so that it unnecessarily defers the transmission.

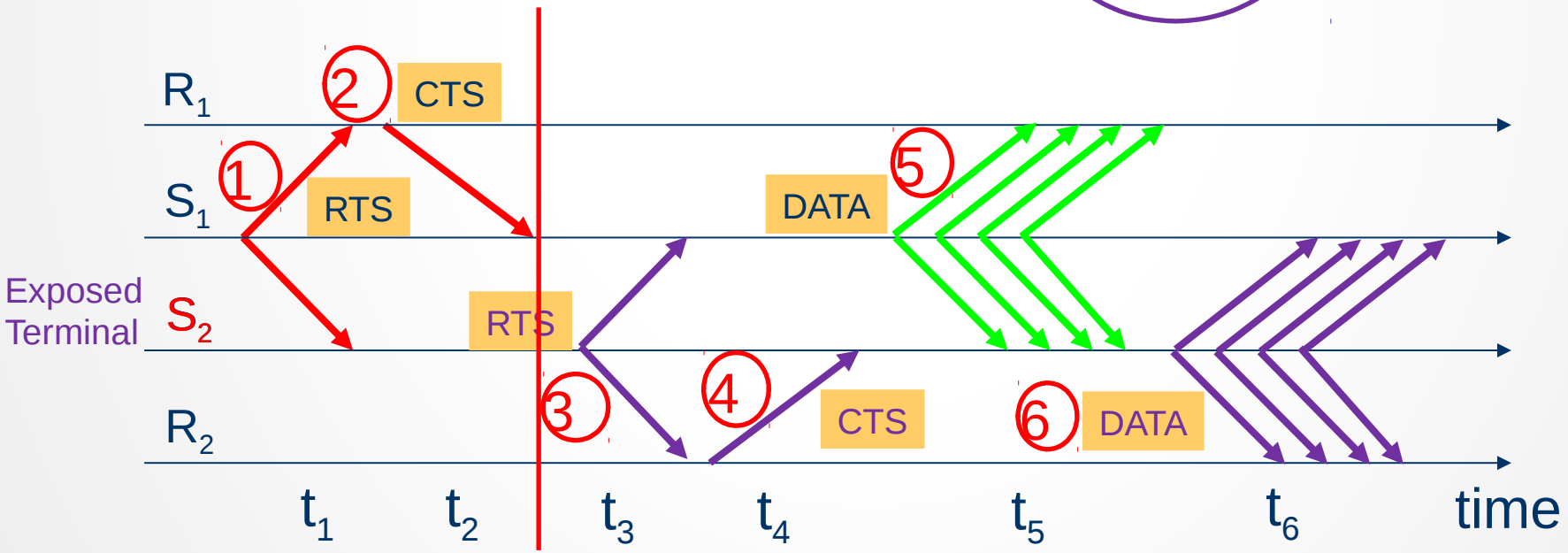




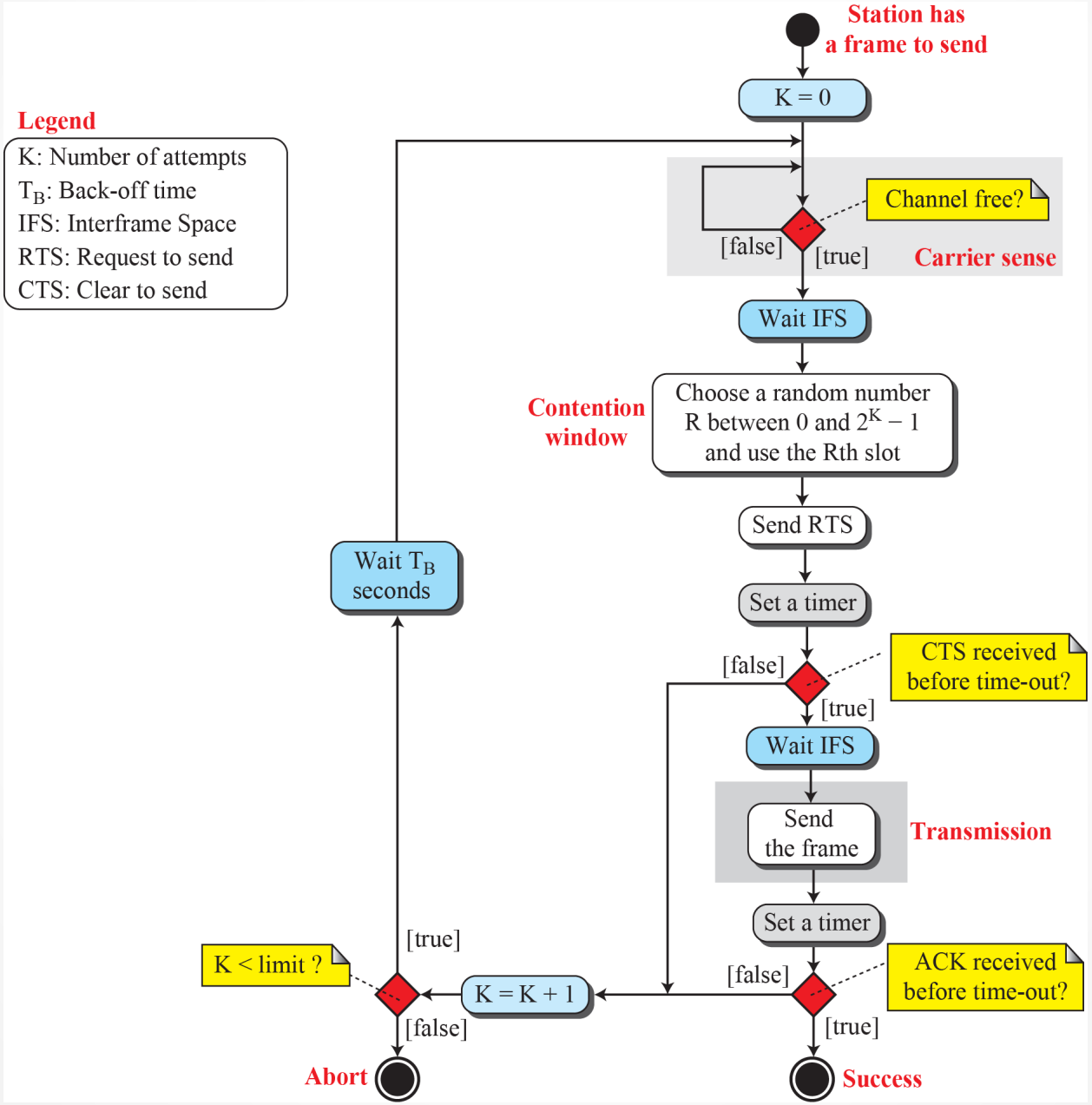
Resolving exposed terminal problem

- When a node hears an RTS from a neighboring node, but not the corresponding CTS, that node can deduce that it is an *exposed terminal* and is permitted to transmit to other neighboring nodes.

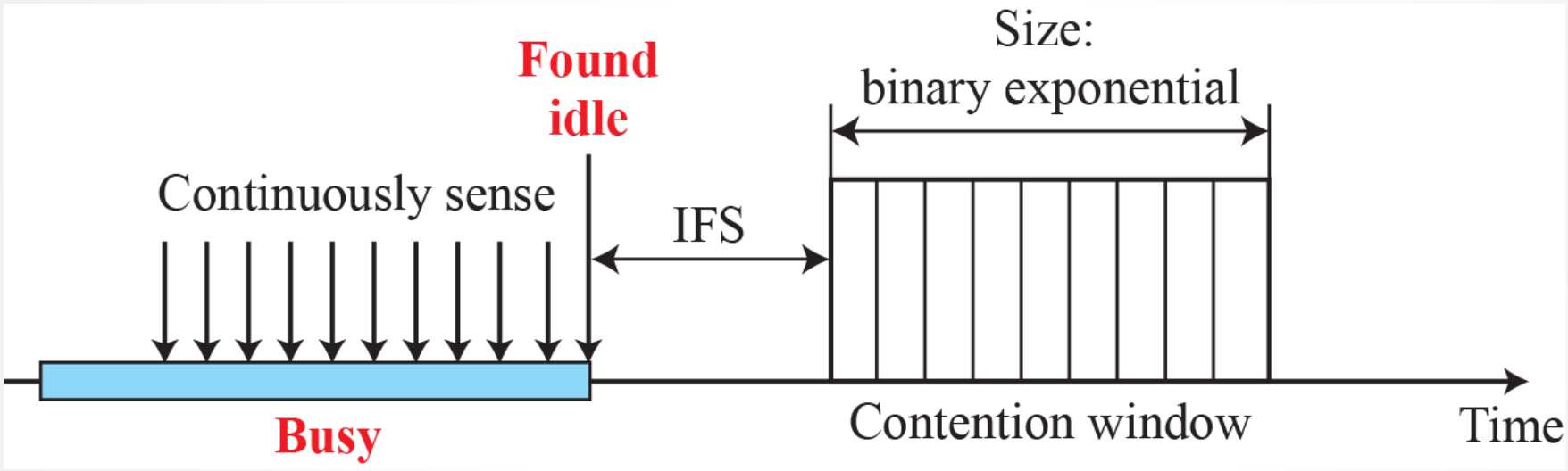




Flow of CSMA/CA



Contention window of CSMA/CA



Contention window of CSMA/CA