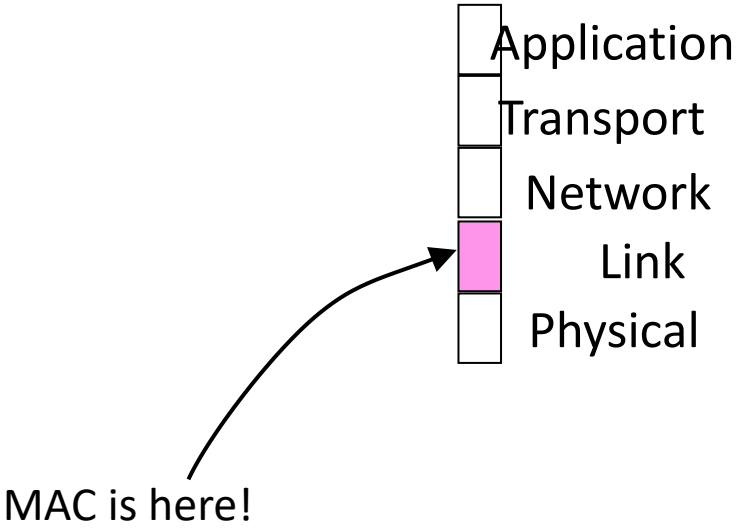


Computer Networks

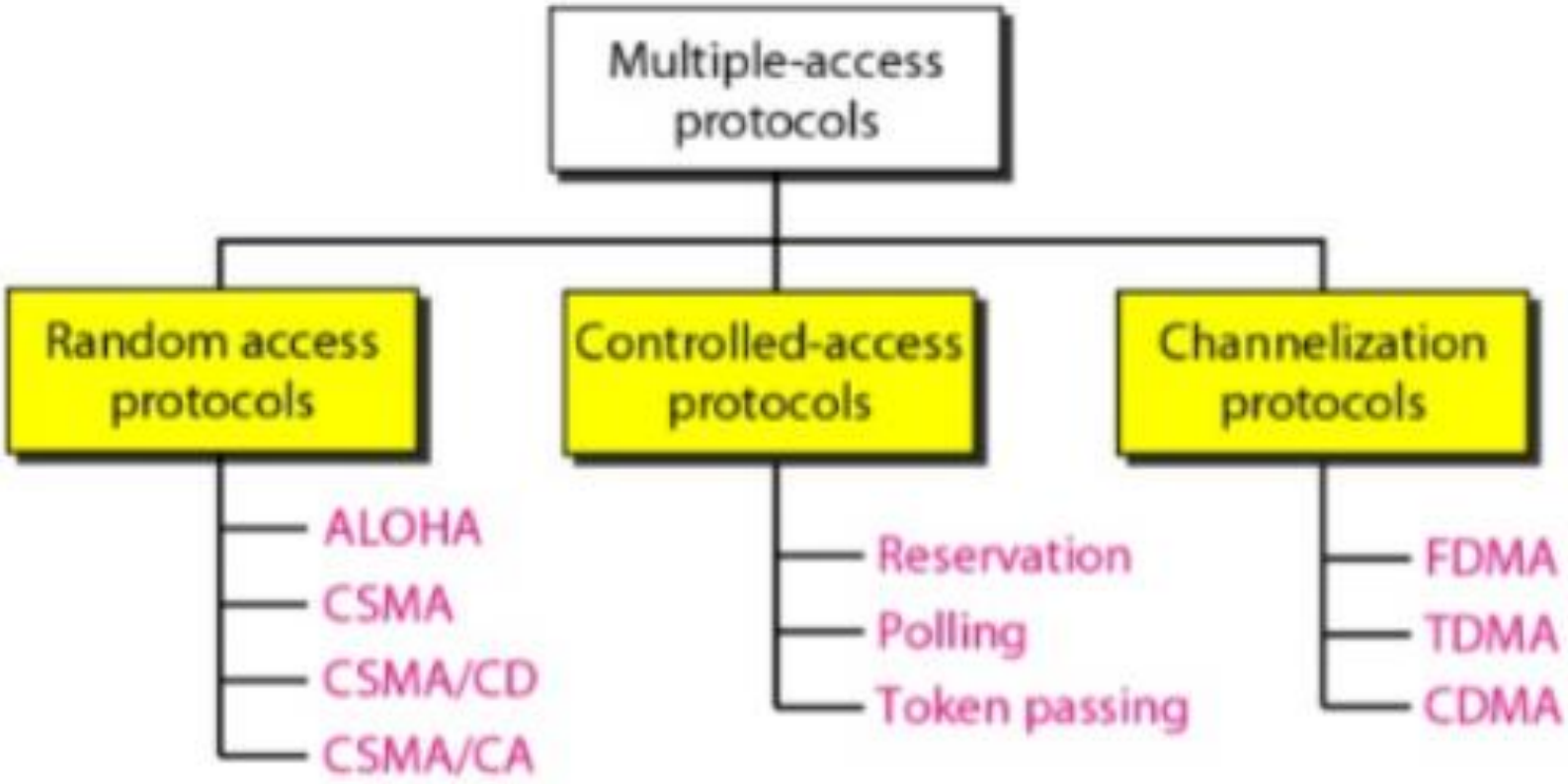
Medium Access Control

Dr. Ajay,
Department of CSE
SRM University-AP

Overview

- In broadcast networks (Multi-access/random-access channels)
  - The key issue is how to determine who gets to use the channel when there is competition for it.
  - MAC=Protocol to determine who goes next on channel.
  - It's important for LANs (Bus topology, WiFi), WANs are point-to-point.

- How to allocate a single broadcast channel among competing users ??
- Can be done using :
  - Static Channel Allocation.
    - FDM and TDM.
  - Dynamic Channel Allocation.
    - ALOHA and Carrier Sense Protocols.


Multiple-access protocols
Random access protocols
Controlled-access protocols
Channelization protocols
ALOHA
CSMA
CSMA/CD
CSMA/CA
Reservation
Polling
Token passing
FDMA
TDMA
CDMA

Static Channel Allocation (FDMA)

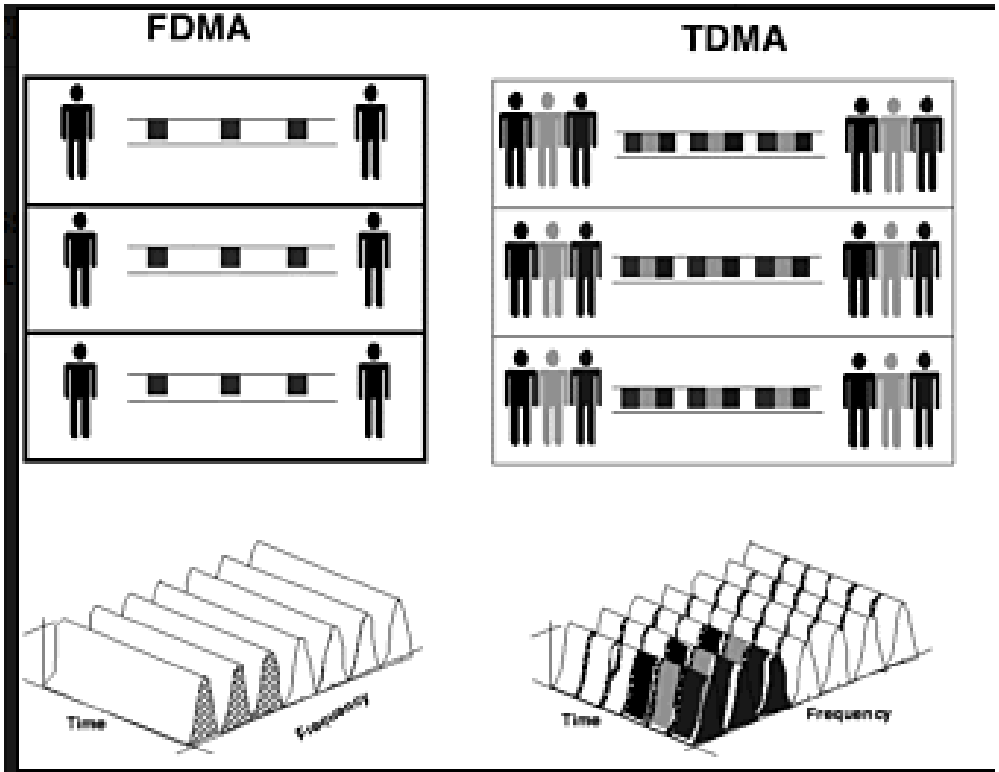
- Let's say N users exist:
  - the available bandwidth is divided into N equal-sized portions.
  - Each user is assigned to one portion (1/N).
  - Since each user has a private frequency band
    - *there is no interference among users.*
    - Example : Wireless FM radio channels (Each station gets a portion of the FM band and uses it most of the time to broadcast its signal.)

- Static channel allocation is efficient when :
  - Number of users are less than available channels.
  - Data transmission should have steady stream.

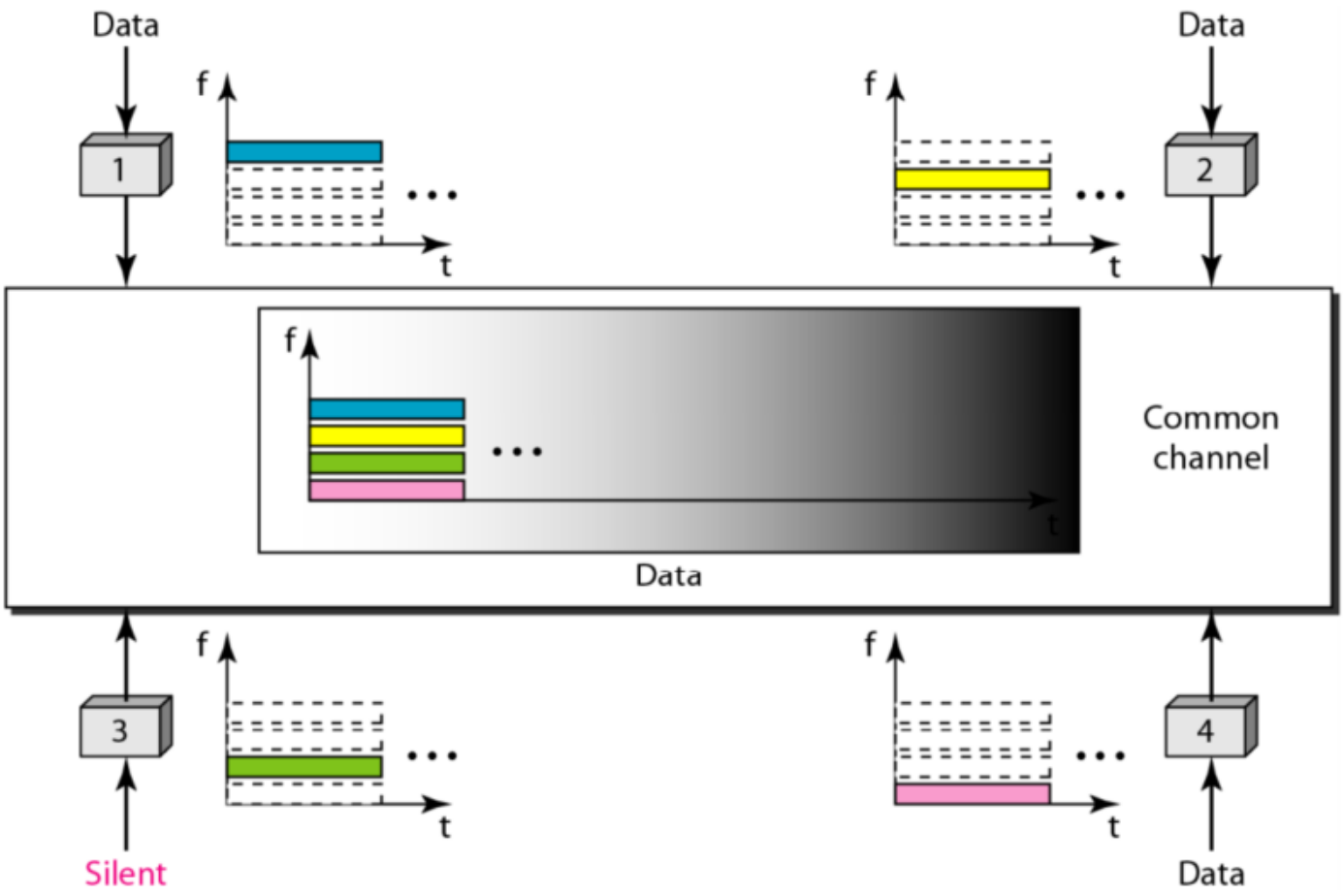
- Inefficient to divide into fixed number of chunks.
  - May not all be used, or may need more.
  - Doesn't handle burst traffics of computer systems.

Static Channel Allocation(TDMA)

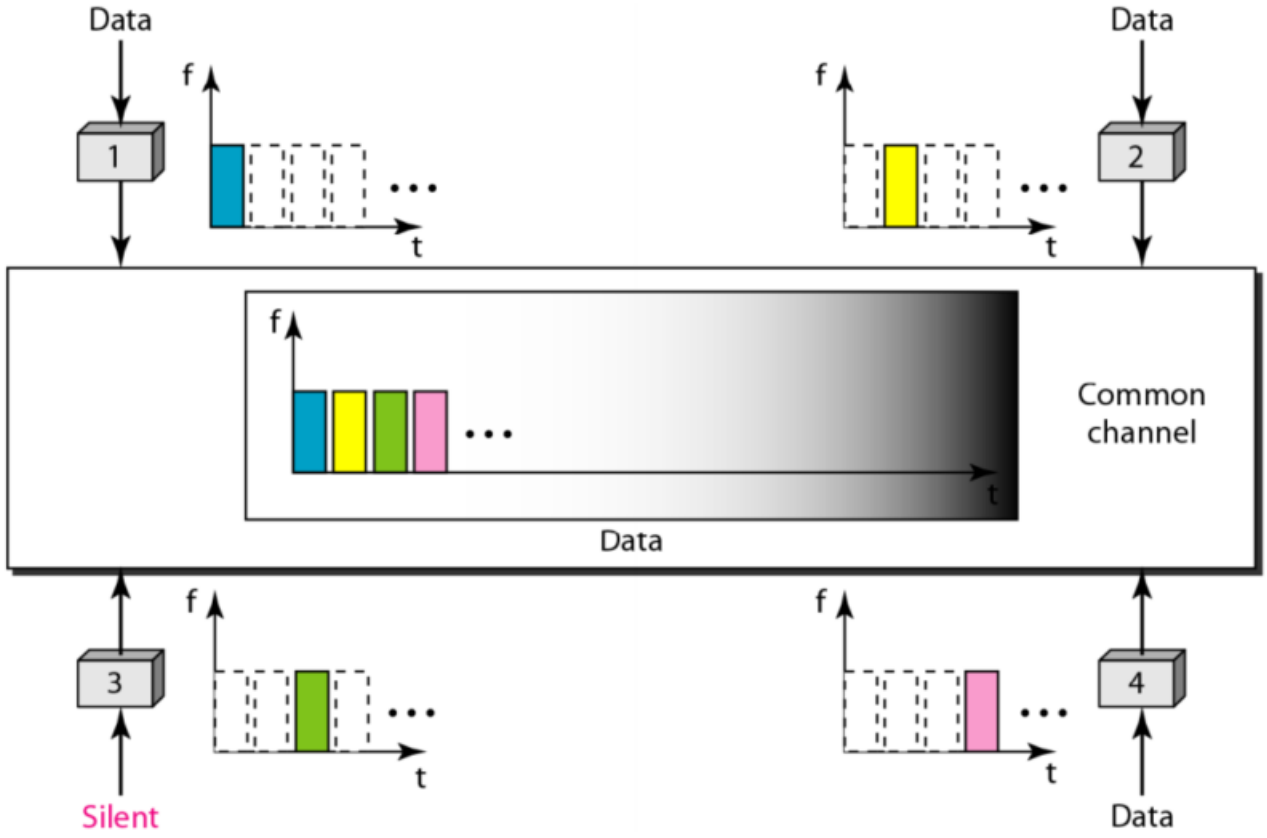
- In a time slot only 1 user transmits (or receives).
- Several users share a single frequency channel.
- Transmission is non-continuous.
- Power consumption is lower than FDMA (e.g., the transmitter can be turned off when idle)
- Synchronization is needed



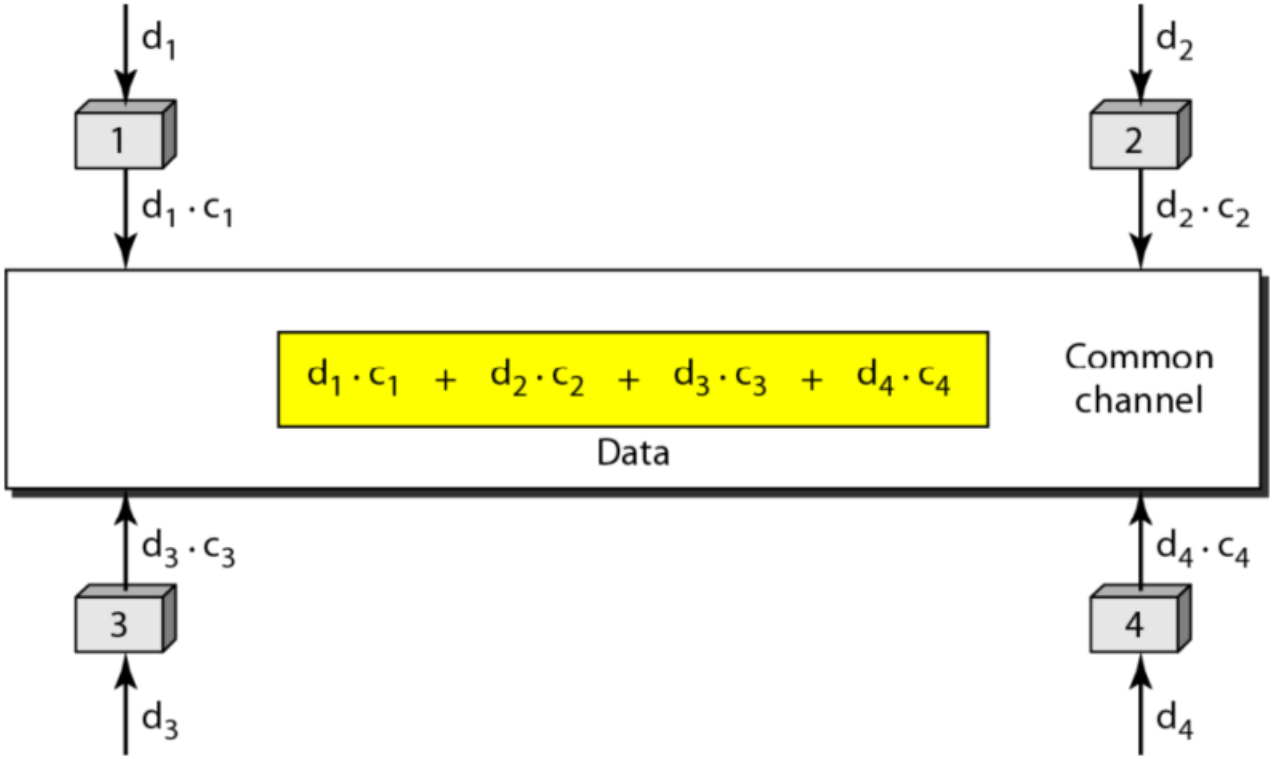
Frequency-division multiple access (FDMA)



TDMA



CDMA


d_1
1
$d_1 \cdot c_1$
d_2
2
$d_2 \cdot c_2$
$d_1 \cdot c_1 + d_2 \cdot c_2 + d_3 \cdot c_3 + d_4 \cdot c_4$
Data
Common channel
$d_3 \cdot c_3$
3
d_3
$d_4 \cdot c_4$
4
d_4

Dynamic channel allocation

- Assumptions:
  - **Station Model:** Assumes that each of N "stations" (packet generators, **Terminal**) independently produce frames. The station generates no new frame until that previous one is transmitted.
  - **Single Channel Assumption:** There's only one channel; all stations are equivalent and can send and receive on that channel.
  - **Collision Assumption:** If two frames overlap in any way time-wise, then that's a **collision**. Any collision is an error, and both frames must be retransmitted. Collisions are the only possible error.
  - **Continuous/ Slotted Time:** Time is not in discrete chunks. Frame transmission can begin at any instant. Alternatively, in slotted, frame transmissions always begin at the start of a time slot. Any station can transmit in any slot (with a possible collision.)
  - **Carrier/No-Carrier Sense:** Stations can tell a channel is busy before they try it. NOTE - this doesn't stop collisions.

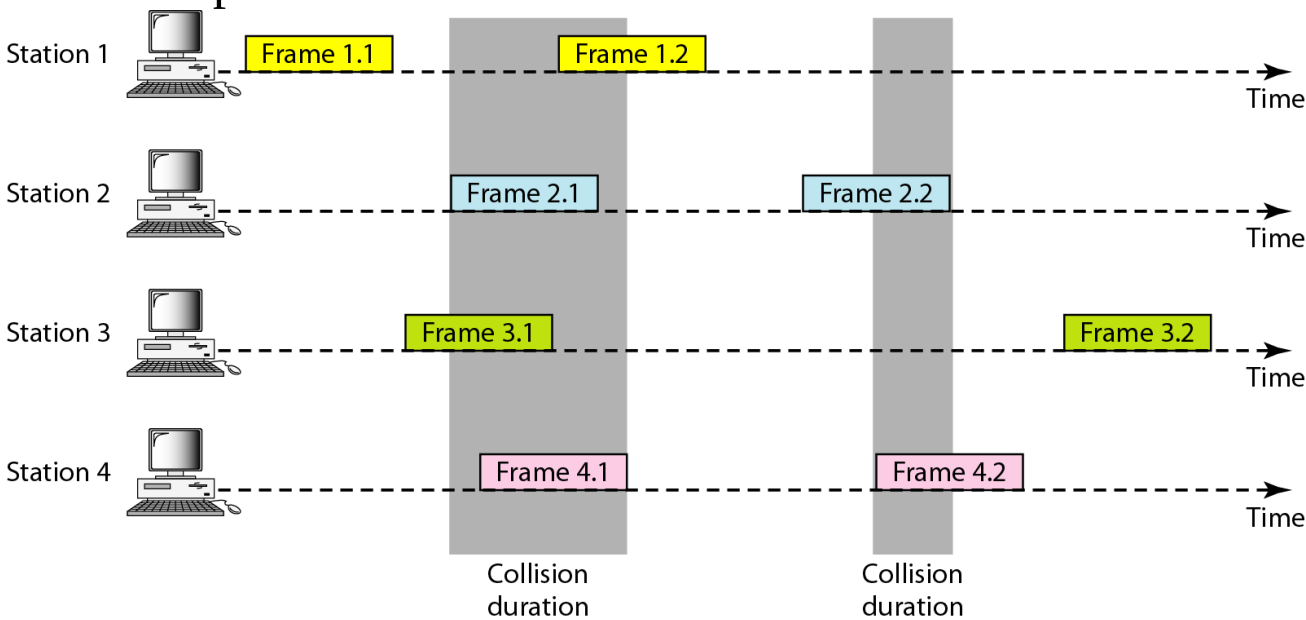
Multiple Access Protocols: ALOHA

ALOHA

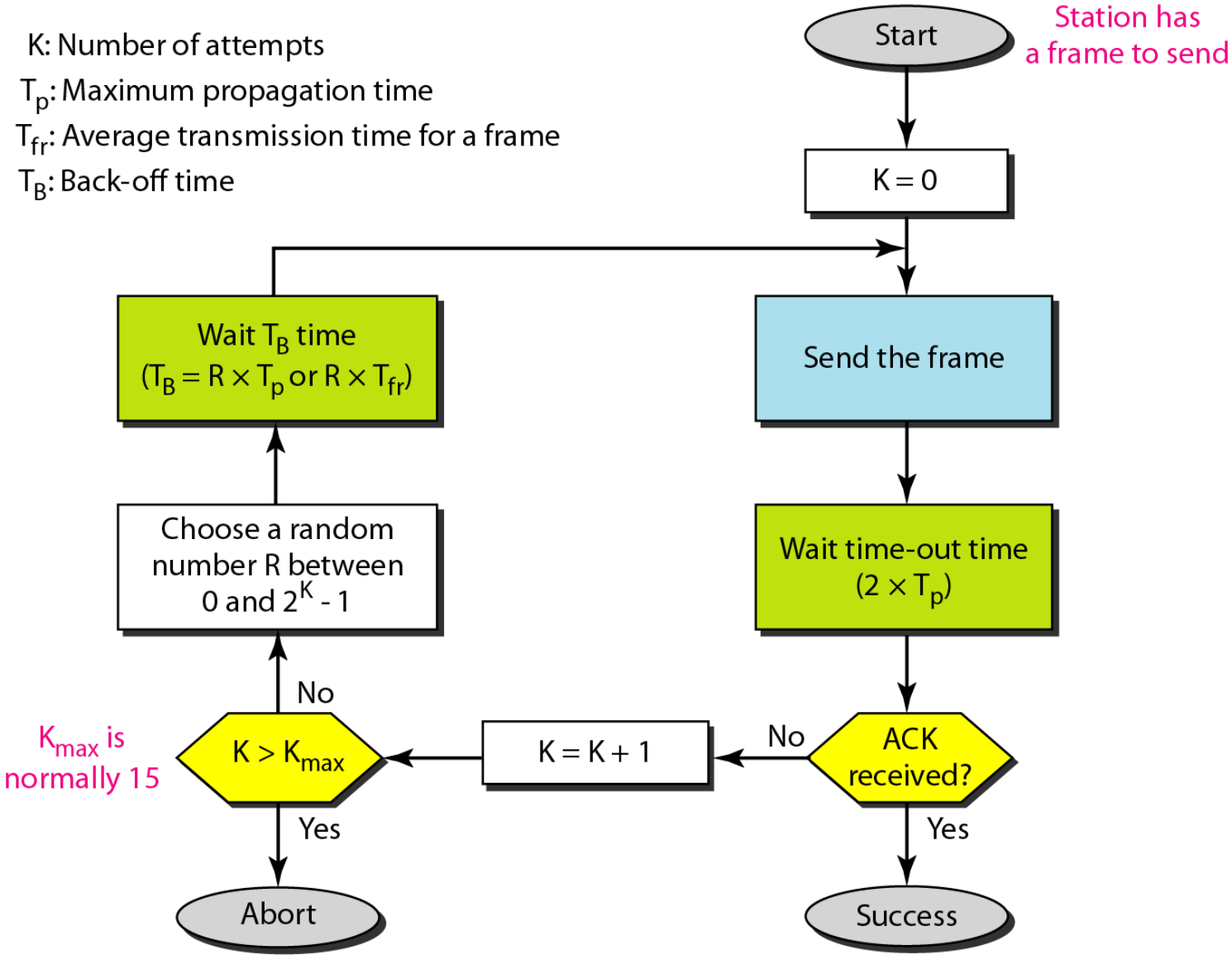
- Developed in Hawaii in the 1970s.

❶ PURE ALOHA:

- Every station transmits whenever it wants to.
- Colliding frames are destroyed. The sender knows if its frame got destroyed using feedback property, and if so waits a random time and then retransmits.
- ANY overlap is a collision.
- Best efficiency if frames are same size.
- A **contention system**: Multiple users share a common channel that can lead to conflict.



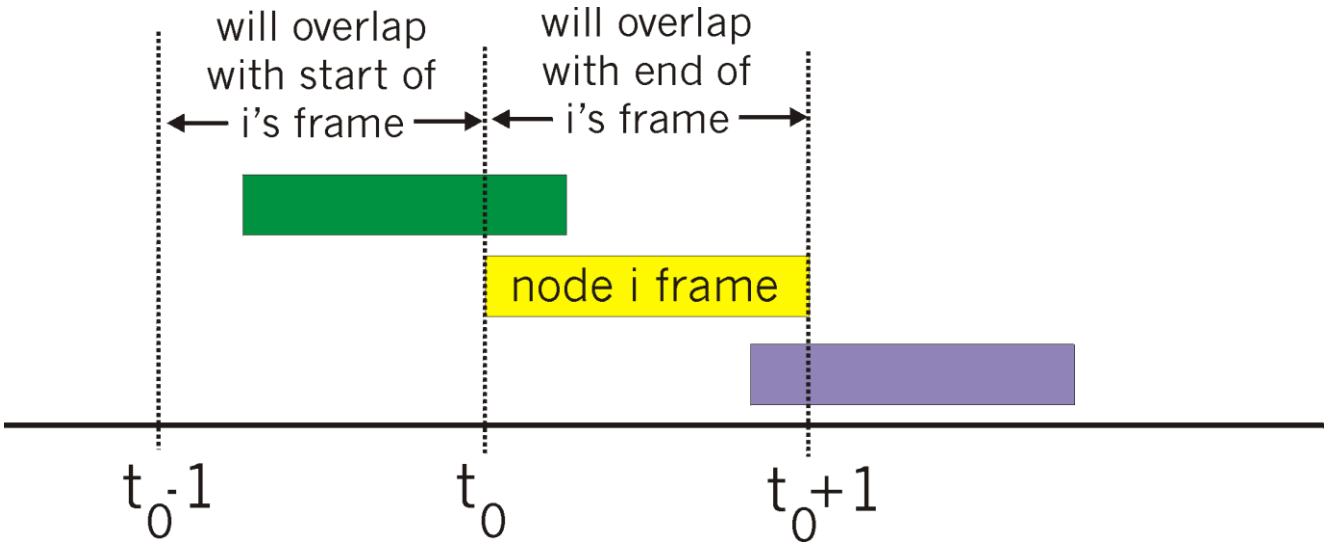
Pure Aloha(2)


K: Number of attempts
T_p: Maximum propagation time
T_{fr}: Average transmission time for a frame
T_B: Back-off time
Start
Station has a frame to send
K = 0
Send the frame
Wait time-out time ($2 \times T_p$)
ACK received?
No
Yes
K = K + 1
$K > K_{max}$
No
Yes
K_{max} is normally 15
Choose a random number R between 0 and $2^K - 1$
Wait T_B time ($T_B = R \times T_p$ or $R \times T_{fr}$)
Success
Abort

Multiple Access Protocols: ALOHA

ALOHA : Performance

- collision probability increases:
- pkt sent at t_0 collide with other pkts sent in $[t_0-1, t_0+1]$



P(success by given node) = P(node transmits) ·
P(no other node transmits in $[t_0-1,t_0]$ ·
P(no other node transmits in $[t_0,t_0+1]$

- Very inefficient : Maximum achievable Throughput (18%)

- The probability of having k arrivals during a time interval of length t is given by:

$$P_k(t) = \frac{(\lambda t)^k e^{-\lambda t}}{k!}$$

- where λ is the arrival rate.

- The vulnerable time for a successful transmission is $2T_f$
i.e. collision probability increases

- So, the probability of good transmission is not to have an "arrival" during the vulnerable time .

$$P_k(t) = \frac{(\lambda t)^k e^{-\lambda t}}{k!}$$

- And setting $t = 2T_f$ and $k = 0$, we get,

$$P_0(2T_f) = \frac{(\lambda \cdot 2T_f)^0 e^{-\lambda 2T_f}}{0!} = e^{-2G}$$

$$\text{becasue } \lambda = \frac{G}{T_f}. \quad \text{Thus, } S = G \cdot e^{-2G}$$

Transmission time of frame is T_t
G is number of host want to transmits in T_t

The probability of K frames are generated in frame time Tt as per the poison distribution is

P(K) = G^K e(-G) / K! = f(G,K)

A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the requirement to make this frame collision-free?

Solution

Average frame transmission time T_{fr} is 200 bits/200 kbps or 1 ms. The vulnerable time is 2×1 ms = 2 ms. This means no station should send later than 1 ms before this station starts transmission and no station should start sending during the one 1-ms period that this station is sending.

A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces

a. 1000 frames per second b. 500 frames per second

c. 250 frames per second.

Solution

The frame transmission time is 200/200 kbps or 1 ms.

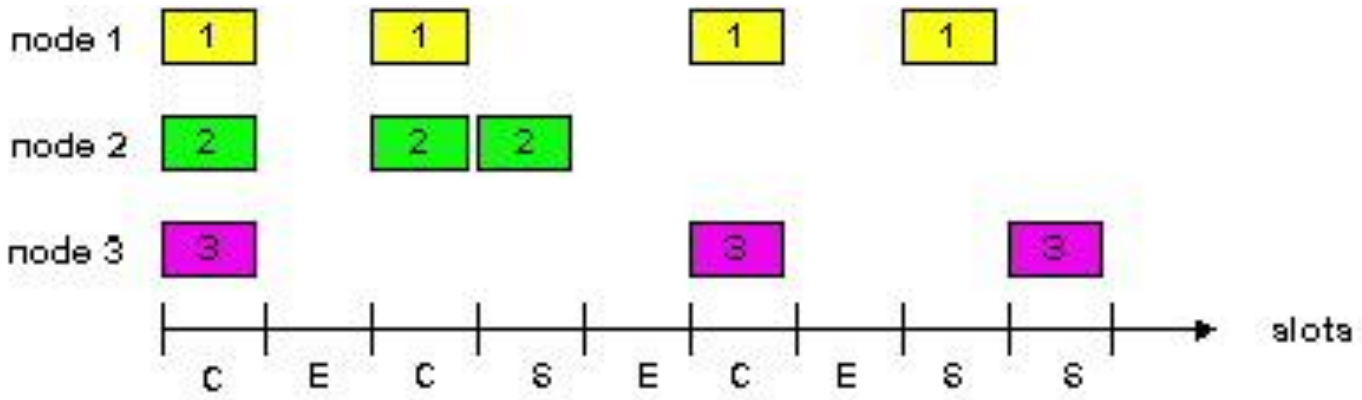
a. If the system creates 1000 frames per second, this is 1 frame per millisecond. The load is 1. In this case $S = G \times e^{-2G}$ *or* $S = 0.135$ *(13.5 percent). This means that the throughput is* $1000 \times 0.135 = 135$ *frames. Only 135 frames out of 1000 will probably survive.*

b. *If the system creates 500 frames per second, this is (1/2) frame per millisecond. The load is (1/2). In this case* $S = G \times e^{-2G}$ *or* $S = 0.184$ *(18.4 percent). This means that the throughput is* $500 \times 0.184 = 92$ *and that only 92 frames out of 500 will probably survive. Note that this is the maximum throughput case, percentagewise.*

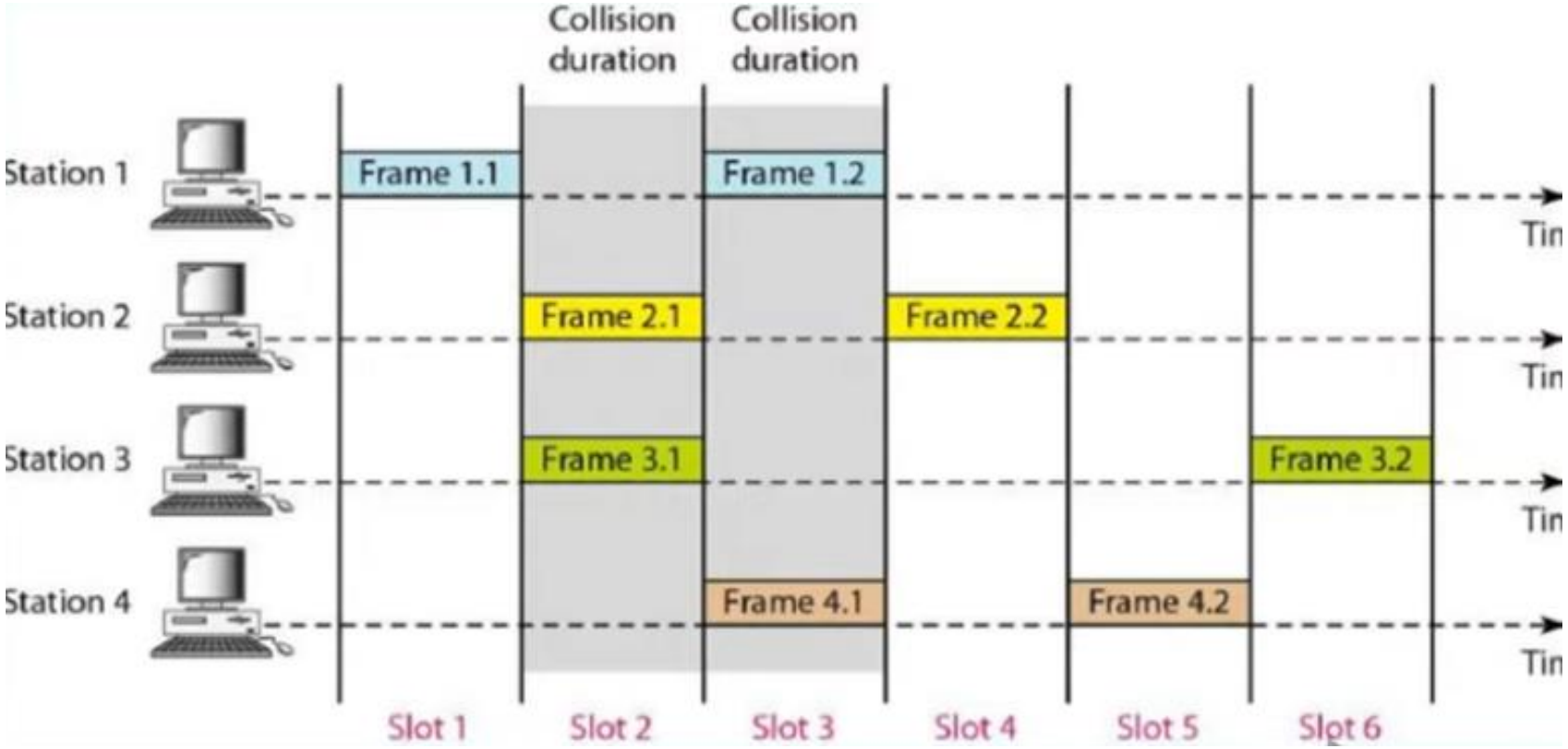
c. *If the system creates 250 frames per second, this is (1/4) frame per millisecond. The load is (1/4). In this case* $S = G \times e^{-2G}$ *or* $S = 0.152$ *(15.2 percent). This means that the throughput is* $250 \times 0.152 = 38$. *Only 38 frames out of 250 will probably survive.*

Slotted Aloha

- Time is divided into equal size slots (= packet trans. time)
- Node with new packet: transmit at beginning of next slot.
- If collision: retransmit packet in future slots with probability p, until successful.



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


Collision duration
Collision duration
Station 1
Station 2
Station 3
Station 4
Frame 1.1
Frame 1.2
Frame 2.1
Frame 2.2
Frame 3.1
Frame 3.2
Frame 4.1
Frame 4.2
Slot 1
Slot 2
Slot 3
Slot 4
Slot 5
Slot 6

Note that the vulnerable period is now reduced in half.

Hence,

$$P_k(t) = \frac{(\lambda t)^k e^{-\lambda t}}{k!}$$

And putting $t = \mathrm{T}_f$ and $k = 0$, we get

$$P_0(T_f) = \frac{(\lambda \cdot T_f)^0 e^{-\lambda T_f}}{0!} = e^{-G}$$

because $\lambda = \frac{G}{T_f}$. Thus, $S = G \cdot e^{-G}$

Throughput of Slotted ALOHA

- The probability of no collision is given by

$$P(0) = e^{-G}$$

- The throughput S is

$$S = G \cdot P(0) = G \cdot e^{-G}$$

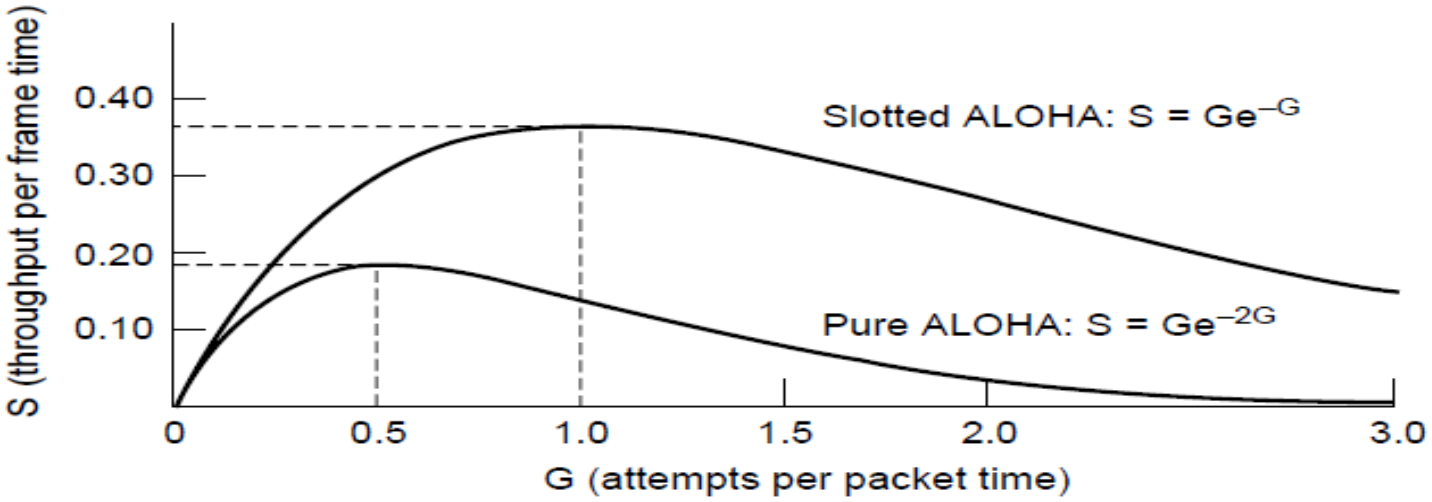
- The Maximum throughput of slotted ALOHA is

$$S_{\max} = \frac{1}{e} \approx 0.368$$

Slotted ALOHA

Slotted ALOHA is twice as efficient as pure ALOHA

- Low load wastes slots, high loads causes collisions
- Efficiency up to 37% (almost twice to PURE ALOHA)



Comparison of the channel utilization versus load for various random access protocols.

Carrier Sense Multiple Access Protocols

- CSMA protocol was developed to overcome :
  - the problem in pure ALOHA and slotted ALOHA.
  - i.e. to minimize the chances of collision.

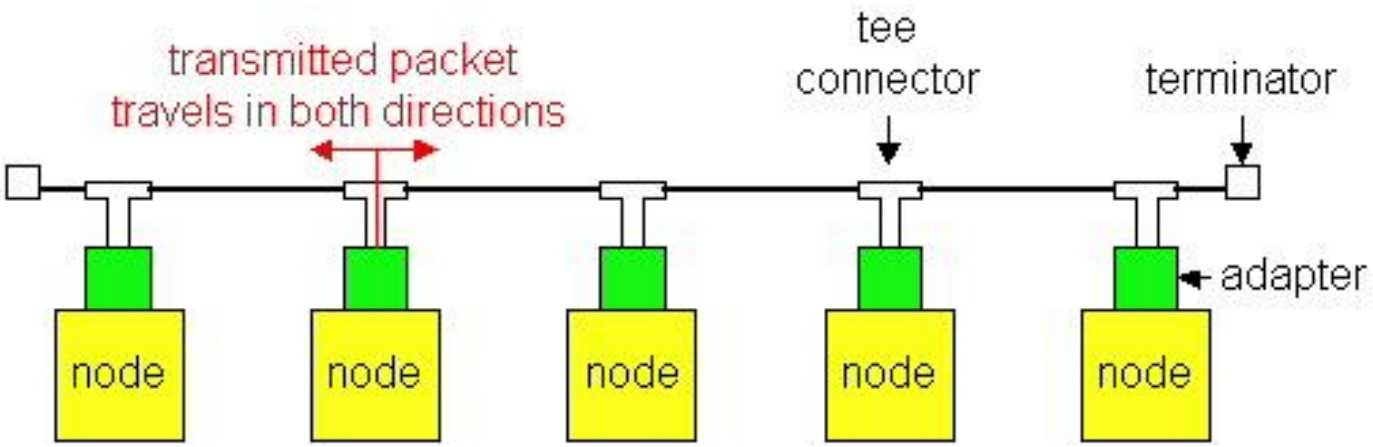
- CSMA protocol is based on the principle of ‘carrier sense’. ("sense before transmit" or "listen before talk).
- Carrier Sense – the ability of a network interface card to sense or detect communication on the network.
- Multiple Access – states that in that network there are multiple stations that could access the network at the same time.

- The chances of collision can be reduce to great extent if a station senses the channel before trying to use it.

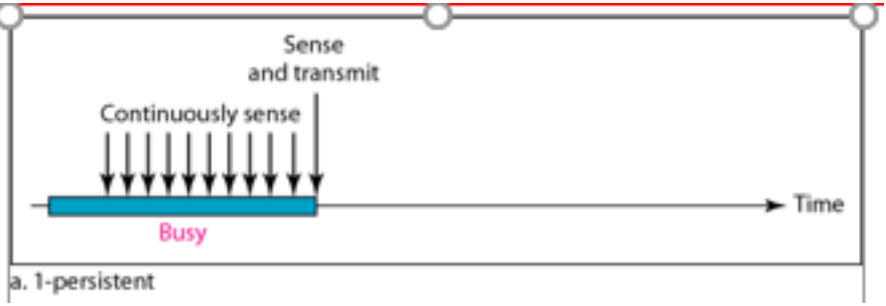
- Although CSMA can reduce the possibility of collision, but it cannot eliminate it completely.

Carrier Sense Multiple Access Protocols

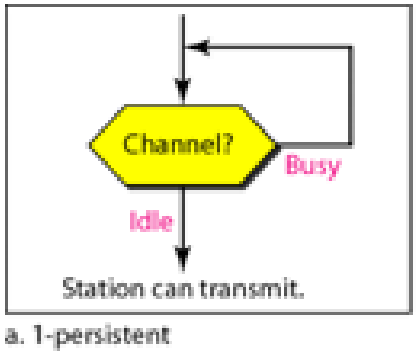
- There are three different types of CSMA protocols :-
  - (i) 1-Persistent CSMA
  - (ii) Non-Persistent CSMA
  - (iii) P-Persistent CSMA



1-Persistent CSMA

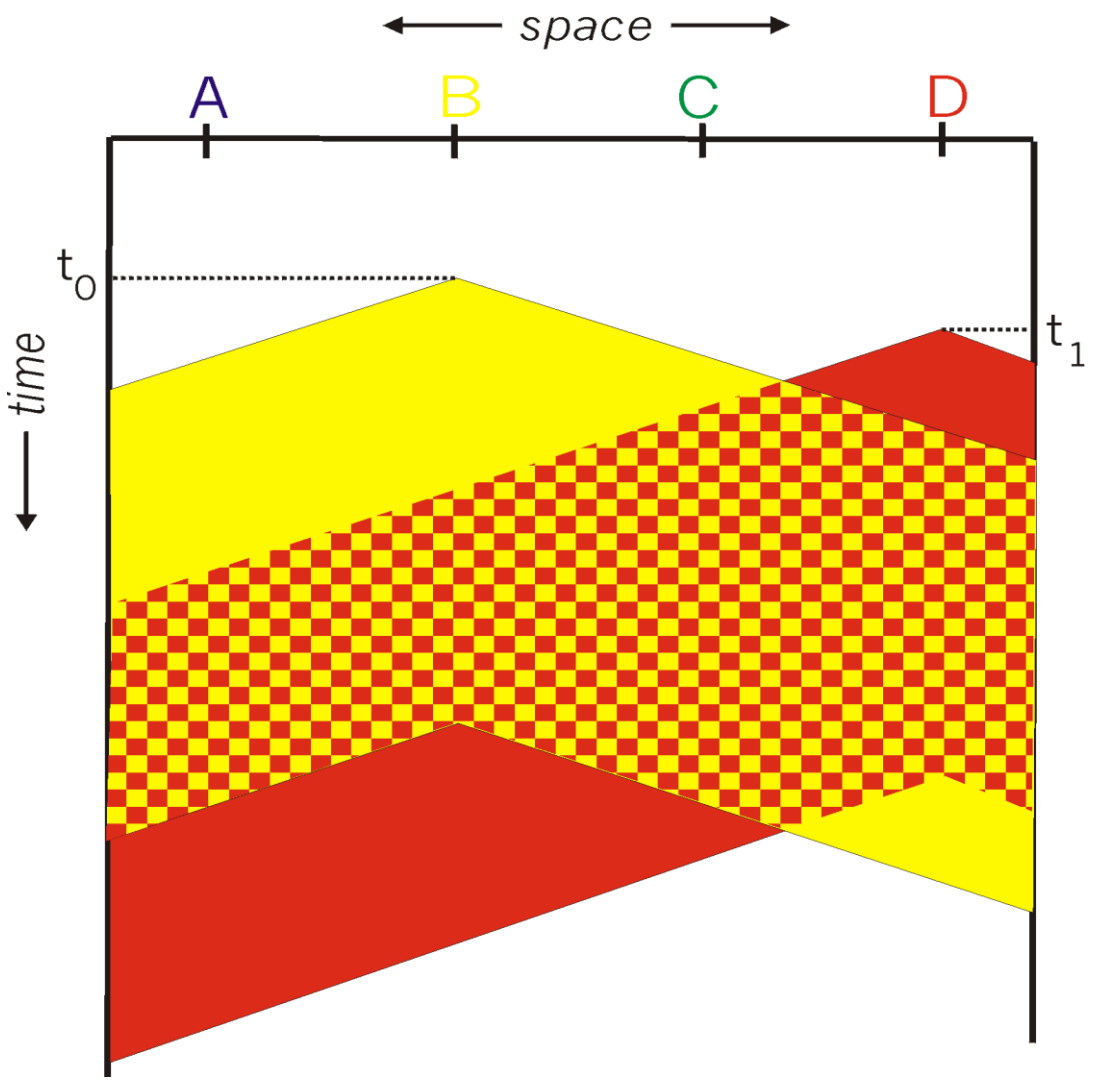


- When a station has data to send :
- it first listens(carrier sense) to the channel to see if anyone else is transmitting at that moment.
- If the channel is idle:
  - the stations sends its data(frame).
- If the channel is busy :
  - the station just waits until the channel becomes idle.
  - Later, the station start transmitting a frame.
- If a collision occurs :
  - the station waits a random amount of time and starts all over again.
- The protocol is called *1-persistent* because the station transmits with a probability of '1' when it finds the channel idle.



a. 1-persistent

CSMA collisions (Propagation delay)



1-Persistent CSMA

- Effect of propagation delay in CSMA :
- If a signal from station A has not reached to station B and station B is ready to send, it will sense the channel to be idle and send its frame.

- Collision can be there even when propagation delay is zero and carrier sense is also there.
  - If stations B and C become ready in the middle of A's transmission, B and C will wait until the end of A's transmission and then both will begin transmitted simultaneously, resulting in a collision.

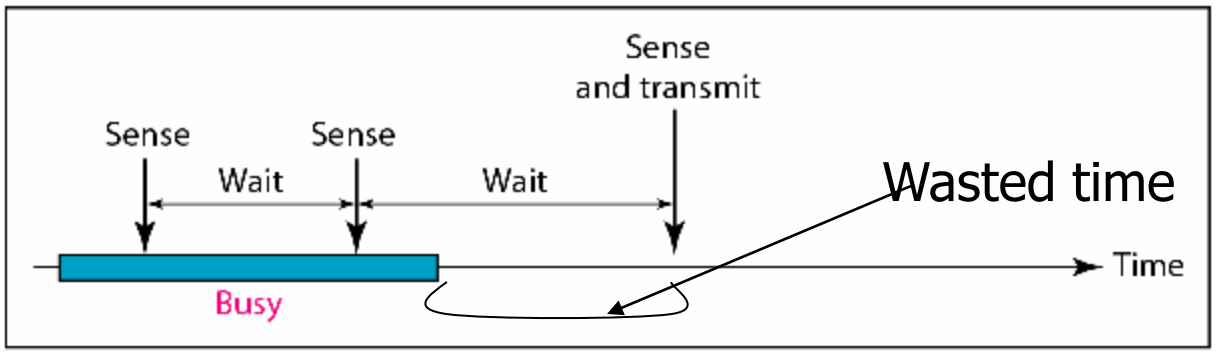
- If B and C were not so greedy, there would be fewer collisions.

Non-Persistent CSMA

- when a station is ready to send a frame , it senses the channel :
  - if busy : waits for random time rather than continuously sense it for the purpose of seizing it.
  - if idle : sends it.
  - if collision : waits for random time and tries again.

- Less greedy than 1-persistent, hence better channel utilization but *longer delays*.
- Reduced collision rate in comparison with 1-persistent CSMA.

Random Waiting times

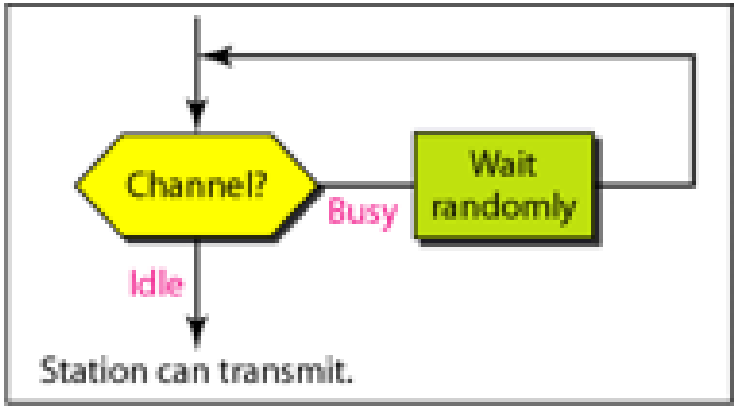


b. Nonpersistent

Non-Persistent CSMA

- Advantages of non-persistent CSMA:
  - Less greedy than 1-persistent.
  - It reduces the chances of collision because the stations wait a random amount of time before transmitting.

- Disadvantages of non-persistent CSMA:
  - Longer delays : This is due to the fact that the stations wait a random amount of time before transmitting.



b. Nonpersistent

P-Persistent CSMA

Time is divided into slots where each Time unit (slot) is typically equals to **maximum propagation delay**

Station wishing to transmit listens to the medium:

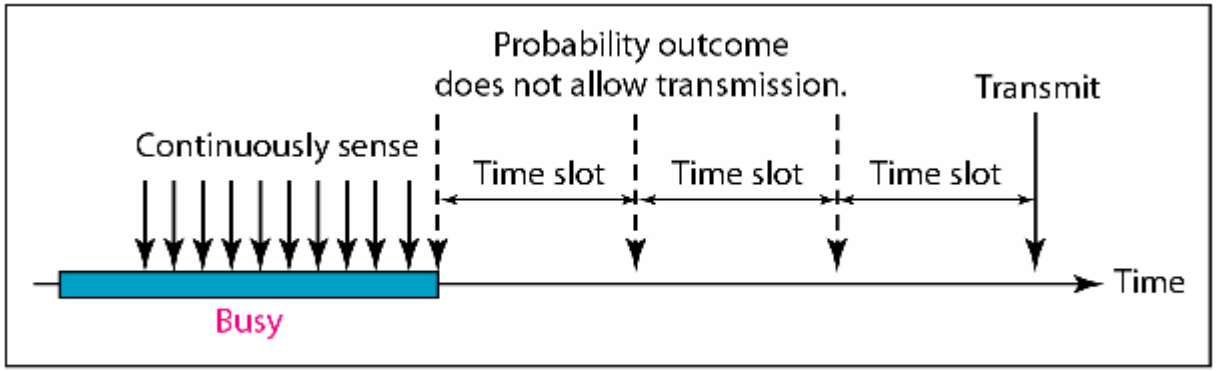
If medium idle,

- transmit the frame with probability (**p**), OR
- wait **one time unit (slot)** with probability (**1 – p**), then repeat 1.

If medium is busy, **continuously listen until idle** and repeat step **1**

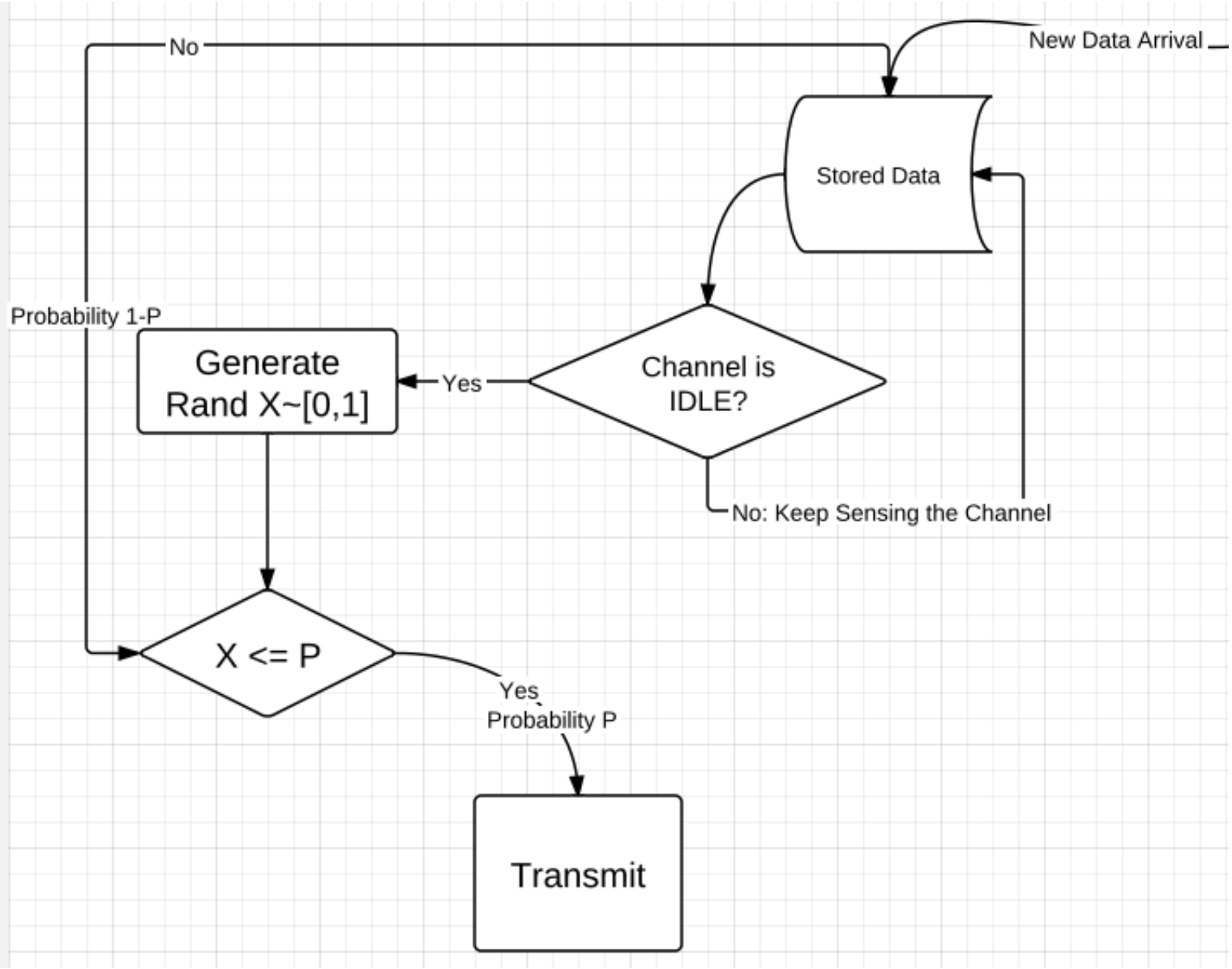
Performance :

- Reduces the possibility of collisions like **1-persistent.**
- Reduces channel idle time like **non-persistent**

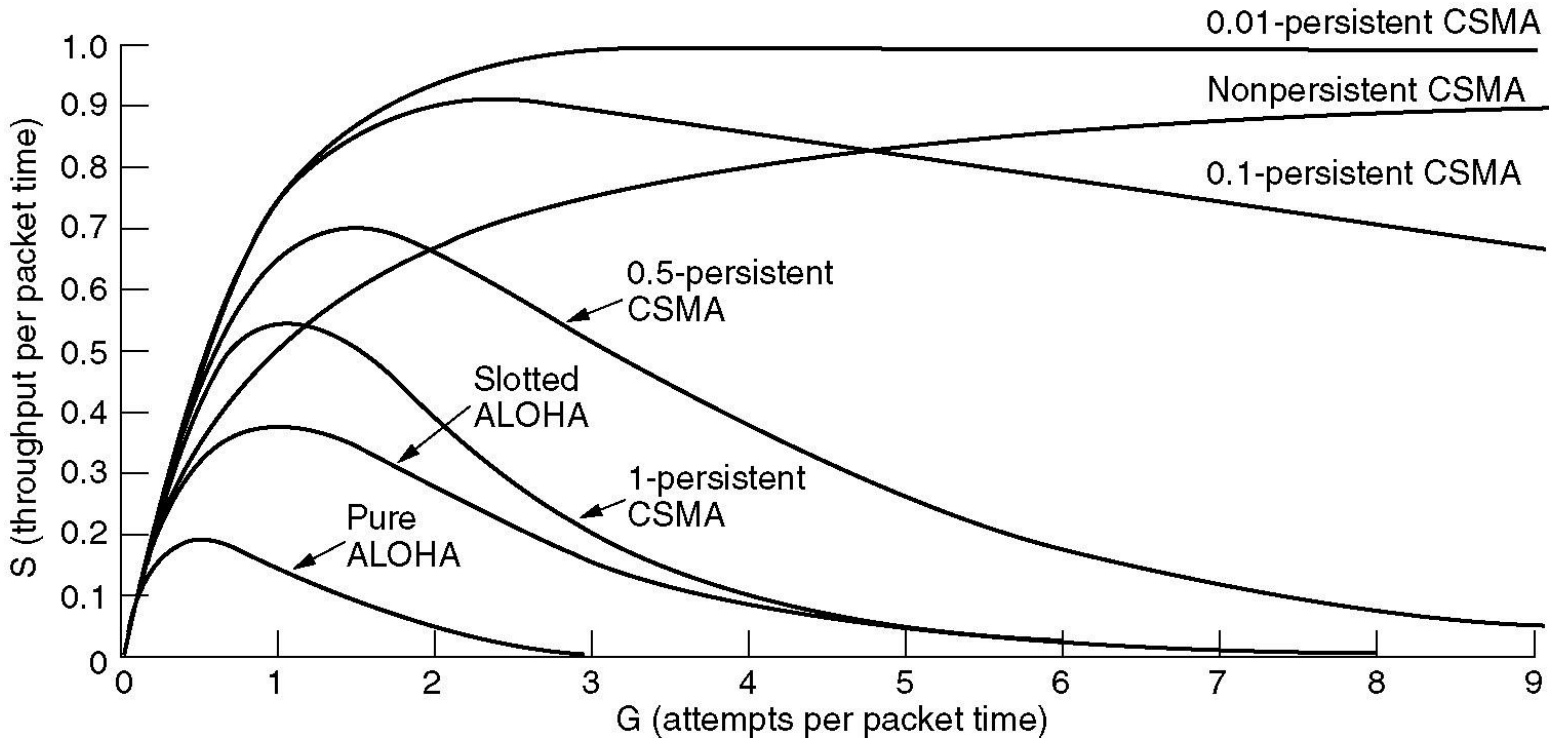


c. p-persistent

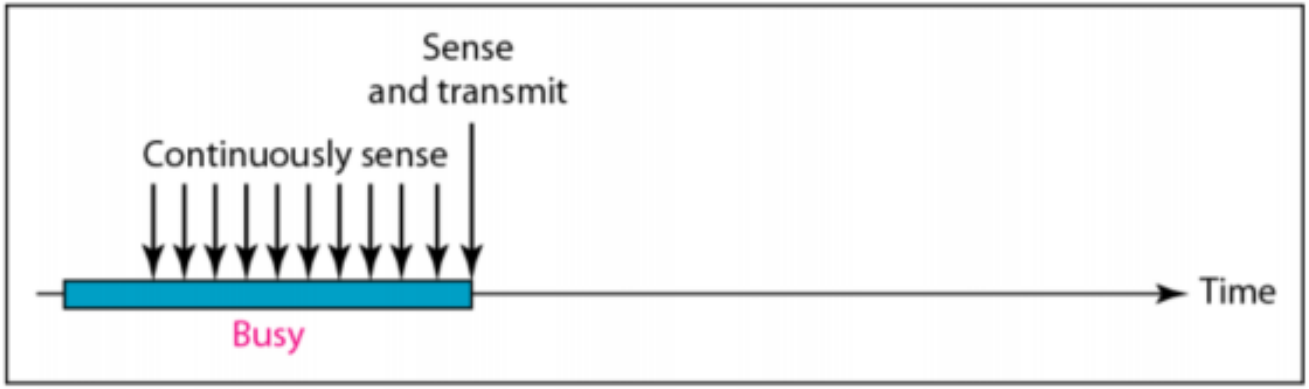
P-Persistent CSMA



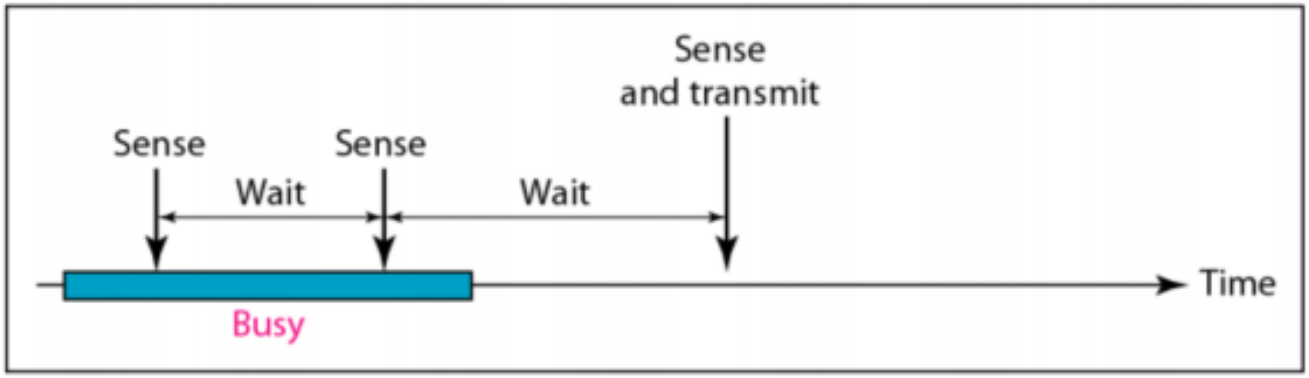
Persistent and Nonpersistent CSMA



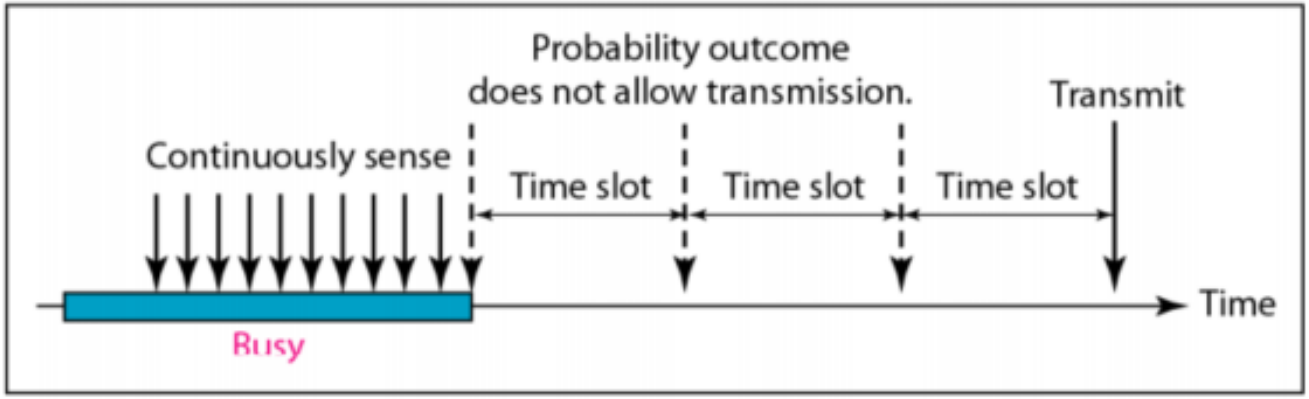
Comparison of the channel utilization versus load for various random access protocols.



a. 1-persistent

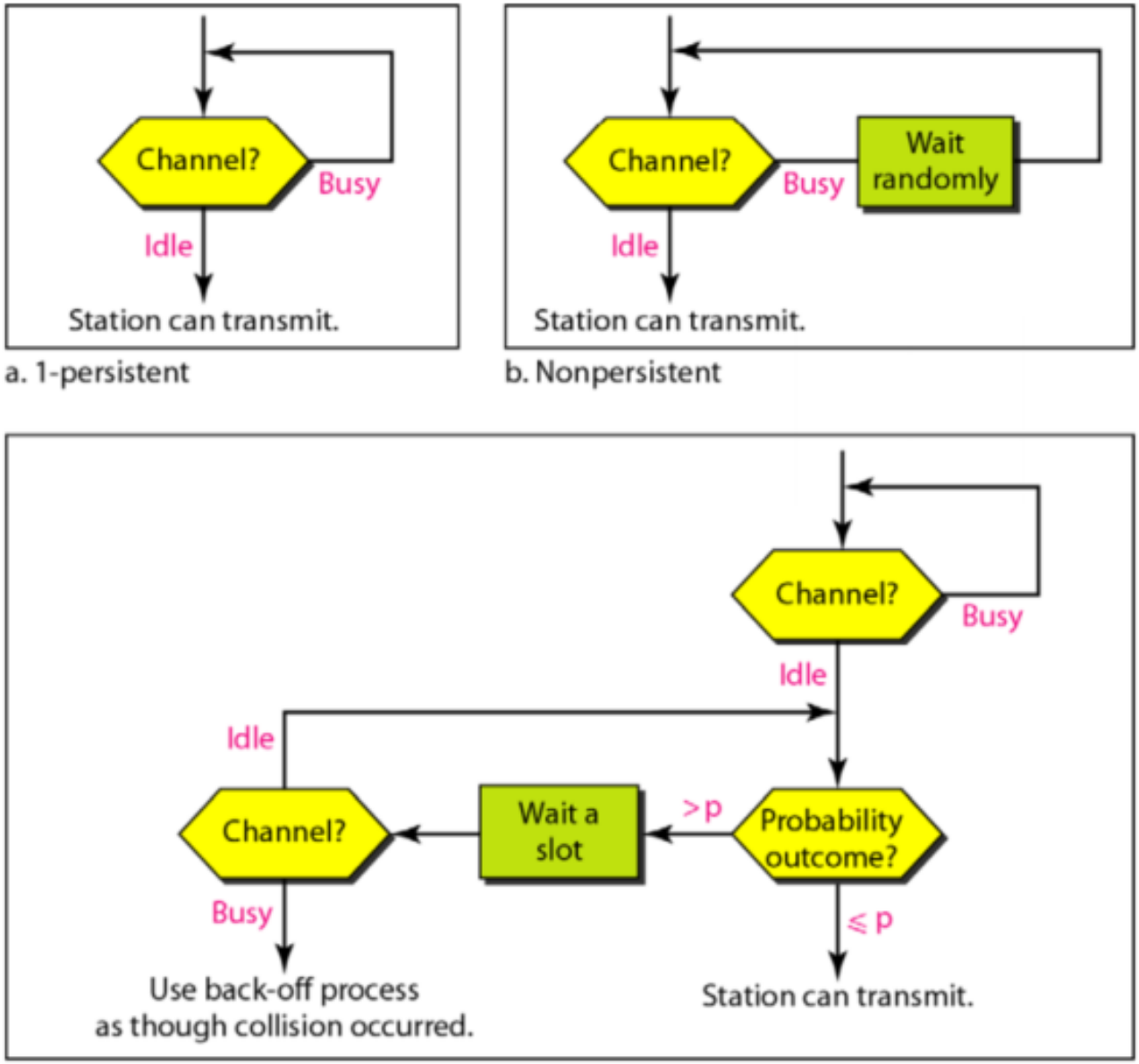


b. Nonpersistent



c. p-persistent

Flow-chart of three persistence methods



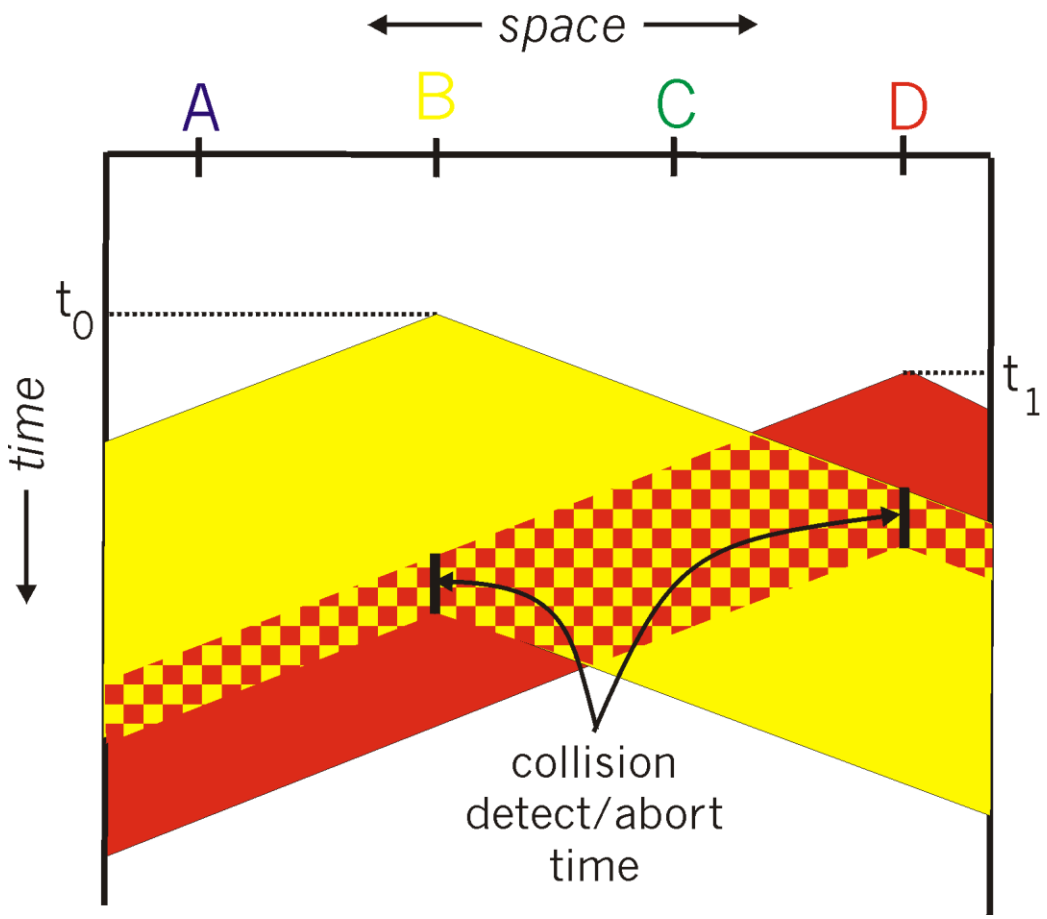
CSMA/CD

- CSMA with collision detection.
- Problem: when frames collide, medium is unusable for duration of both (damaged) frames.
- For long frames (when compared to propagation time), considerable waste.
- What if station listens while transmitting?

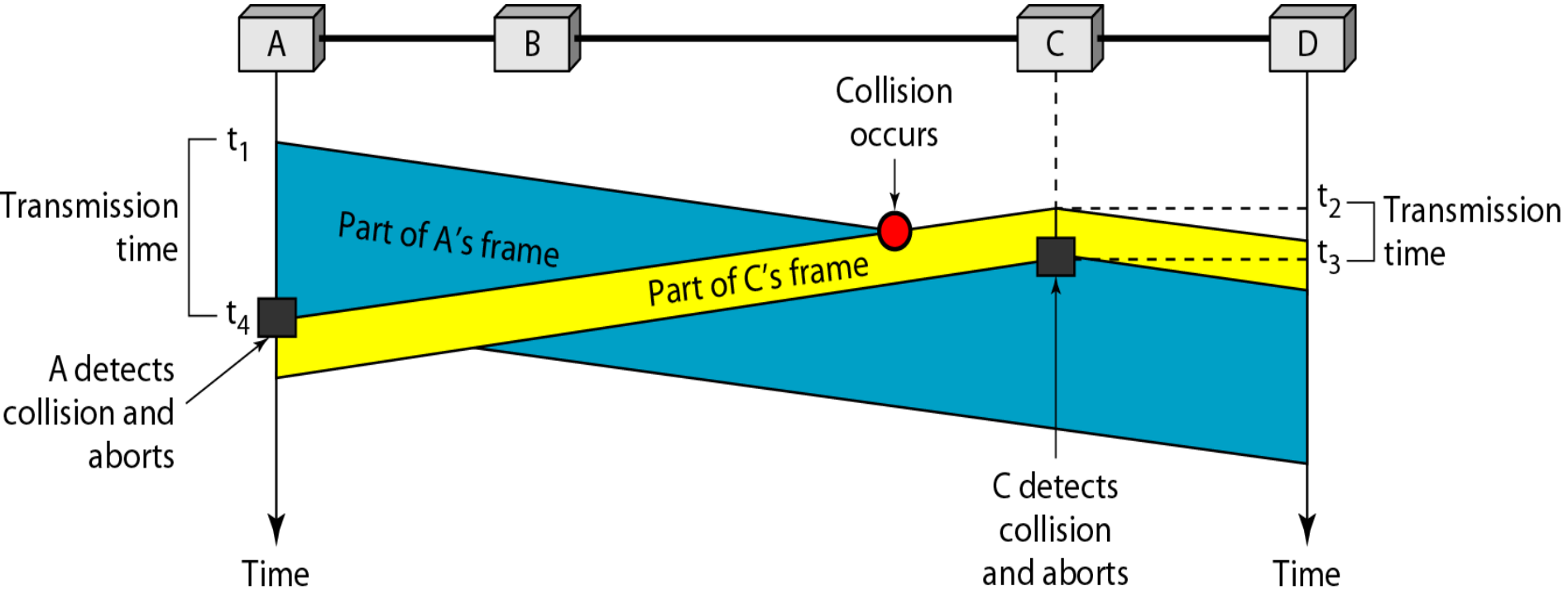
Ethernet CSMA/CD

- Use any persistent CSMA for frame transmission.
- Transmit packet only if channel is sensed idle.
- During the packet transmission, the node's computer hardware monitors(listens) its own transmission to see if the packet has experienced a collision.
  - An additional XOR gate is implemented at the transmitter.
  - If received signal XOR with transmitted signal is "0" then no collision.
  - If received signal XOR with transmitted signal is "1" then there is a collision.
  - Stop the ongoing frame transmission(when XOR=1).
  - Collisions are detected within a few bit times.
  - Transmission is then aborted, reducing the channel wastage considerably.
  - Sends a jamming signal to all of its neighbour stations.

CSMA/CD collision detection



Collision and abortion in CSMA/CD



CSMA/CD

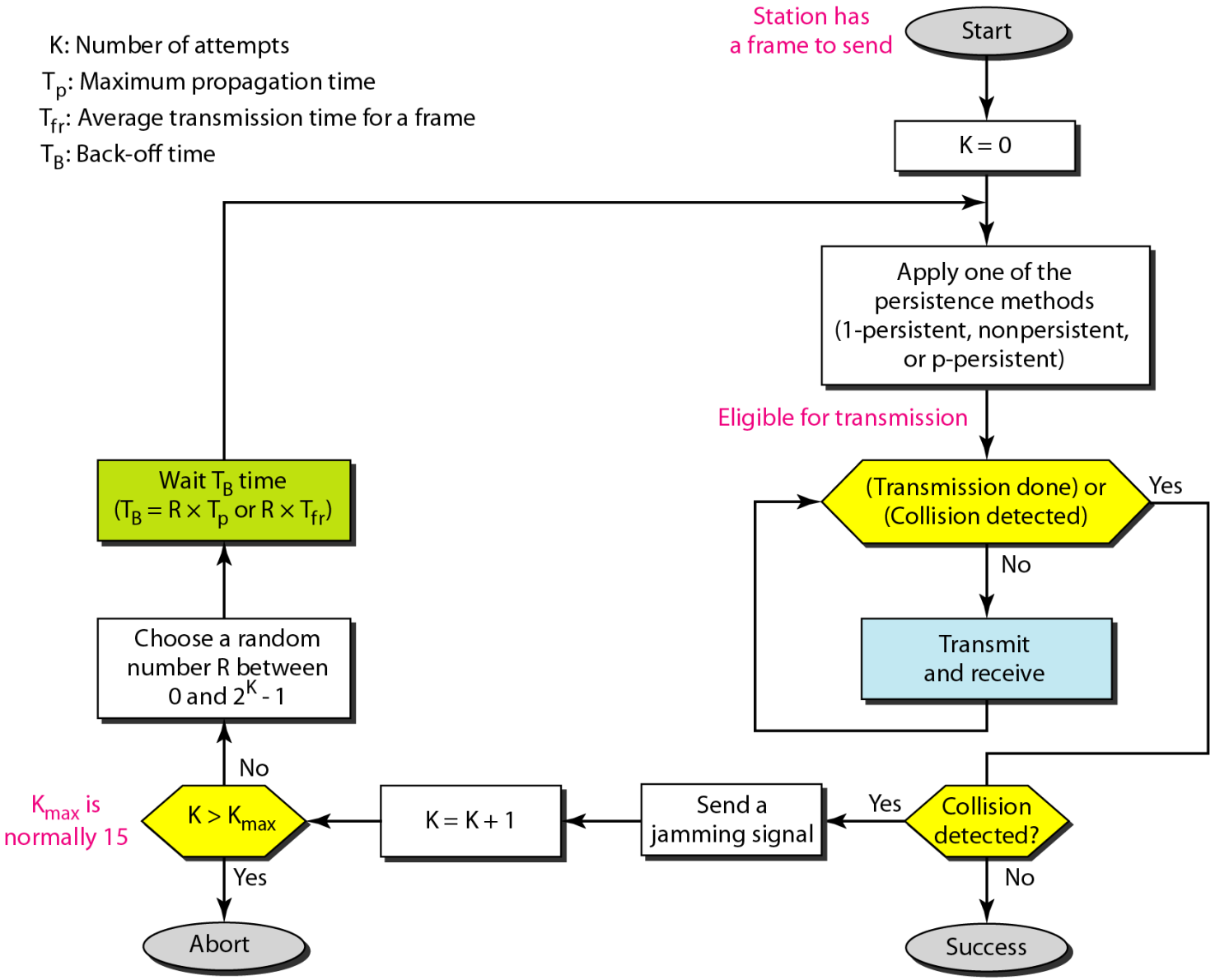
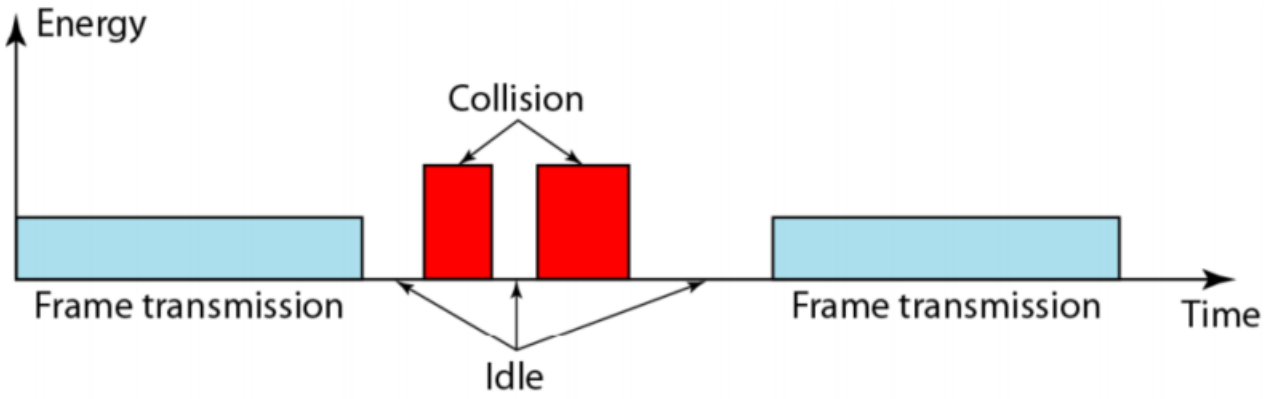

K: Number of attempts
T_p: Maximum propagation time
T_{fr}: Average transmission time for a frame
T_B: Back-off time
Station has a frame to send
Start
K = 0
Apply one of the persistence methods (1-persistent, nonpersistent, or p-persistent)
Eligible for transmission
(Transmission done) or (Collision detected)
Yes
No
Transmit and receive
Wait T_B time ($T_B = R \times T_p$ or $R \times T_{fr}$)
Choose a random number R between 0 and $2^K - 1$
No
K_{max} is normally 15
$K > K_{max}$
K = K + 1
Send a jamming signal
Yes
Collision detected?
No
Yes
Abort
Success

Figure 12.15 *Energy level during transmission, idleness, or collision*



CSMA/CD Performance

- Wasted capacity is restricted by time to detect collision.
  - Time to detect collision < 2*maximum propagation delay.

- **Rule in CSMA/CD protocols:** frames are long enough to allow collision detection prior to end of transmission.
  - Assumption : Transmission time is equal to maximum propagation time.

- What happens if the collision detection happens after transmission time ?
  - This case is true if collision happens close to the receiver.
  - A jamming Signal will be broadcasted in the shared medium
  - Nodes that receive the jamming signal will wait for backoff time.

Figure 12.16 *Timing in CSMA/CA*

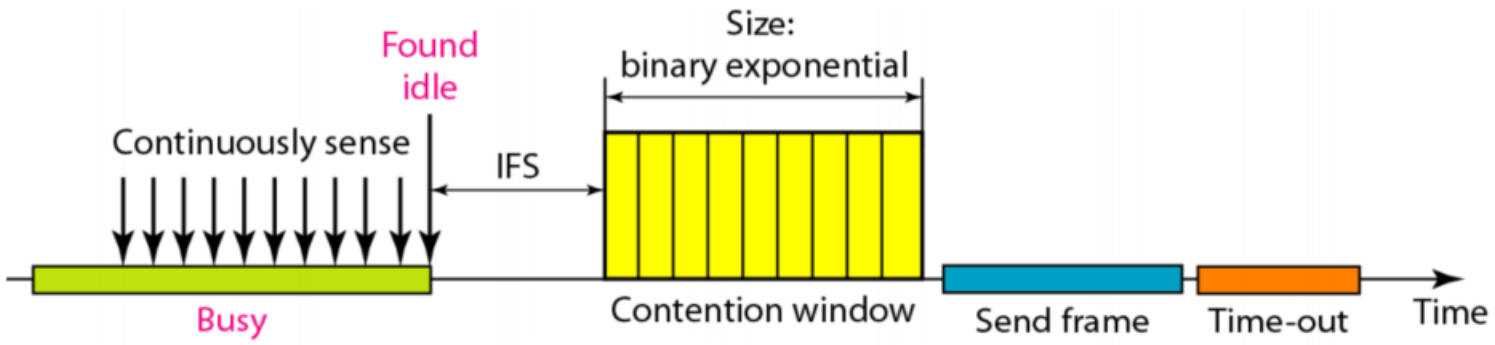
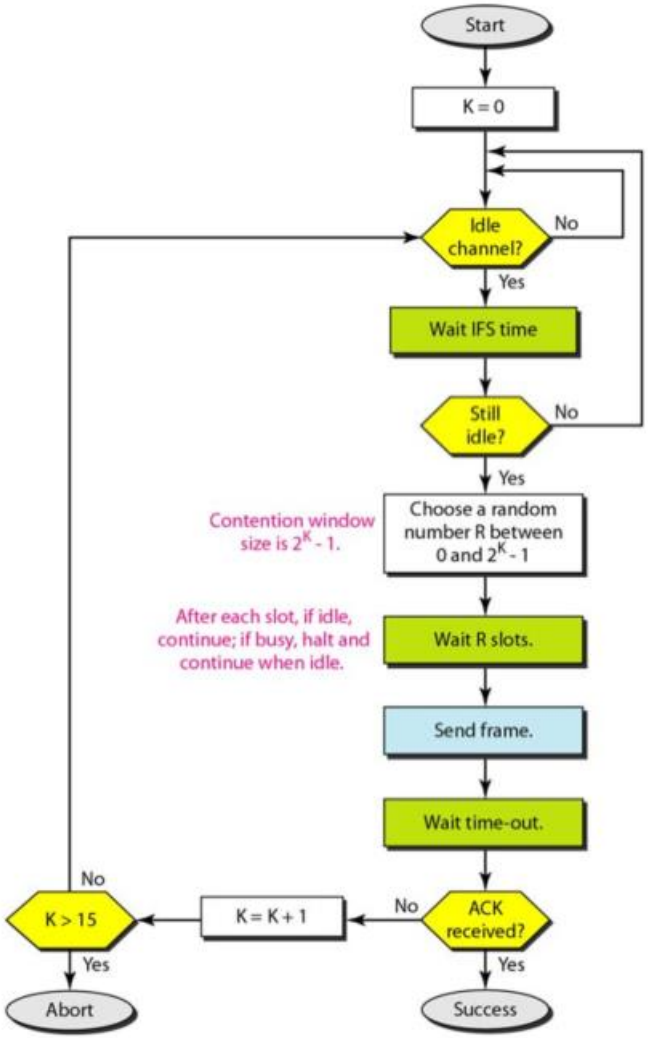


Figure 12.17 *Flow diagram for CSMA/CA*



Collision Free Protocols

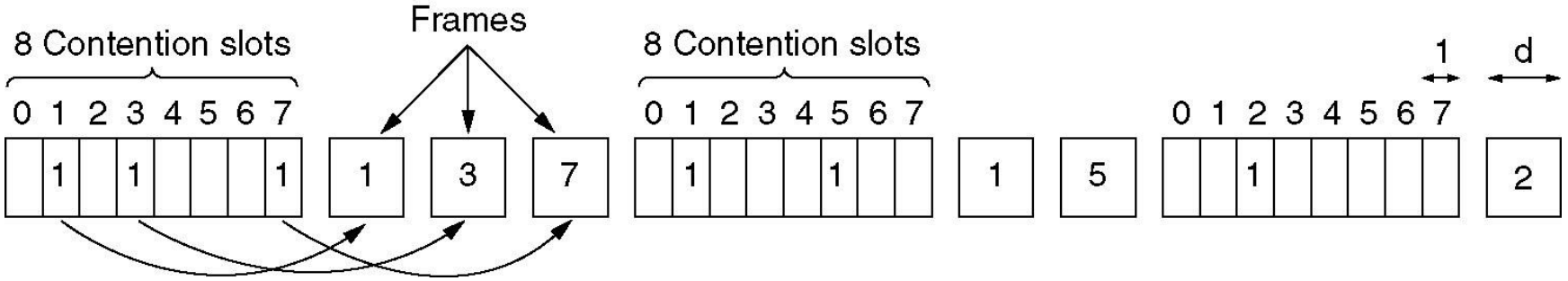
- Pure ALOHA, slotted ALOHA, CSMA and CSMA/CD are contention based protocols
  - try. If collide, retry.
  - No guarantee of performance.
  - What happens if the network load is high?
- Collision free protocols:
  - pay constant overhead to achieve performance guarantee
  - Good when network load is high

Collision Free World

- Provides in *order access* to shared medium so that every station has chance to transfer (fair protocol)
- Eliminates collision completely.
- Three methods for controlled access:
  - Reservation (Bitmap protocol)
  - Polling
  - Token Passing

Reservation – Bit Map Protocol

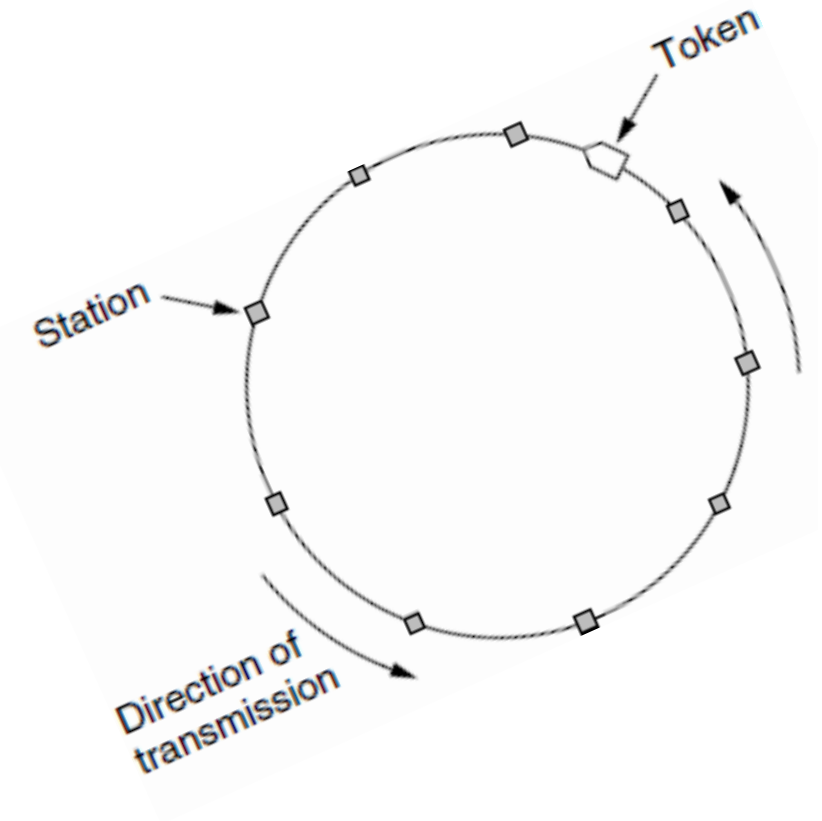
- Two rounds of transmission cycle
  - First Round (Contention Period)
    - Consists of N slots each reserved for a particular station
    - In this period, each station transmits
      - 1 if it has a frame to transmit
      - 0 if it has no frame to transmit
  - At the completion of the first round everybody knows who wants to transmit
  - Second Round (Transmission Period)
    - Stations transmit according to the order formed in the first round
    - There will not be any collisions

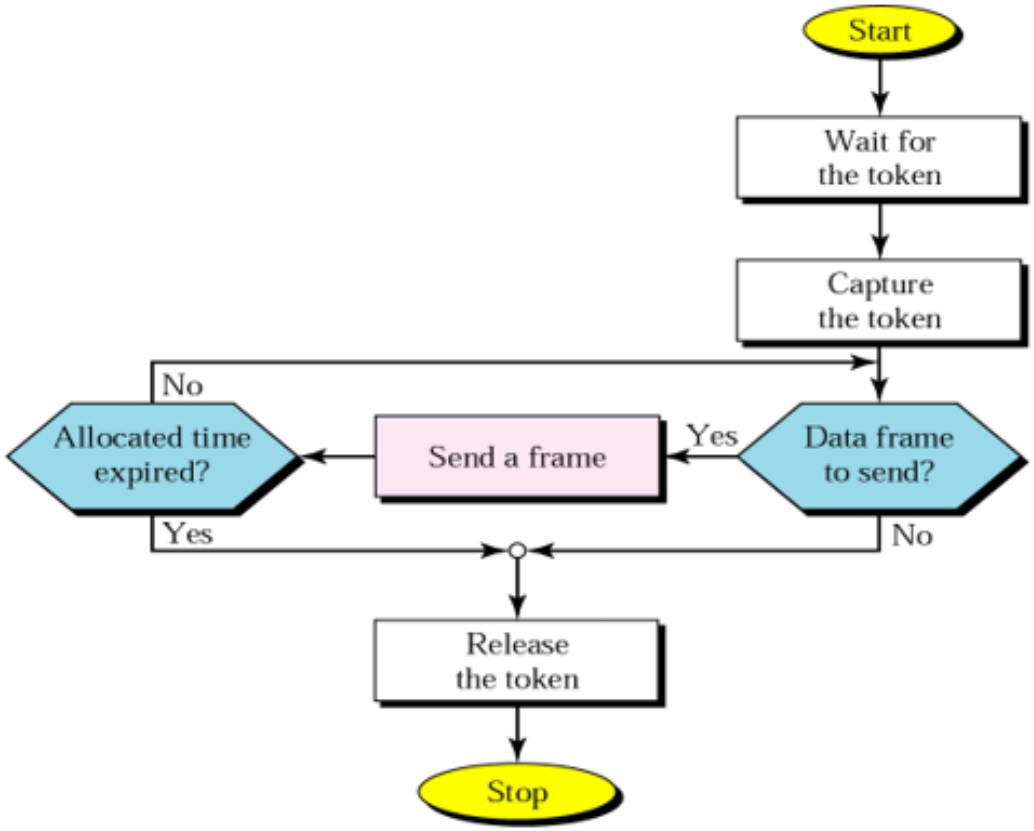


Bit Map - Reservation Based

- When a station needs to send a data frame, it makes a contention in its own 1-bit mini-slot.
- By listening to the contention interval, every station knows which stations will transfer frames, and in which order.
- The stations that made reservations can send their data frames after the reservation frame.

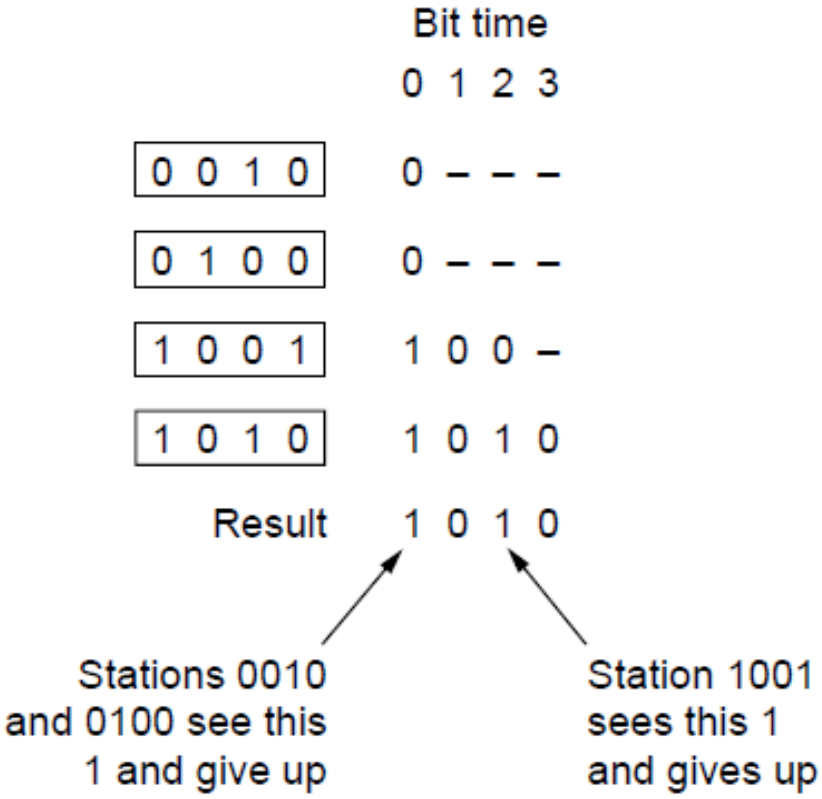
Token Ring



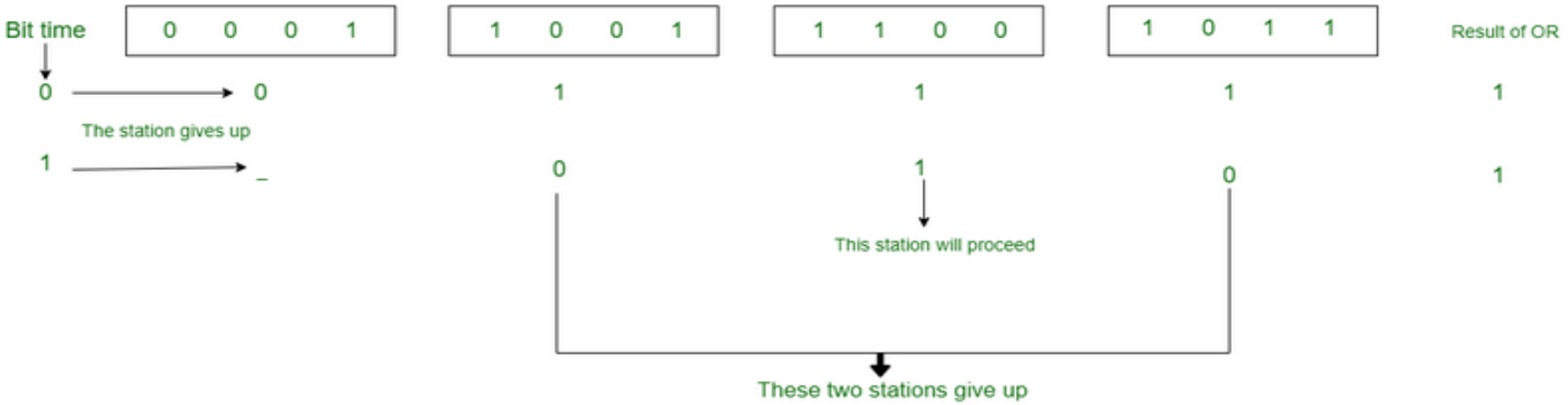


- Token pass.
  - There is only one token in the network.
  - The token is passed through every node in the network.
  - Only the node that has the token can transfer data.

Binary Countdown



The binary countdown protocol. A dash indicates silence.


Bit time
0 0 0 1
1 0 0 1
1 1 0 0
1 0 1 1
Result of OR
0
0
1
1
1
The station gives up
1
_
0
1
0
1
This station will proceed
These two stations give up

Contention vs. Collision-Free

- Contention better under low load. *Why*?
  - Less collisions under low load.
- Collision-free better under high load. *Why*?
  - Channel utilization is better at high load.
- How about combining their advantages -- limited contention protocols.
  - Behave like the ALOHA scheme under light load
  - Behave like the bitmap scheme under heavy load.

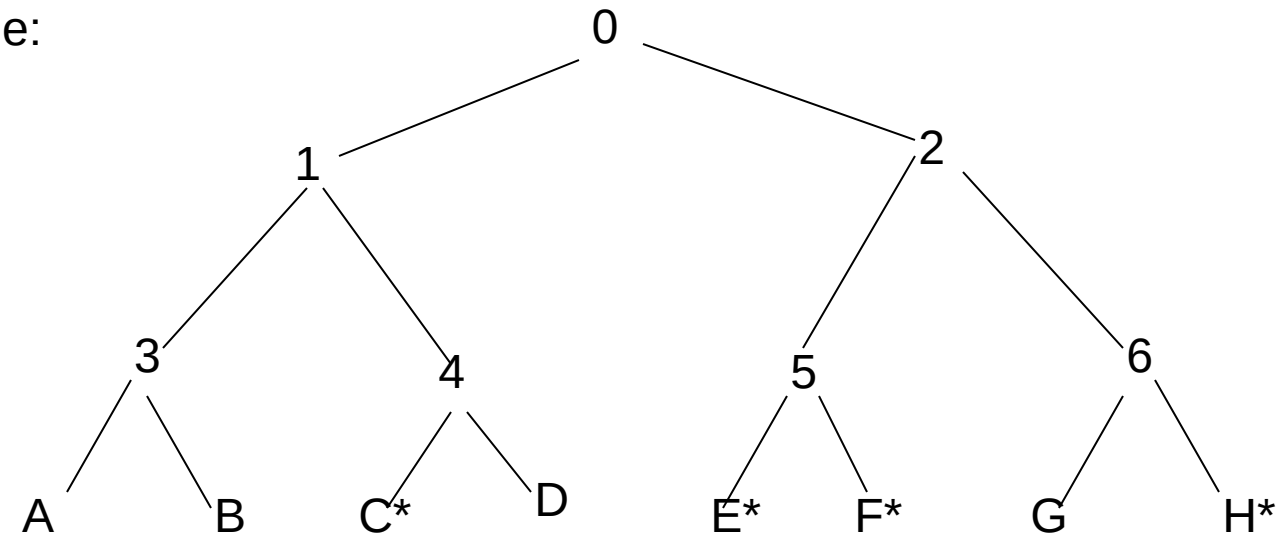
Limited contention protocols

- collision based protocols (ALOHA,CSMA/CD) are good when the network load is low.
- collision free protocols (bit map, binary countdown) are good when load is high.
- How about combining their advantages -- limited contention protocols.
  - Behave like the ALOHA scheme under light load
  - Behave like the bitmap scheme under heavy load.

Limited contention protocols:

- adaptive tree walk protocol
  - trick: partition the group of station and limit the contention for each slot.
    - under light load, every one can try for each slot like aloha
    - under heavy load, only a small group can try for each slot
    - how do we do it
      - » treat stations as the leaf of a binary tree.
      - » first slot (after successful transmission), all stations (under the root node) can try to get the slot.
      - » if no conflict, fine.
      - » if conflict, only nodes under a subtree get to try for the next one. (depth first search)

Example:

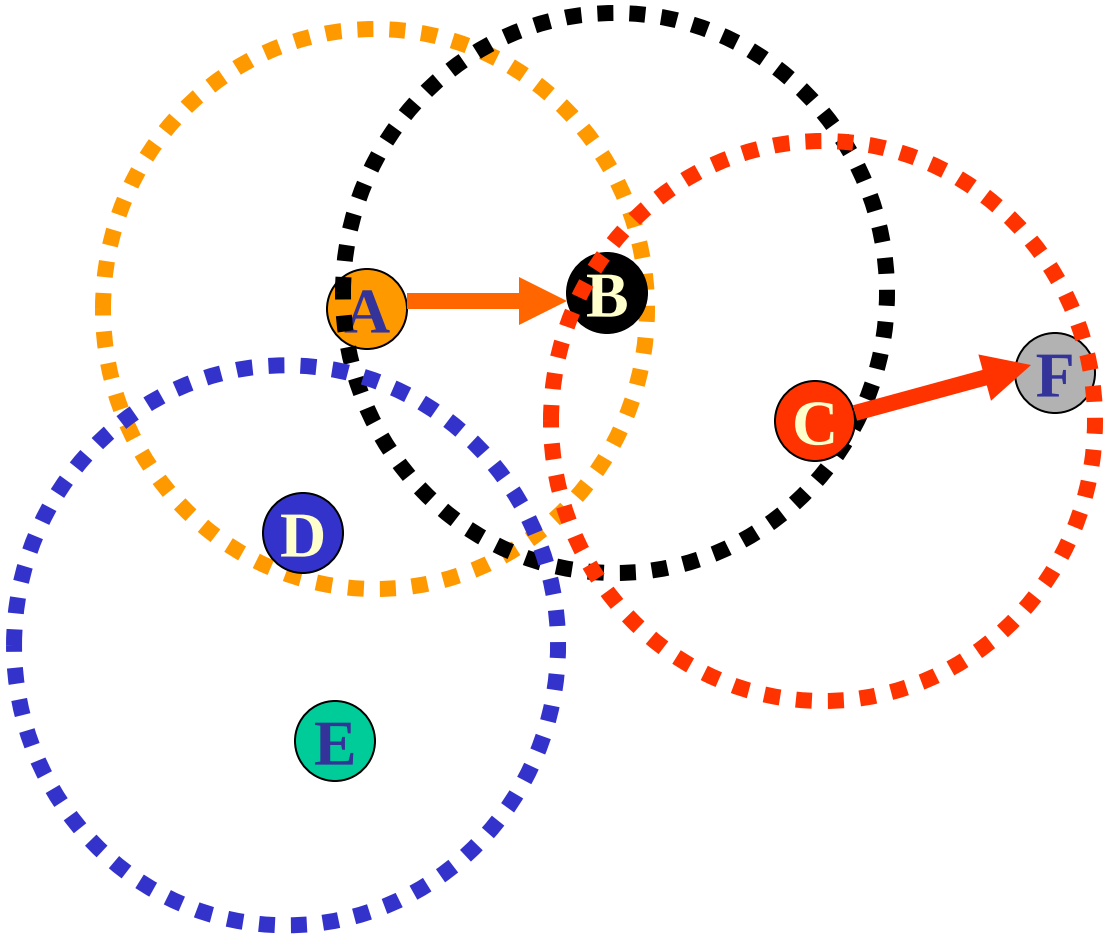


Slot 0: C*, E*, F*, H* (all nodes under node 0 can try), conflict
slot 1: C* (all nodes under node 1 can try), C sends
slot 2: E*, F*, H*(all nodes under node 2 can try), conflict
slot 3: E*, F* (all nodes under node 5 can try), conflict
slot 4: E* (all nodes under E can try), E sends
slot 5: F* (all nodes under F can try), F sends
slot 6: H* (all nodes under node 6 can try), H sends.

Motivation for Wireless MAC

- Can we apply media access methods from fixed networks?
- Example CSMA/CD
  - **C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection
  - send as soon as the medium is free, listen into the medium if a collision occurs (original method in IEEE 802.3)
- Problems in wireless networks
  - Signal strength decreases proportional to the square of the distance
  - Sender would apply CS and CD, but the collisions happen at the receiver (Hidden terminals)
  - it might be the case that a sender cannot “hear” the collision, i.e., CD does not work

Hidden and Exposed Terminals

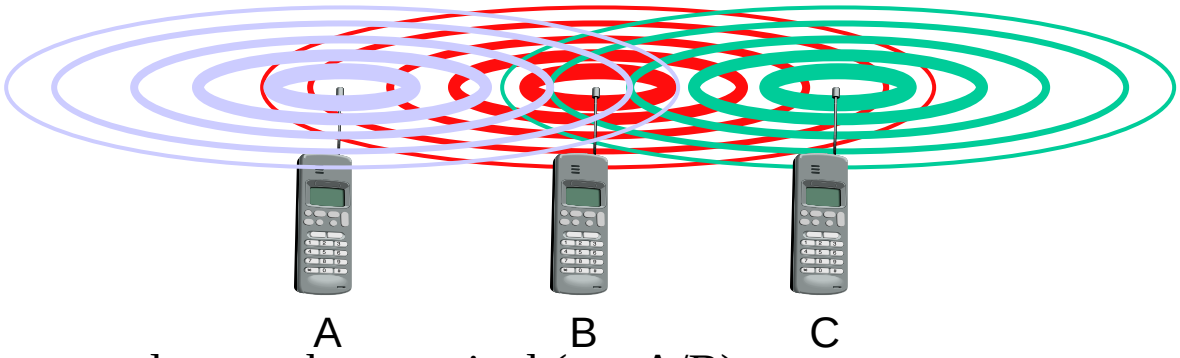


- A wants to transmit to B.
- C senses channel – no idea A is transmitting.
- C initiates transmission to F.
- Collision at B. – C and A are hidden from each other.

- D could potentially transmit to E but does not – senses A's carrier. D is exposed to A. Loss in throughput.

Hidden and exposed terminals

- Hidden terminals
  - A sends to B, C cannot receive A
  - C wants to send to B, C senses a “free” medium (CS fails)
  - collision at B, A cannot receive the collision (CD fails)
  - A is “hidden” for C



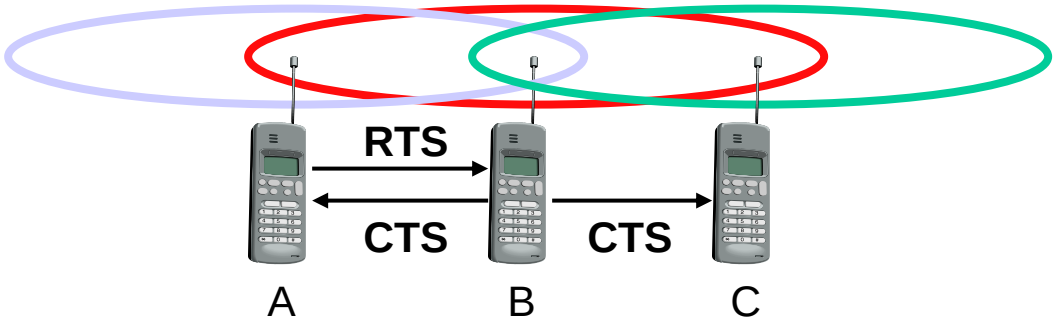
- Exposed terminals
  - B sends to A, C wants to send to another terminal (not A/B)
  - C has to wait, CS signals a medium in use
  - but A is outside the radio range of C, therefore waiting is not necessary
  - C is “exposed” to B

MACA - collision avoidance

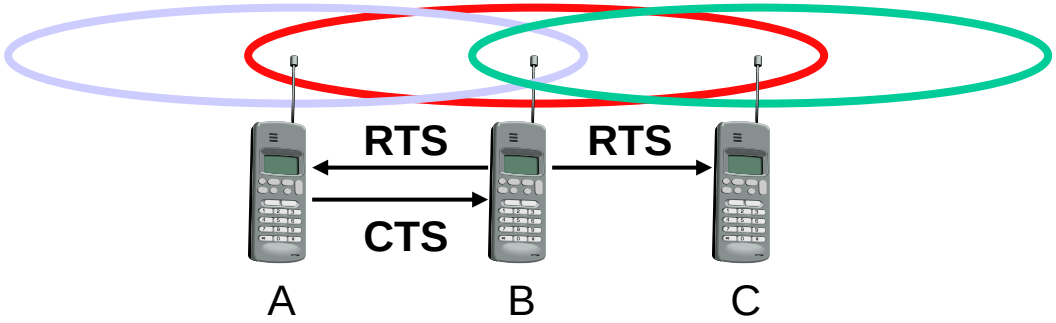
- No carrier sense (CS)
- MACA (Multiple Access with Collision Avoidance) uses short signaling packets for collision avoidance
  - RTS (request to send): a sender request the right to send from a receiver with a short RTS packet before it sends a data packet
  - CTS (clear to send): the receiver grants the right to send as soon as it is ready to receive
- Signaling packets contain
  - sender address
  - receiver address
  - packet size
- Variants of this method can be found in IEEE 802.11.

MACA examples

- MACA avoids the problem of hidden terminals
  - A and C want to send to B
  - A sends RTS first
  - C waits after receiving CTS from B



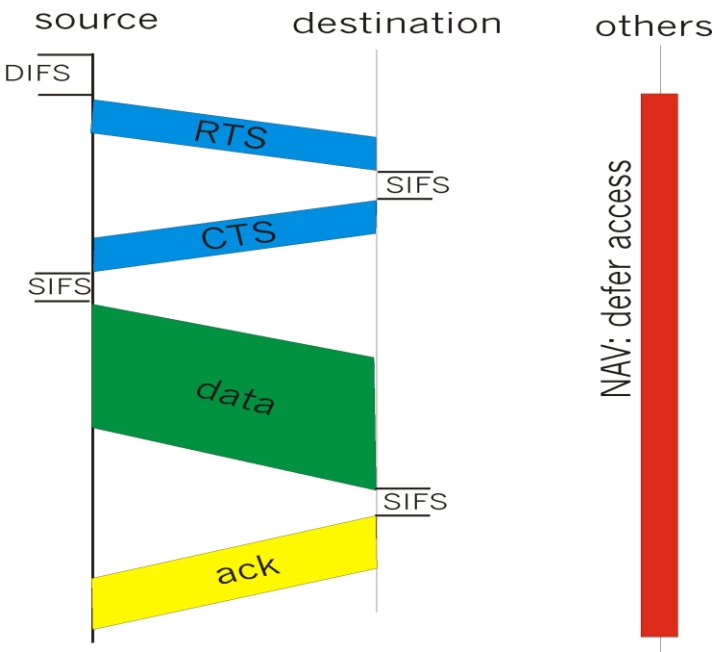
- MACA avoids the problem of exposed terminals?
  - B wants to send to A,
  - C to another terminal
  - now C does not have to wait for it cannot receive CTS from A



Alternative Approach: MACAW

Multiple Access with Collision Avoidance for Wireless

- No carrier sense, no collision detection
- Collision avoidance:
  - Sender sends RTS
  - Receiver sends CTS
  - Sender sends DATA
  - Receiver sends ACK
- Backoff mechanism:
  - Exponential backoff with significant changes for improving fairness and throughput



MACA

- A sends out RTS and set a timer and waits for CTS
- If A receives CTS before timer go to zero, OK! sends data packet
- Otherwise, A assumes there is a collision at B
- Double the backoff counter interval
- Randomly pick up a timer from [1,backoff counter]
- Send next RTS after timer go to zero
- B sends out CTS, then set a timer and waits for data packet
- If data packet arrives before timer go to zero, OK!
- Otherwise, B can do other things
- C overhears A's RTS, set a timer which is long enough to allow A to receive CTS. After the timer goes to zero, C can do other things
- D overhears B's CTS, set a timer which is long enough to allow B to receive data packet.
- E overhears A's RTS and B's CTS, set a timer which is long enough to allow B to receive data packet.
- RTS and CTS can also contain info to allow sender A to adjust power to reduce interference

Comparisonof various protocols:

Protocol	Transmission behavior	Collision detection method	Efficiency	Use cases
Pure ALOHA	Sends frames immediately	No collision detection	Low	Low-traffic networks
Slotted ALOHA	Sends frames at specific time slots	No collision detection	Better than pure ALOHA	Low-traffic networks
CSMA/CD	Monitors medium after sending a frame, retransmits if necessary	Collision detection by monitoring transmissions	High	Wired networks with moderate to high traffic
CSMA/CA	Monitors medium while transmitting, adjusts behavior to avoid collisions	Collision avoidance through random backoff time intervals	High	Wireless networks with moderate to high traffic and high error rates

Ethernet Cabling

Type	Cable	Max Seg.	Nodes/seg	Remark
10Base5:	Thick coax	500m	100	Original cable/ obsolate
10Base2:	Thin Coax	185 m	30	No hub Needed
10BaseT:	Twisted Pair	100 m	1024	cheapest system
10BaseF:	Fiber Optics	2000m	1024	Best between buildings

- Repeater: receive, amplify and retransmit signals in both directions.
  - used for thick and thin coax cables to connect multiple segments.
- Hub: logically connects UTP cables into 1 long ethernet cable
  - may contain electronics to detect and disconnect faulty UTP and also reshapes the signals

Ethernet Cabling

- 10Base5 (Thick Ethernet)
  - 10Mbps
  - Base: Baseband transmission (digital Signals)
  - Its max segment length = 500 m
- **Thick Coax**
  - *Advantages:* Low attenuation, excellent noise immunity, superior mechanical strength
  - *Disadvantages:* Bulky, difficult to pull, transceiver boxes too expensive.

* *Wiring represented a significant part of total installed cost.*

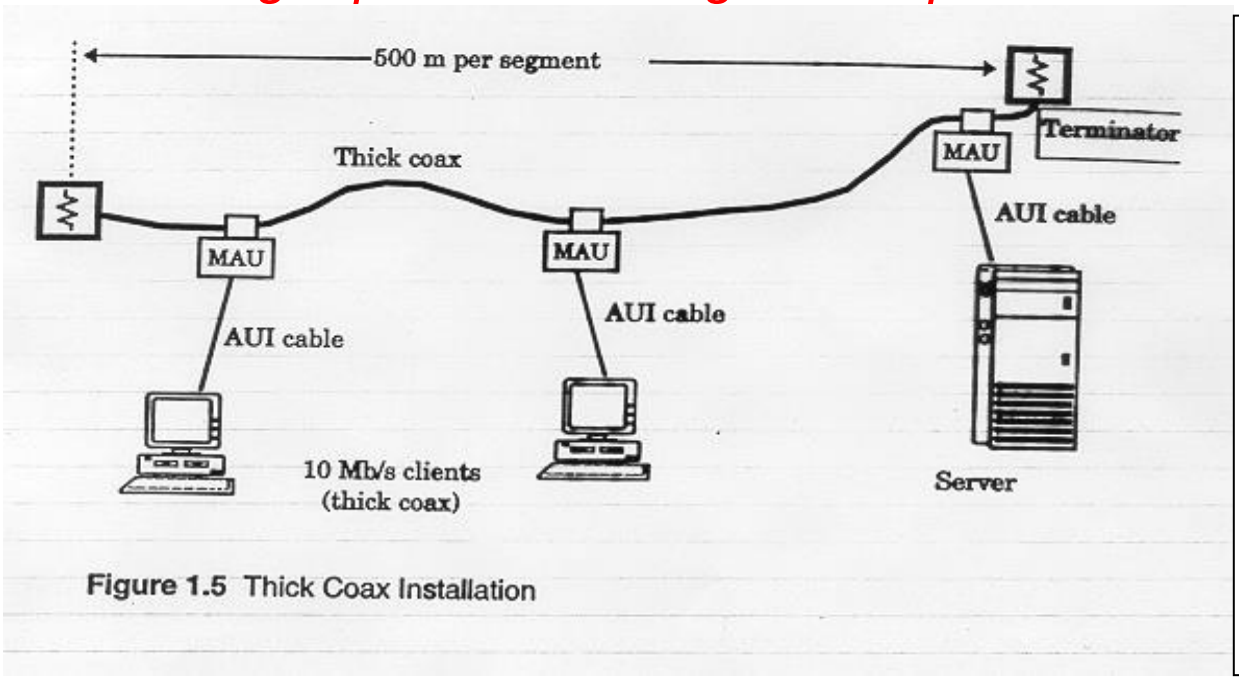


Figure 1.5 Thick Coax Installation

AUI: Attachment unit interface cable

MAU Connectors: Multistation Access Unit

MAU device is physically hooked on main cable.

50 meter AUI cable from MAU to station.

Ethernet Cabling

- 10Base2 (Thin Ethernet) ***Cheapernet***
  - 10 Mbps
  - 185 meter segment length
  - Signal-regenerating repeaters
  - Transceiver was integrated onto the adapter
  - **Thin Coax (coax thinner and lighter)**
  - *Advantages:* Easier to install, reduced hardware cost, BNC connectors widely deployed ➔ lower installation costs.
  - *Disadvantages:* Attenuation not as good, could not support as many stations due to signal reflection caused by BNC Tee Connector.

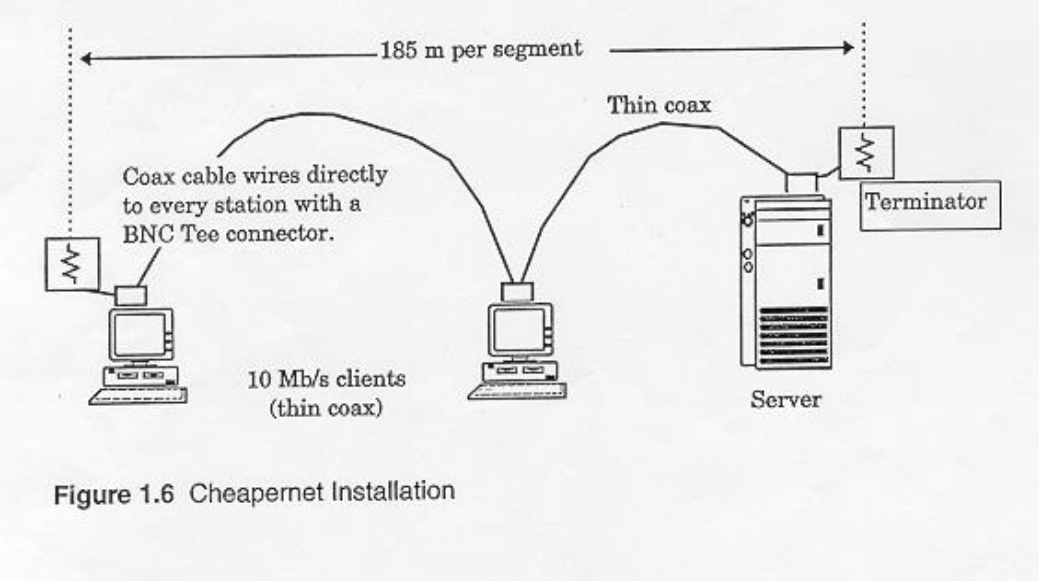


Figure 1.6 Cheapernet Installation

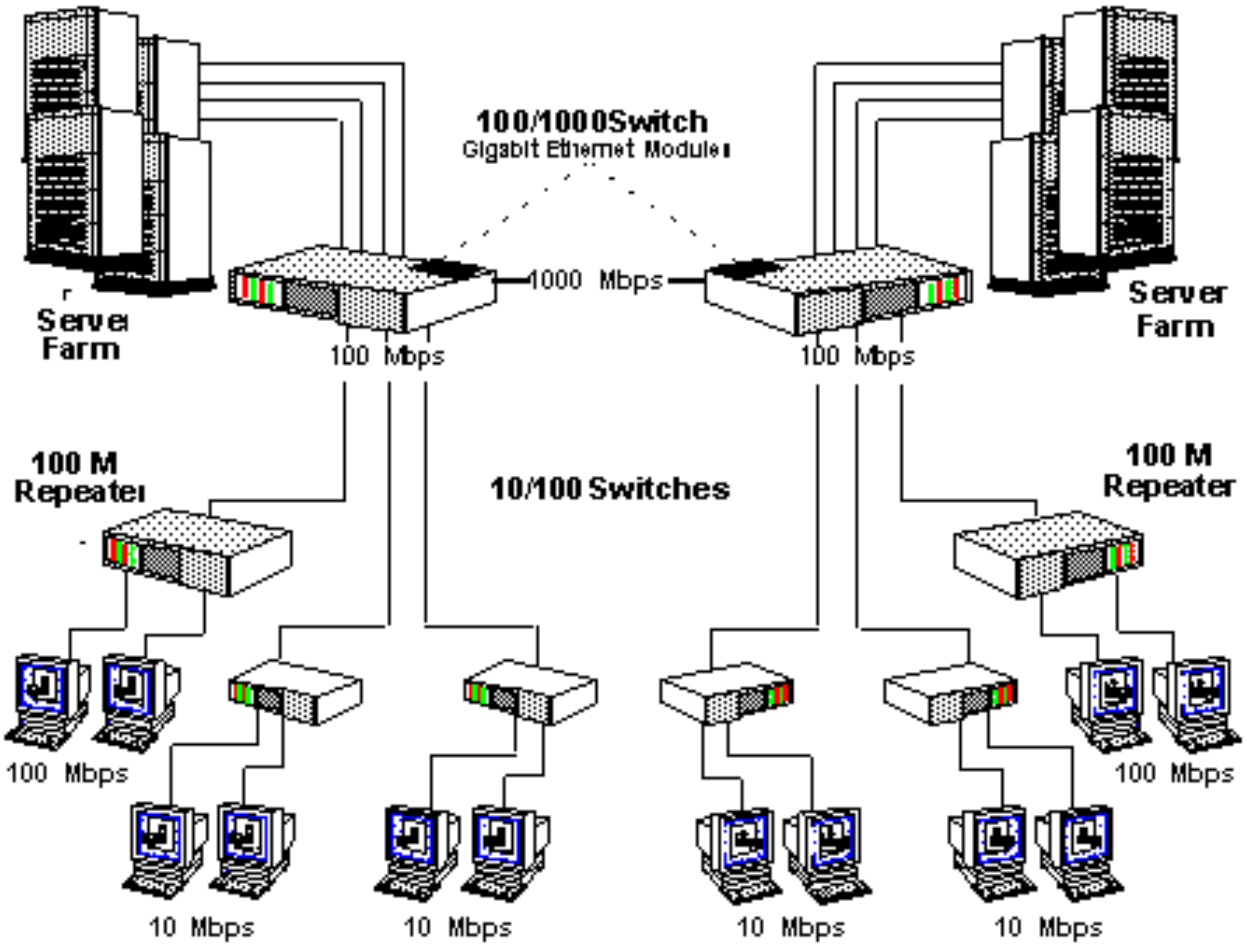
IEEE 802.u 100Mb Fast Ethernet

- The basic idea was simple: keep all the old packet formats, interface and procedural rules, just reduce the bit time from 100 ns to 10 ns, to reach 100 Mbps.
- Coax cables are not used any more; in our old building in 2000 replaced by Cat5 UTP
- Cat 5 UTP: 2 pairs; 125 MHz, 4 bits encoded in 5 signals

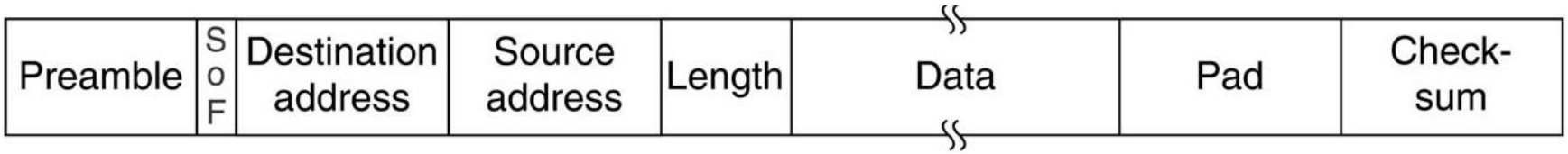
100Base-T4	Cat 3 UTP 4 pairs		100 m	cheap cat 3
100Base-TX	Cat 5 UTP 2 pairs		100 m	full duplex at 100 Mbps
100Base-F	Fiber multi-mode		2000 m	full duplex, long runs

Gigabit Ethernet Cat 5 UTP

Name	Cable	Max. segment	Advantages
1000Base-SX	Fiber optics	550 m	Multimode fiber (50, 62.5 microns)
1000Base-LX	Fiber optics	5000 m	Single (10 μ) or multimode (50, 62.5 μ)
1000Base-CX	2 Pairs of STP	25 m	Shielded twisted pair
1000Base-T	4 Pairs of UTP	100 m	Standard category 5 UTP

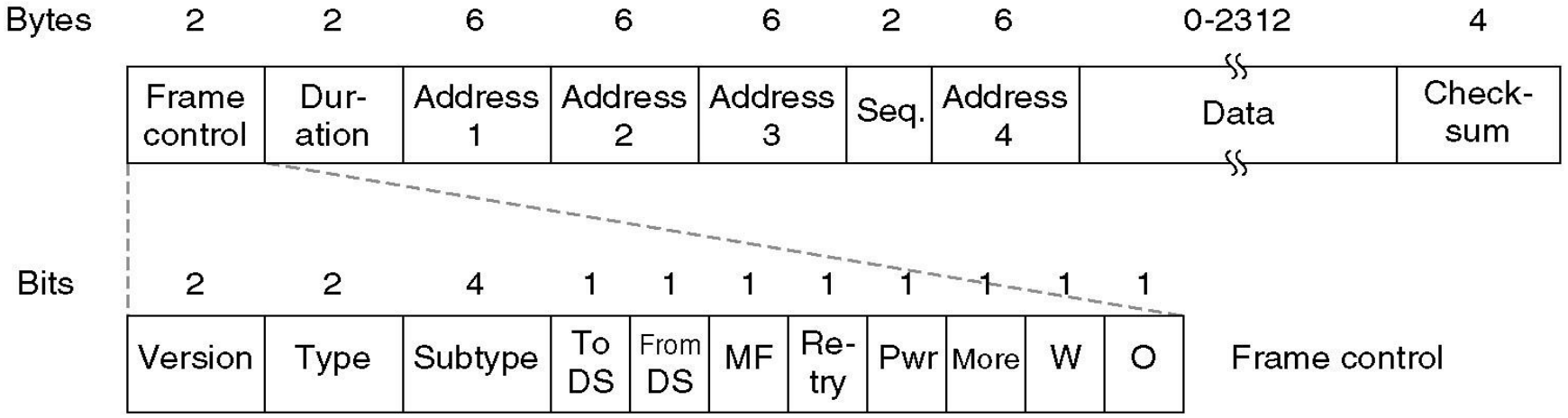


Ethernet frame format



- Preamble of 7 bytes used to synchronize clocks.
- The Start Of Frame delimiter contains 10101011
- Addresses are 6 bytes.
- The addresses are unique in the world.
- The address containing all 1's is reserved for **broadcast**, a message destinated to all recievers
- There were many variations in using the 2 byte length
  - Most common now is to use it as a Type field, indicating that the data is a higher level protocol packet, e.g. 0x0800 for IPv4 and 0x86DD for IPv6

The 802.11 Frame Structure



The data frame header contains 4 addresses, each in the standard 802 format. Two are used to identify the sending and receiving stations. The other two are used for the source and destination of base stations for intercell traffic.

The W bit indicates **WEP** (Wired Equivalent privacy)

- 802.11b 2.4 GHz up to 11 Mb/s
- 802.11a 5 GHz up to 54 Mb/s
- 802.11g 2.4 GHz up to 54 Mb/s
- 802.11n 5 GHz, up to 200 Mb/s

Interconnecting LANs

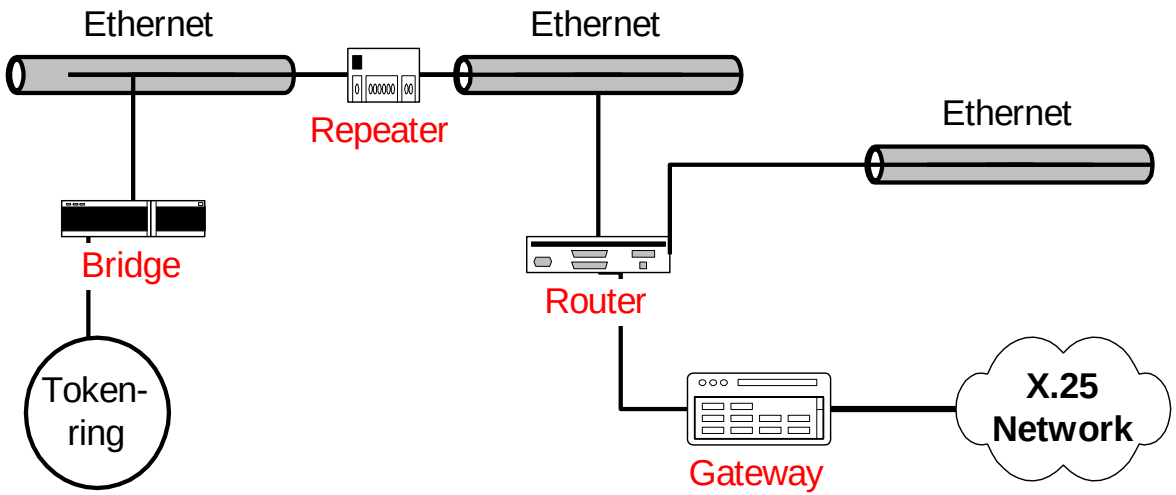
Q: Why not just one big LAN?

- Limited amount of supportable traffic: on single LAN, all stations must share bandwidth
- limited length: 802.3 (Ethernet) specifies maximum cable length
- large “collision domain” (can collide with many stations).

- Multiple LANs are connected through :
  - HUB/Repeater :Connect two LANs at physical layer.
  - Switch : Connect two LANs at the link layer(MAC address)
  - Router : Connect two subnets at the network layer (IP address)

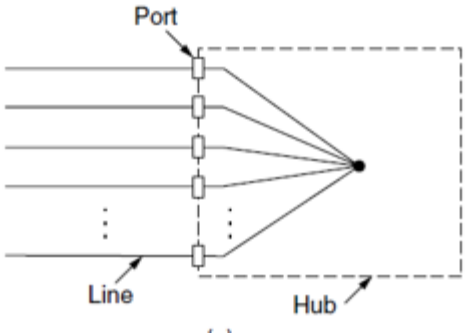
Interconnection Devices

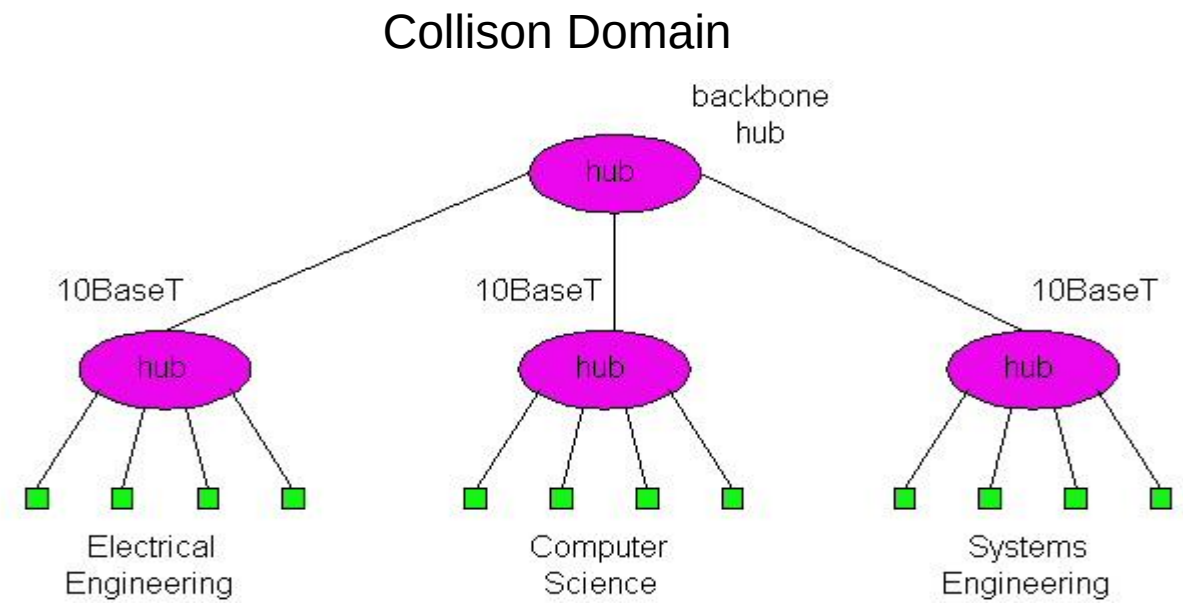
- There are many different devices for interconnecting networks.



Hubs/Repeaters

- 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
  - portions of the Multi-tier Hub LAN continue to operate if one hub malfunctions
  - extends maximum distance between node pairs (100m per Hub)

- Hub Limitations:

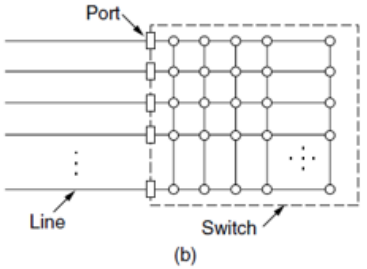
•single collision domain results in no increase in max throughput

multi-tier throughput same as single segment throughput

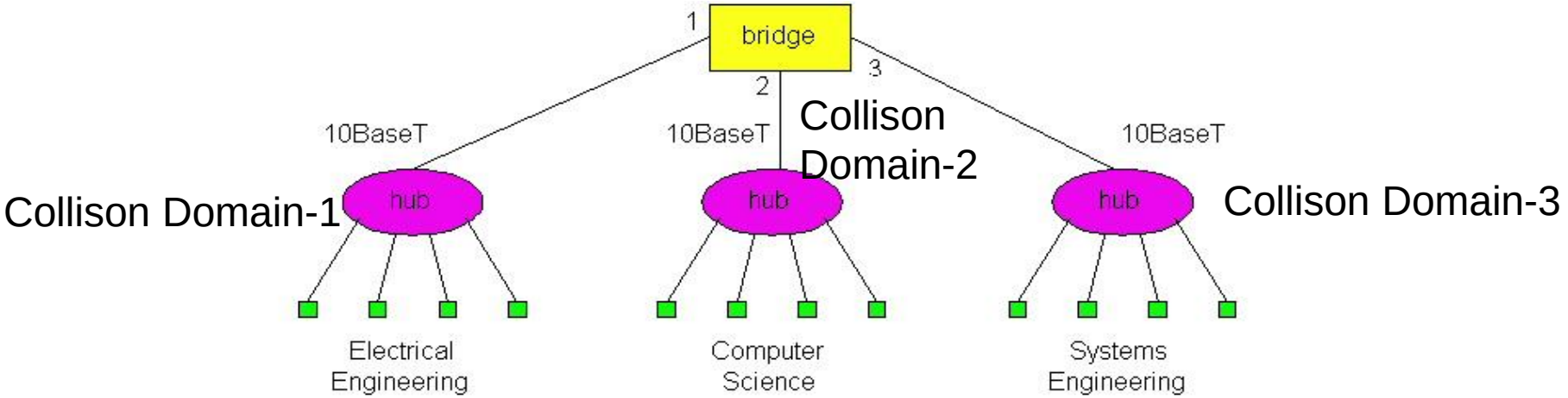
•cannot connect different Ethernet types (e.g., 10BaseT and 100baseT)

Bridges

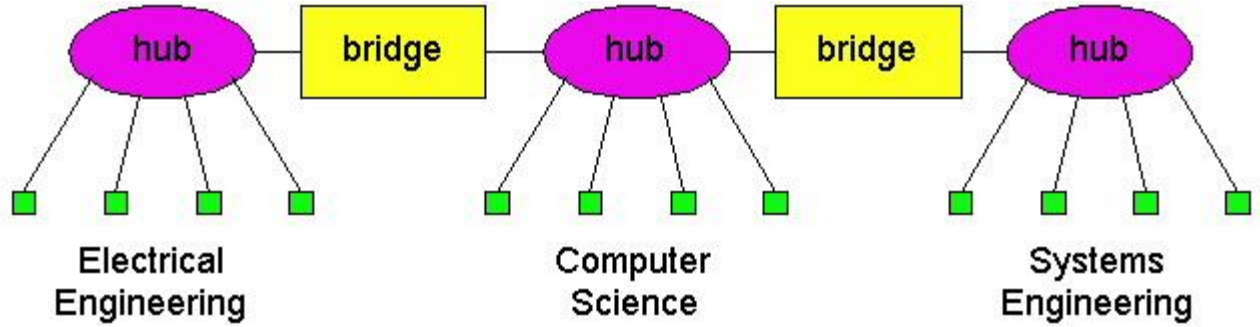
- Link Layer devices: operate on Ethernet frames, examining frame header and selectively forwarding frame based on its destination.
- Bridge isolates collision domains since it buffers frames.
- When frame is to be forwarded on segment, bridge uses CSMA/CD to access segment and transmit.



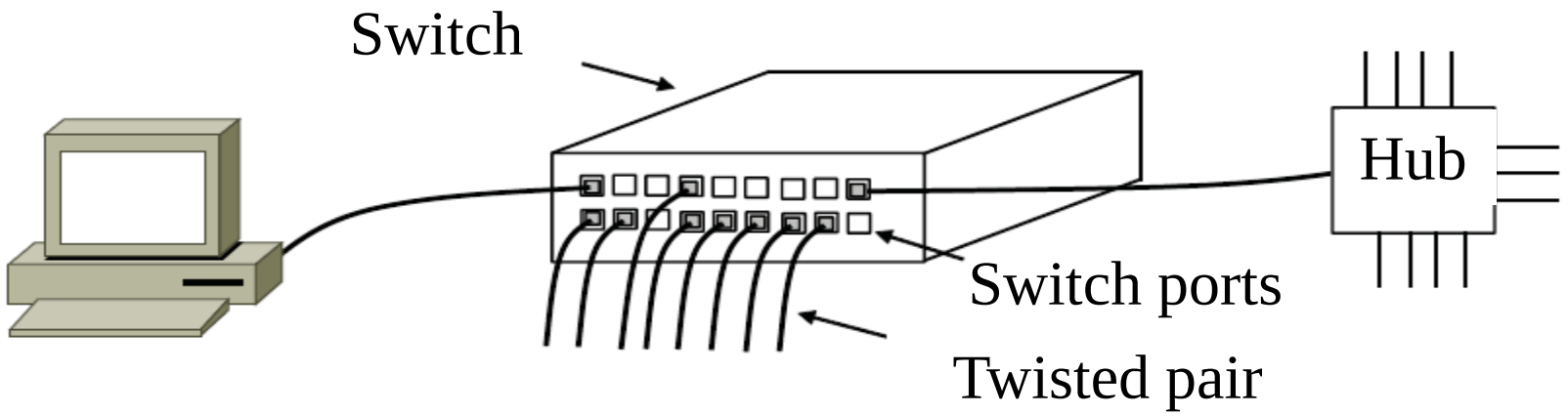
- Bridge advantages:
  - Isolates collision domains resulting in higher total max throughput, and does not limit the number of nodes nor geographical coverage.
  - Can connect different type Ethernet since it is a store and forward device



Interconnection Without Backbone

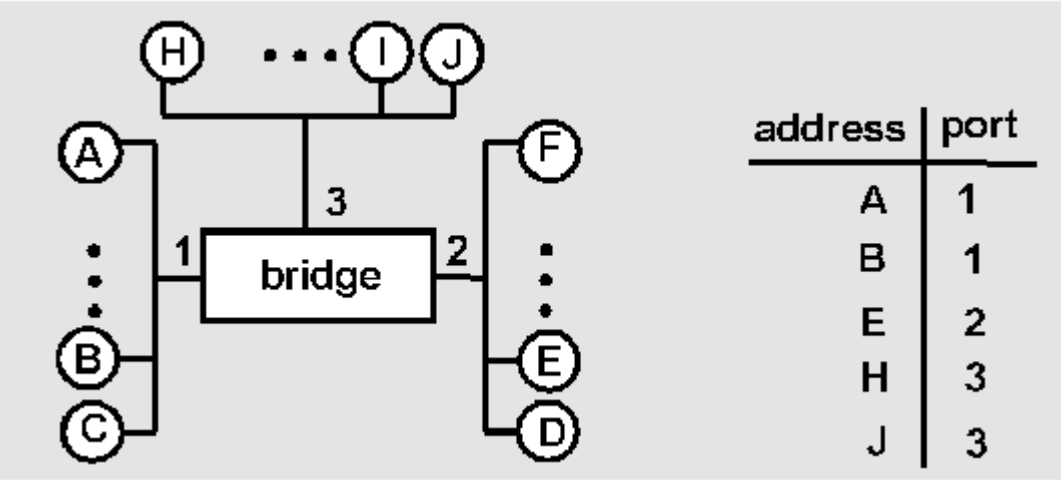


- Not recommended for two reasons:
  - - single point of failure at Computer Science hub
  - - all traffic between EE and SE must path over CS segment



Bridge Learning: example

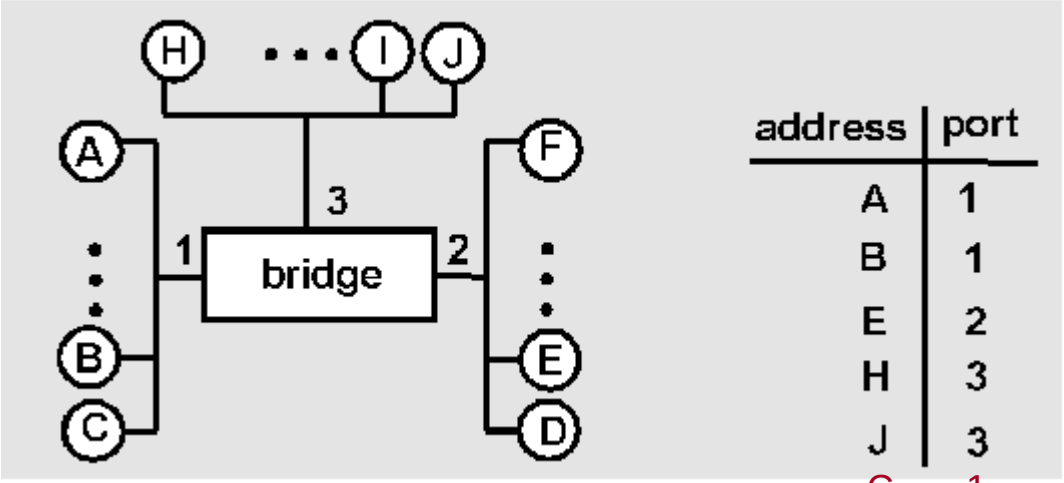
Suppose C sends frame to D and D replies back with frame to C



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

- C sends frame to bridge
  - bridge notes that C is on port 1 in the filtering table
  - bridge has no info about D, so floods to all the LANs
  - Nodes will compare the destination address of the frame
  - frame received by D

Bridge Learning: example



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

- 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 Operation

bridge procedure(in_MAC, in_port,out_MAC)

Set filtering table **(in_MAC)** to **in_port** /*learning*/

lookup in filtering table **(out_MAC)** receive **out_port**

if (out_port not valid) /* no entry found for destination */

then flood; /* *forward on all but the interface on which the frame arrived*/*

if (in_port = out_port) /*destination is on LAN on which frame was received */

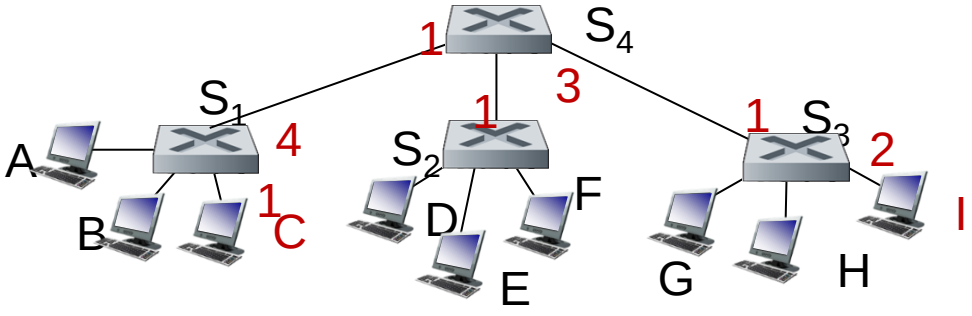
then drop the frame

Otherwise (out_port is valid) /*entry found for destination */

then forward the frame on interface indicate

Self-learning multi-switch example

Suppose C sends frame to I, I responds to C



- Q: show switch tables and packet forwarding in S_1, S_2, S_3, S_4

S1

Address	Port
C	1
I	4

S4

Address	Port
C	1
I	3

S3

Address	Port
C	1
I	2

S2

Address	Port
C	1

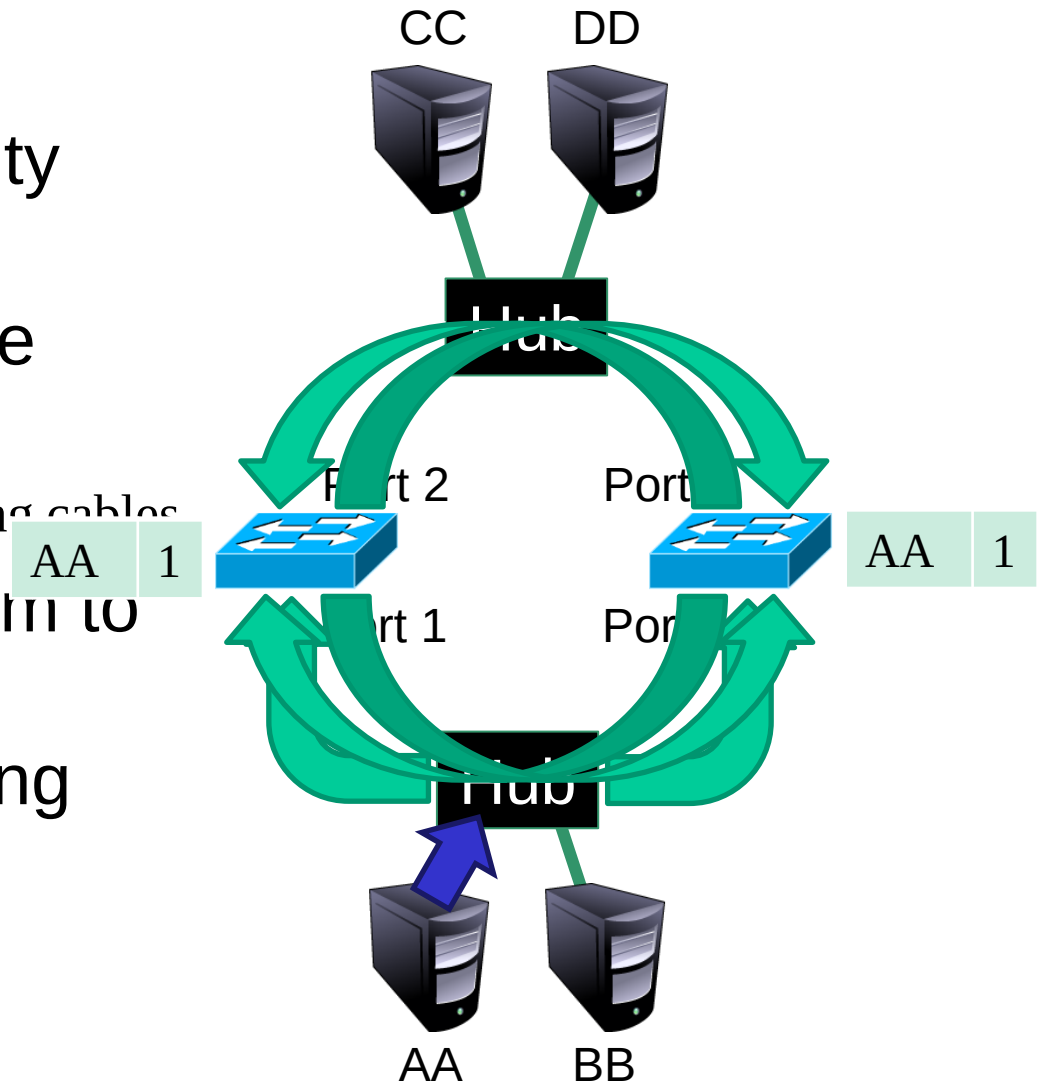
The Danger of Loops

a) <Src=AA, Dest=DD>

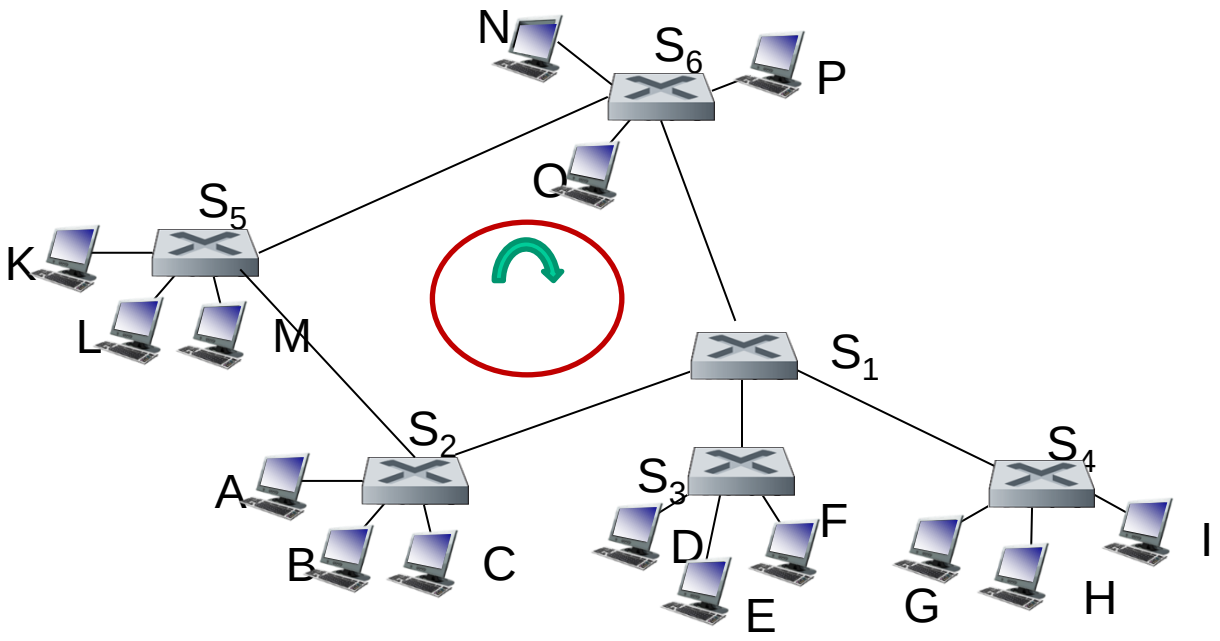
b) This continues to infinity
   - How do we stop this?

c) Remove loops from the topology
   - Without physically unplugging cables

d) 802.1 uses an algorithm to build and maintain a spanning tree for routing



Loops and Routing

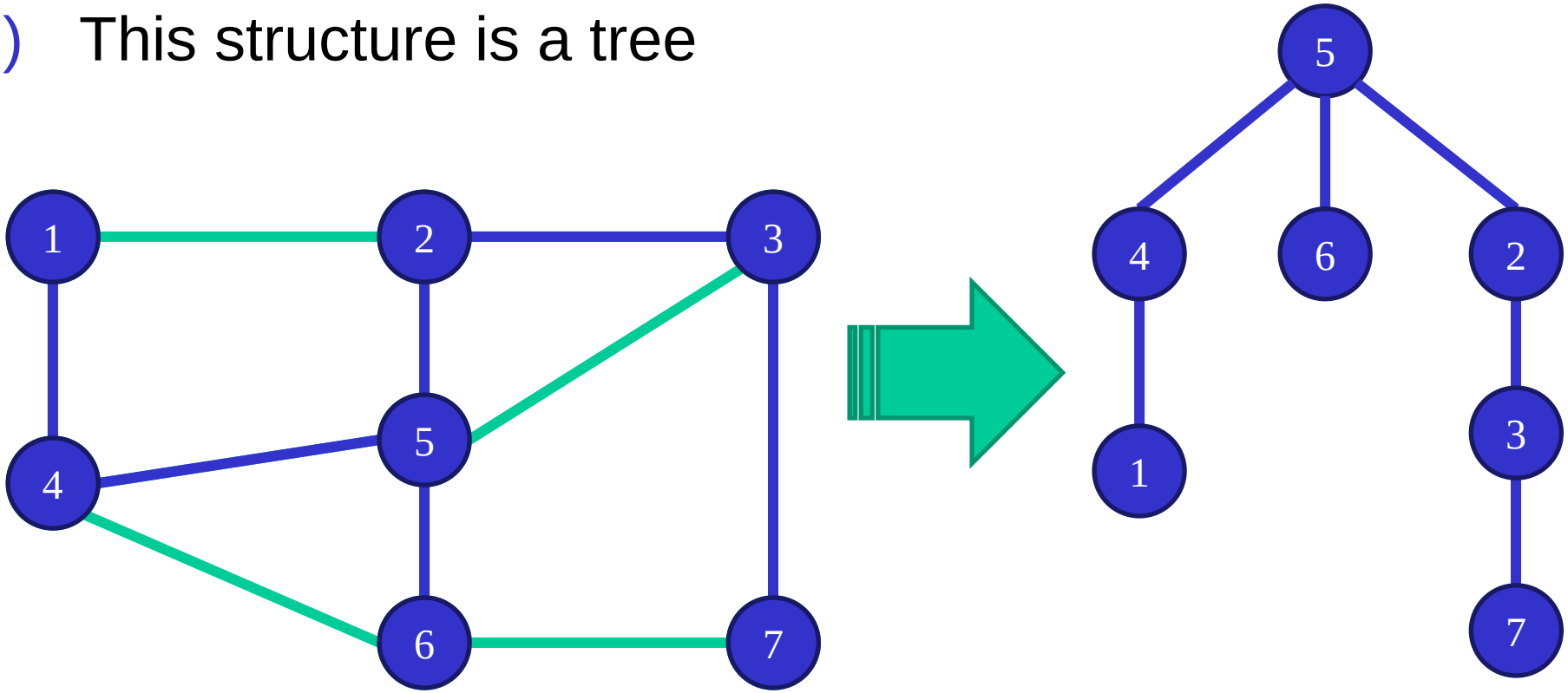


There should be *only one* path exist from the Source to Destination to avoid the loops at the data link layer.

Spanning Tree Definition

a) A subset of edges in a graph that:
   - Span all nodes
   - Do not create any cycles

b) This structure is a tree



802.1 Spanning Tree Approach

- Elect a bridge to be the root of the tree
- Every bridge finds shortest path to the root
- Union of these paths becomes the spanning tree

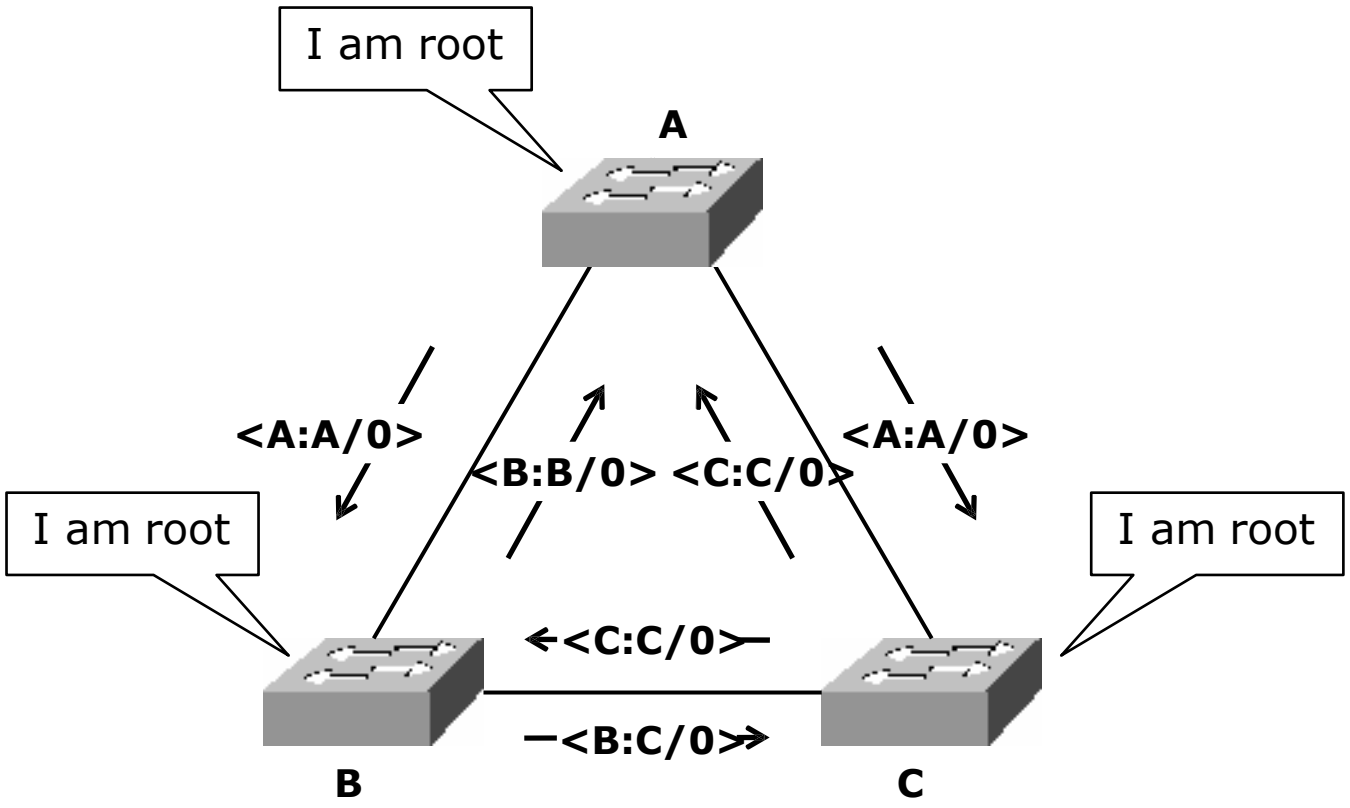
- Bridges exchange Configuration Bridge Protocol Data Units (BPDUs) to build the tree
  - Used to elect the root bridge
  - Calculate shortest paths
  - Locate the next hop closest to the root, and its port
  - Select ports to be included in the spanning trees

Definitions

- Bridge ID (BID) = <Random Number>
- Root ID: bridge with the lowest BID in the tree.
- Path Cost: cost (in hops) from a transmitting bridge to the root
- Each port on a bridge has a unique Port ID.
- Root Port: port that forwards to the root on each bridge
- Designated Bridge: the bridge on a LAN that provides the minimal cost path to the root
  - The designated bridge on each LAN is unique

Initial State

<designated Bridge ID: Root Path Cost/ Root ID>



Determining the Root

- Initially, all hosts assume they are the root.
- Bridges broadcast BPDUs:

- Based on received BPDUs, each switch chooses:
  - A new root (smallest known Root ID)
  - A new root port (what interface goes towards the root)
  - A new designated bridge (who is the next hop to root)

Comparing BPDUs

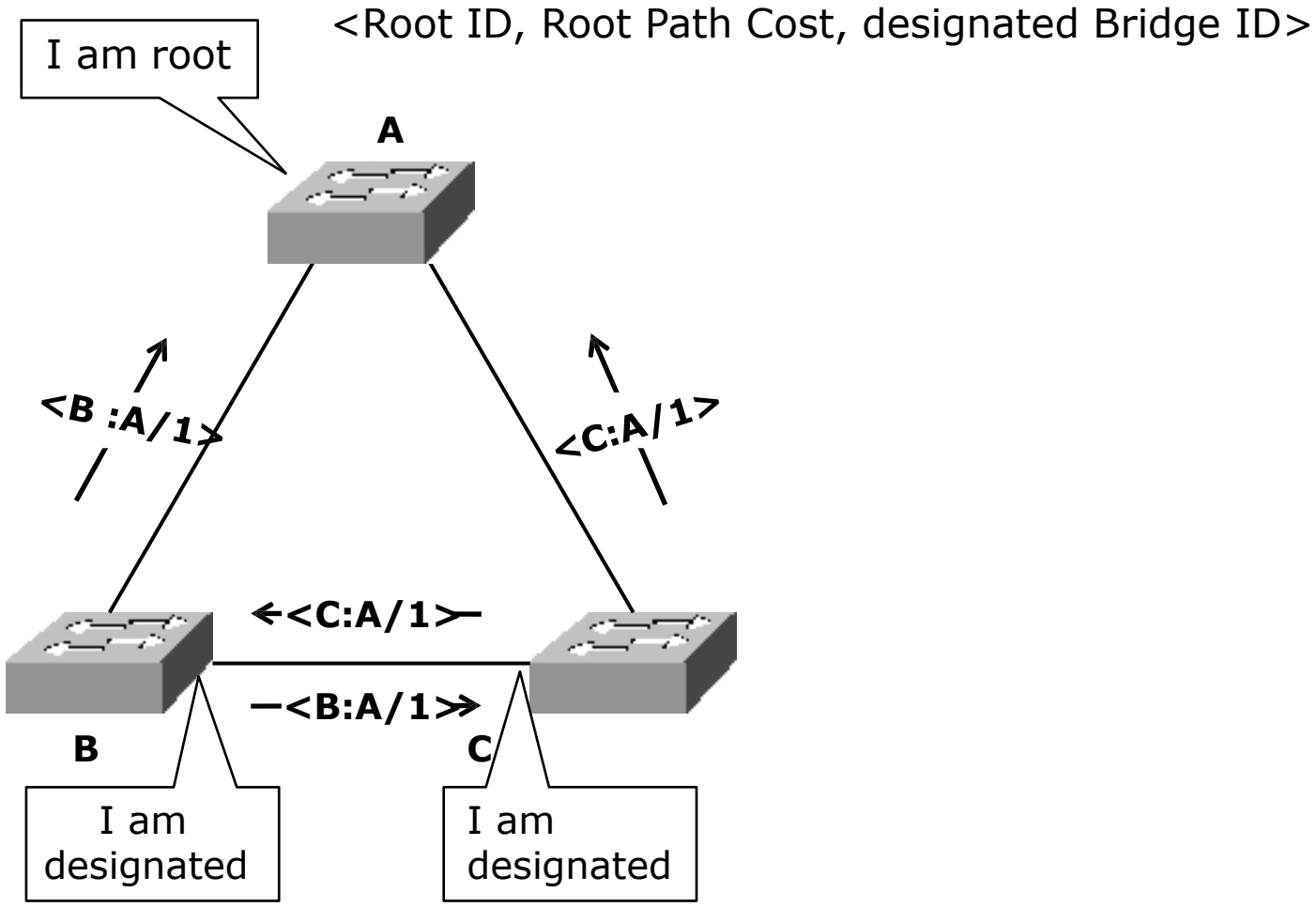
if R1 < R2: use BPDU1

else if R1 == R2 and Cost1 < Cost2: use BPDU1

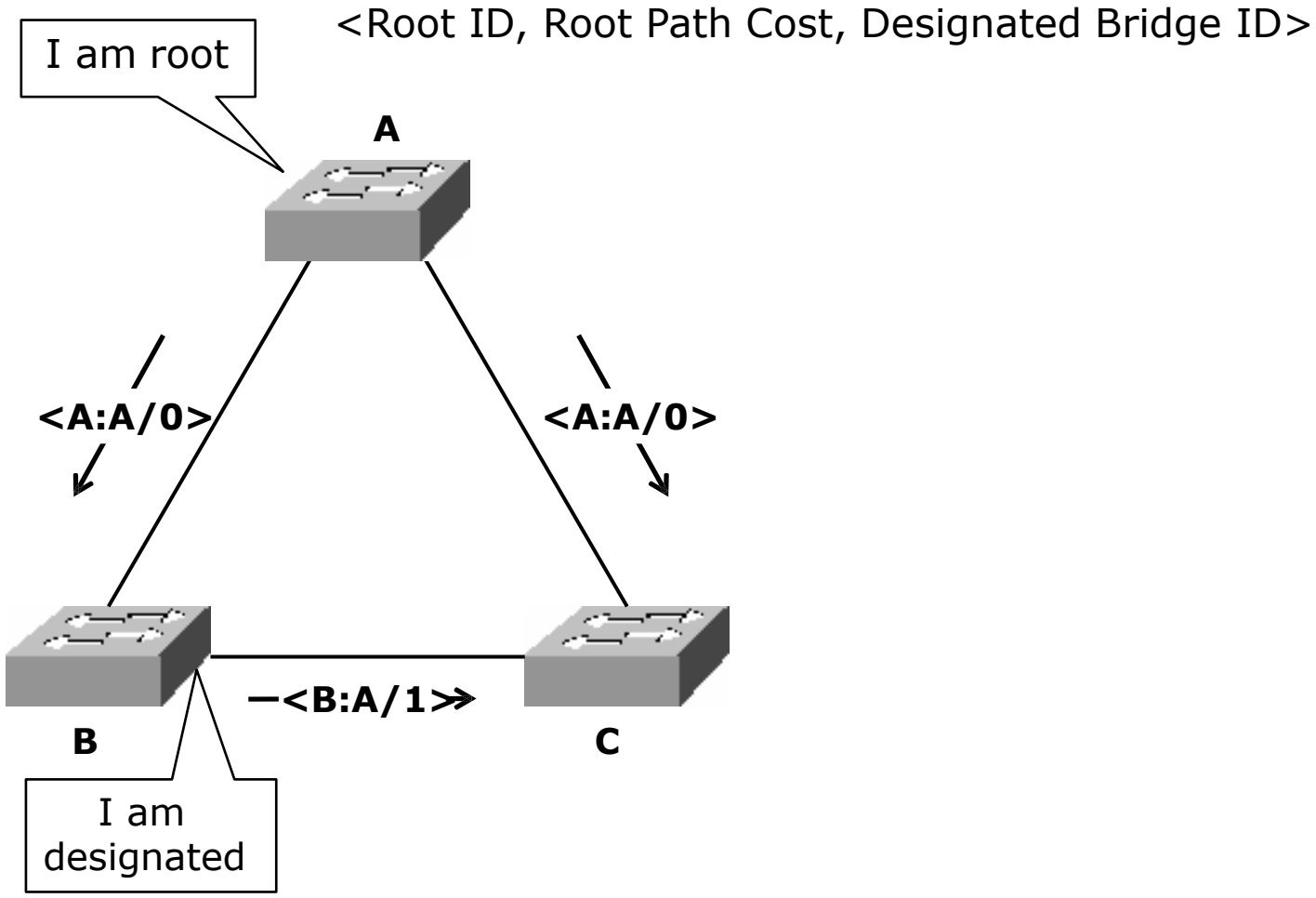
else if R1 == R2 and Cost1 == Cost 2 and B1 < B2: use BPDU1

else: use BPDU2

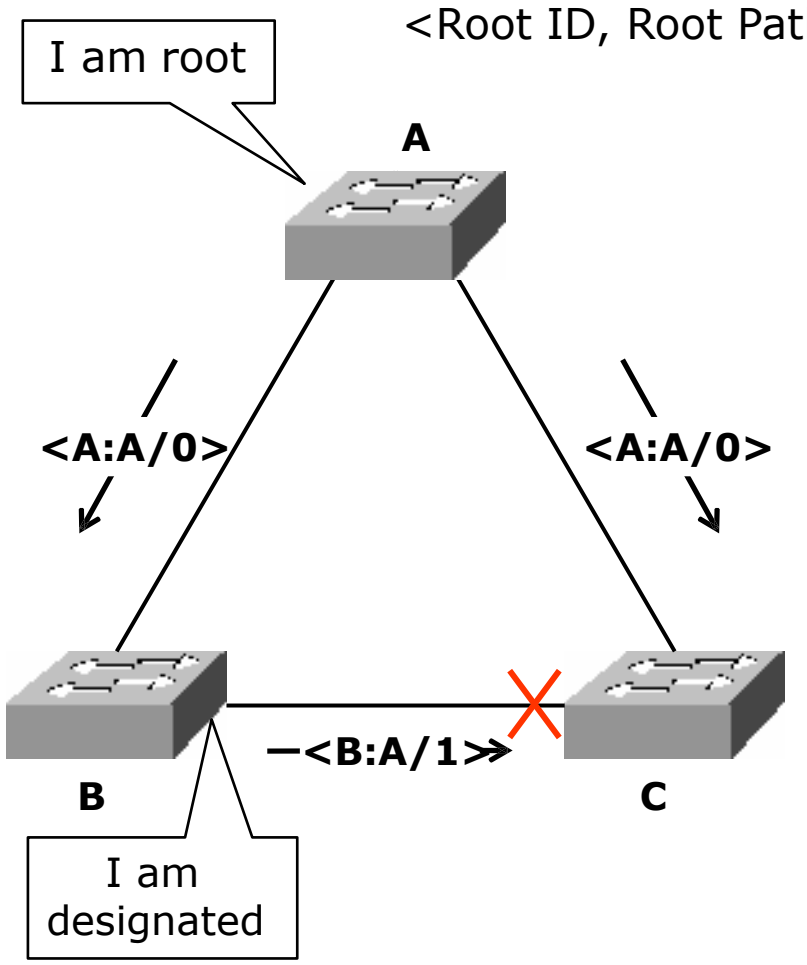
Root Bridge Recognized



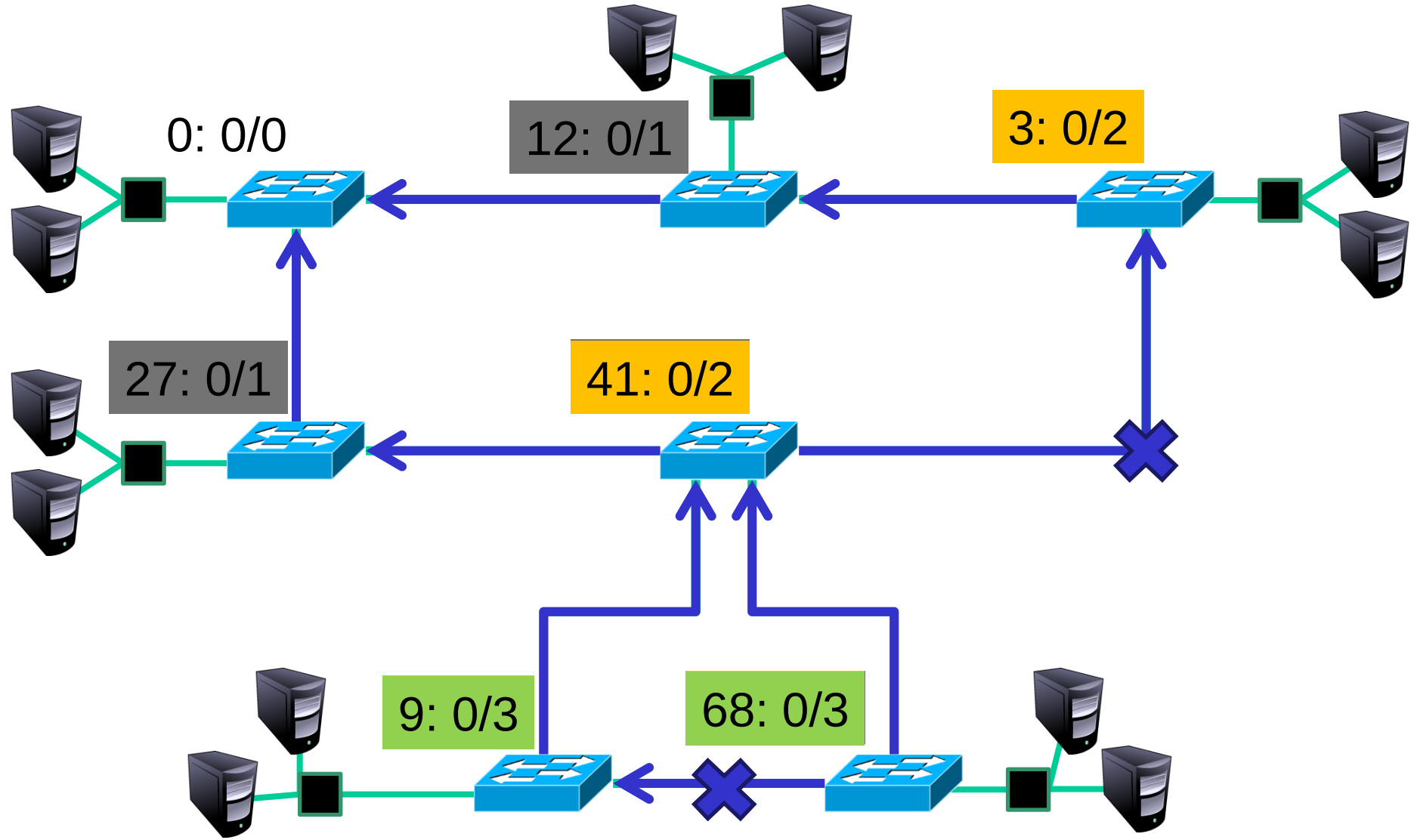
Designated Bridge Recognized



Ports Disabled



Spanning Tree Construction



A seven-bit Hamming code is received as 1111101. What is the correct code?

1. 1101111
2. 1011111
3. 1111111
4. 1111011

Which of the following combinations is correct?
a. MAC and IP addresses are used in network layer
b. MAC, IP addresses and port numbers are used in application layer
c. MAC is used in Data link layer, IP addresses and port numbers are used in network layer
d. MAC addresses are used in physical layer, IP in Network layer and port numbers in Transport layer

Question

What is the sender window size in selective-repeat protocol is _____, given **m** is the number of bits.

The size of the sender's window is **2^(m-1)**
The window size of the receiver is the same as that of the sender i.e. 2^(m-1)

1. We have categorized access methods into _____ groups.

A. two

B. three

C. four

D. five

three

3. In _____, the chance of collision can be reduced if a station senses the medium before trying to use it.

A. MA

B. CSMA

C. FDMA

D. CDMA

CSMA

5. _____ augments the CSMA algorithm to detect collision

A. CSMA/CA

B. CSMA/CD

C. either (a) or (b)

D. both (a) and (b)

CSMA/CD

21. In _____, the available bandwidth is divided into frequency bands.

A. FDMA

B. TDMA

C. CDMA

D. none of the above

FDMA

22. In _____, each station is allocated a band to send its data. In other words, each band is reserved for a specific station, and it belongs to the station all the time.

A. FDMA

B. TDMA

C. CDMA

D. none of the above

FDMA

26. In _____ each station sends a frame whenever it has a frame to send.

A. pure ALOHA

B. slotted ALOHA

C. both (a) and (b)

D. neither (a) nor (b)

Pure Aloha

27. In _____, the stations use different codes to achieve multiple access.

A. FDMA

B. TDMA

C. CDMA

D. none of the above

CDMA

28. In pure ALOHA, the vulnerable time is _____ the frame transmission time.

A. the same as

B. two times

C. three times

D. none of the above

Two times

30. The maximum throughput for pure ALOHA is _____ per cent.

A. 12.2

B. 18.4

C. 36.8

D. none of the above

18.4

36. In the _____ method, after the station finds the line idle, it sends its frame immediately. If the line is not idle, it continuously senses the line until it finds it idle.

A. nonpersistent

B. 1-persistent

C. p-persistent

D. none of the above

1-persistent

38. In the _____method, after the station finds the line idle it sends or refrain from sending based on the outcome of a random number generator. If the line is busy, it tries again

A. nonpersistent

B. 1-persistent

C. p-persistent

D. none of the above

P-persistent