Computer Network and Distributed Systems

MAC Sub Layer

- "Technically, the MAC sublayer is the bottom part of the data link layer, so logically we should have studied it before examining all the point-to-point protocols in Chap. 3. Nevertheless, for most people, it is easier to understand protocols involving multiple parties after two-party protocols are well understood. For that reason we have deviated slightly from a strict bottom-up order of presentation."

- *From - Computer Networks,*
- *Andrew S. Tanenbaum and David J. Wetherall*

Medium Access Control (MAC) Protocols

- Also called Random Access or Contention Protocols
- Protocol followed by nodes to decide who should transmit when
- No station is superior to another station and none is assigned the control over another
- No station permits, or does not permit, another station to send
- Any node may have data to transmit at any point of time
- Needs to avoid collision, i.e. two or more stations transmitting through the medium at the same time

Random Access Protocol Types

- ALOHA
- Carrier Sense Multiple Access (CSMA)
- Carrier Sense Multiple Access with Collision Detection (CSMA-CD)
- Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA)

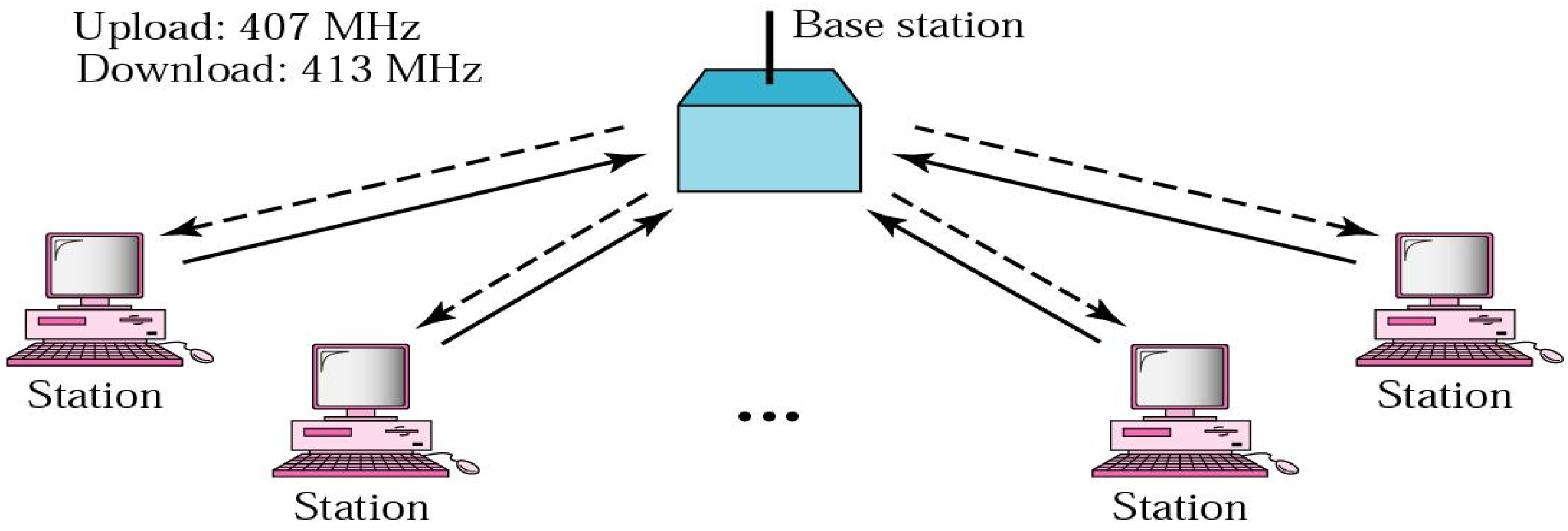
ALOHA

ALOHA

- Developed in University of Hawaii in early 70s
  - ❑Originally developed for packet radio networks
  - ❑Transmission to and from a central station
  - ❑All other sources transmit using same frequency, central station uses another frequency

- Whenever a station has a frame, it sends immediately
  - ❑Station listens for maximum round trip time (plus small increment) for ACK
  - ❑If ACK, fine. If not, wait for a random time and then retransmit frame
  - ❑If no ACK after repeated transmissions, give up

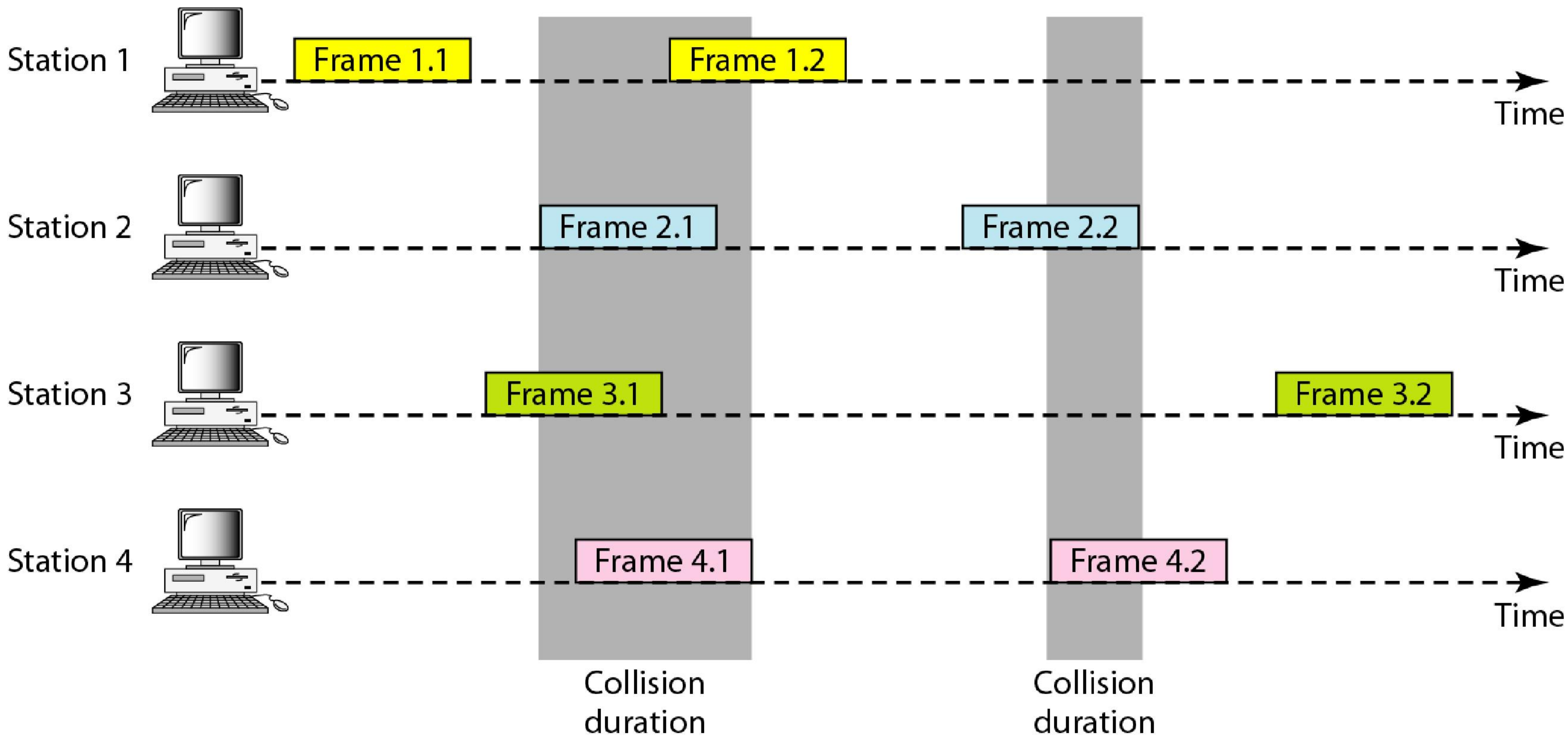
ALOHA network



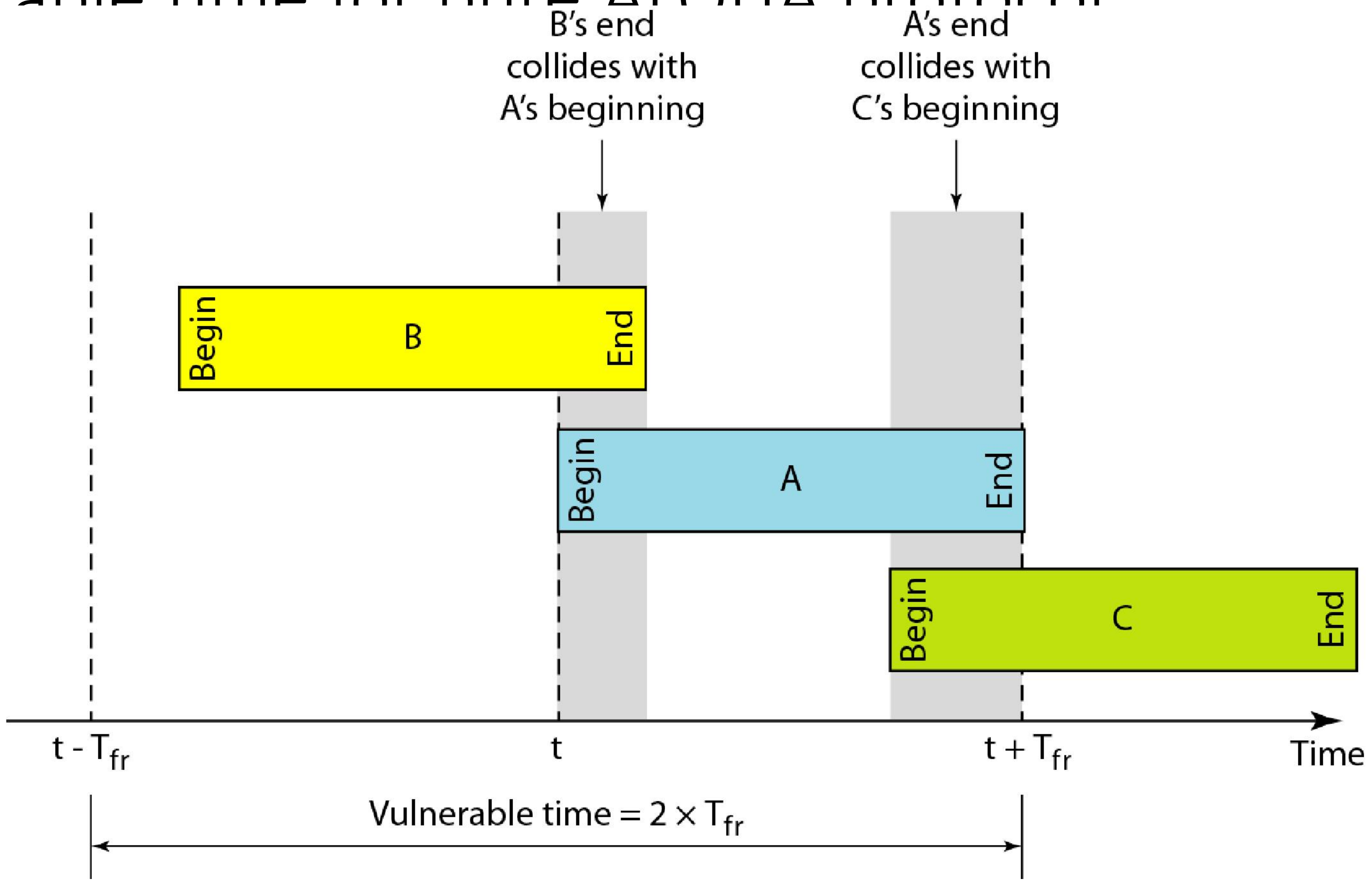
ALOHA (contd.)

- When a station receives a frame:
  - If frame ok (using FCS) and address matches this station, send ACK frame immediately
  - ACK frames sent on a different frequency
- Frame may become invalid due to noise, or because another station transmitted a frame at about the same time: collision
- How is collision detected?
  - If frame found to be invalid, receiver NOT send ACK
  - If no ACK received within some time, sender assumes collision
- Max utilization 18%, very low for large nos. of nodes or for higher transmission rates

Frames in a pure ALOHA network



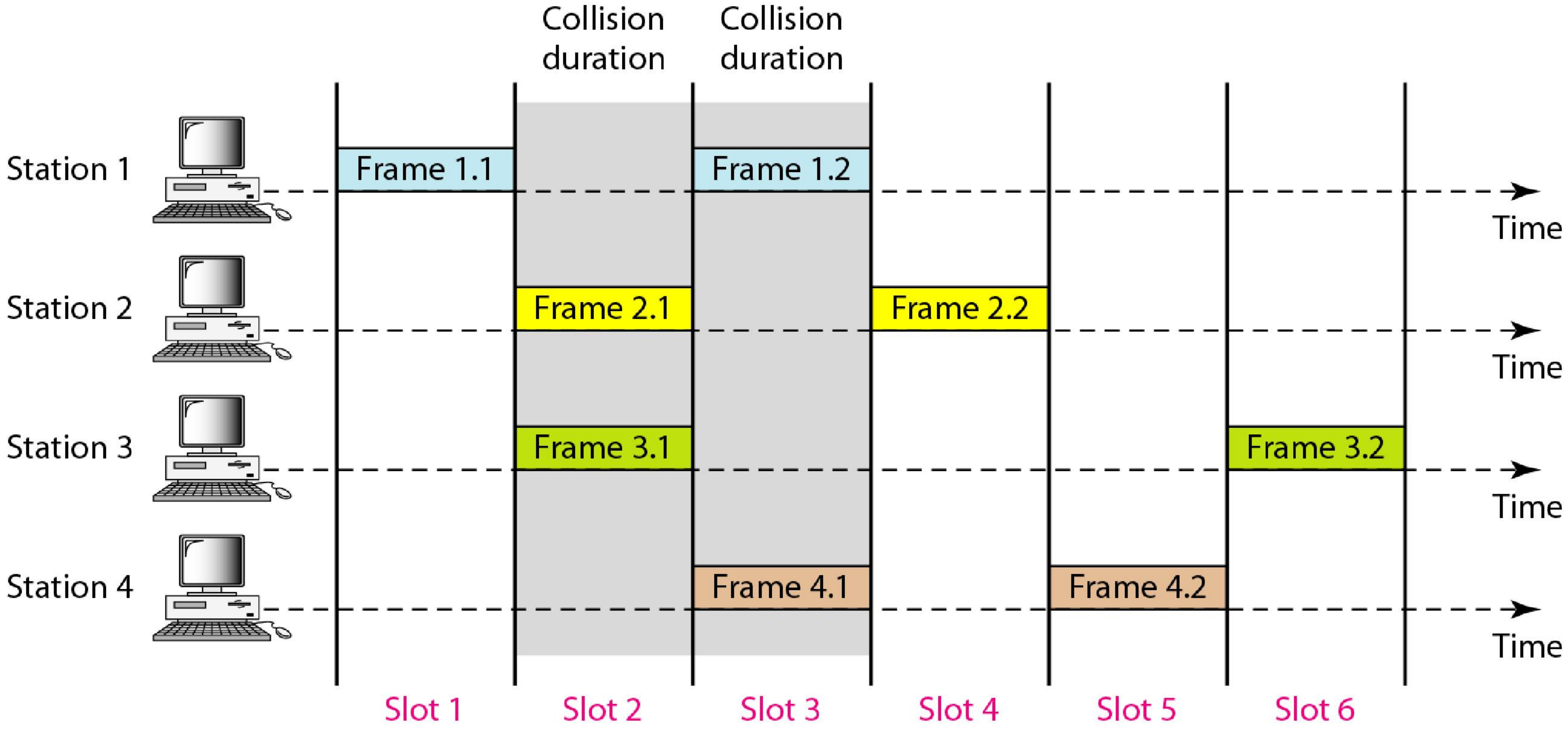
Vulnerable time for pure ALOHA protocol



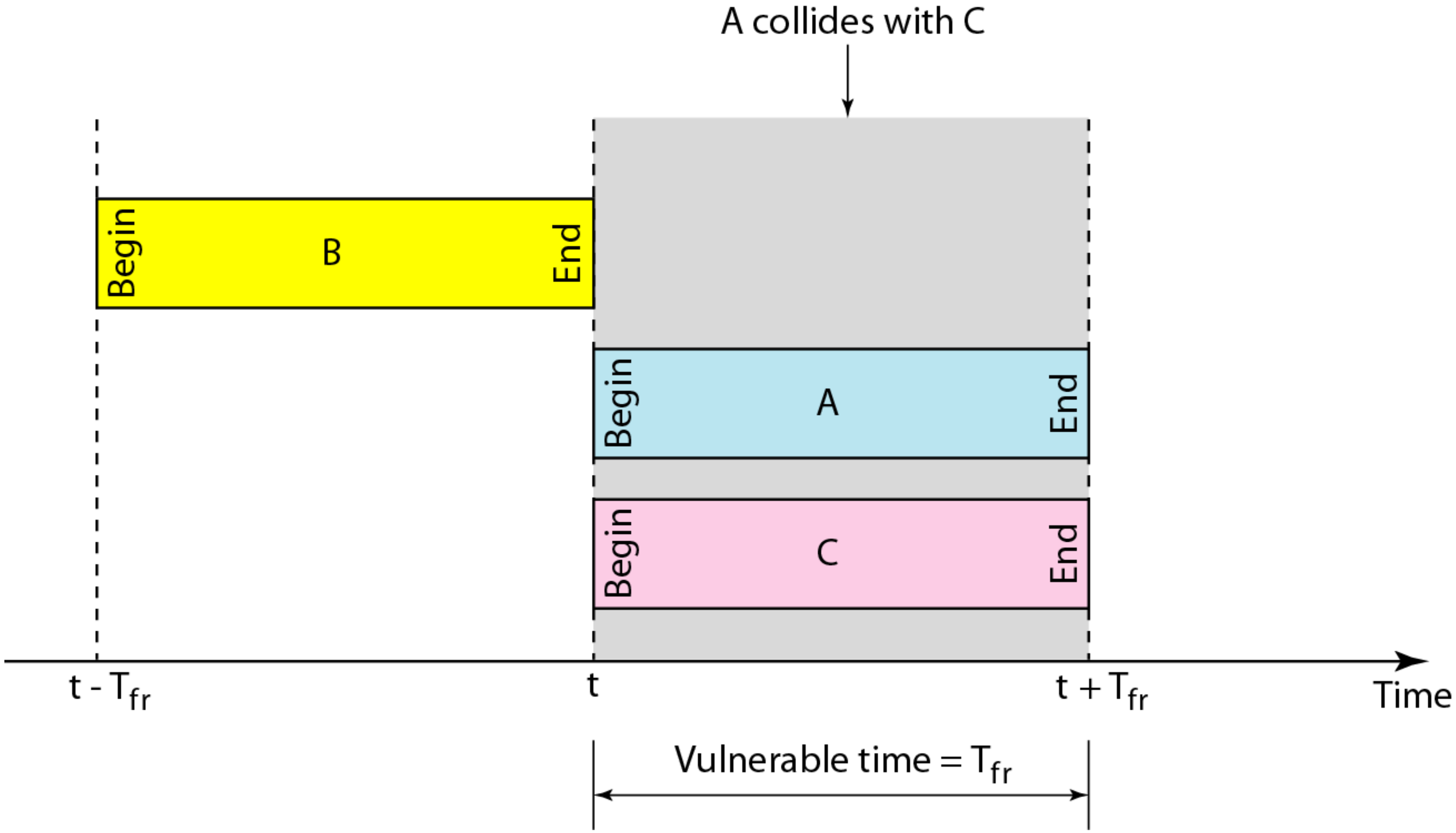
Slotted ALOHA

- Time on the channel divided into slots equal to frame transmission time
  - Needs central clock to synchronize all nodes
  - A source can start sending only at the beginning of a slot
- Reduces number of collisions over ALOHA
  - Contention period (time interval in which frames can overlap or collide) is halved compared to ALOHA
  - Collision possible only if more than 1 sources become ready to transmit within the same slot
- Max utilization 37%

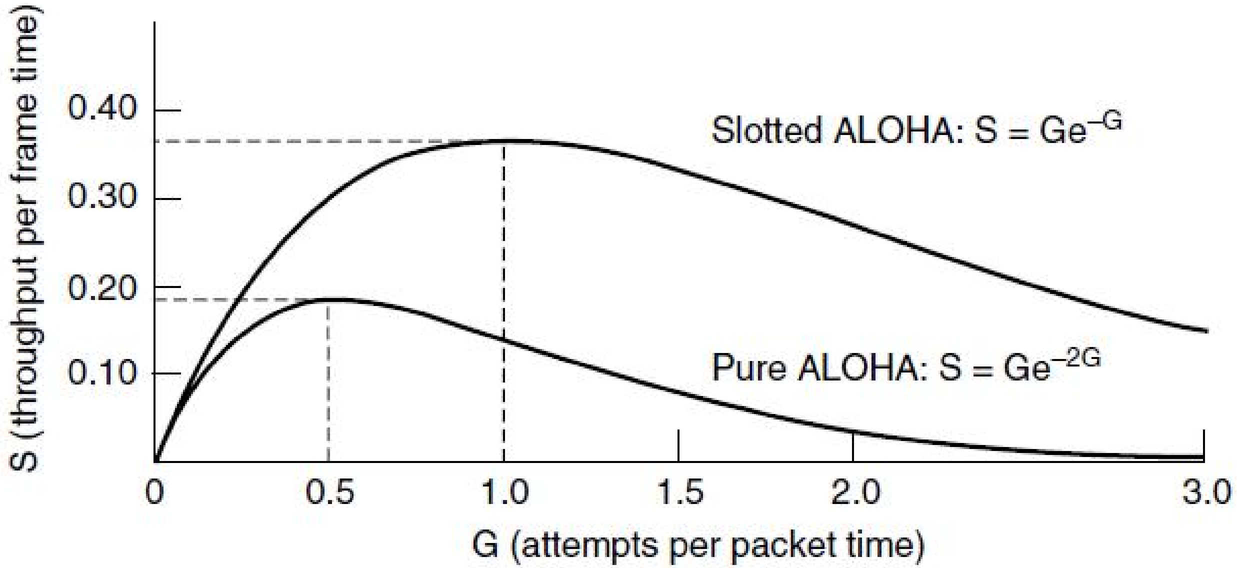
Frames in a slotted ALOHA network



Vulnerable time for slotted ALOHA protocol



Channel utilization of ALOHA and slotted ALOHA



Throughput versus offered traffic for ALOHA systems.

Carrier Sense Multiple Access (CSMA)

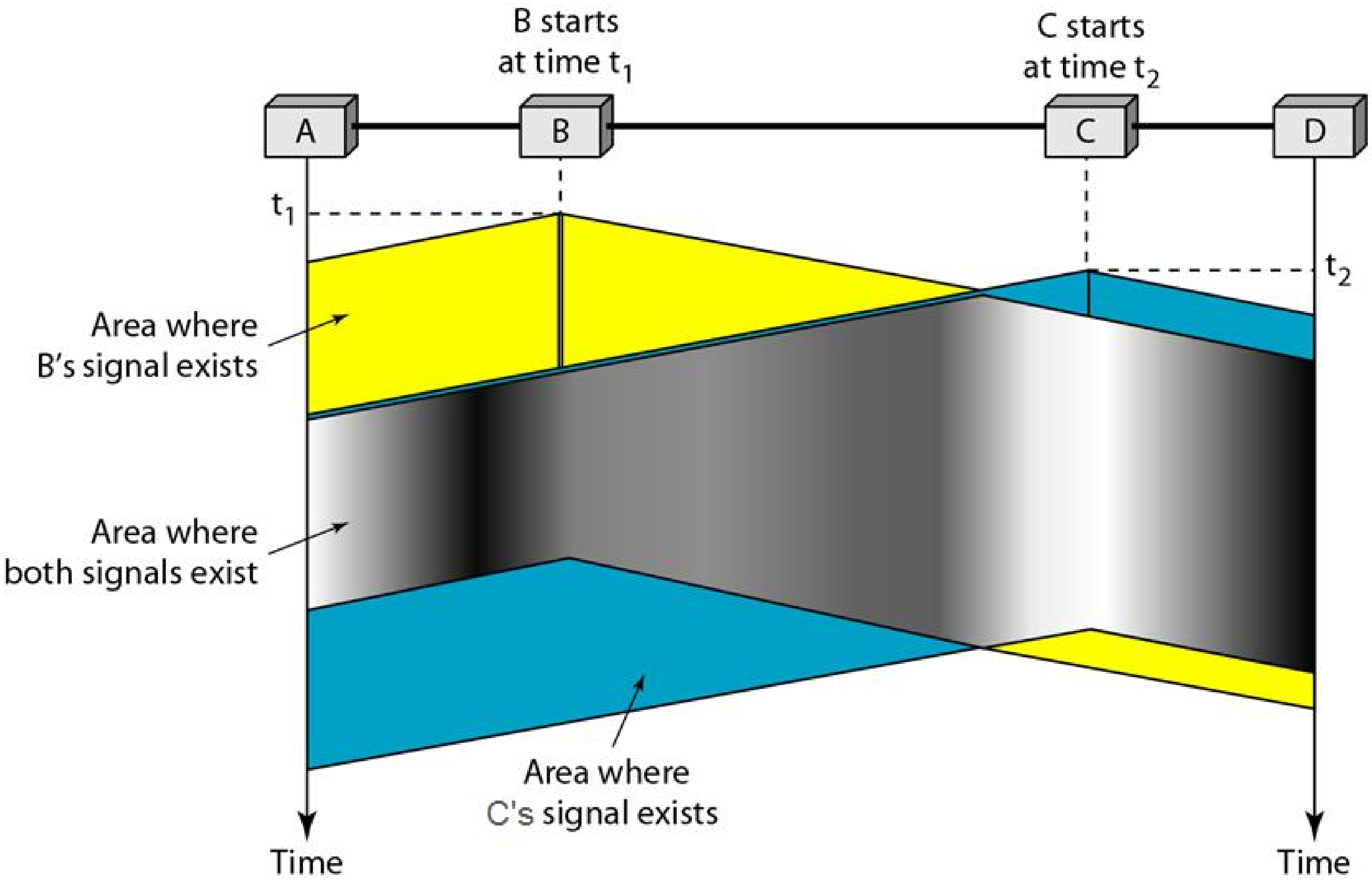
Carrier Sense Multiple Access (CSMA)

- Motivation
  - In most small networks, propagation time is much smaller compared to frame transmission time
- Whenever node N becomes ready to transmit a frame, sense the medium (carrier sense)
- If line idle, N <u>may</u> transmit frame immediately
- If line not idle
  - Alternatives: non-persistent, 1-persistent, p-persistent
  - Tradeoff between line utilization and chance of collision

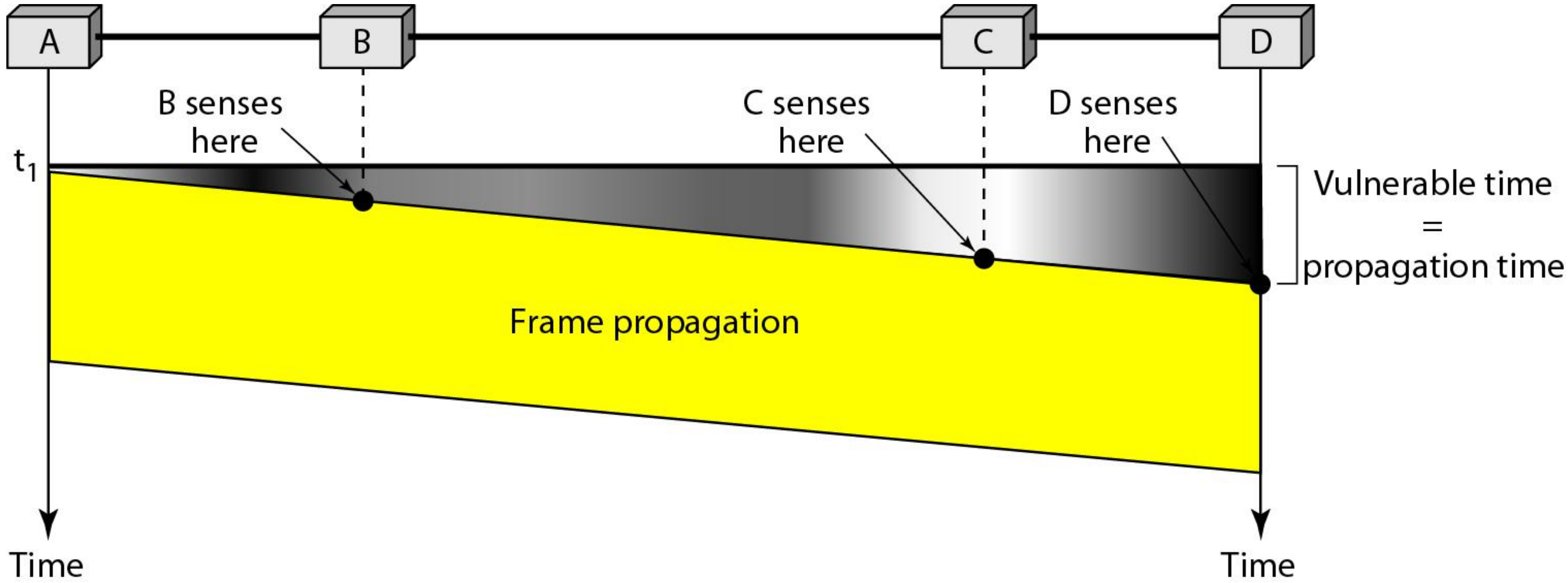
CSMA: collisions

- After transmitting, station waits for ACK for a reasonable time
  - RTT + some allowance (because Rx must also contend for the channel in order to send ACK)
- If no ACK, then repeat process for transmitting
  - Sense medium; if idle, transmit; else wait …
- Collision occurs if another node N’ starts transmitting within the time it takes for the first bit sent by N to reach this node N’ (within the propagation delay)

Space/time model of the collision in CSMA



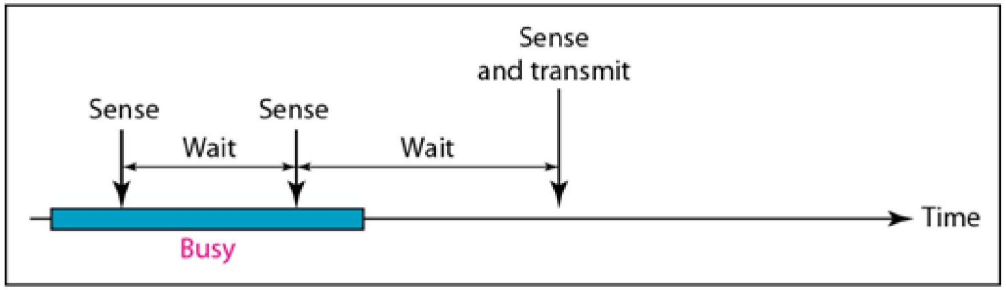
Vulnerable time in CSMA

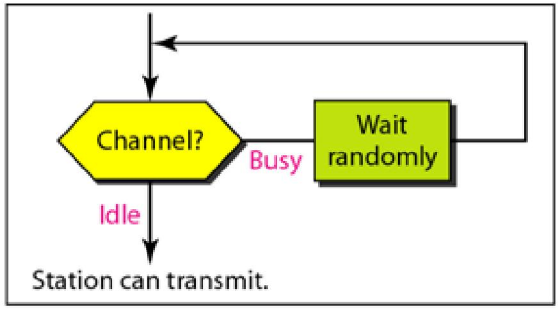


CSMA – what must a node do if line is busy

- Non-persistent CSMA

1. sense medium
2. if medium idle
   - ✓transmit frame
3. else (if medium busy)
   - ✓wait for a random time
   - ✓repeat from step 1





CSMA – what must a node do if line is busy (Contd)

•p-persistent CSMA, 0≤p≤1

1.sense medium

2.if medium idle,

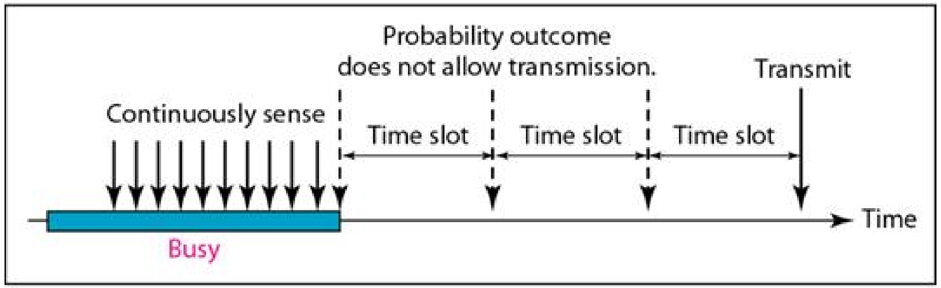
✓transmit frame with probability p, or

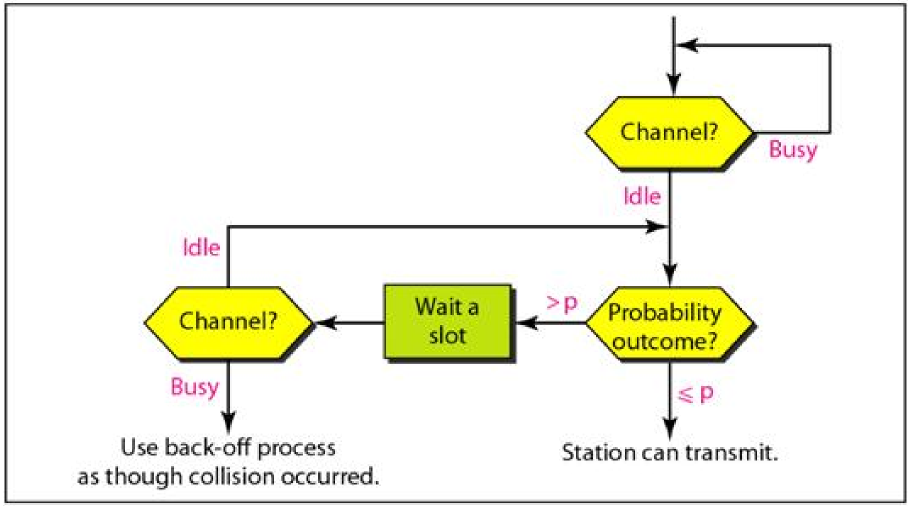
✓Delay one time slot with probability q = 1-p and repeat from step 1

3.else (if medium busy)

✓continue to sense medium until it is idle

✓after medium becomes idle, repeat from step 2



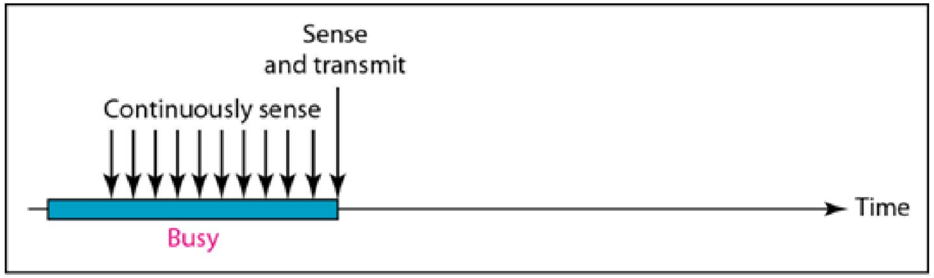


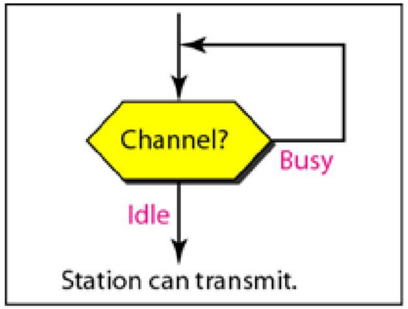
CSMA – what must a node do if line is busy (Contd 2)

•1-persistent CSMA : Special case of p-persistent (with p=1)

1. Sense medium
2. if medium idle
   - transmit frame
3. else (if medium busy)
   - continue to sense medium until it is idle
   - transmit frame as soon as medium found idle

•If two or more stations waiting to transmit, surely collision





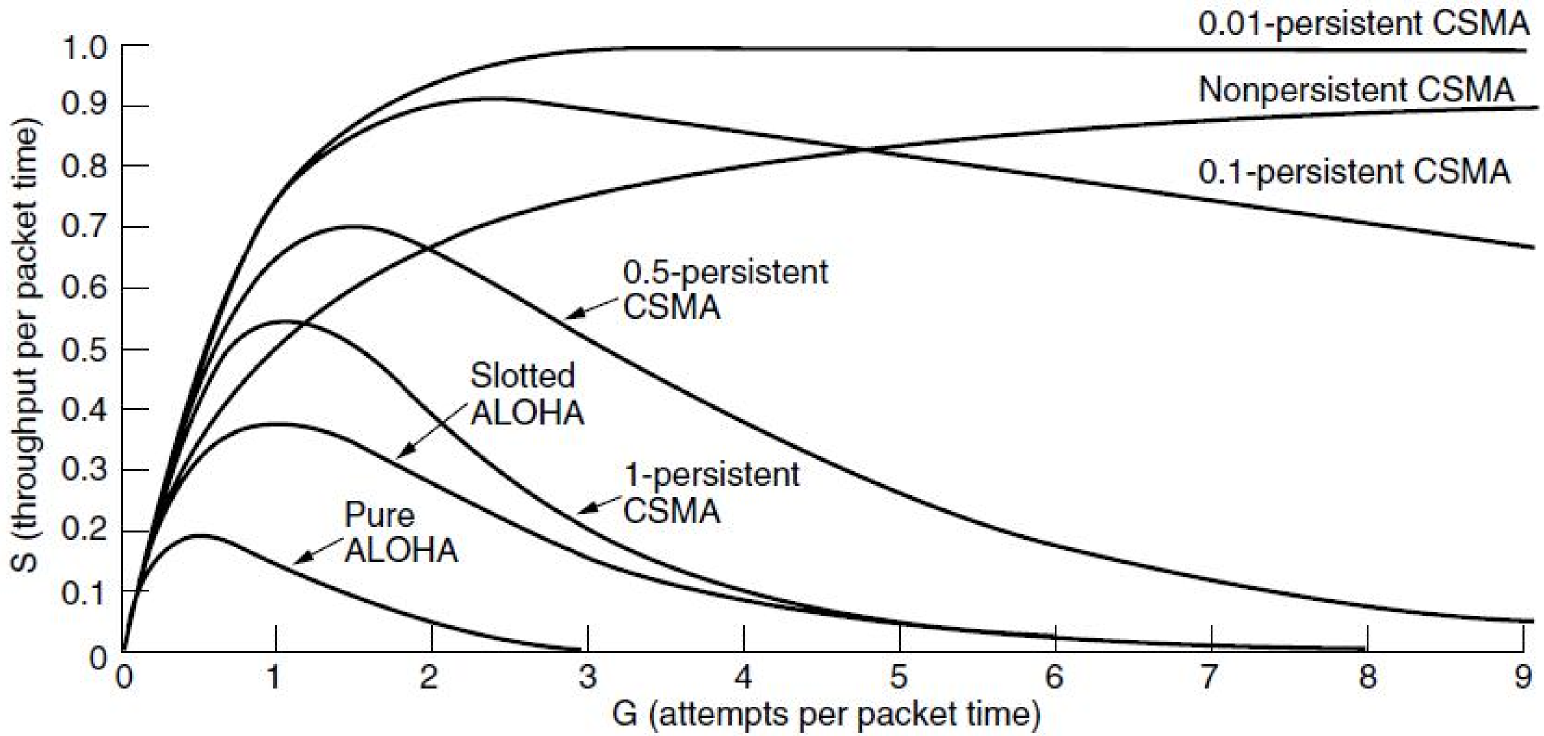
Evaluation of CSMA

- Low values of p
  - Lower chances of collision
  - But, lower channel utilization (medium will generally remain idle after the end of a transmission even if there are one or more stations ready to transmit)

- Higher values of p
  - Good channel utilization
  - But, more chances of collision

- 1-persistent
  - Low load: good (prevents unnecessary wait without sensing medium)
  - High load: higher chances of collision

Channel utilization of MAC protocols



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

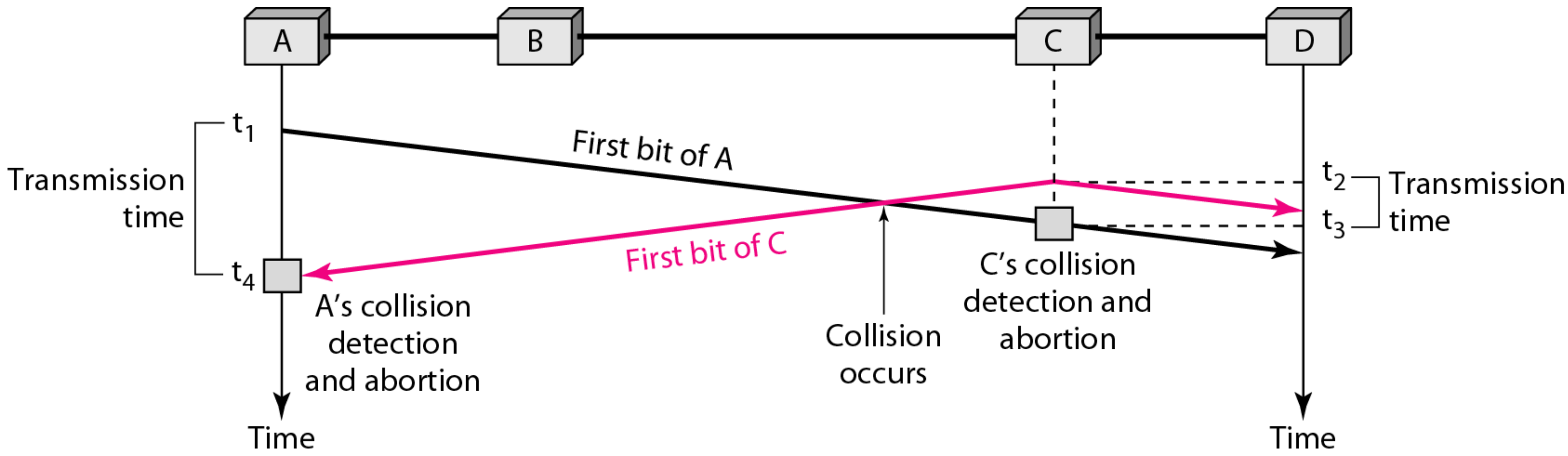
Carrier Sense Multiple Access – Collision Detection (CSMA-CD)

CSMA/CD

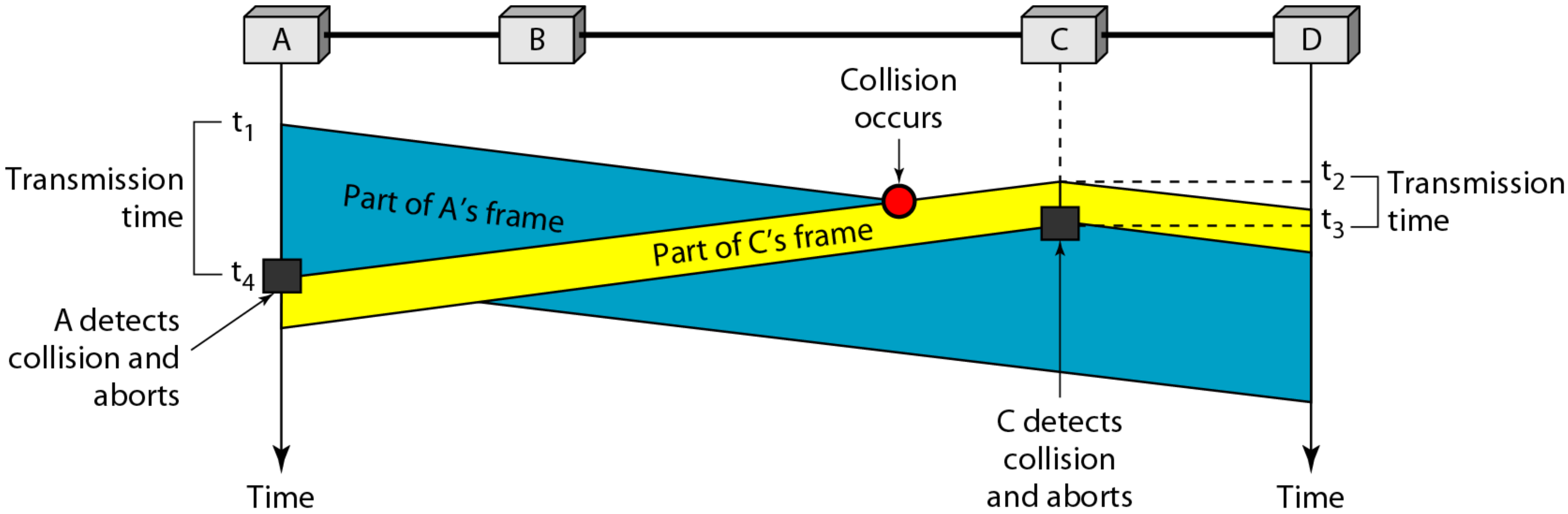
- When node N is ready to transmit

1. Sense medium
2. If medium busy
   - apply standard CSMA using value of p set apriori
3. If medium idle
   - transmit, listen while transmitting
   - If collision detected during transmission
     - ✓ Transmit a brief jamming signal (specified by protocol) to ensure that all stations know there has been a collision
     - ✓ After sending jamming signal, wait for a random amount of time (binary exponential backoff),
     - ✓ Then repeat all above steps starting from step 1

Collision of the first bit in CSMA/CD



Collision and abortion in CSMA/CD



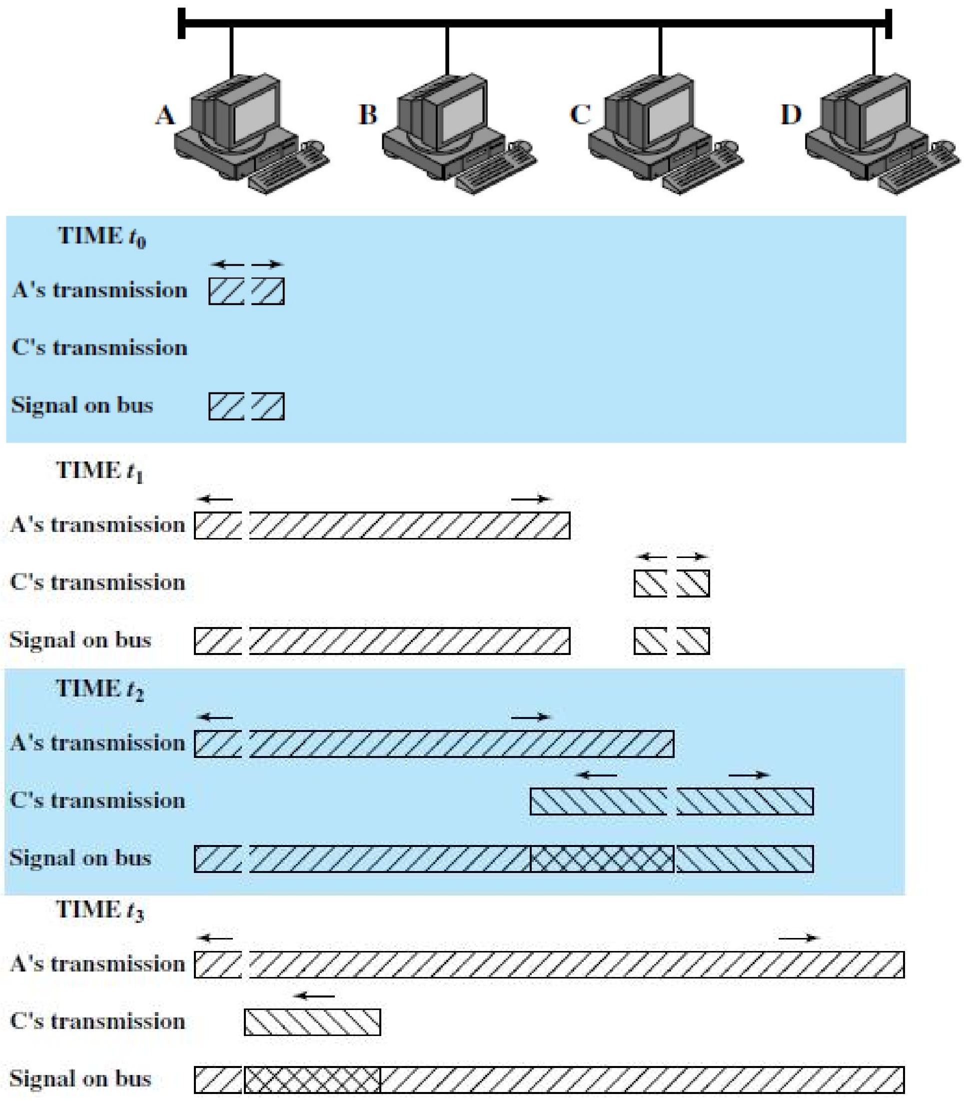
CSMA/CD Operation

At time ***t0***, station A begins transmitting a packet addressed to D.

At ***t1***, both B and C are ready to transmit. B senses a transmission and so defers. C, however, is still unaware of A's transmission and begins its own transmission

At ***t2***, when A's transmission reaches C, at C detects the collision and ceases transmission

At ***t3***, the effect of the collision propagates back to A, and then A ceases transmission



Ethernet Frame Format (*to be discussed later*)

PA	SFD	DA	SA	LEN	LLC PDU	PAD	FCS	IEEE 802.3
PA		DA	SA	Type	DATA	PAD	FCS	DIX Ethernet
7	1	6	6	2	46-1500		4	

- ❖ PA: Preamble --- 7 bytes 10101010s for synchronization
- ❖ SFD: Start of frame delimiter --- 10101011 to start frame
- ❖ DA, SA: Destination & source MAC address
- ❖ LEN: Length --- number of data bytes
- ❖ Type: Identify the higher-level protocol
- ❖ LLC PDU + Pad: minimum 46 bytes, maximum 1500
- ❖ FCS: Frame Check Sequence, using CRC

CSMA/CD and Minimum Frame Size

For CSMA/CD to work, there is a need a restriction on the frame size

- Before sending the last bit of the frame, the sending station must detect a collision(if any) and abort the transmission, because
  - once the entire frame is sent, sender does not keep a copy of the frame
  - and does not monitor the line for collision detection
- Therefore, the frame transmission time T_{fr} must be at least two times the maximum propagation time T_p. **But Why ?**
  - Consider the worst-case scenario - the two stations involved in a collision are the maximum distance apart
    - ✓ the signal from the first takes time T_p to reach the second
    - ✓ and the effect of the collision takes another time T_p to reach the first
- So the requirement is that the first station must still be transmitting after $2T_p$

CSMA/CD and Minimum Frame Size

A network using CSMA/CD has a bandwidth of 10 Mbps. If the maximum propagation time (*including the delays in the devices and ignoring the time needed to send a jamming signal*) is 25.6 μs, what is the minimum size of the frame?

Solution:

- The frame transmission time is atleast $T_{fr} = 2 \times T_p = 51.2$ μs.
  - This means, in the worst case, a station needs to transmit for a period of 51.2 μs to detect the collision.
- The minimum size of the frame is 10 Mbps × 51.2 μs = 512 bits or 64 bytes.
- This is actually the minimum size of the frame for Standard Ethernet

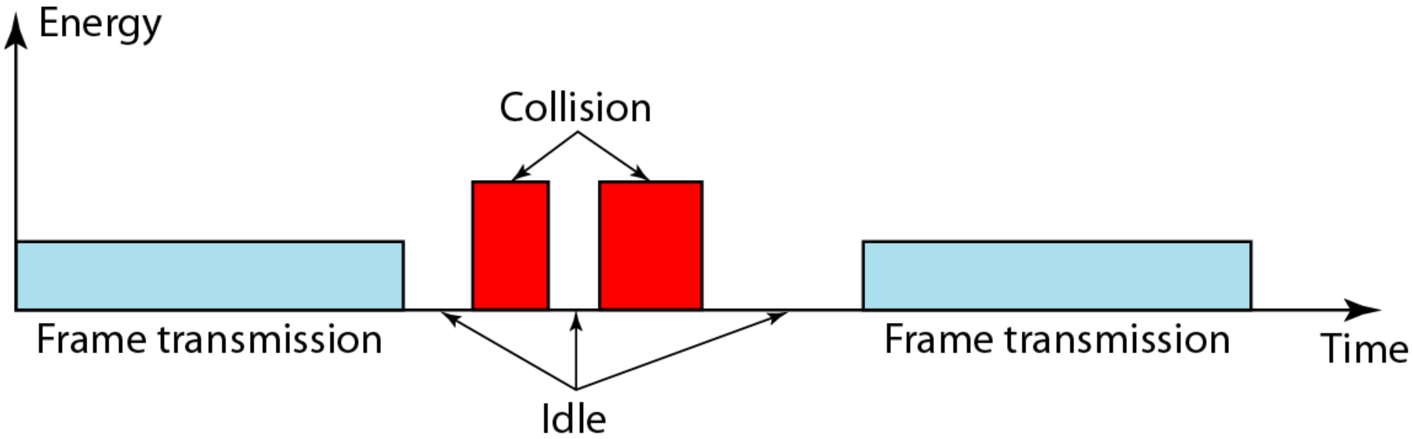
CSMA/CD and Maximum Frame Size

The standard defines the maximum length of a frame (without preamble and SFD field) as 1518 bytes. If we subtract the 18 bytes of header and trailer, the maximum length of the payload is 1500 bytes.

It has two historical reasons

- First, memory was very expensive when Ethernet was designed: a maximum length restriction helped to reduce the size of the buffer.
- Second, the maximum length restriction prevents one station from monopolizing the shared medium, blocking other stations that have data to send.

Contention, transmission, or idle state and their energy level in CSMA/CD

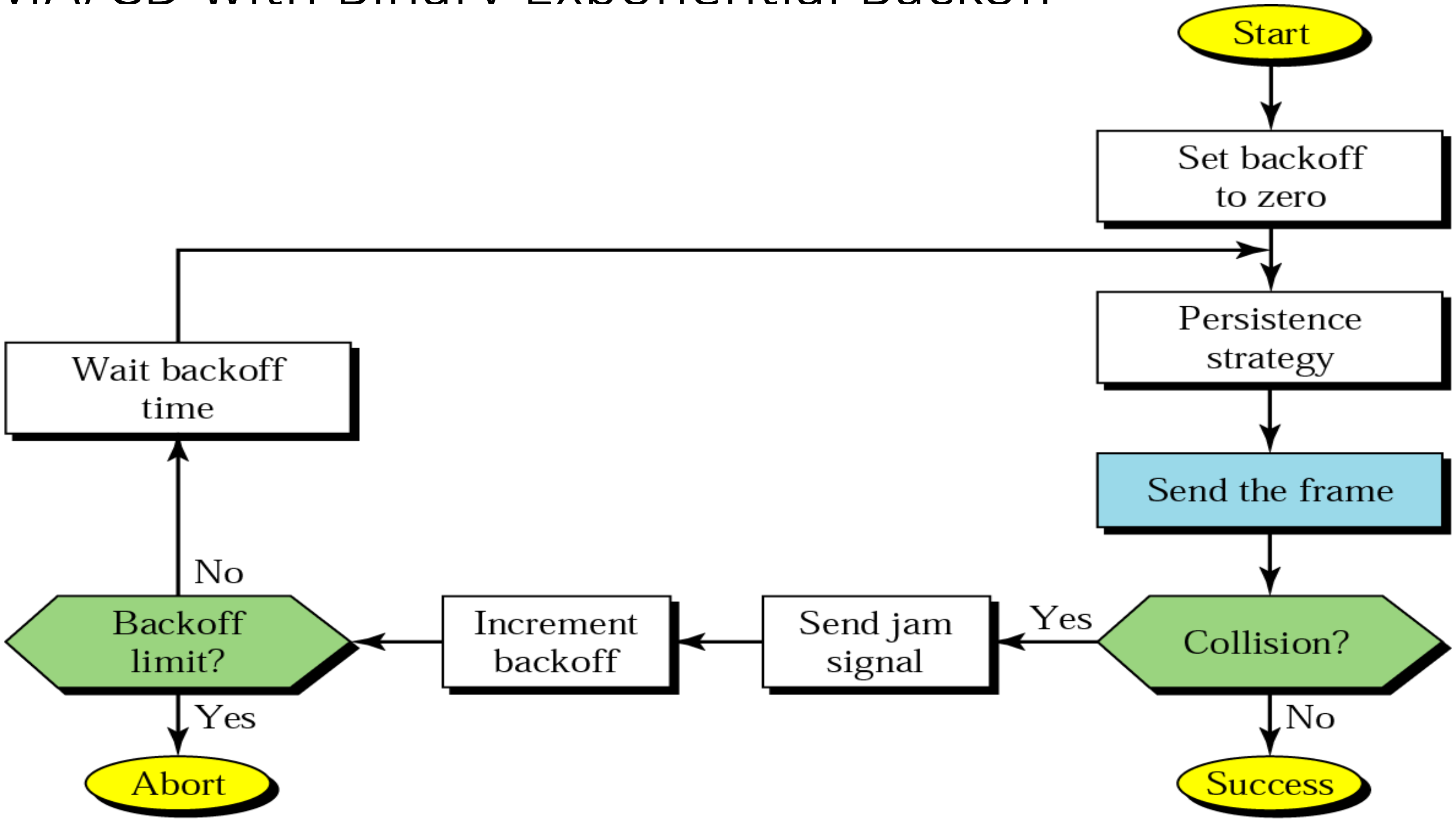


Binary exponential backoff algorithm

- After collision has been detected, waiting time must be adaptive to load
  - Low load => low wait time (high wait time may cause low channel utilization)
  - High load => relatively high wait time (low wait time may cause frequent collisions)

- How to estimate load? By number of repeated collisions
  - After k collisions, choose a waiting time randomly between $0,1,2,\ldots,2^k-1$ slots, $k<=10$
  - After 10 collisions, for $10 <= k <= 16$, choose a waiting time between 0 and $2^{10}-1$
  - After 16 collisions, give up

CSMA/CD with Binary Exponential Backoff



Carrier Sense Multiple Access - Collision Avoidance (CSMA-CA)

For Your Study

Computer Network and Distributed Systems

Local Area Network

Local Area Network (LAN)

- Characteristics
  - Small geographical area, limited distance
  - Small number of directly-connected machines
  - Relatively high data rate
  - Single management
- Specifications mostly at physical layer and data link layer

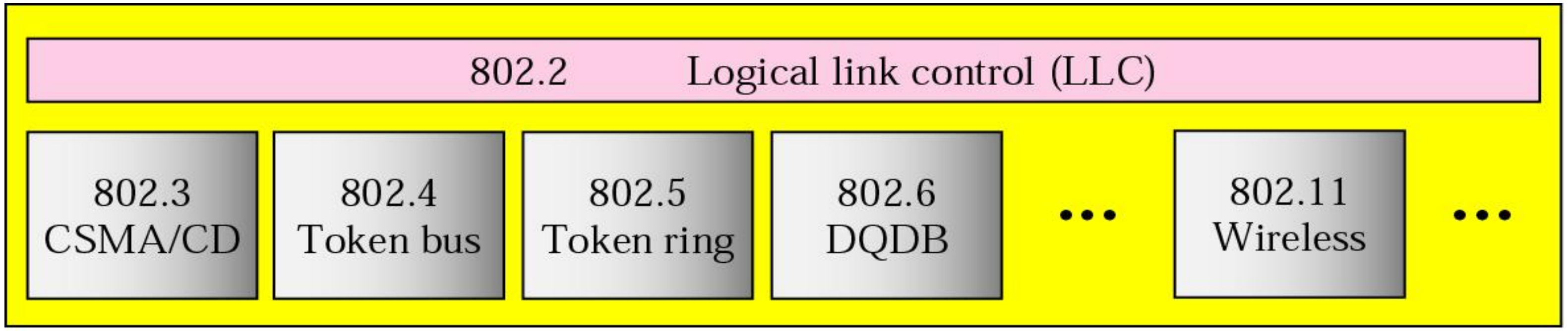
- The most used example: Ethernet
- Developed in early/mid 70's in Xerox PARC

Ethernet – two standards

- DIX standard
  - **D**igital / **I**ntel / **X**erox standardized 10 Mbps Ethernet in early 80's
  - Specifies details of physical layer and MAC layer using CSMA/CD

- IEEE 802 standard (1985) split Data Link layer into two sub-layers
  - Logical Link Control: error control, flow control, etc
  - Medium Access Control: error detect (FCS), decides how to access shared medium (CSMA/CD, token ring, wireless, …)

IEEE 802 family of protocols



Project 802

IEEE 802.2 plus one of 802.3, 802.4, … specifies the complete physical & data link layers

Relation between DIX Ethernet standard and IEEE 802 standard

- Frame format for both standards almost same, except for small differences

- TCP/IP implementations use original DIX Ethernet frame format, LLC sub-layer used not used
  - Network layer directly uses Ethernet frames

- Nodes using both types can coexist on same LAN

No LLC

- In real-world *wired* networks (most use TCP/IP), the LLC sub-layer almost never implemented
  - Error & flow control has to be handled from source to destination (over multiple links)
  - Data can be lost within links and at intermediate nodes
  - LLC controls error & flow over a single link only

  - So, ensure error & flow control from source to destination (end nodes) at higher layers, and
  - Do away with the LLC sub-layer

IEEE 802.3 (CSMA/CD)

- Multiple types within this depending on speed, media type, etc
  - Standard 10 Mbps Ethernet versions
    - 10Base5 : 10 Mbps, thickwire coaxial cable
    - 10Base2 : 10 Mbps, thinwire coax or cheapernet
    - 10Base-T : 10 Mbps, twisted pair, hub-based
    - 10Base-FL : 10 Mbps, optical fiber, hub-based
  - Fast Ethernet (100 Mbps) versions
  - Gigabit Ethernet (1000 Mbps) versions
- All the above have the same frame format, same addressing format
  - differences mostly in physical layer details like medium, connector, encoding used, etc

Bus topology – used in Ethernet

- Transmission propagates throughout medium, heard by all stations (bi-directional medium)
  - Each station needs unique address
- Signal balancing
  - Signal must be strong enough to meet receiver's minimum signal strength requirements
- Need to regulate transmission
  - To avoid collisions
  - To avoid hogging by a single node, break data into frames
- Multiple segments can be joined by repeaters

Repeaters

- Joins two (or more) segments of cable
- Function
  - Input signal at one of the ports
  - Extracts data from input signal (filters out noise)
  - Amplifies data: encodes data in signal and transmits along all other ports
- Does not understand frame format, does not look inside frame
- There should be only one path of segments and repeaters between any two stations

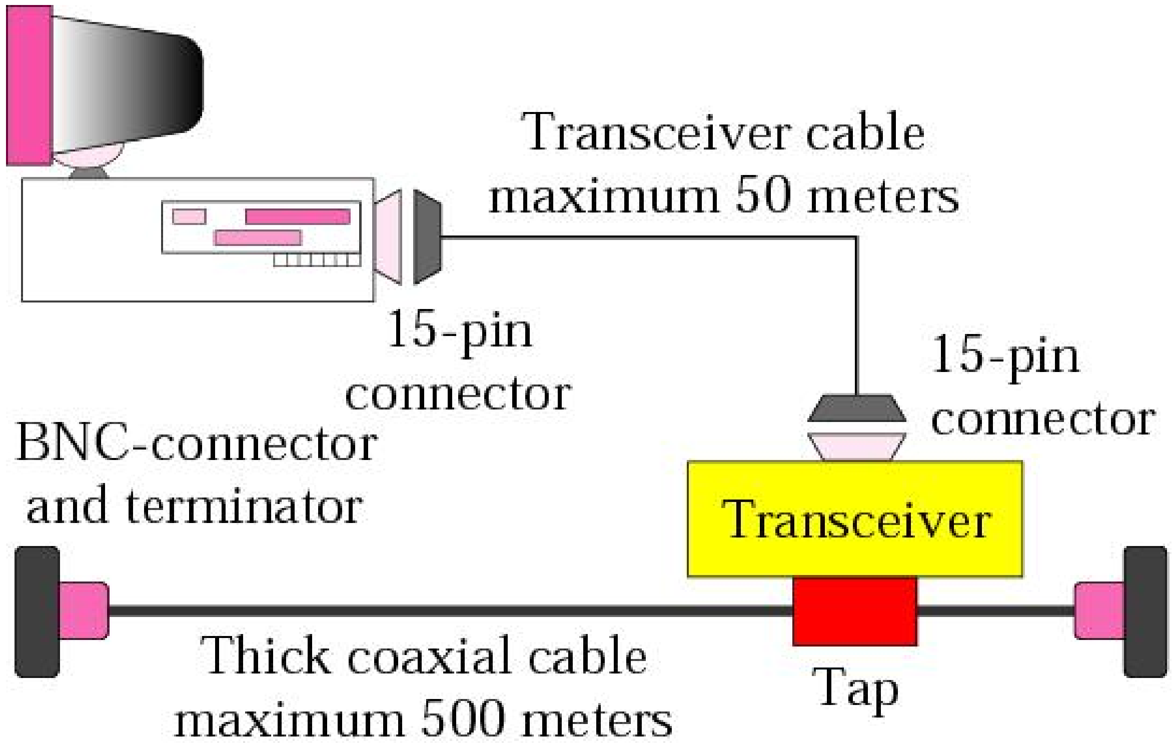
Example of a specific technology: 10Base5

- 10Base5 is the original implementation of Ethernet and 802.3
- Uses shared bus medium – thick coaxial cable (0.4 inch diameter) at 10 Mbps
  - Bus topology
  - Max cable length 500m between repeaters
  - Maximum 4 repeaters => maximum distance between two nodes is 2500 meters
- Distance between taps (nodes): a multiple of 2.5m
  - Hence, maximum 1000 taps
- Manchester encoding used

10Base5 technology (contd.)

- How to sense carrier (to see if line is idle)
  - Is there a transition in the middle of bit-time?
- How to detect collision
  - If two signals overlap, the average DC voltage increases above a threshold value
- Jamming signal
  - 32 or 48 bits of 01010101…
- How to understand end of frame
  - Is there a transition in the middle of bit-time?
- MAC layer specification
  - 1-persistent CSMA/CD for transmission
  - binary exponential backoff for retransmission

Connection of a station to the medium using 10Base5

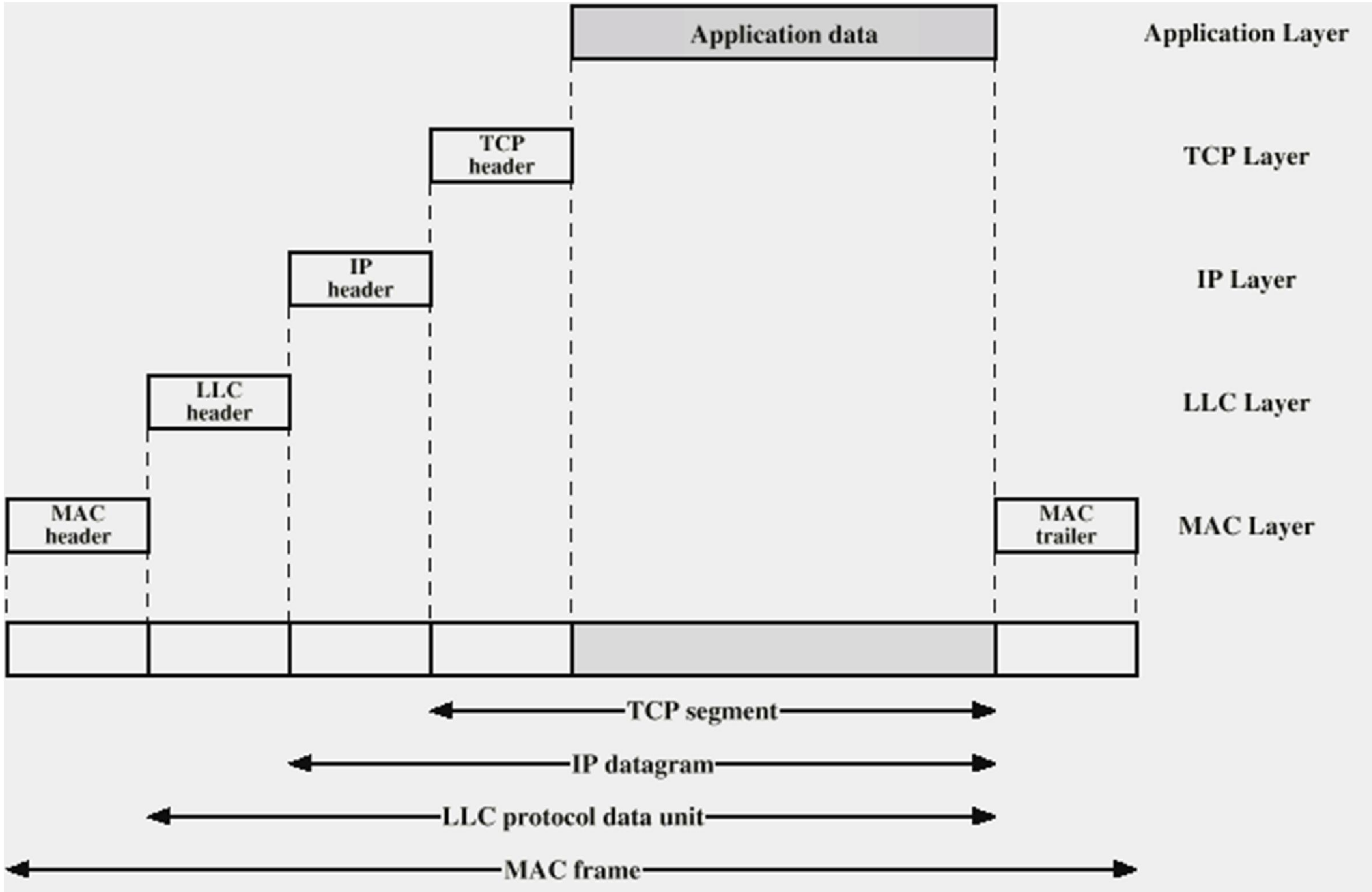


a. 10BASE5

MAC address

- A unique hardware address for each LAN interface
- Hard-coded into Network Interface Card
- 48-bit address, expressed as 12 hex digits
  - 24-bit vendor code, 24-bit serial number
  - Different NIC vendors given different vendor codes
- ff.ff.ff.ff.ff.ff is broadcast address: this is Layer 2 broadcast

MAC Layer PDU



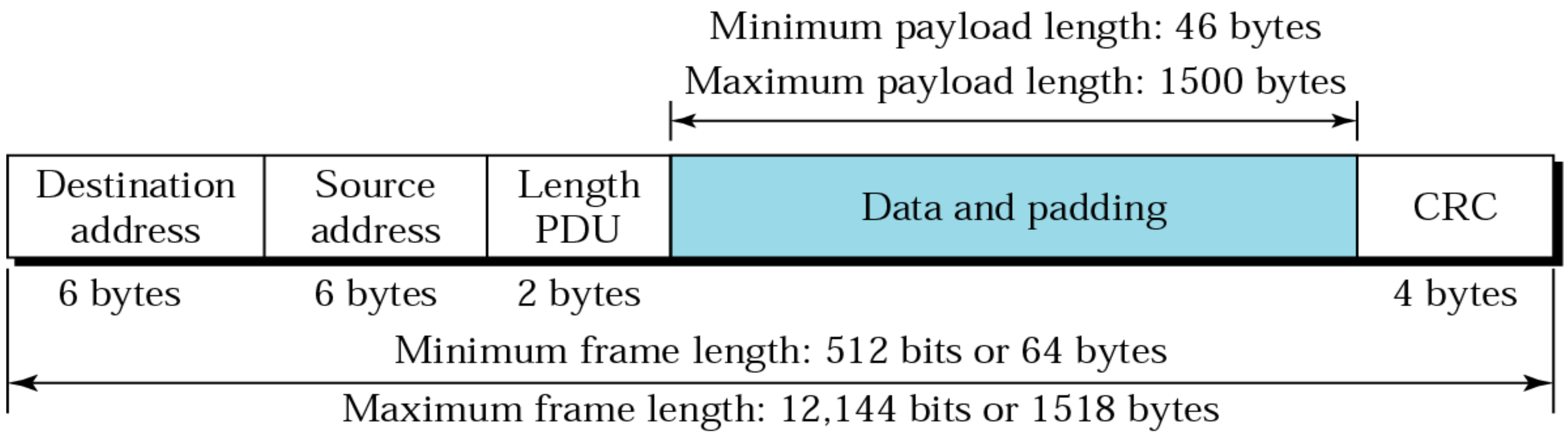
Ethernet Frame Format

PA	SFD	DA	SA	LEN	LLC PDU	PAD	FCS	IEEE 802.3
PA		DA	SA	Type	DATA	PAD	FCS	DIX Ethernet
7	1	6	6	2	46-1500		4	

- ❖ PA: Preamble --- 7 bytes 10101010s for synchronization
- ❖ SFD: Start of frame delimiter --- 10101011 to start frame
- ❖ DA, SA: Destination & source MAC address
- ❖ LEN: Length --- number of data bytes
- ❖ Type: Identify the higher-level protocol
- ❖ LLC PDU + Pad: minimum 46 bytes, maximum 1500
- ❖ FCS: Frame Check Sequence, using CRC

Minimum frame size in Ethernet

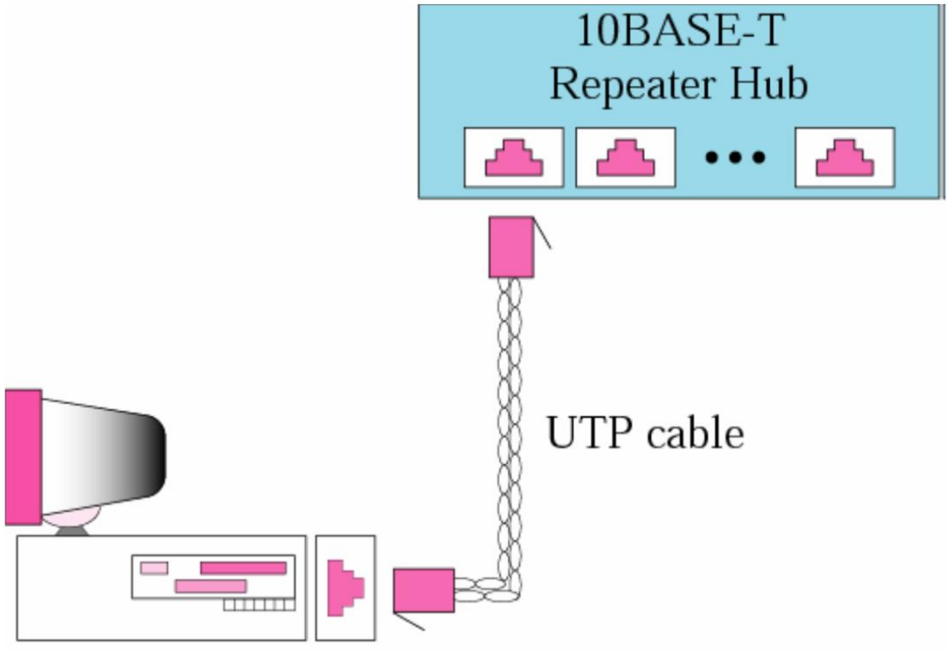
- A frame must take at least 2t time to send (t = maximum one-way propagation delay)
- For Ethernet, 2t = 51.2 microseconds
  - This includes delay introduced by four repeaters



Example of a LAN using Hub: 10BaseT

- 10 Mbps, baseband, Unshielded Twisted Pair (two pairs) Cat 3 or better used
- Logical topology bus, physical topology star using hub
- Maximum distance from station to hub = 100 m
- Collision domain: all machines connected to a hub
- Manchester encoding
- 1-persistent CSMA/CD for transmission, binary exponential backoff for retransmission
- Base wait period (Ethernet Slot Time) of 51.2 μsec, Inter-frame gap of 9.6 μsec

Connection of stations to the medium using 10Base-T



c. 10BASE-T

Switched Ethernet

(Formerly Bridge Ethernet)

Two terms

- Segment
  - Part of medium without any repeater
  - One or more stations can connect to a segment
  - Segments can be connected using repeaters
- Collision domain
  - Set of machines such that two machines transmitting can cause collision
  - One or more segments
- Repeaters (physical layer devices) do NOT guard against collision
  - Several segments connected by repeaters are within the same collision domain

Hubs

- Hub: a multi-port repeater
  - all nodes in a LAN may be connected to a central Hub (physically a star topology)
  - inside hub is a simple medium connecting all nodes, messages sent by each node reach all other nodes (logically a bus topology)

- Hub functions at the physical layer, similar to a repeater
  - Does not guard against collision (logically bus)

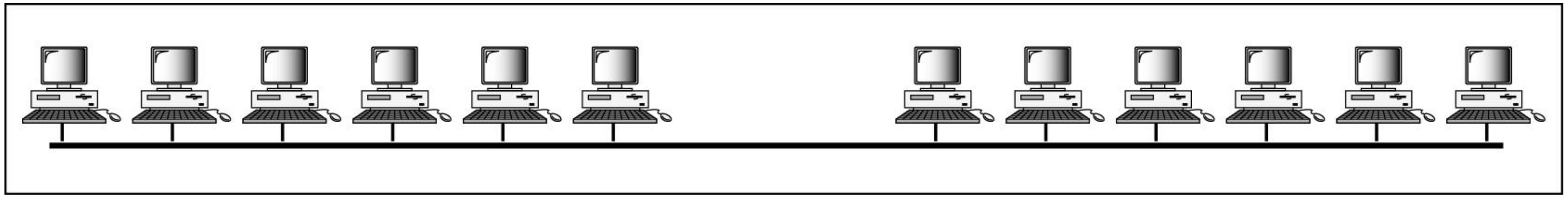
Switches in place of Hubs

- Switch (also called Layer 2 switch)
  - Hubs are nowadays replaced by switches
  - Frames NOT always broadcast, sent to only that port to which destination node is connected

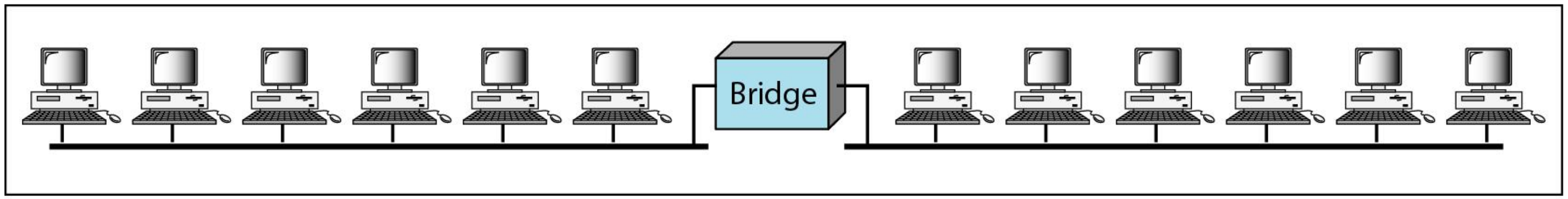
- Advantages of switch over hubs
  - Separates the single collision domain of to multiple collision domains
  - Allows more than one pair of nodes to communicate parallely

A network with and without a bridge

- The first step in the Ethernet evolution was the division of a LAN by bridges.
- Bridges have two effects on an Ethernet LAN:
  - They raise the bandwidth and they separate collision domains.

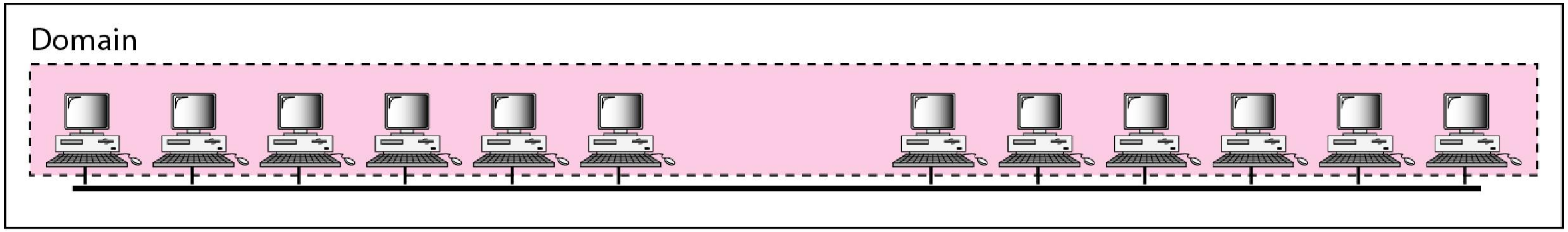


a. Without bridging

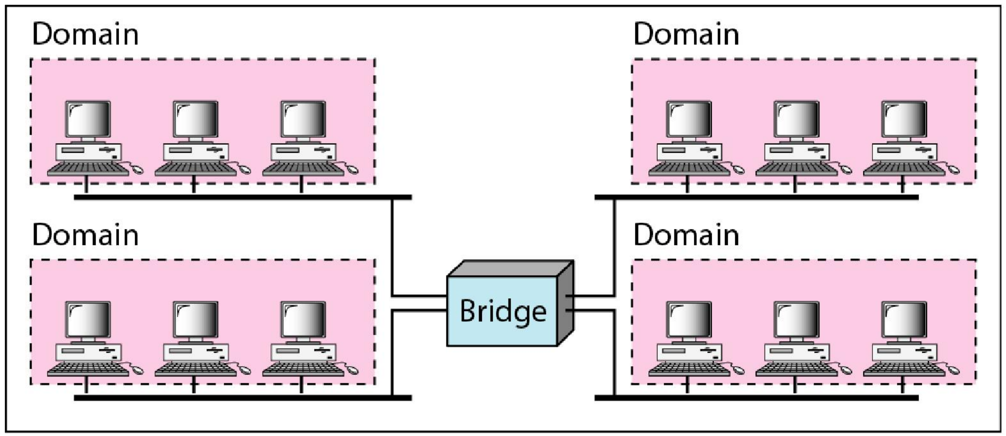


b. With bridging

Collision domains in an unbridged network and a bridged network



a. Without bridging

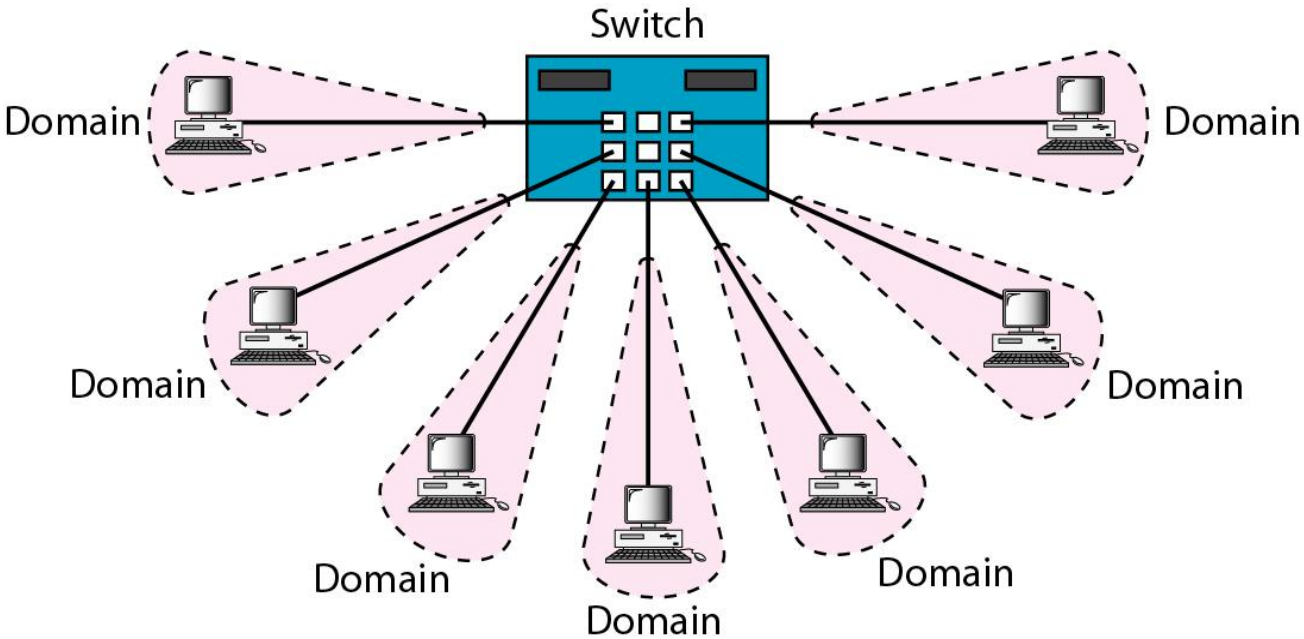


b. With bridging

Switches

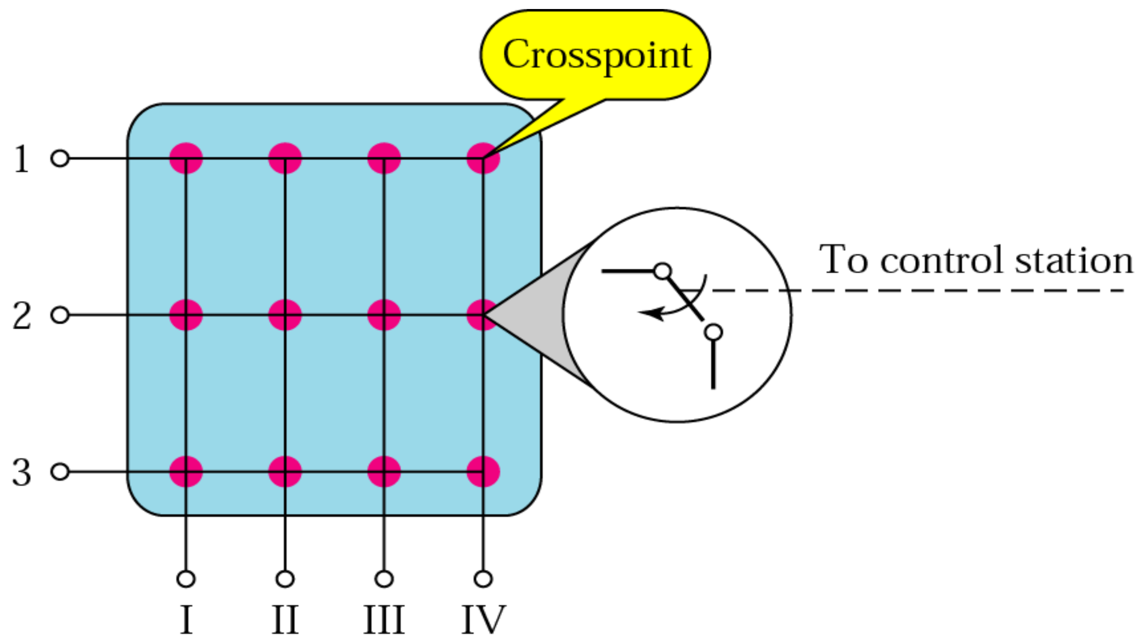
- A layer 2 switch is an N-port bridge with additional sophistication
- For selective send of frames, switch needs to know which node is connected to which port
- Switch learns – switch builds up a table of MAC address of nodes and port numbers
- Suppose m/c A sends frame to m/c B
  - Switch knows nothing initially, so broadcasts to all ports
  - But switch now knows which port A is connected to!
  - Hereafter, if a frame comes for A, it will be forwarded to only A's port
  - Internal table completely built up when every m/c has sent at least one frame

Switched Ethernet (modern days LAN)



Switches (contd.)

- Inside a switch is a cross-bar switch, allows selected pairs of nodes to communicate parallely
- Expensive but fast



References

- *Data Communications & Networking, 5th Edition, Behrouz A. Forouzan*
- *Data and Computer Communication, William Stallings*
- *Computer Networks, Andrew S. Tanenbaum and David J. Wetherall*