Wireless LAN (WLAN) IEEE802.11 (WiFi)

Sachin Gajjar
sachin.gajjar@gmail.com

Reading Material

- DATA COMMUNICATIONS AND NETWORKING, Fourth Edition by Behrouz A. Forouzan, Tata McGraw-Hill
  - Chapter 14 Wireless LANs
- Computer Networks, Fourth Edition by Andrew S Tanenbaum
  - Chapter 4, Topic 4.4

Wireless LAN

- PC's to be connected for sharing resources
- Ethernet (802.3) – wired network
- Explore use of radio waves and infrared for interconnection.
- This emerged WLAN – IEEE 802.11
- Wireless transmission at physical layer of hardware.
- Wireless Ethernet

Uses

- Flexible and can use different topologies according to need.
- Surf net, check mail on move
- During disaster setup an adhoc network
- When wiring is not allowed or can't be done (Historical places)

WiFi

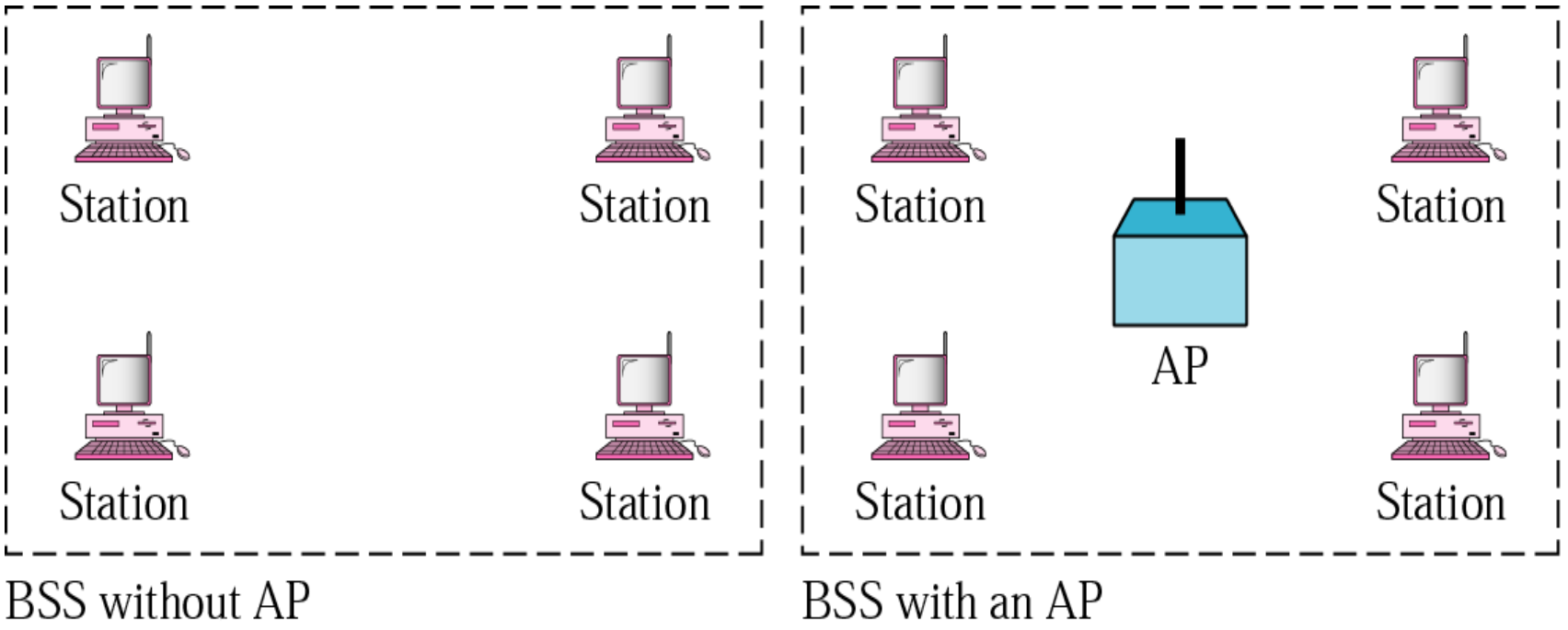
- Almost all wireless LANs now are IEEE 802.11 based
- 802.11 is also known as WiFi = “Wireless Fidelity”
- Fidelity = Compatibility between wireless equipment from different manufacturers
- WiFi Alliance is a non-profit organization that does the compatibility testing (WiFi.org)

Architecture

- The standard defines two kinds of services:
  - The basic service set (BSS)
  - The extended service set (ESS)

Basic Service Set (BSS)

- Building block of a wireless LAN
- BSS is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP)
- Figure shows two sets in this standard



Basic Service Set

A BSS without an AP is called an ad hoc network;
a BSS with an AP is called an infrastructure network.

- BSS without an AP is a stand-alone network and cannot send data to other BSSs
- Stations form a network without the need of an AP
- Stations can locate one another and agree to be part of a BSS

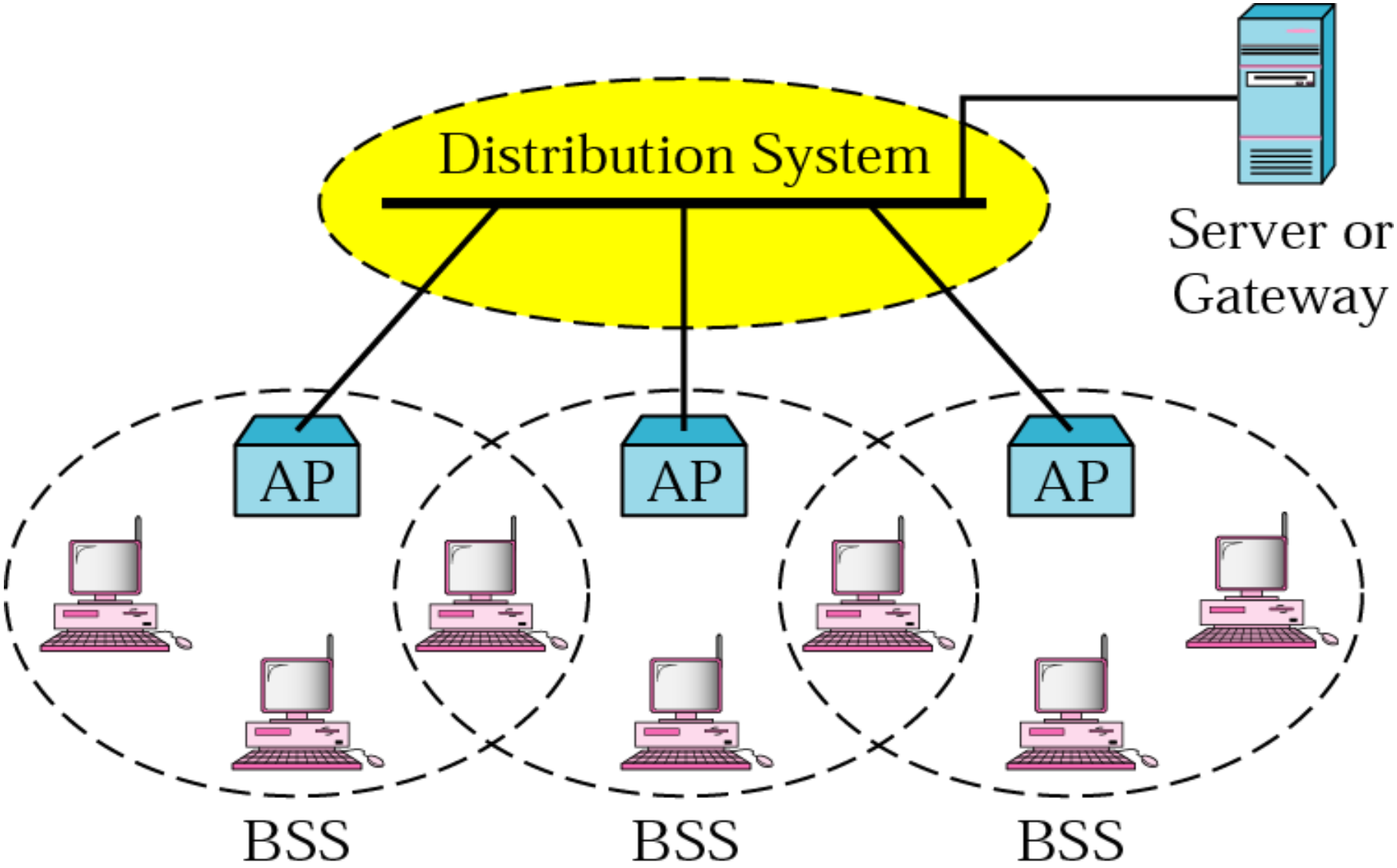
Extended Service Set (ESS)

- ESS is made up of two or more BSSs with APs
- In this case, BSSs are connected through a *distribution system,* which is usually a wired LAN
- The distribution system connects the APs in the BSSs
- IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet

Extended Service Set (ESS)

- ESS uses two types of stations: mobile and stationary
- The mobile stations are normal stations inside a BSS
- The stationary stations are AP stations that are part of a wired LAN

Extended Service Set



Extended Service Set (ESS)

- When BSSs are connected, the stations within reach of one another can communicate without the use of an AP
- However, communication between two stations in two different BSSs usually occurs via two APs
- Idea is similar to communication in a cellular network, each BSS=cell and each AP=base station
- A mobile station can belong to more than one BSS at the same time

Station Types on mobility

- no-transition
  - Stationary or moving inside BSS
- BSS transition
  - can move from BSS to BSS but within ESS
- ESS transition
  - can move from ESS TO ESS
- Does’t guarantee continuous communication during movement

Access Points

Figure 1-1: Access point with four Ethernet ports.

Figure 1-2: Access point with one Ethernet port.

Stations with WiFi Card

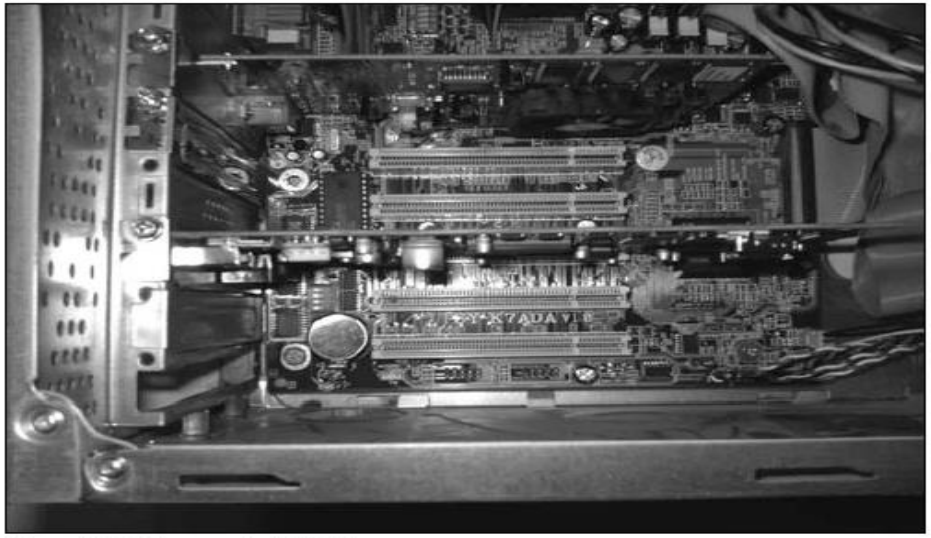


Figure 3-1: Four empty PCI slots.

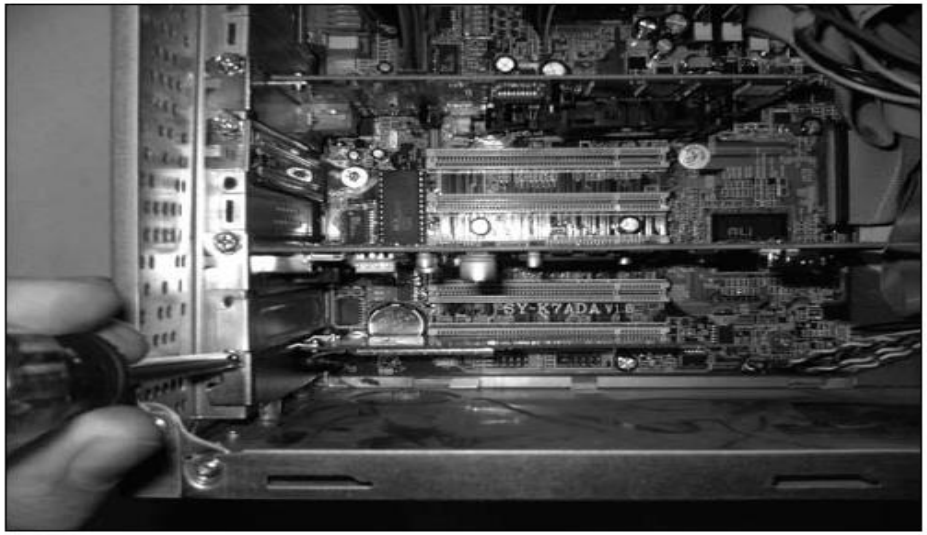


Figure 3-2: Secure the card in the case.

Figure 3-4: Cardbus Wi-Fi cards are compatible with most laptops.

laptops have a cardbus slot , USB

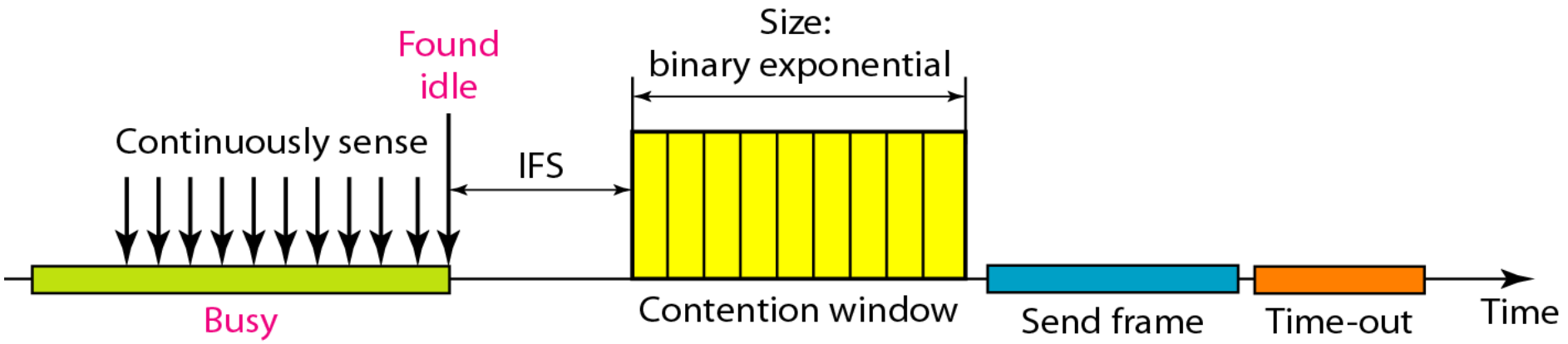
Accept's a cardbus, USB Wi-Fi adapter

MAC Problems with Wireless Networks

- In wired networks collision can be detected when signal power almost doubles (two signals detected)
- In wireless networks much of signal power is lost in transmission
- Collison may add only 5-10% power which is not useful in collision detection
- So need to avoid collisions
- Use CSMA/CA

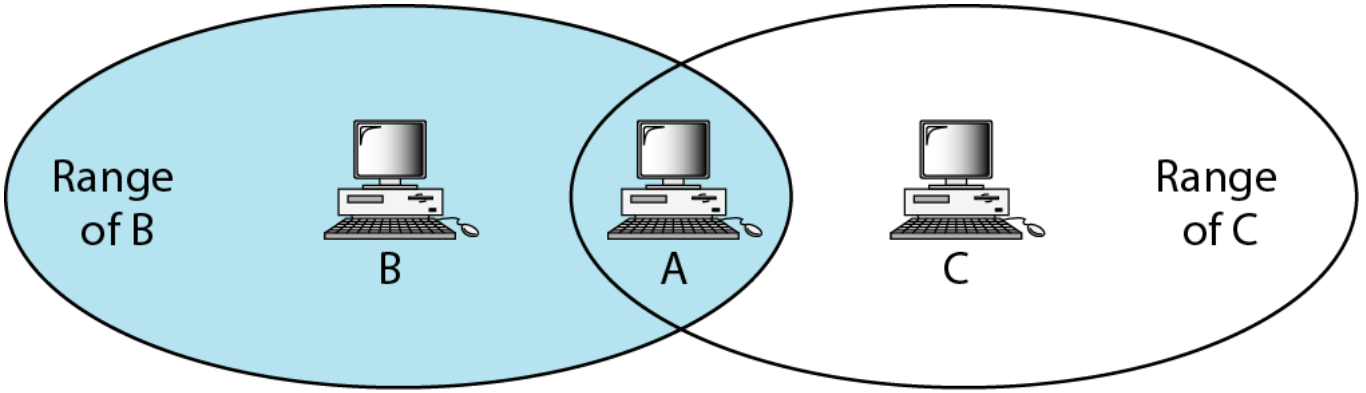
Medium Access by CSMA/CA

- Avoid collisions by:
- Interframe spacings
  - When an idle channel is found, station does not send immediately
  - It waits for a period of time called interframe space or IFS
  - Can be used to define priority of station or frame
- Contention Window
  - A station that is ready to send chooses a random number of time slots (CW) as its wait time.
  - It is set to one slot first time and then doubles each time station cannot detect an idle channel after the IFS time

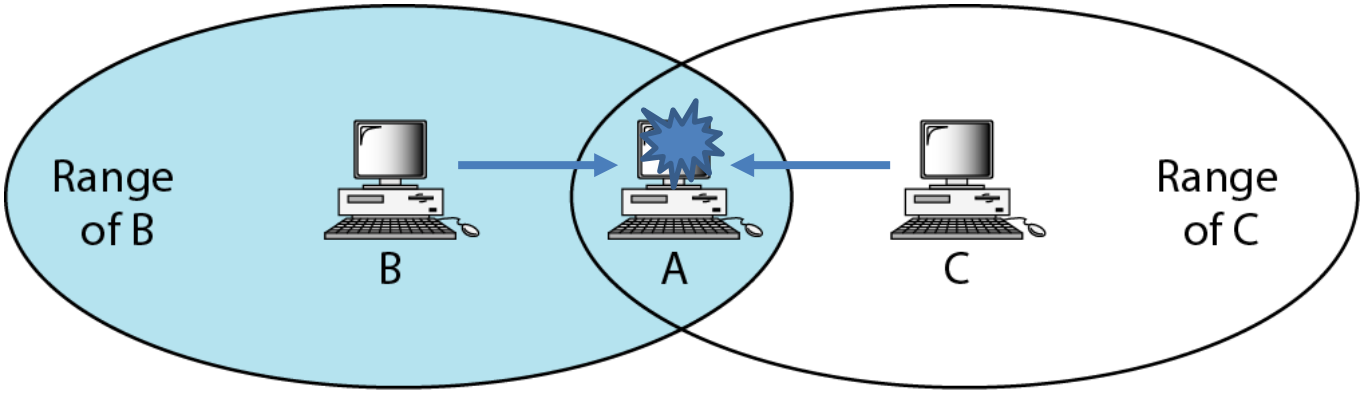


MAC Problems -Hidden Station Problem

- Station B has a transmission range shown by the left oval (sphere in space); every station in this range can hear any signal transmitted by station B
- Station C has a transmission range shown by the right oval (sphere in space); every station located in this range can hear any signal transmitted by C
- Station C is outside the transmission range of B; likewise, station B is outside the transmission range of C
- Station A, however, is in the area covered by both Band C; it can hear any signal transmitted by B or C



B and C are hidden from each other with respect to A.



B and C are hidden from each other with respect to A.

- Assume that station B is sending data to station A
- In the middle of this transmission, station C also has data to send to station A
- However, station C is out of B's range and transmissions from B cannot reach C
- Therefore C thinks the medium is free
- Station C sends its data to A, which results in a collision at A because this station is receiving data from both B and C
- In this case, we say that stations B and C are hidden from each other with respect to A
- Hidden stations can reduce the capacity of network because of possibility of collision

- The solution to the hidden station problem is the use of the handshake frames (RTS and CTS)
- Figure shows that the RTS message from B reaches A, but not C
- However, because both B and C are within the range of A, CTS message, which contains the duration of data transmission from B to A reaches C
- Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over

Destination add., source add., time for communication in RTS, CTS

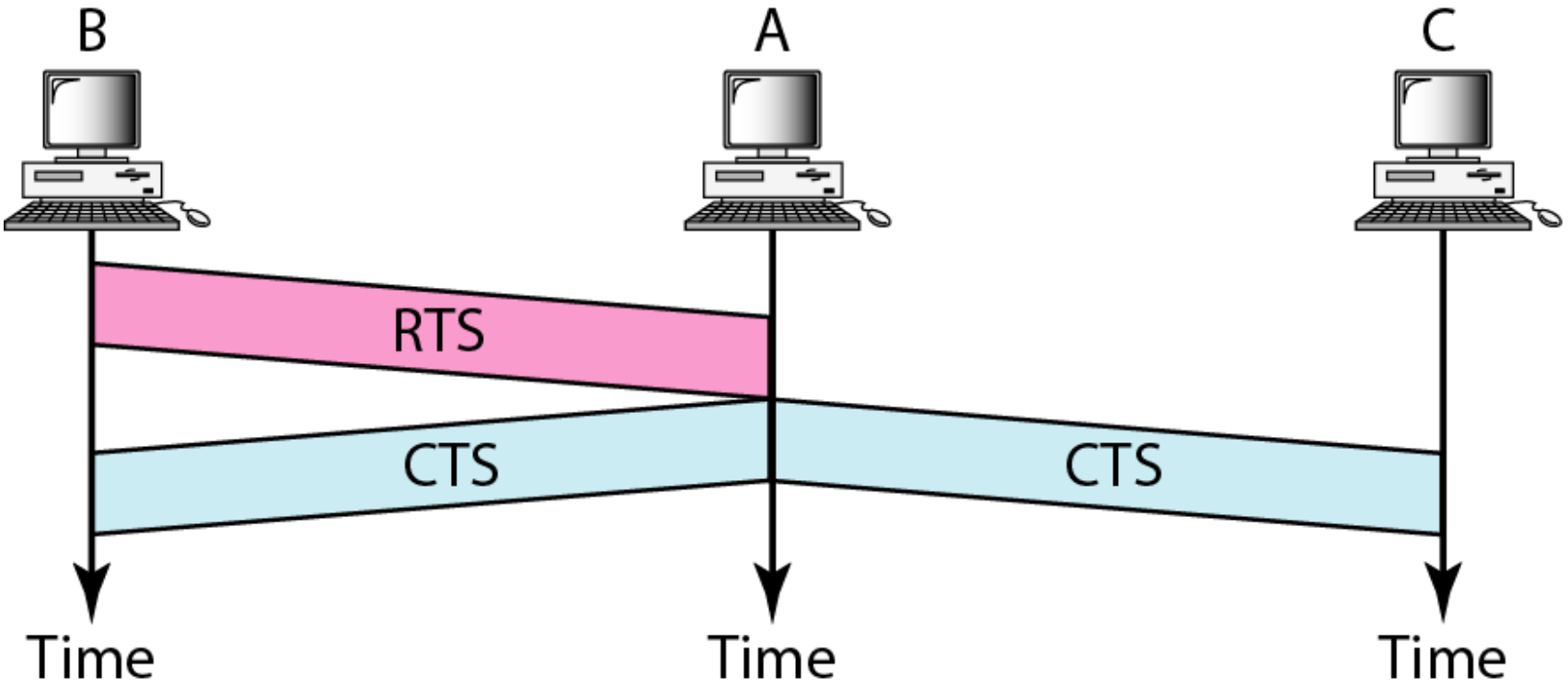
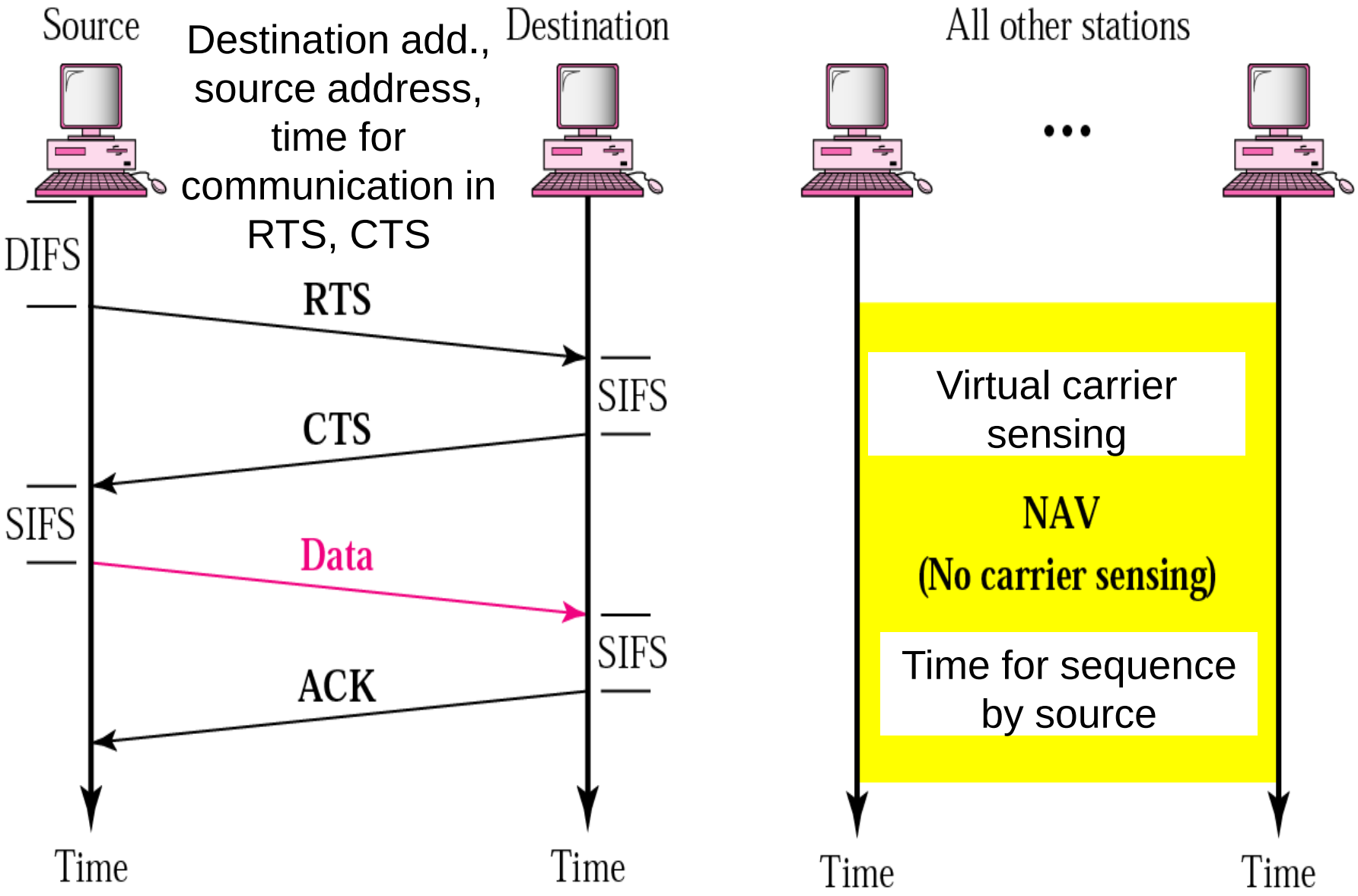


Figure 14.11 *Use of handshaking to prevent hidden station problem*

Collision Avoidance (CA)

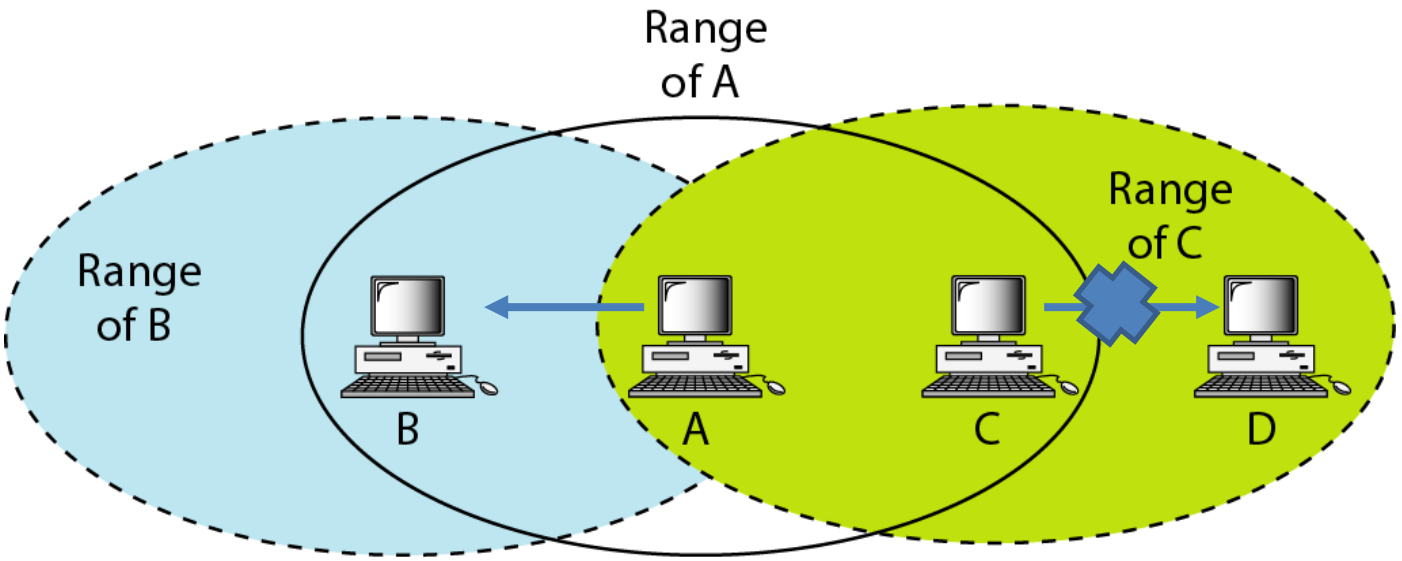
- RTS (Request to Send) frame by Source/Transmitter
- RTS frame includes the duration of time that it needs to occupy the channel
- CTS (Clear to Send) frame by Destination/Receiver
- RTS content copied to CTS
- RTS/CTS received by neighbours of Source/Destination
- These stations that are affected by transmission start a timer called a network allocation vector (NAV) that keeps tract of how much time must pass before these stations are allowed to check the channel for idleness
- Stations will do the channel sensing when its NAV has expired

CSMA/CA and NAV



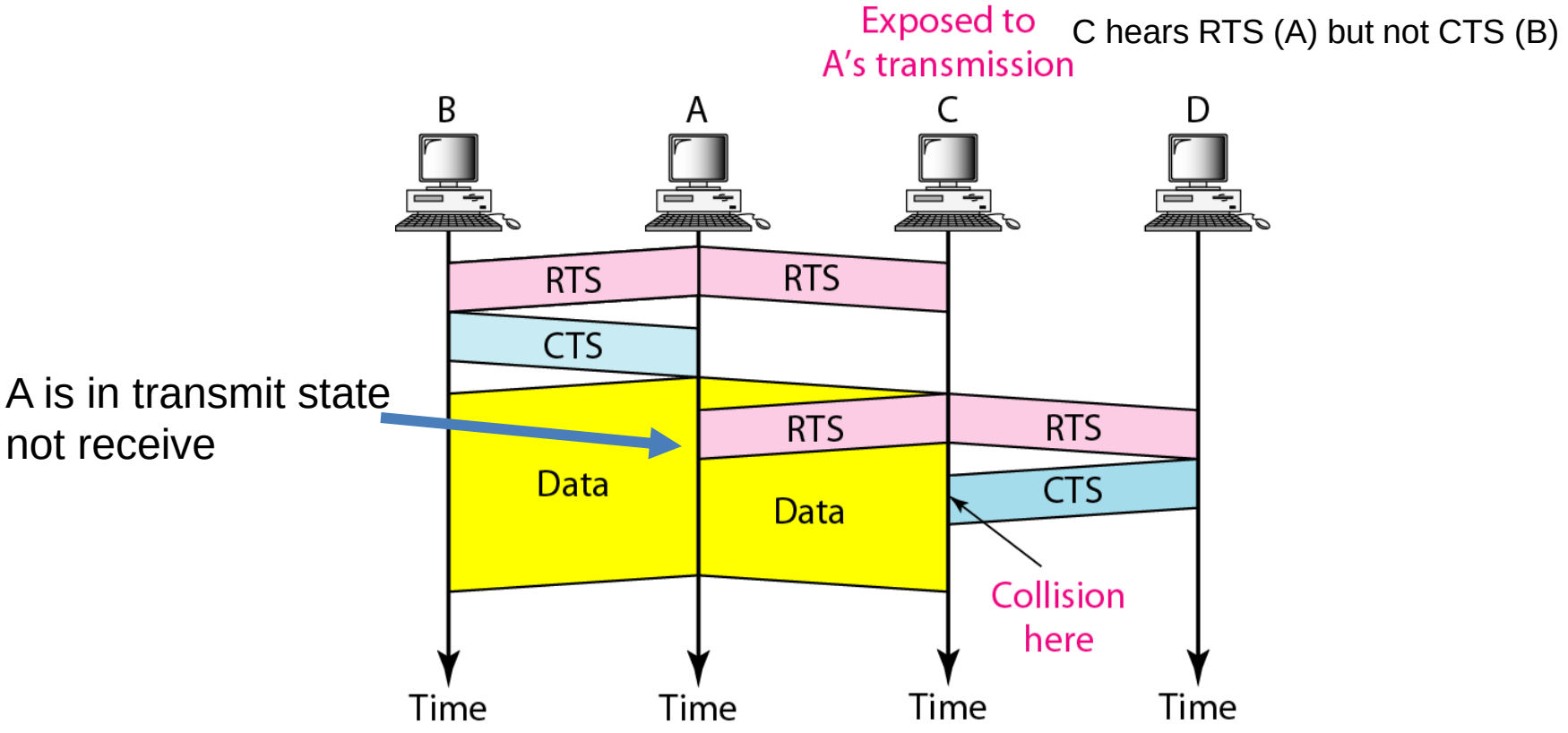
Exposed Station Problem

- In this problem a station refrains from using a channel when it is, in fact, available
- In Figure, station A is transmitting to station B
- Station C has some data to send to station D, which can be sent without interfering with the transmission from A to B
- However, station C is exposed to transmission from A; it hears what A is sending and thus refrains from sending
- In other words, C is too conservative and wastes the capacity of the channel

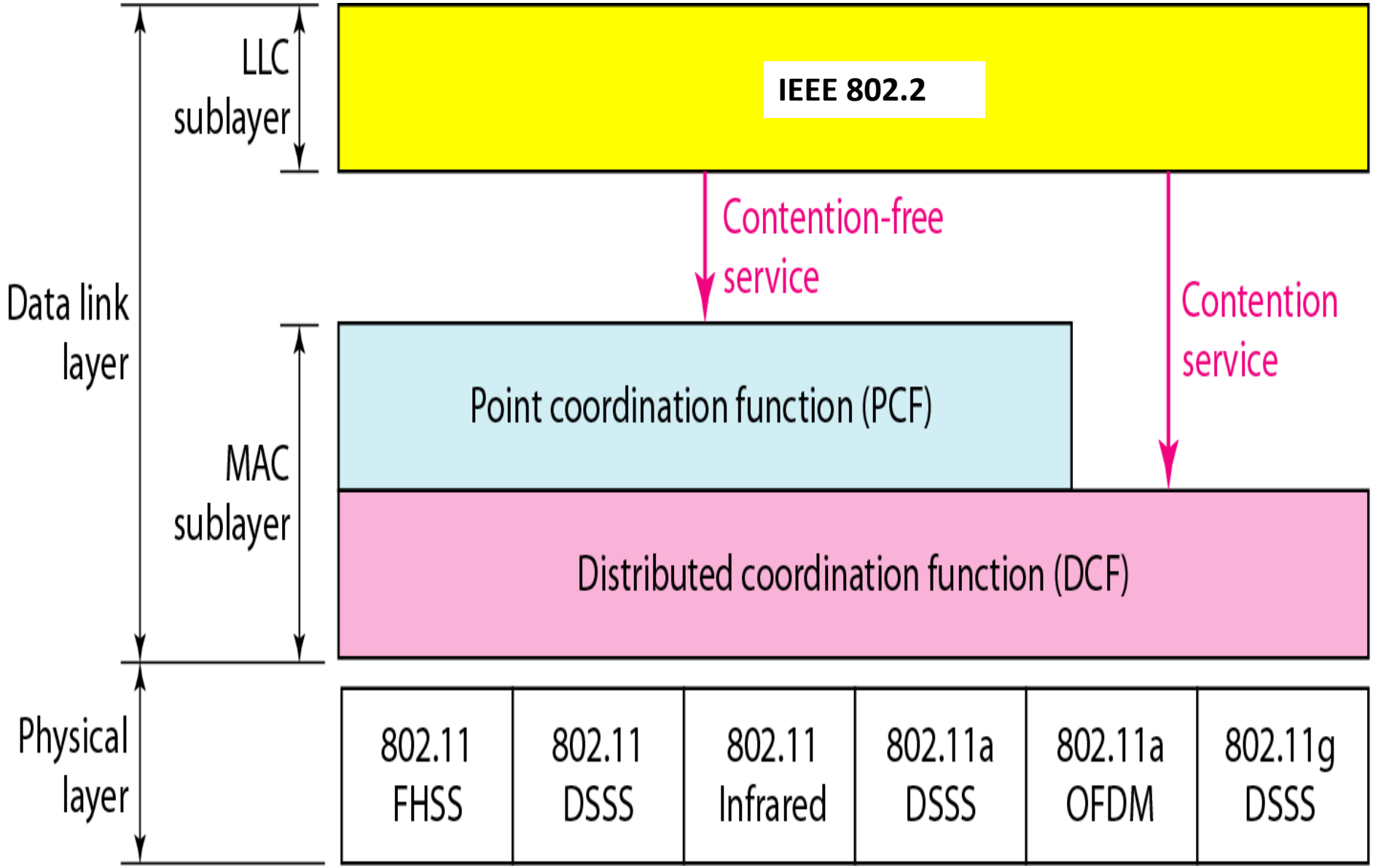


C is exposed to transmission from A to B.

- The handshaking messages RTS and CTS cannot help in exposed terminal problem
- Station C hears RTS from A, but does not hear the CTS from B
- Station C, after hearing the RTS from A, can wait for a time so that the CTS from B reaches A; it then sends an RTS to D to show that it needs to communicate with D
- D hears this RTS, but station A is in the sending state, not the receiving state
- Station D, however, responds with a CTS
- If station A has started sending its data, station C cannot hear the CTS from station D because of the collision; it cannot send its data to D
- It remains exposed until A finishes sending its data as Figure



IEEE 802.11 Layers (PHY and MAC)



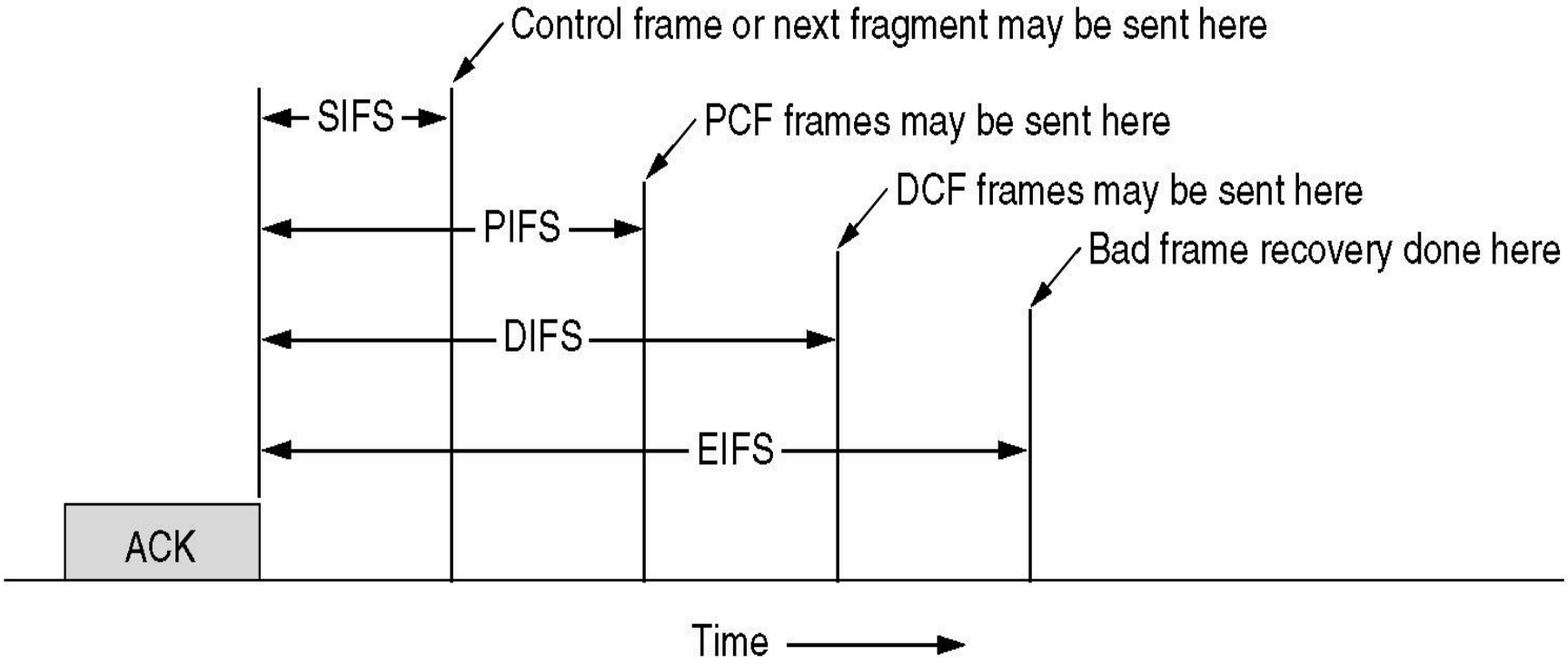
MAC Sublayer

- Logical Link Control (LLC)
  - Flow control, Error control, Framing
  - IEEE 802.2 standard – common for all 802 variants (802.3, 802.11, 802.15 (BT, ZB)), 802.16 (WiMax), 802.20 (Mobile Broadband WL) , makes these variants appear same to network layer
- 2 MAC sublayers
  - DCF – for adhoc network, Uses Carrier Sense Multiple Access (*CSMA)/Collision Avoidance (CA)* as the medium access method
  - PCF – for infrastructure based network

Interframe spacings

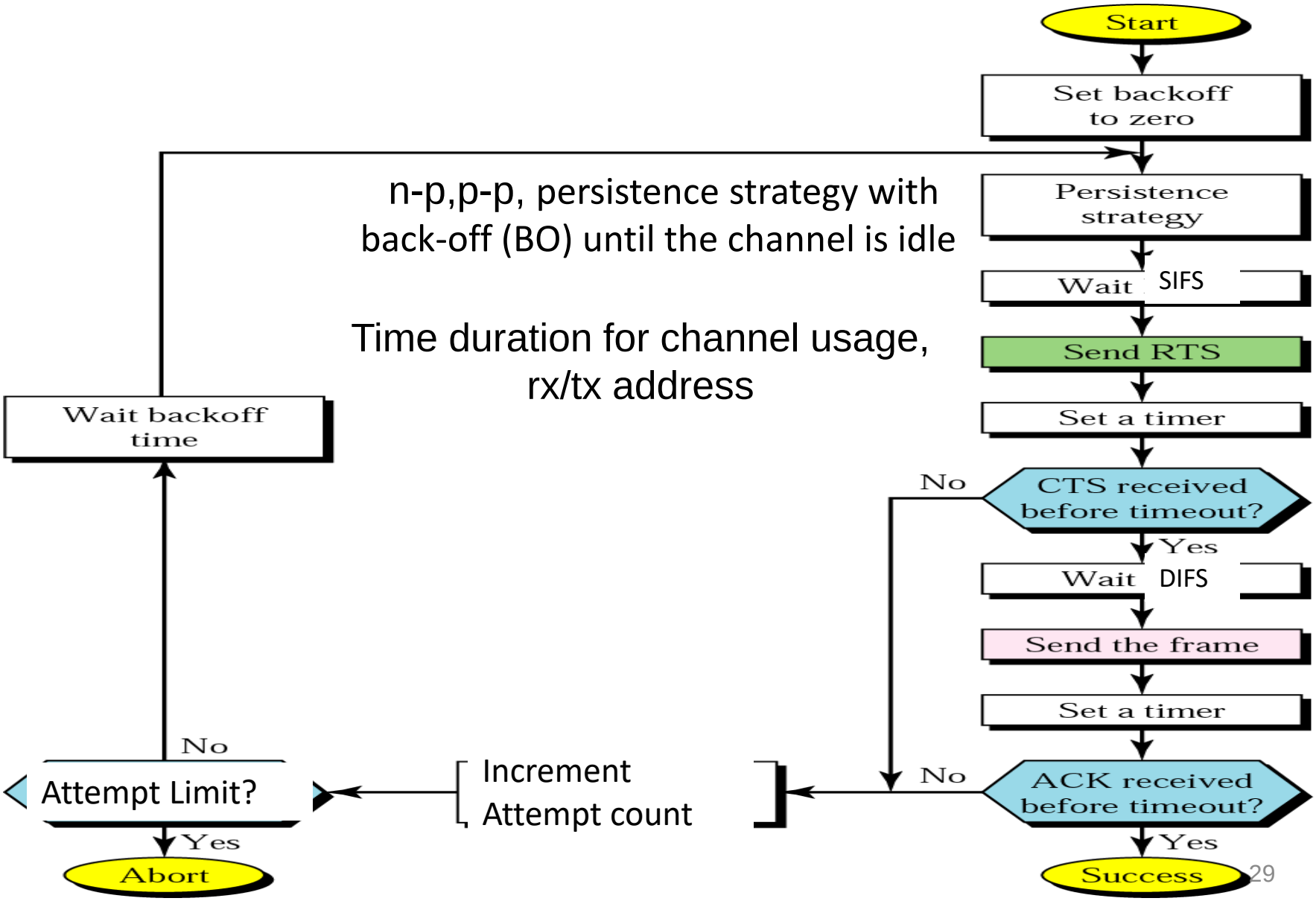
- PCF and DCF can coexist within one BSS
- By carefully defining the interframe time interval
- After frame has been sent, certain amount of dead time is set before next transmission – interframe spacing
- Four different intervals are defined

Interframe spacing in 802.11



- SIFS (Short InterFrame Spacing) – ACK, RTS, CTS
- PIFS (PCF InterFrame Spacing) – AP sends beacon/poll
- DIFS (DCF InterFrame Spacing) – MS attempts to get channel
- EIFS (Extended InterFrame Spacing) – station to report that it has just received a bad or unknown frame

CSMA/CA


Start
Set backoff to zero
Persistence strategy
Wait SIFS
Send RTS
Set a timer
CTS received before timeout?
No
Yes
Wait DIFS
Send the frame
Set a timer
ACK received before timeout?
No
Yes
Success
Increment Attempt count
Attempt Limit?
No
Yes
Abort
Wait backoff time
n-p,p-p, persistence strategy with back-off (BO) until the channel is idle
Time duration for channel usage, rx/tx address

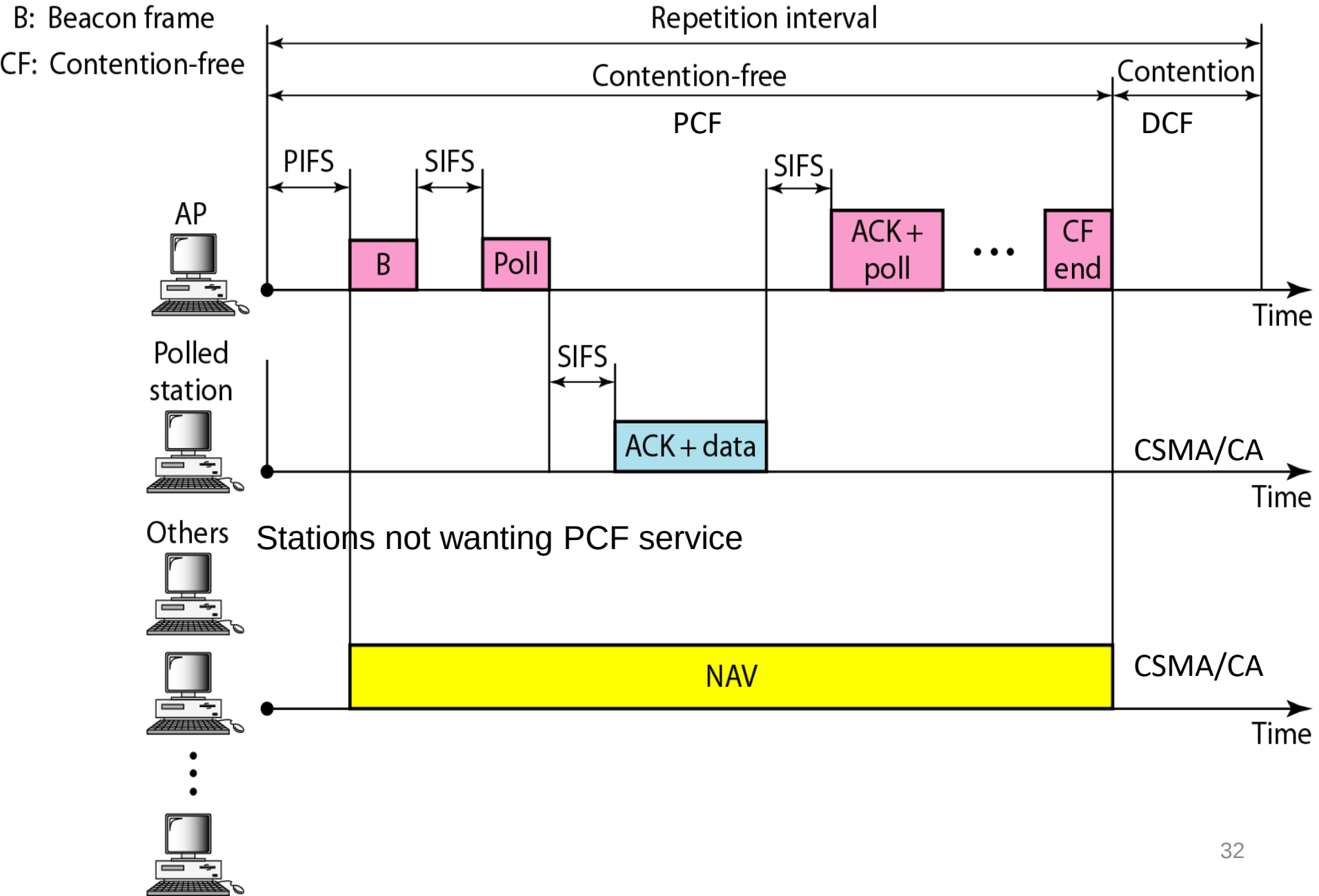
CSMA/CA

1. Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency
   a. The channel uses a persistence strategy with back-off until the channel is idle
   b. After the station is found to be idle, the station waits for a period of time called the short interframe space (SIFS); then the station sends a control frame called the request to send (RTS)
2. After receiving the RTS and waiting a period of time called the short interframe space (SIFS), the destination station sends a control frame, called the clear to send (CTS), to the source station. This control frame indicates that the destination station is ready to receive data
3. The source station sends data after waiting an amount of time equal to SIFS
4. The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received. Acknowledgment is needed in this protocol because the station does not have any means to check for the successful arrival of its data at the destination.

Point Coordination Function (PCF)

- Optional access method
- For infrastructure based network
- Centralized, contention-free polling access method
- On top of DCF for time sensitive transmission (video/audio)
- Access Point AP polls stations one after the another for data if any
- Polled station send any data they have to the AP
- To give priority to PCF over DCF , PIFS < DIFS
- DCF station may not gain access to medium
- To avoid it repeated interval (PCF-DCF intervals) is designed

Example of repetition interval



What is use of Backoff timer in CSMA/CA?

- Incorporates fairness among nodes
- If there is no backoff timer all stations will have same chance of accessing medium in next contention slot irrespective of time for it has waited to get the medium
- With backoff timer the stations who has got the chance to access the medium will have to wait more to get it again

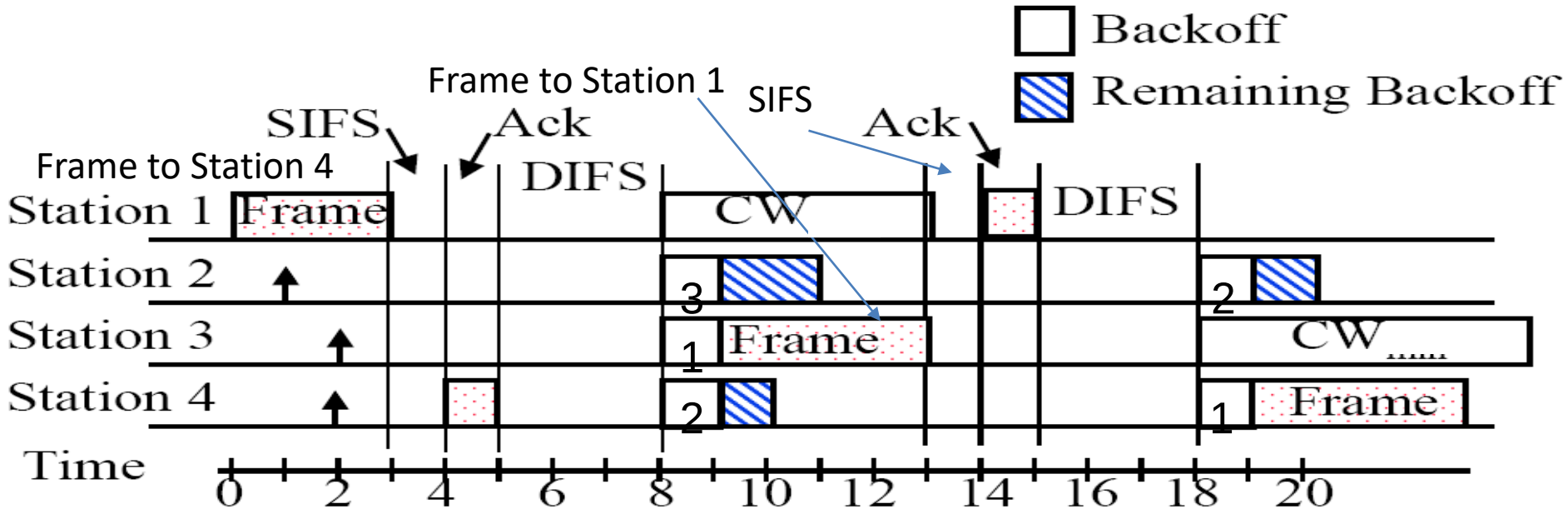
IEEE 802.11 Back Off Operation

- Three Variables
  - Contention Window (CW)
  - Backoff Count (BO)
  - Network Allocation Vector (NAV)
- If RTS, CTS heard NAV set to duration of the frame, station sense medium after NAV expires
- If medium idle for DIFS, and backoff (BO) is not already active, station draws a random BO in [0, CW] and sets backoff timer
- If another station starts transmitting, waiting stations pause their backoff counter and restart it after end of frame + DIFS time

DCF: Example

- T=1 Station 2 wants to transmit but the media is busy
- T=2 Stations 3 and 4 want to transmit but the media is busy
- T=3 Station 1 finishes transmission.
- T=4 Station 1 receives ack for its transmission (SIFS=1)
- T=5 Medium becomes free
- T=8 DIFS expires.
  Stations 2, 3, 4 draw backoff count between 0 and 5.
  The counts are 3, 1, 2
- T=9 Station 3 starts transmitting.
  Station 2 and 4 pause backoff counter at 2 and 1 resp.
- T=13 Station 3 finishes transmission
- T=14 Station 3 receives Ack.
- T=15 Medium becomes free
- T=18 DIFS expires
  Stations 2 and 4 start their backoff counter
- T=19 Station 4 starts transmitting

- Example: Slot Time = 1, CW = 5, DIFS=3, PIFS=2, SIFS=1,



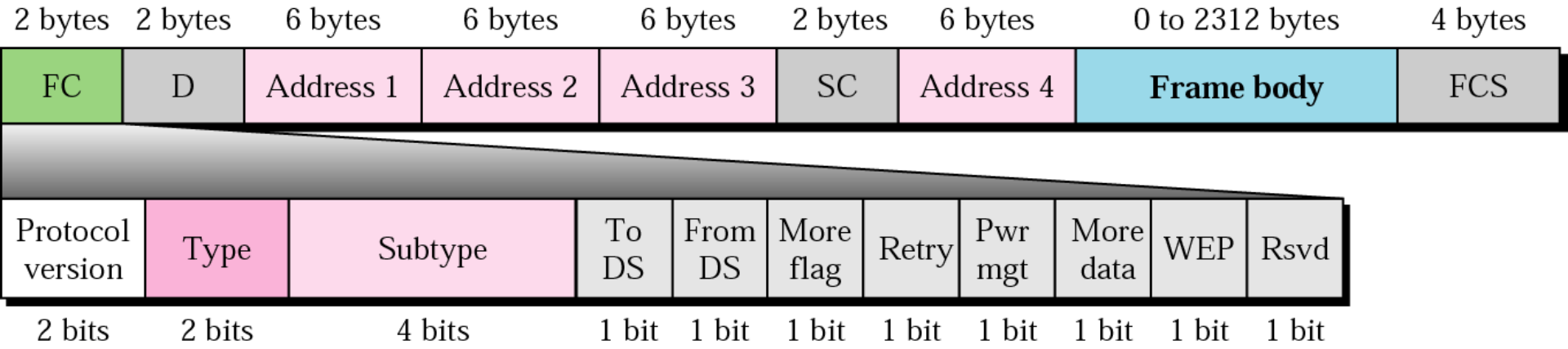
Fragmentation

- The wireless environment is very noisy; a corrupt frame has to be retransmitted
- Standard recommends fragmentation-the division of a large frame into smaller ones
- It is more efficient to resend a small frame than a large one

Frame Categories

- **Management Frames**: used for initial communication between stations and access points.
- **Data Frames**: used for carrying data and control information
- **Control Frames:** used for accessing the channel and acknowledging frames

MAC Frame Format



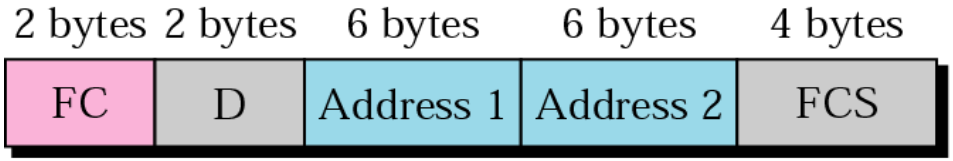
- Frame control (FC) field - 2 bytes- defines type of frame & control information
- D – Duration how long the frame and its acknowledgement will occupy the channel, for NAV. In one control frame, this field defines ID of frame.
- Addresses- There are four address fields, each 6 bytes (48 bits) Meaning of each address field depends on value of *To DS and From DS subfields*
- Sequence control - sequence number of frame to be used in flow control.
- Frame body- can be between 0 and 2312 bytes, contains information based on the type and the subtype defined in the FC field
- FCS contains a CRC-32 (Cyclic Redundancy check) error detection sequence

Subfields in FC field

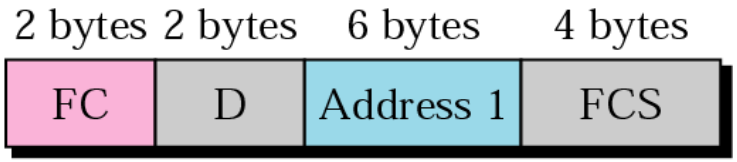
Field	Explanation
Protocol Version	two versions of the protocol to operate at the same time in the same cell, current version is 0
Type	Type of information: management (00), control (01), or data (10).
Subtype	Defines the subtype of each type RTS or CTS
To DS	the frame is going to or coming from the intercell (two BSS) distribution system (e.g., Ethernet)
From DS	
More flag	When set to 1, means more fragments.
Retry	When set to 1, means retransmitted frame.
Pwr mgt	When set 1, means station is in sleep mode
More data	When set to 1, sender has additional frames for the receiver
WEP	When set to 1, frame body has been encrypted using the WEP (Wired Equivalent Privacy) algorithm
Rsvd	Reserved.

Control Frames

- Type field = 0 1
- Values of subtype fields for frames are shown in Table



RTS

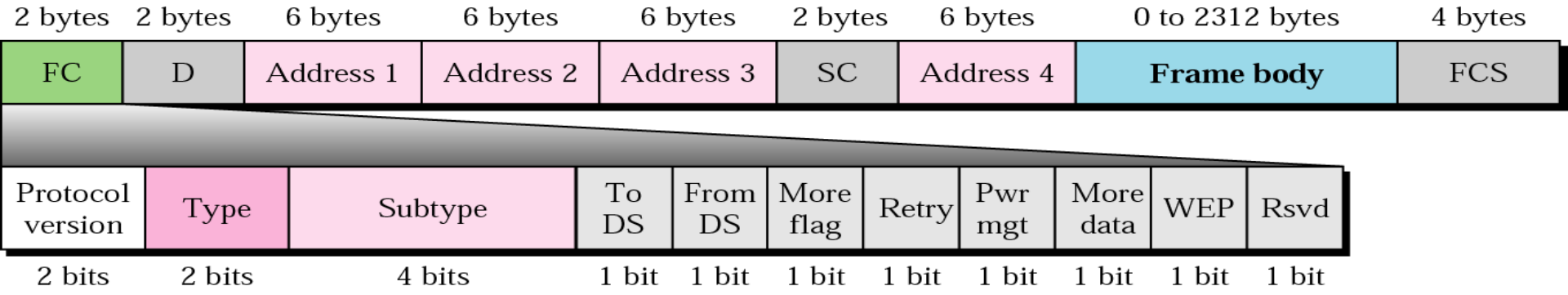


CTS or ACK

Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

Addressing Mechanism

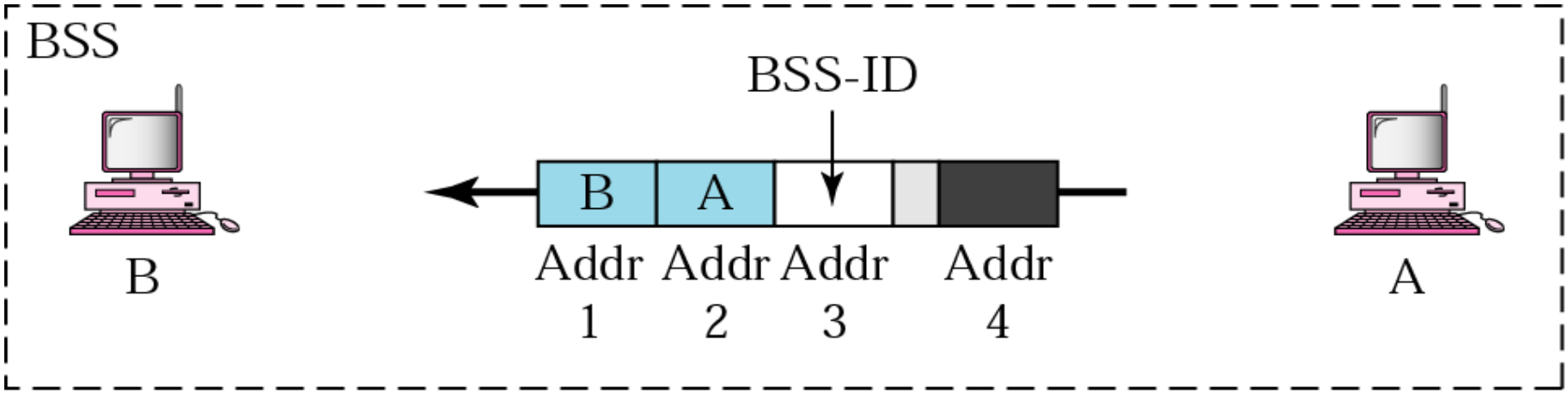
- Interpretation of four addresses (address 1 to address 4) in MAC frame depends on value of To DS/From DS flags, as shown in Table



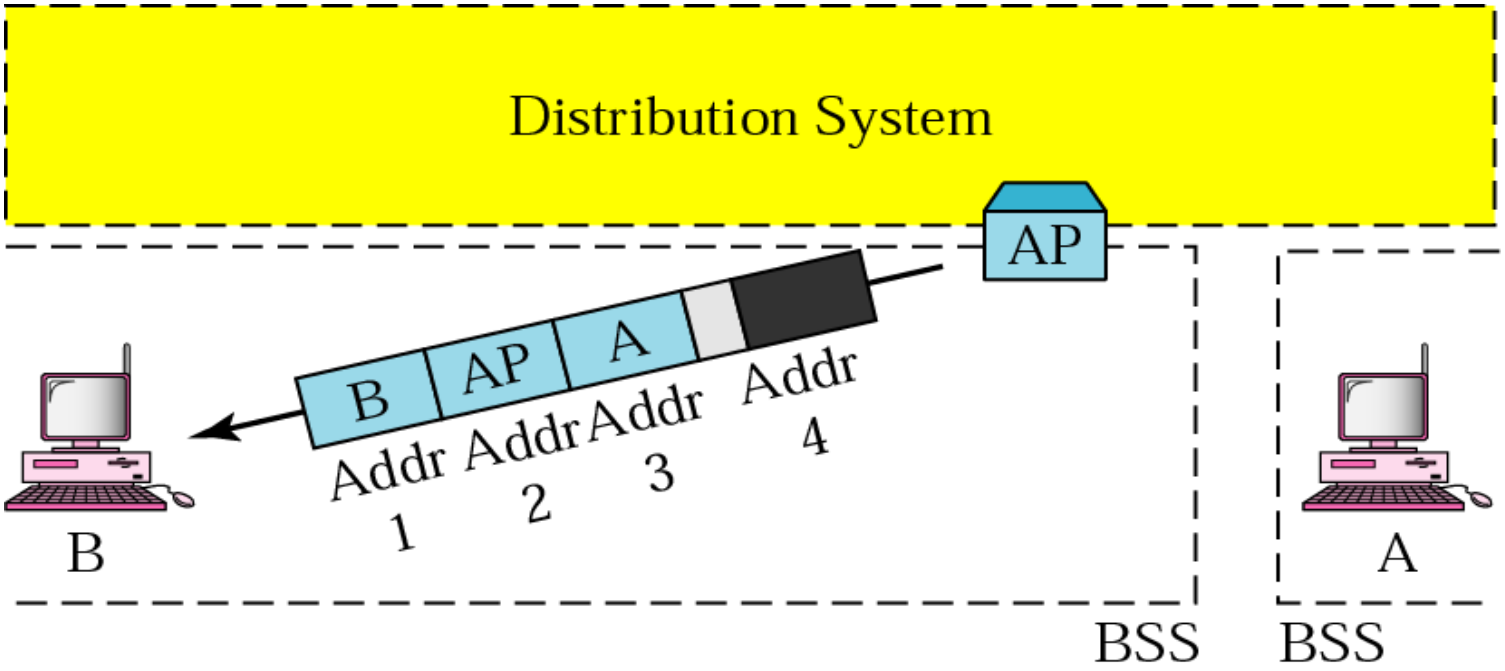
To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination station	Source station	BSS ID	N/A
0	1	Destination station	Sending AP	Source station	N/A
1	0	Receiving AP	Source station	Destination station	N/A
1	1	Receiving AP	Sending AP	Destination station	Source station

- Address 1 is always the address of the next device
- Address 2 is always the address of the previous device
- Address 3 is address of the final destination station if it is not defined by address 1
- Address 4 is the address of the original source station if it is not the same as address 2.

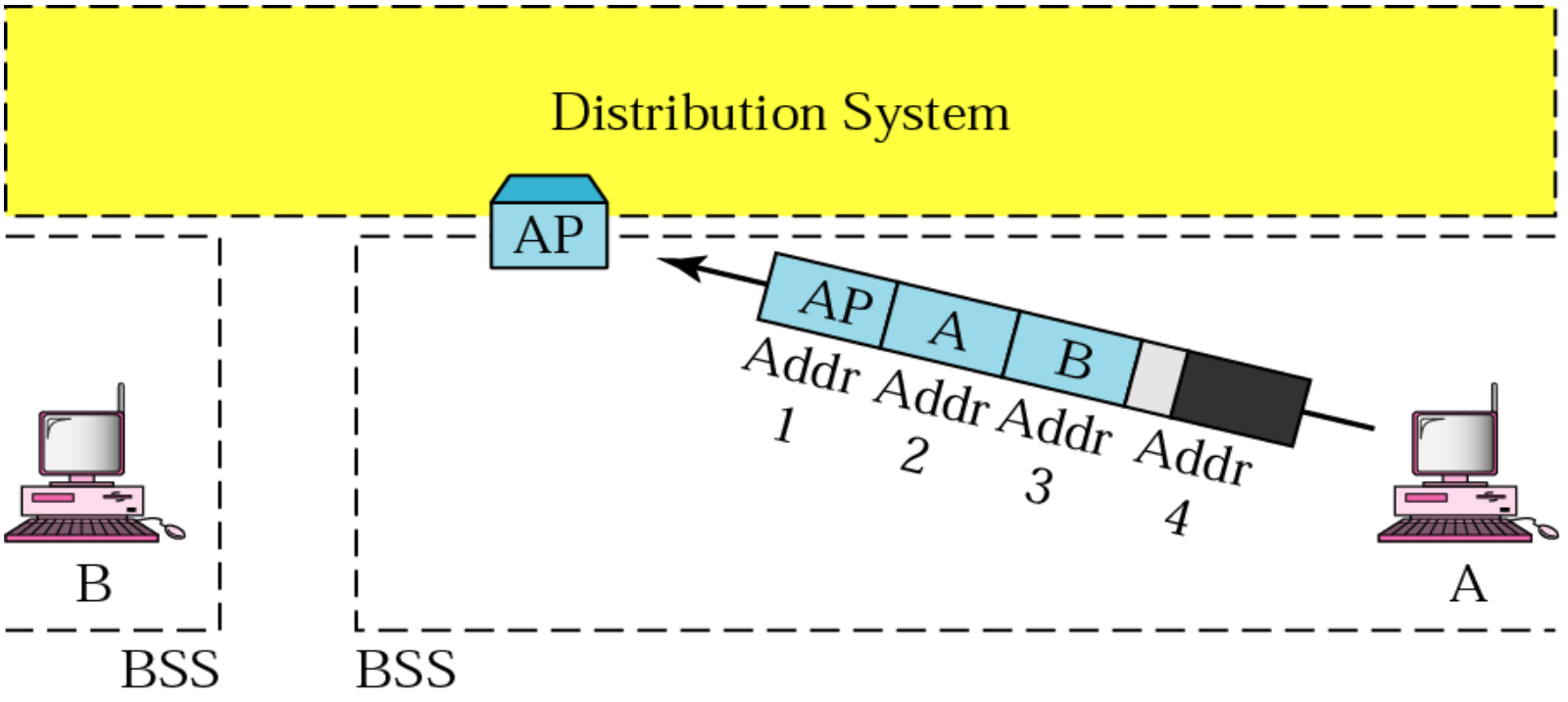
- Case 1: 00 In this case, To DS = 0 and From DS = 0
- Means that frame is not going to a distribution system (To DS = 0) and is not coming from a distribution system (From DS =0)
- The frame is going from one station in a BSS to another without passing through the distribution system
- The ACK frame should be sent to the original sender



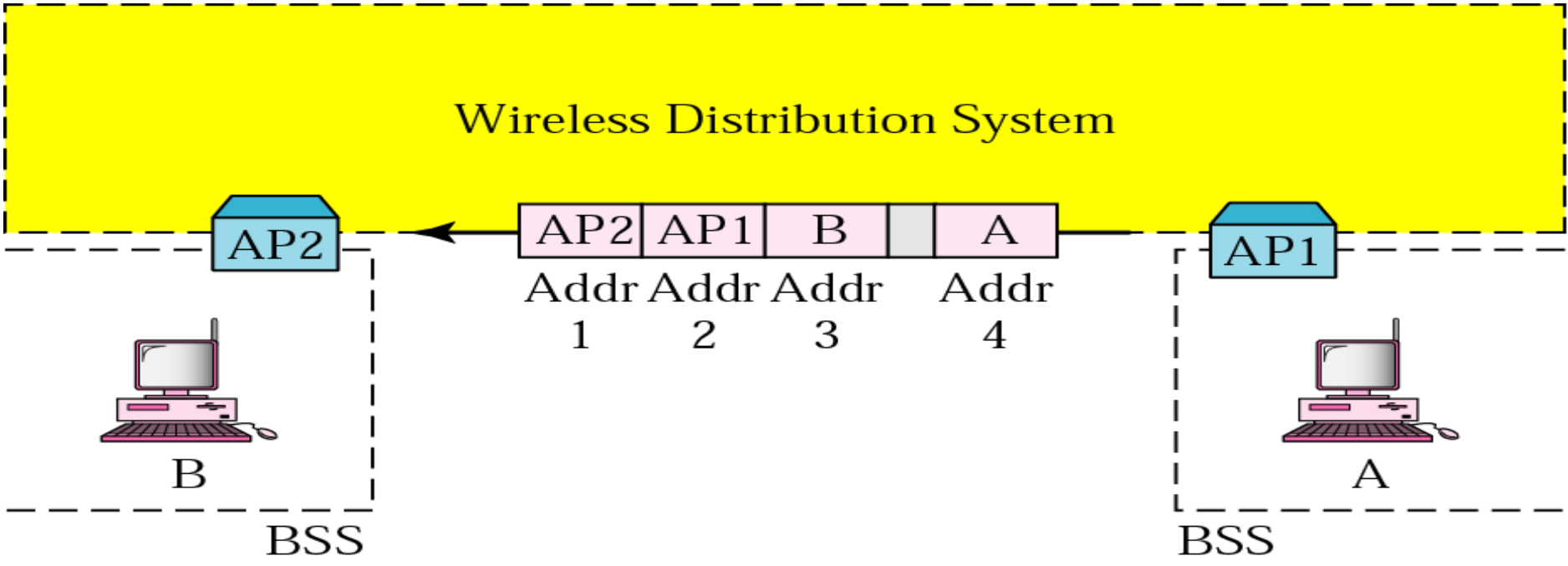
- Case 2: 01 In this case, To DS = 0 and From DS = 1
- Means frame is coming from a distribution system (From DS = 1)
- Frame is coming from an AP and going to a station
- ACK should be sent to the AP
- Address 3 contains the original sender of the frame (in another BSS).



- Case 3: 10 In this case, To DS =1, From DS =O.
- Means frame is going to a distribution system (To DS = 1)
- The frame is going from a station to an AP.
- ACK is sent to the original station
- Address 3 contains final destination of frame (in another BSS).



- Case 4:11 In this case, To DS =1 and From DS =1
- This is the case in which the distribution system is also wireless
- The frame is going from one AP to another AP in a wireless distribution system
- Here, we need four addresses to define the original sender, the final destination, and two intermediate APs



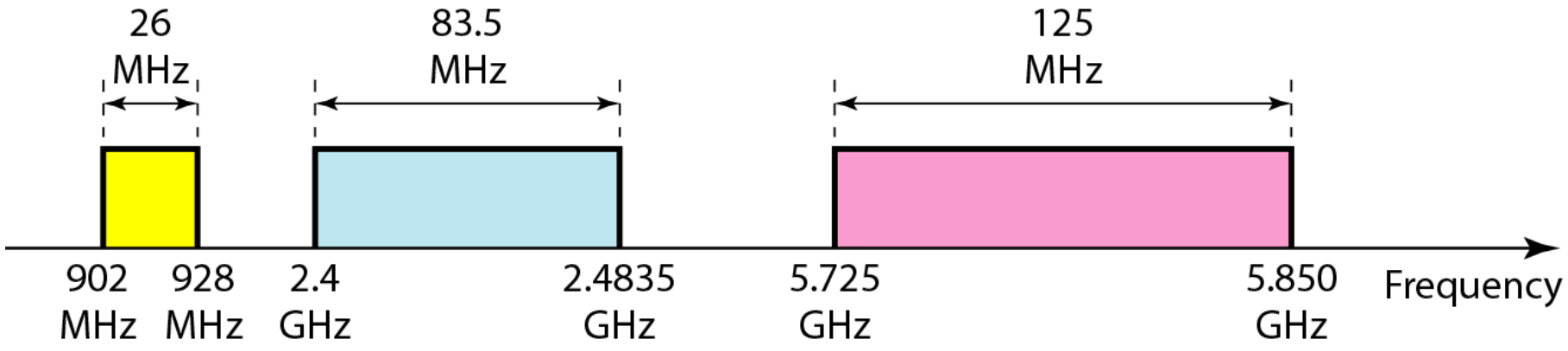
Physical Layer

- Six specifications

IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.4 GHz	FSK	1 and 2
	DSSS	2.4 GHz	PSK	1 and 2
		Infrared	PPM	1 and 2
802.11a	OFDM	5.725 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.4 GHz	PSK	5.5 and 11
802.11g	OFDM	2.4 GHz	Different	22 and 54

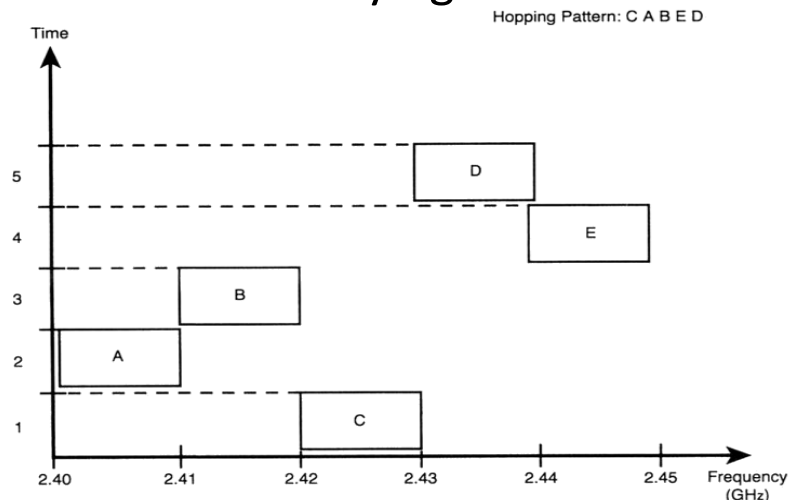
Physical Layer

- All implementations, except infrared, operate in industrial, scientific, and medical (ISM) band,
- ISM defines three unlicensed bands in three ranges 902-928 MHz, 2.4-2.4835 GHz, and 5.725-5.850 GHz



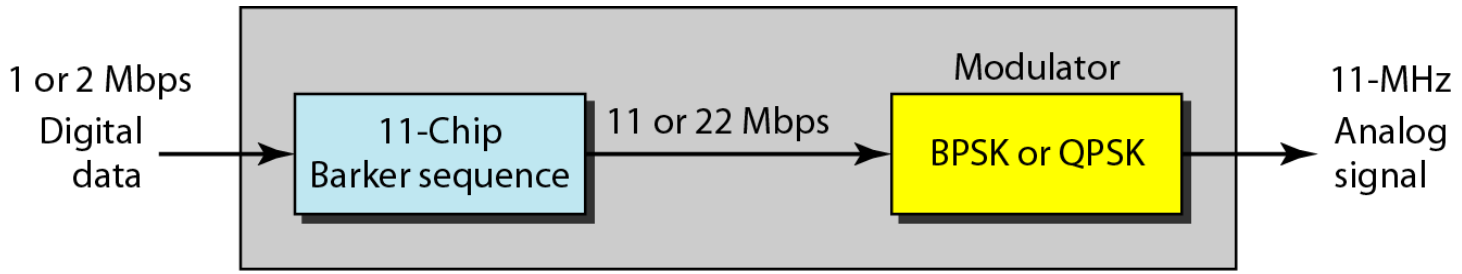
IEEE 802.11 FHSS

- Uses the frequency-hopping spread spectrum (FHSS) method
- FHSS uses the 2.4-GHz ISM band
- Band is divided into 79 sub-bands of 1 MHz (and some guard bands)
- Pseudorandom number generator selects hopping sequence for the carrier frequency
- amount of time spent at each frequency, dwell time, is an adjustable parameter < 400 msec
- FHSS gives tolerance to multi-path, narrow band interference, gives security
- Low speed (1 and 2 Mbps), small range (upto 50mtr) due to FCC (Federal Communications Commission) Transmission power regulation (10mW)
- The modulation technique in this specification is Phase Shift Keying



IEEE 802.11 DSSS

- Uses direct sequence spread spectrum (DSSS) method
- 1 to 2 Mbps
- DSSS uses the 2.4-GHz ISM band
- The modulation technique is Phase Shift Keying
- Power limits 1000mW in US, 100mW in EU, 200mW in Japan
- Immune to interference, cheaper hardware , gives security
- DSSS expands bandwidth of original signal, by replacing each data bit with n bits using a spreading code
- Each bit is assigned a code of n bits, called chips (here 11 chips Barker code for spreading)



IEEE 802.11 Infrared

- Uses infrared light in the range of 800 to 950 nm
- Modulation technique is pulse position modulation (PPM)
- 1 Mbps and 2 Mbps transmission rate
- signals cannot penetrate walls, cells in different rooms are well isolated
- low bandwidth, sunlight swamps infrared

Services to be provided by (MS=Mobile Station) (AP=Access Point)

- Association – for MS to connect to AP
  - MS →identity/capability (data rate, PCF services)→ AP
  - MS ← accept/reject ← AP
  - If accept authenticate
- Dissociation – for MS or AP to break connection
  - MS → leaving/shutting → AP
  - MS ← on maintenance ← AP
- Reassociation – for MS changing its AP, moving one BSS to other
  - MS →changing cell → AP
  - no data loss during handover if used correctly.
  - best effort service.
- Distribution
  - For routing frames send to AP so that it reaches the destination
  - if destination in same BSS ,frame sent over AIR.
  - otherwise forward through DS (wired network)

Services

- Integration-when frame sent to non IEEE 802.11
  - 802.11 frames format → non IEEE 802.11
- Authentication-stations to authenticate before sending frames via AP
  - MS → Username/Password → AP
  - AP checks with Authentication Server if Username/Password are correct
- Deauthenciation
  - authenciated station wants to leave network.
  - Can’t use network after deauthenciation.
- Privacy
  - message content encrypted by using WEP, encrypt algorithm RC4.

Services

- Data Delivery
  - way to transmit/receive data.
  - transmission is not guaranteed to be completely reliable.
  - higher layer must deal with error detection and connection.

IEEE 802.11 variants

Protocol	Frequency	Maximum data rate (theoretical)
802.11ax	2.4 or 5GHz	2.4 Gbps[1]
802.11ac wave2	5 GHz	1.73 Gbps[2]
802.11ac wave1	5 GHz	866.7 Mbps[2]
802.11n	2.4 or 5 GHz	450 Mbps[3]
802.11g	2.4 GHz	54 Mbps
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
Legacy 802.11	2.4 GHz	2 Mbps

https://www.intel.in/content/www/in/en/support/articles/000005725/network-and-i-o/wireless.html

QOS FOR VOICE AND VIDEO PACKETS

- Delay sensitive voice and video given priority to get ahead of less time critical file transfer
- Given weighted priority
  1. Use HCF hybrid coordination function, AP poles station in weighted way to offer QOS
  2. Extended DCF : High priority station choose random backoff interval for small CW

LAN and WAN design

- Determine transmission time of 22 KB file with mobile data network (ADRIS) with bandwidth 10 Kbps
- Repeat same for Legacy WLAN 802.11 with bandwidth 2 Mbps
- For mobile data network
  - Transmission Time of 22 KB file
  = Message size/Bandwidth
  =22x8/10=**17.6 sec**
  - Hence old mobile data networks limited file length of data around 20 KB (short messages, SMS)
- For legacy 802.11
  - Transmission time = 22x8/2000000 = **88 ms**
- 88 ms << 17.6 sec

LAN and WAN design

- What is the length of file that WLAN can carry in the time that mobile data network carried 20 KB file?
- For mobile data network
  - Transmission time of 20 KB file

  = Message size/Bandwidth

  =20x8/10 = 16 sec
- In 16 sec bits that WLAN can transfer

  = 16 x 2000000 bits (Time x BW)

  =32000000 bits

  = 32000000/8 bytes

  = 4000 KB

LAN and WAN design

- What do you infer from the answers?
- LAN is designed to operate
  - with smaller propagation delay (88 ms v/s 17.6 s)
  - larger file transfer
  - higher data rate (2 Mbps v/s 10 Kbps)
- So length of packet is longer in LAN than that in WAN (mobile data network)
- WAN (mobile data network) are low speed and developed for communicating short messages
- With smaller propagation delay and long packets collisions can be easily detected and CSMA/CA can be used to avoid the collisions

Thank You!