Wireless Networking

Instructor course: Dr.Hanal Abuzant

66554, Computer Engineering

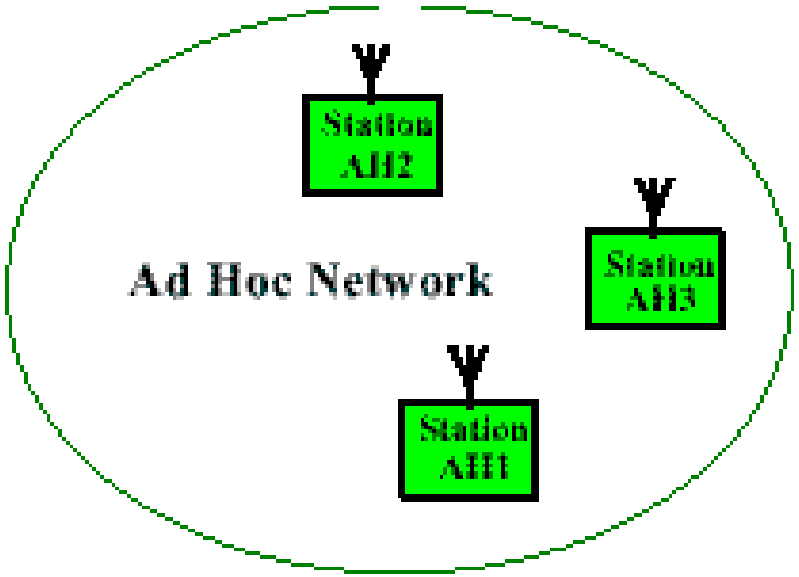
An-Najah National University

System Architecture

- Two basic system architectures:-

  a) Ad hoc

  b) Infrastructure based



- A BSS without an AP is called as Ad hoc network.
- A group of stations using the same radio frequency.

Ad-hoc network

- It is the simplest form of Wireless LAN
- All nodes are equal and may join or leave at any time, and have equal right to the medium.
- all nodes must be able to see all the other nodes of the network, to be able to establish communication with them.
- When a node goes out of range, it just loose connection with the rest of the ad-hoc network.

MAC Sublayer (wireless protocols)

IEEE 802.11 defines two MAC sublayers:-

i) Distributed Coordination Function(DCF)

ii) Point Coordination Function(PCF)

DCF:- One of the two protocols defined by IEEE at the MAC sublayer is called the distributed coordination function. Which is designed for Adhoc networks

PCF:- -The point coordination function is an optional access method that can be implemented in an infrastructure network.

-PCF has a centralized,contention-free access method. The AP performs polling for stations that are capable of being polled.

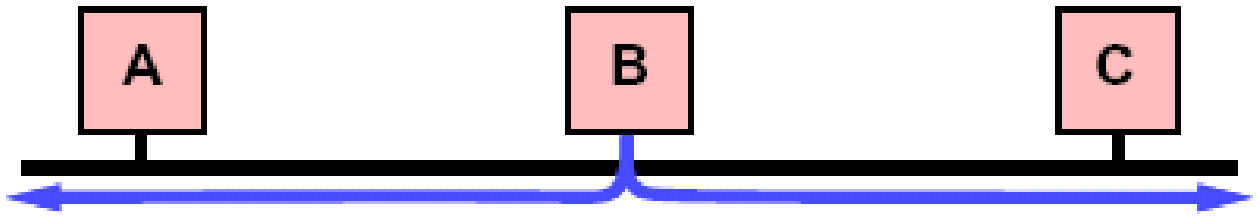
Access Channel

access to the shared medium

Carrier Sense Multiple Access (CSMA)

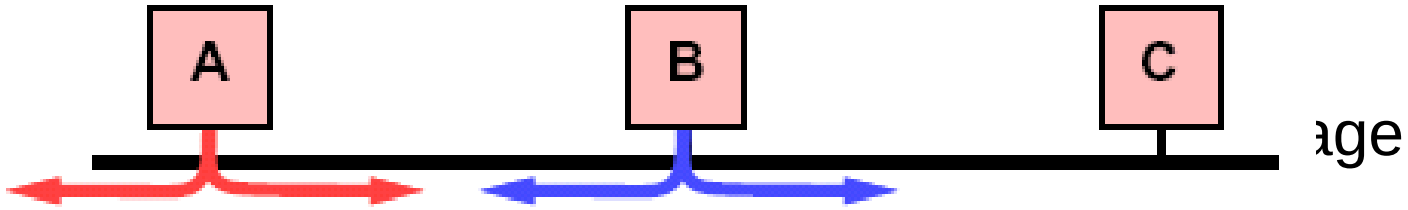
How to share a common channel?

- Listen for **carrier** before transmitting
- Carrier means: the channel is busy
- While you hear carrier, wait before transmitting



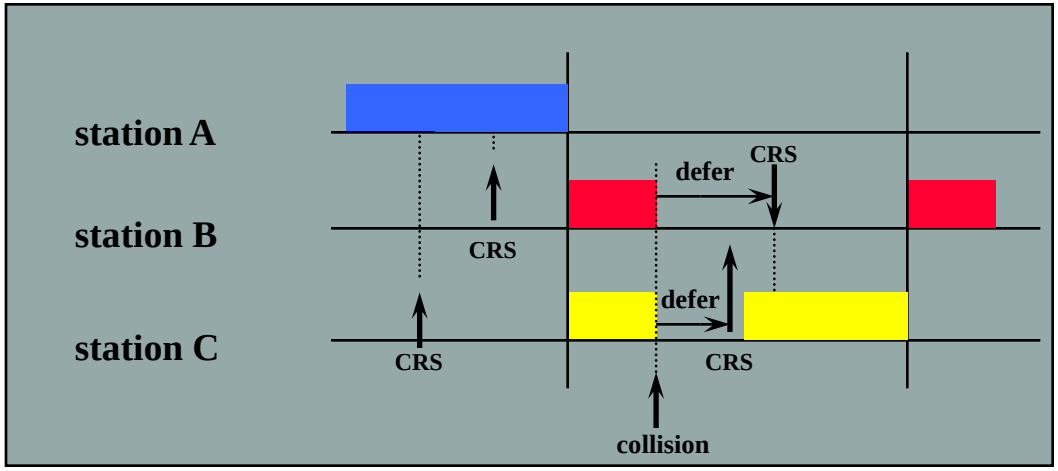
Collision Detect (CD) algorithm

- Listen channel while transmitting
- If what you hear isn't what you're sending, then ***collision***:
  - Abort transmission of current packet



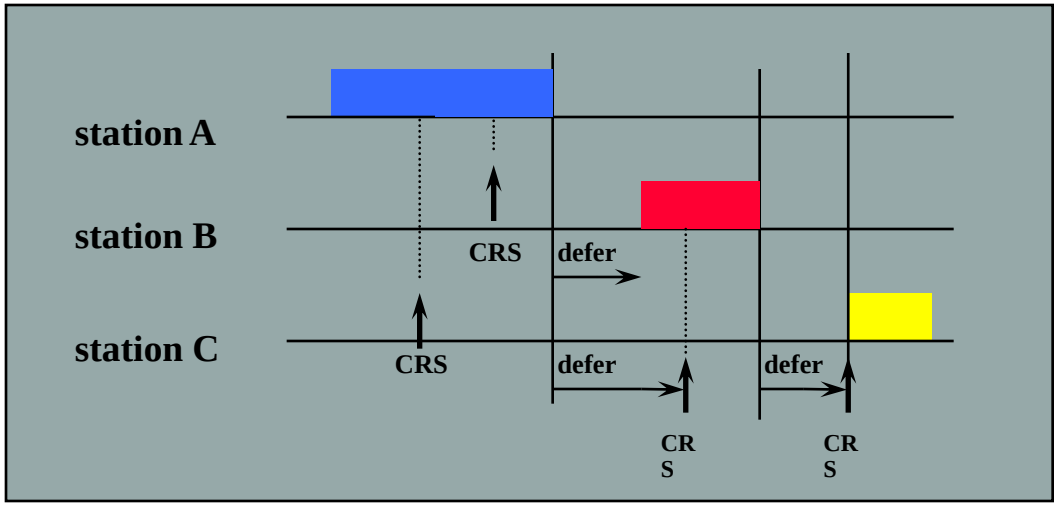
•If two wireless stations transmit at the same time, the radio energy of the two frames will be combined, and all the receivers will just get garbage. This is known as a ***collision***.

Accessing the medium CSMA/CD



- Wired networks can detect collisions (e.g. Ethernet adapters)
  - Carrier Sensing: listen to the media to determine if it is free oe idle
  - Initiate transmission as soon as carrier drops
  - When collision is detected station defers
  - When defer timer expires: repeat carrier sensing and start transmission

Accessing the medium CSMA/CA



- Wireless LAN adapters cannot detect collisions:
  - Carrier Sensing - listen to the media to determine if it is free
  - Collision Avoidance - minimize chance for collision by starting (random) back-off timer, when medium is sensed free, and prior to transmission

CSMA/CA

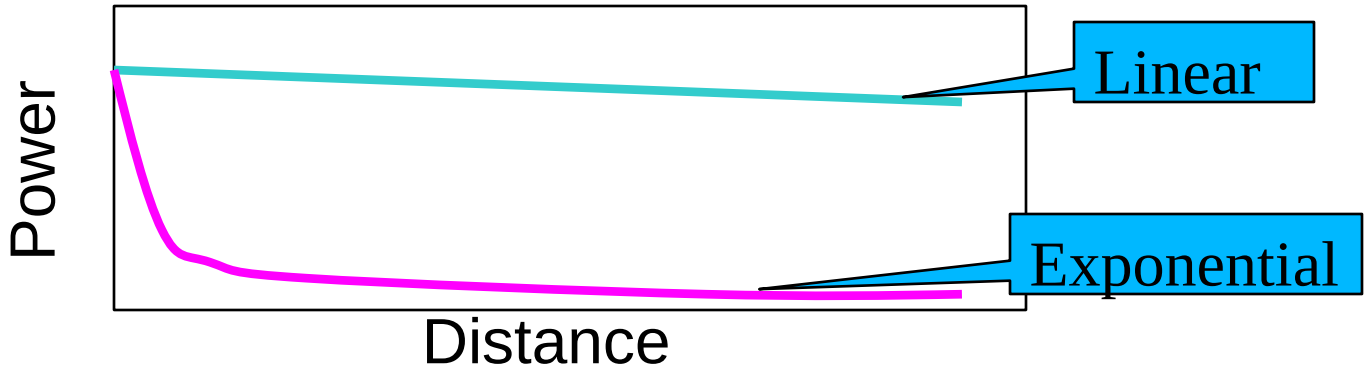
Wireless LANs cannot implement CSMA/CD for a lot of reasons:-

- For collision detection a station must be able to send data & receive collision signals at the same time.
- Collision may not be detected because of the hidden station problem.
- The distance between stations can be great. Signal attenuation could prevent a station at one end from hearing a collision at the other end.
- Unlike wired LANs where a station can transmit a frame at any time to the directly connected switch, wireless stations have to share a single set of transmitting frequencies.

Wireless CSMA

CSMA can be used in wireless, but has problems

- ***wired*** network: signal strength at sender and receiver are essentially the same
- ***wireless*** network: ***inverse square law*** applies ($P_{recv} = P_{xmit}/D^2$)



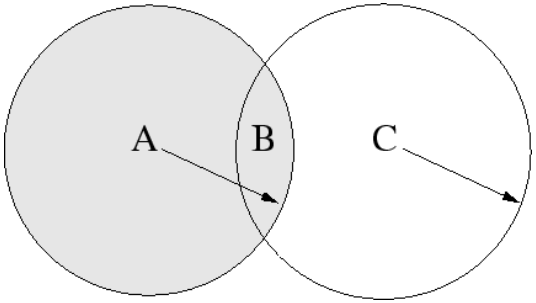
CSMA does not give the right information in wireless:

- Carrier sense detects signals at the ***transmitter***
- But collisions occur ***at the receiver***

Collisions in wireless

Collisions are a big problem for wireless, for several reasons:

- In order for a transmitting station to detect a collision, it needs to be "receiving" at the same time as transmitting. This is expensive and very few wireless cards can do it; nearly all cannot send and receive at the same time.
- The Hidden Transmitter Problem. Consider stations A, B and C in the diagram. The circles show the transmission range for A and C. If stations A and C send a frame at the same time, station B will sense the collision, but neither transmitter will. They will assume that their frame was sent successfully.



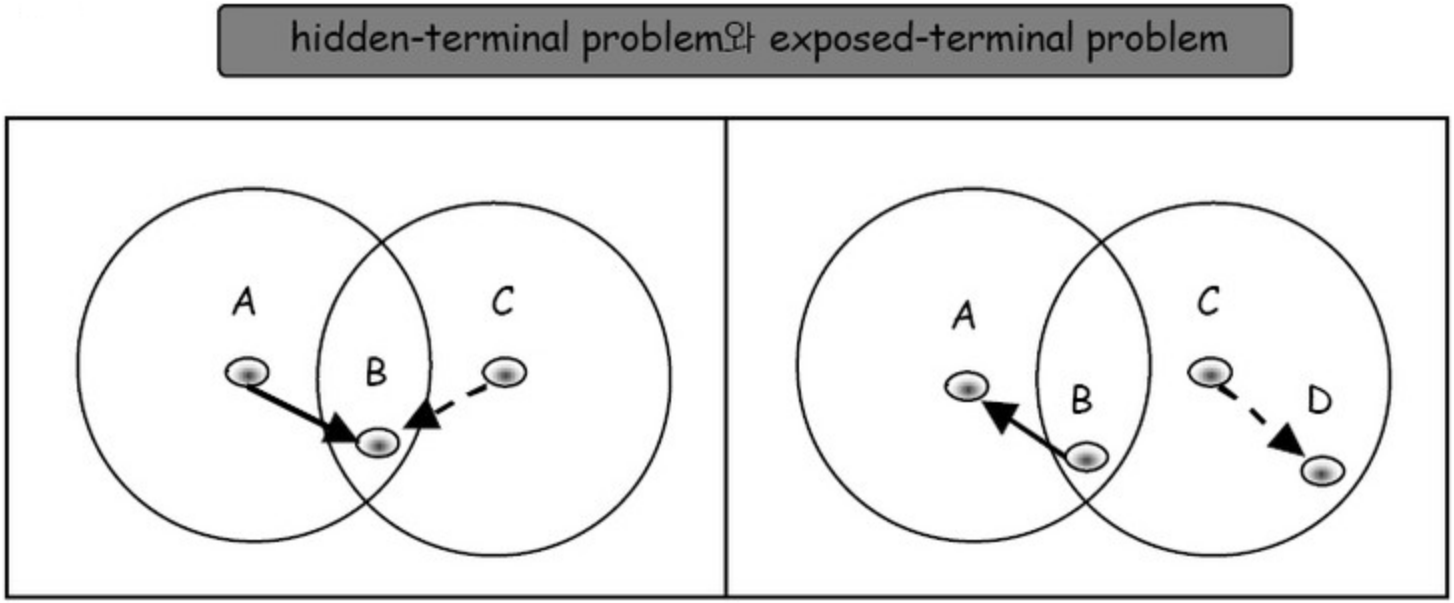
Collisions in wireless

- For these reasons, wireless uses a *medium access control* (MAC) mechanism called CSMA/CA: carrier sense medium access with collision avoidance.
- Because stations cannot detect collisions while they are transmitting, there must be an algorithm to avoid them in the first place.
- CSMA/CA uses a number of control frames as well as data frames, to make the MAC work.
- The term "carrier sense" here means listening on the wireless frequencies to see if another station is transmitting. If the carrier is idle/clear, every station contend for transmitting.

Problems need solution

CSMA does not give the right information in wireless:

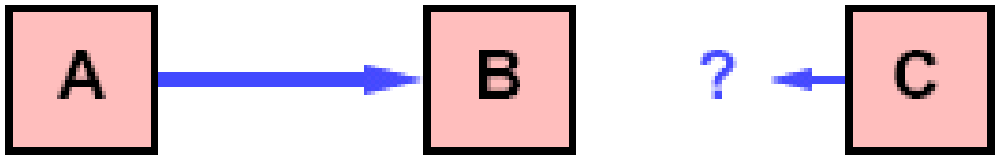
- Carrier sense detects signals at the ***transmitter***
- But collisions occur ***at the receiver***



The Hidden Terminal Problem

Consider the following situation:

- A is sending to B
- C is ***out of range*** of A's transmissions to B
- C wants to send (to anybody)



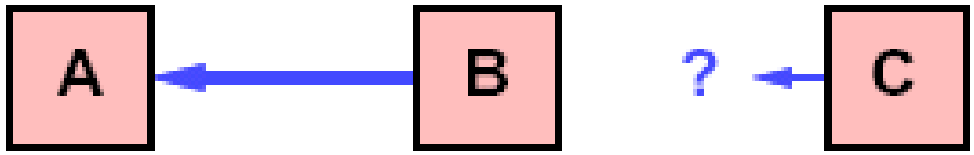
CSMA doesn't work well for wireless here:

- C can't know to wait since it can't hear carrier from A
- B can hear both A and C, thus collision at B
- A is "hidden" to C

The Exposed Terminal Problem

Consider the following situation:

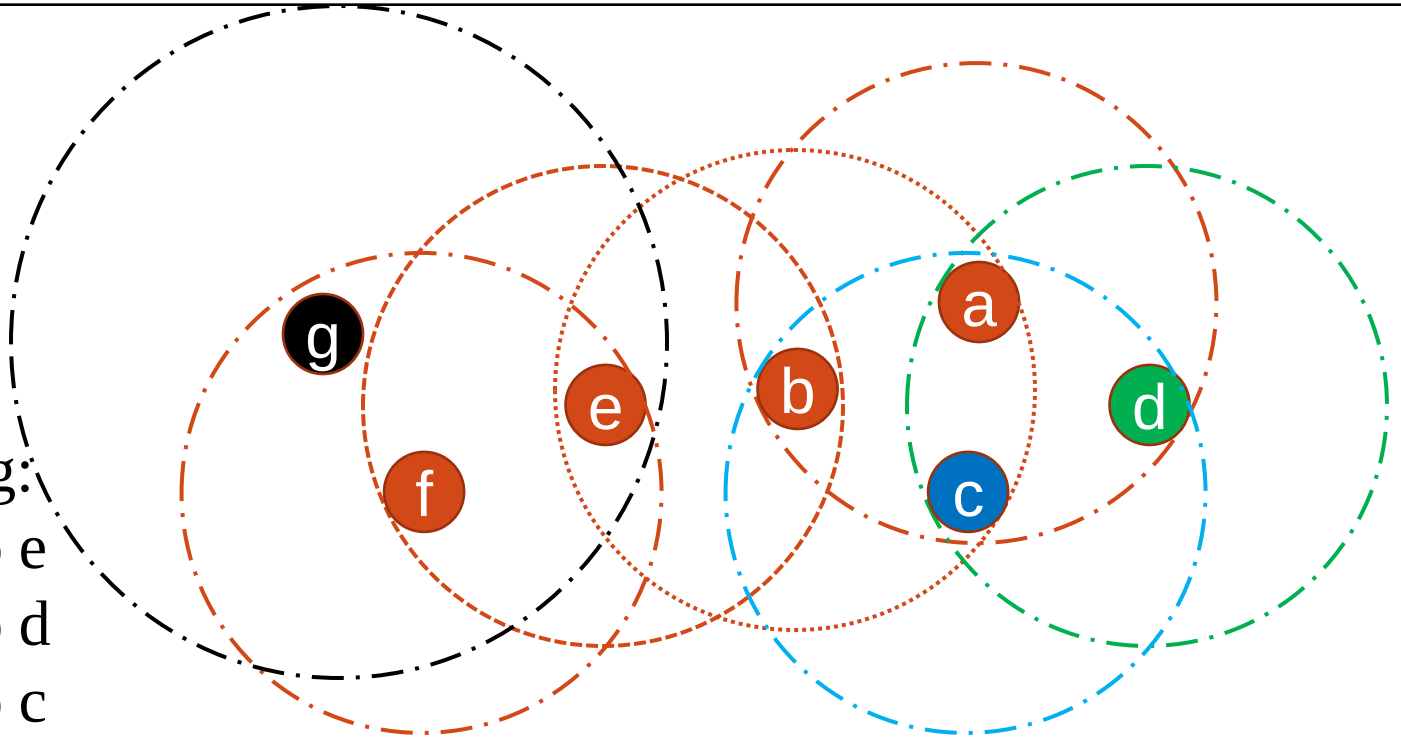
- B is sending to A
- C is ***in range*** of B's transmissions to A
- C wants to send to anybody except B



CSMA doesn't work well for wireless here either:

- C thinks it should wait since it can hear carrier from B
- If A is out of range of C, then C waits needlessly
- C is "exposed" to B

Example:



Solve following:

- A to c and b to e
- A to d and c to d
- B to c and d to c
- G to f and e to f
- E to g and f to g
- E to b and g to f

Which node could send successfully?
Which node will wait before sending?
Which node receive successfully?
Where is the collision for each case?

Partial Solution: control packets

Packet types:

- ***Request-to-Send*** (RTS): Sender sends to receiver before sending a data packet
- ***Clear-to-Send*** (CTS): Receiver replies if ready for data packet to be sent
- ***Acknowledgment*** (ACK): receiver sends if data is received successfully

All packets contain:

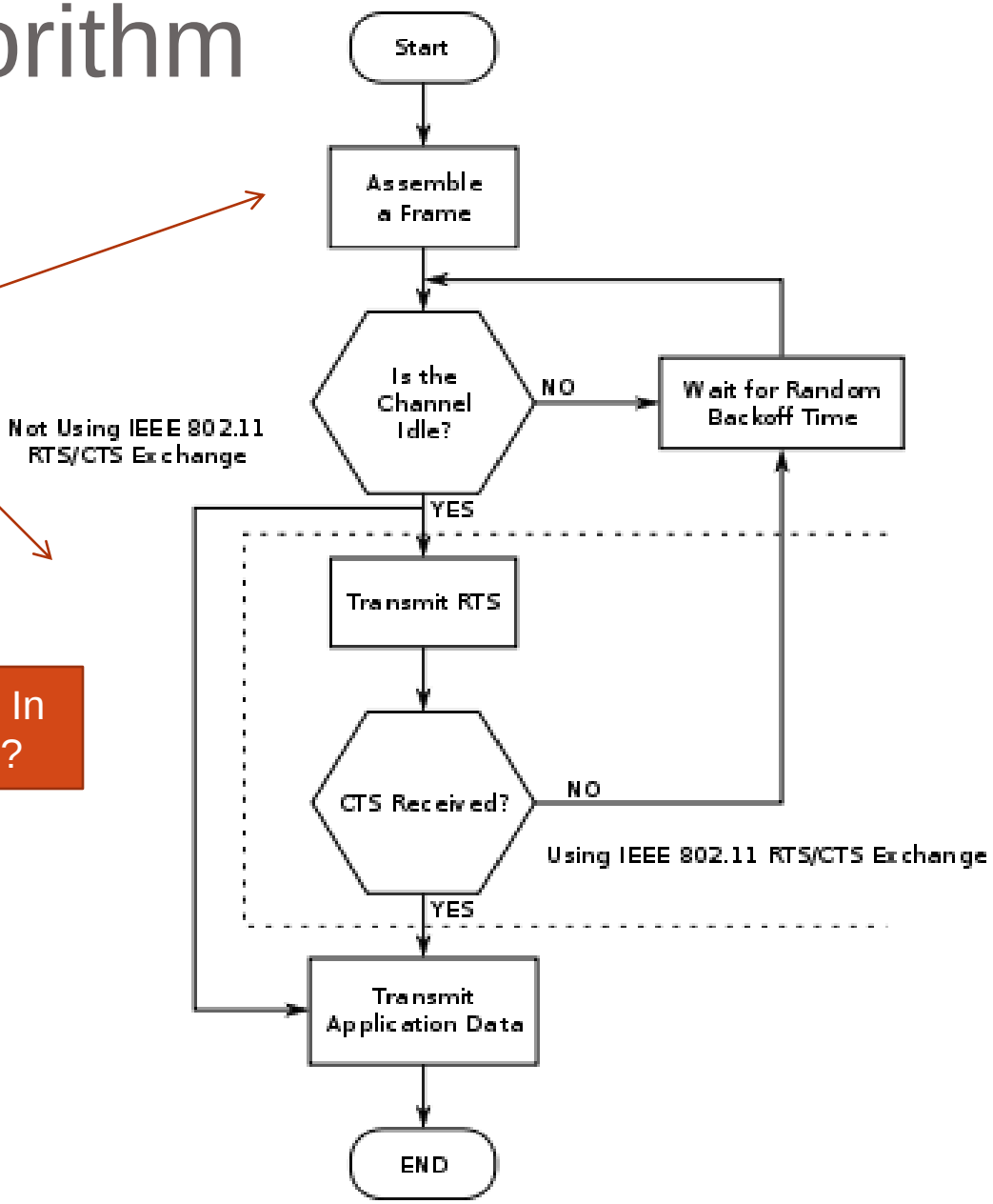
- Address of the ***sender*** of the intended data packet
- Address of the ***receiver*** of the intended data packet

Simplified Algorithm of CSMA/CA

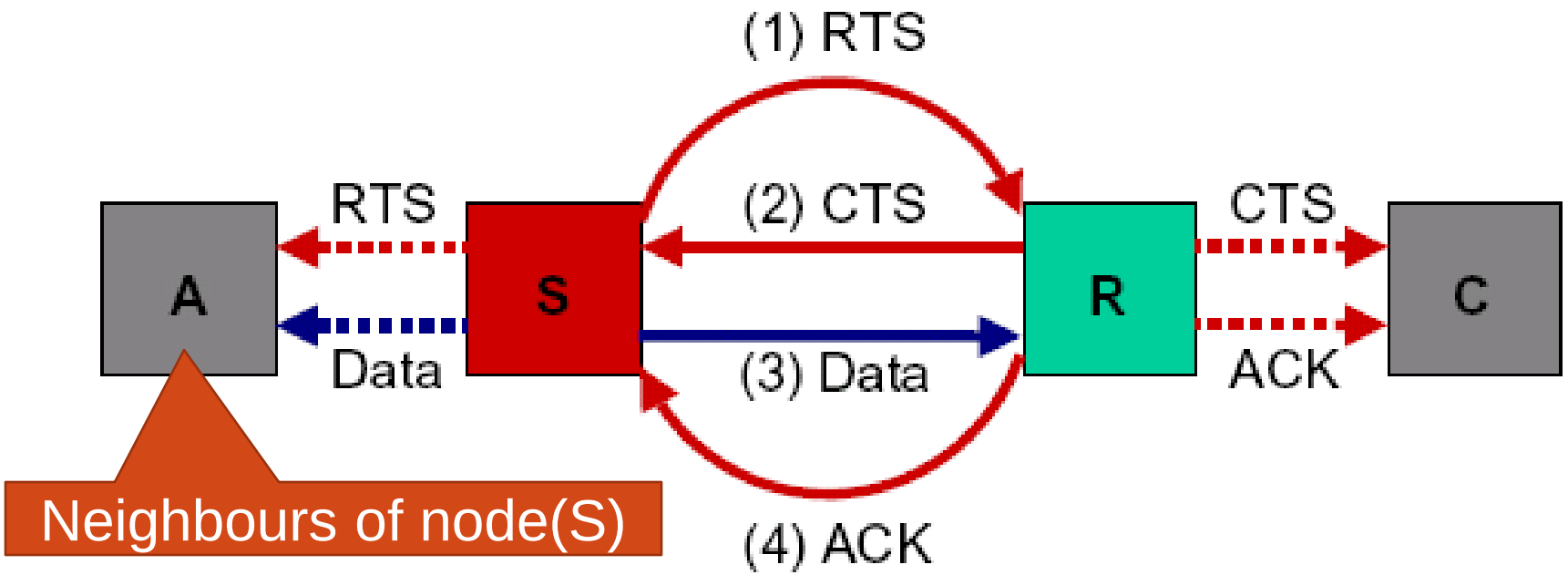
There are some problems in the protocol, describe them with your teacher

Where could the protocol be applied? In the sender or receiver or else nodes?

Extend the protocol to be a complete CSMA/CA

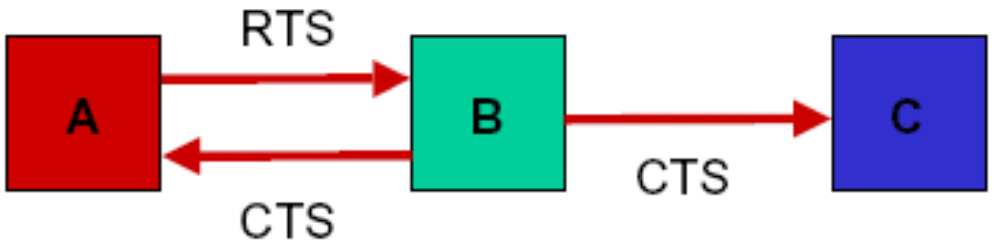


control packets



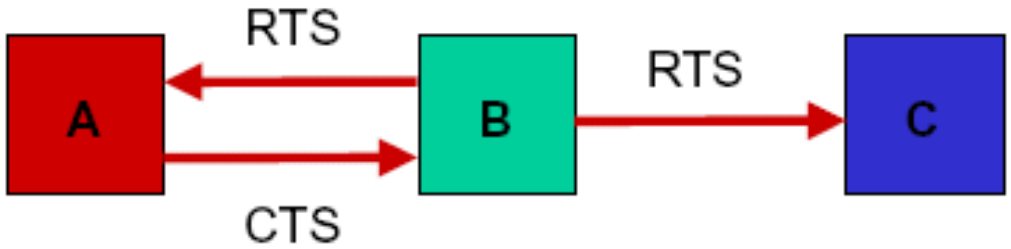
Did the control packets solve the problems?

- Hidden terminal problem is avoided:



C waits to send since it hears B's CTS

- Exposed terminal problem is avoided:



C does not wait to send since it does not hear A's CTS

Does (and cannot) ***not*** prevent all collisions!

RTS/CTS

- It may optionally be used to access to the shared medium to solve discussed problems.
- the Access Point only issues a *Clear to Send* to one node at a time.
- wireless 802.11 implementations do not typically implement RTS/CTS for all transmissions.
- At least it is not used for small packets
- the overhead of RTS, CTS and transmission is too great for small data transfers.
- wireless 802.11 may turn it off completely,

IEEE 802.11 Usage Model

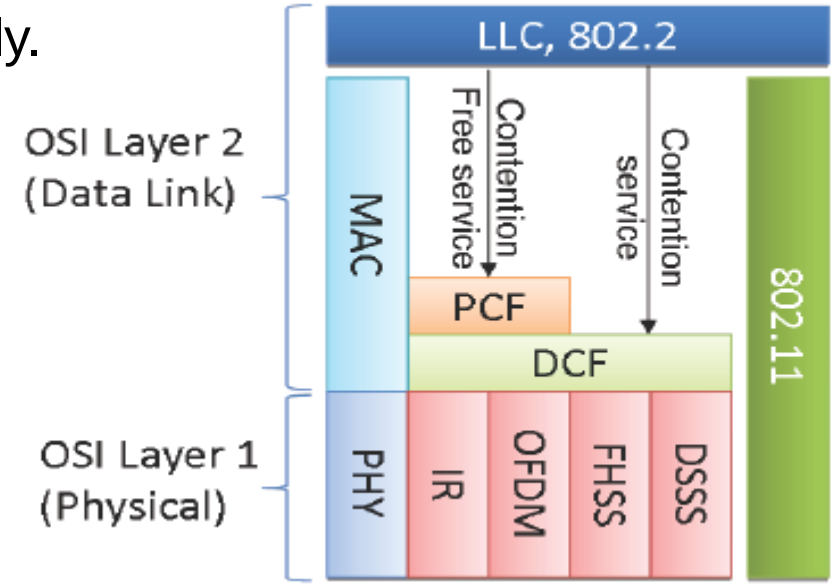
Host computer sees an “Ethernet interface”

- Just like a wired LAN
- Uses 48-bit 802.3 MAC addresses
- All hosts “in range” of each other see common shared channel
- Can directly communicate with neighbors

IEEE 802.11 Modes of Operation

Media Access Control modes (DCF)

- Distributed Coordination Function (DCF)
- Used in ad-hoc mode
- DCF is a method to access the channel in a distributed way.
- which is used for the contention based services
  - (i.e. initiating the back-off counter)
- It is an asynchronous
- method to access the channel randomly.
- Nodes communicate directly with each other



The CSMA/CA Algorithm

- Here are the basic rules for CSMA/CA:
  - Every frame sent and successfully received must be immediately acknowledged. If after a short timeout period the sender doesn't get an acknowledgment message it will retransmit the frame. Every time a frame is re-sent the sender increments a counter; if the counter reaches some limit the 802.11 data link tells the higher layer software that the transmission failed.
  - When the carrier is idle a station is able to send, but it cannot send immediately; it must wait for a short period of time, called the DIFS. If two or more stations have been waiting to send then when the carrier has been idle for a DIFS time they will all send at the same time and cause a collision. So they all add an extra random time to reduce the chance of collision.
  - When a sender doesn't get an acknowledgment (probably due to a collision so there will be other stations also getting failures) it will retransmit. When the carrier is idle it will wait for a DIFS period to which it adds a further random time but the random time will probably be longer; for every retransmission the range of values used for the random time is increased. This increasing range of delays is called the *contention window*. When the frame is acknowledged, or it gives up trying, the contention window is reset to its starting value.
  - Between any two frame transmissions of any type there must be a short delay called an *inter-frame space* IFS. There are 4 different IFS times: SIFS, PIFS, DIFS and EIFS. The reason for having four times is to permit higher priority transmissions to use the carrier. When a station wants to send a new frame it waits for a DCF IFS (DIFS) time. When a receiver sends an acknowledgment it waits for a *short* IFS (SIFS). This guarantees that the acknowledgment will be sent with no collisions from other frames as the SIFS is shorter than the DIFS.

802.11 Carrier Sensing

802.11 uses both ***physical*** and ***virtual*** carrier sensing:

- Physical carrier sense provided by PHY
- Virtual carrier sense provided by MAC

Virtual carrier sensing:

- Maintained by station through ***Network Allocation Vector (NAV)***
- NAV records prediction of future traffic on medium
- Counter that counts down busy time at uniform rate
- Set based on Duration field in received packets (e.g., RTS, CTS)
- When nonzero, virtual carrier sense thinks medium is busy

Carrier sense mechanism combines both mechanisms:

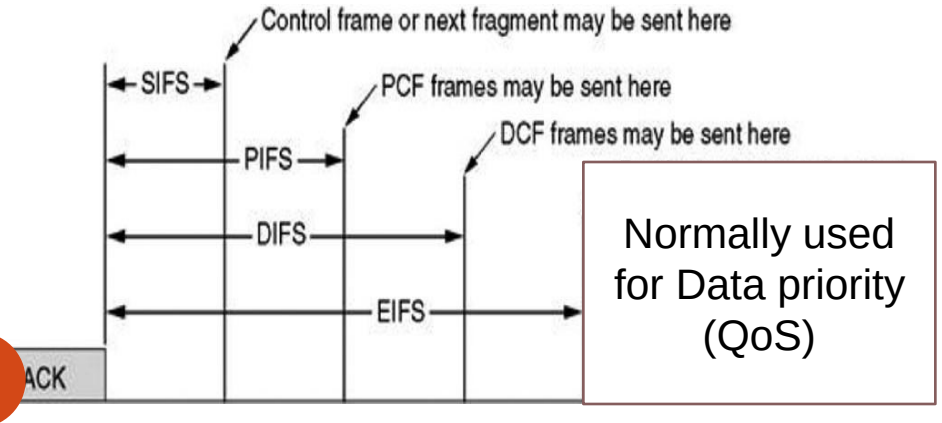
- Medium considered busy whenever either indicates carrier
- Medium also considered busy whenever our own transmitter is on

IFS - Inter Frame Spacing

The IEEE 802.11 DCF controls priority access to the wireless channel through the use of Inter Frame Space (IFS) time intervals between the transmissions of frames. The IEEE 802.11 DCF specifies four IFS intervals, which are used to provide different priorities:

- Short IFS (**SIFS**) time intervals that have the highest priority access to the channel and are used for control packets
- Distributed coordination function IFS (**DIFS**) time intervals, which are used in the basic access method in IEEE 802.11 DCF (Adhoc)
- Point coordination function IFS (**PIFS**) time intervals which are used in the IEEE 802.11 PCF (infrastructure mode)
- Extended IFS (EIFS) time intervals. EIFS is a longer IFS used a collision occurred and QoS

IFS	802.11b	802.11g	802.11a	802.11n 2.4GHz	802.11n 5GHz
SIFS	10µs	10µs	16µs	10µs	16µs
Slot Time	20µs	Long = 20µs Short = 9µs	9µs	Long = 20µs Short = 9µs	9µs
DIFS	50µs	Long = 50µs Short = 28µs	34µs	Long = 50µs Short = 28µs	34µs



Normally used for Data priority (QoS)

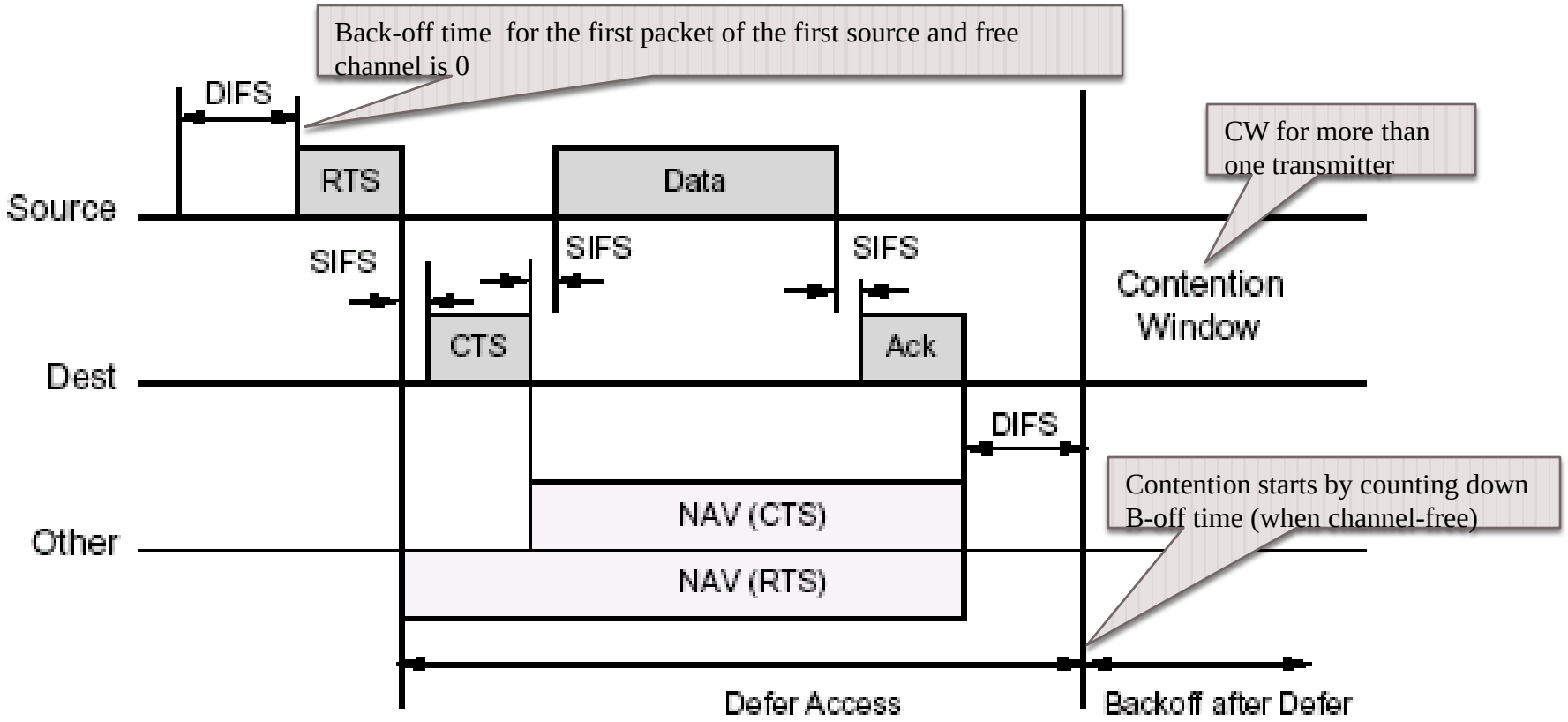
In most versions of IEEE802.11, DIFS is defined by

DIFS = SIFS + 2 SlotTime

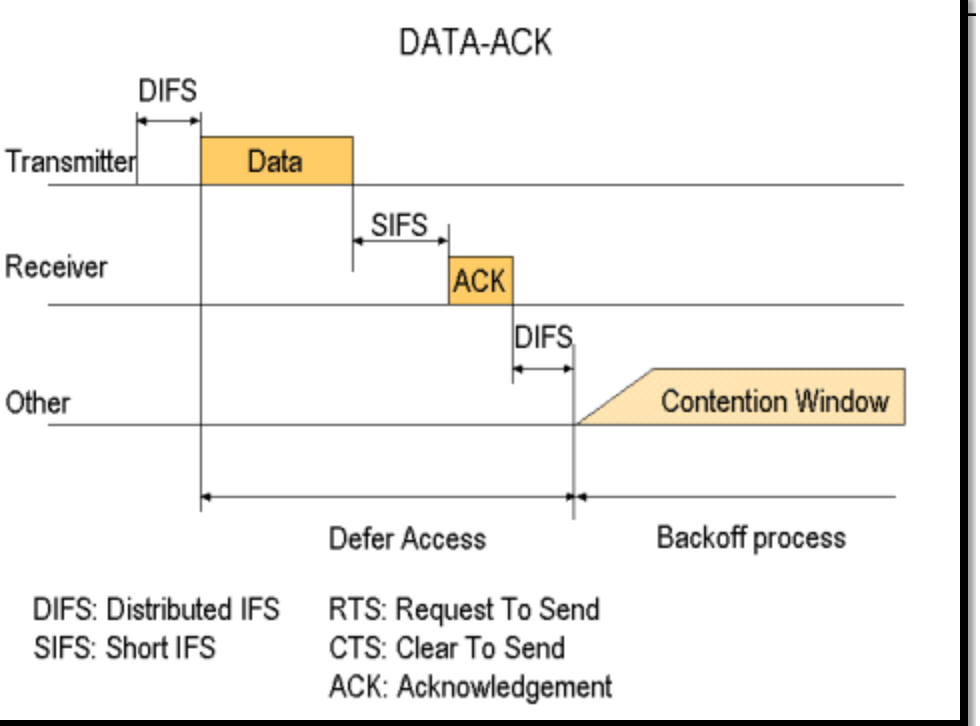
DIFS (MAX) > PIFS > SIFS (MIN)

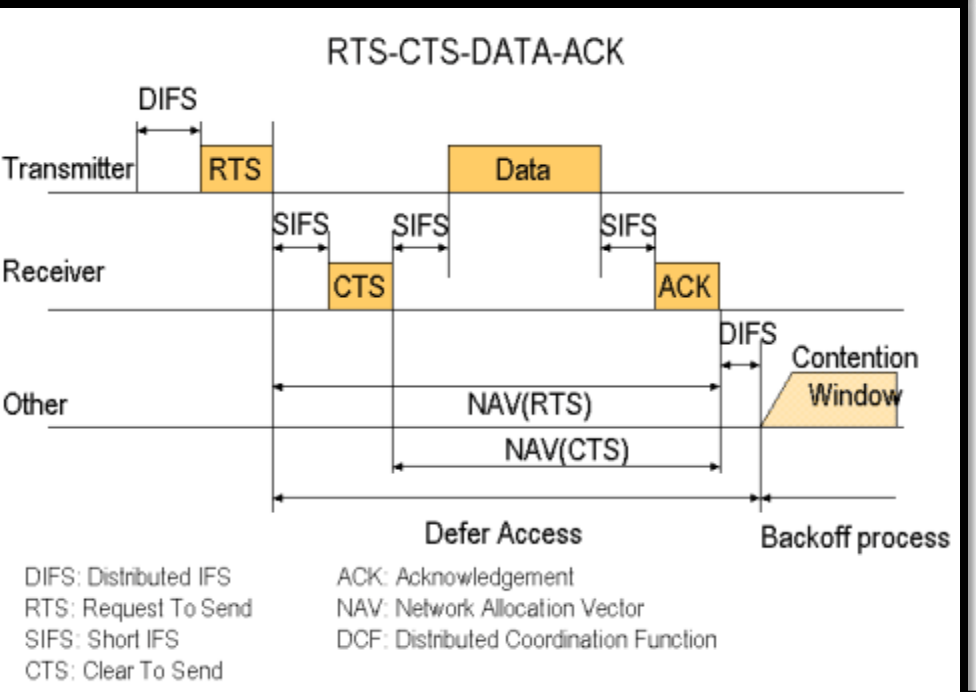
Use of RTS and CTS

Other data senders must wait until entire RTS/CTS/Data/ACK finished



RTS/CTS only used for data packets larger than some threshold --- You can tune this!





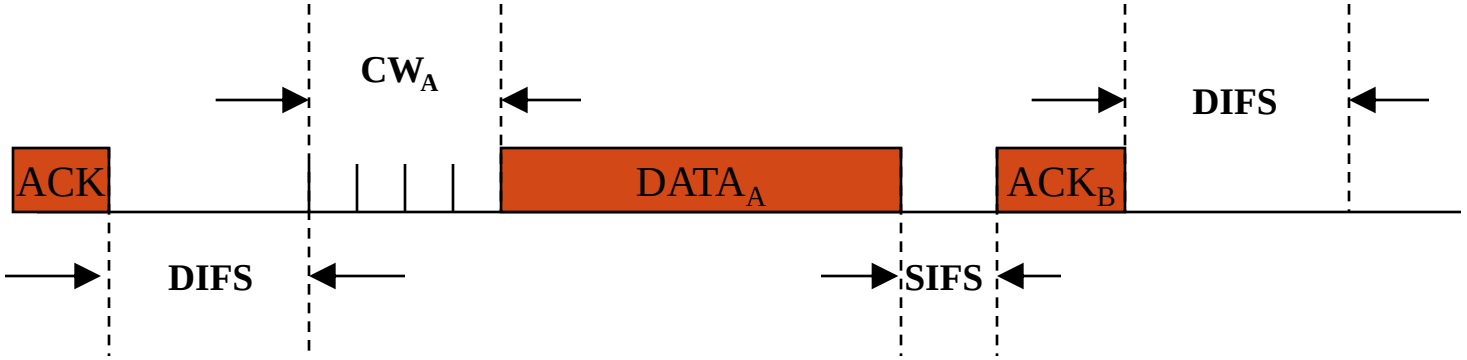
Algorithm 1 DCF access channel

Require: Receiving_packet_from_upper_layer
  $attempt \Leftarrow 1; backoff \Leftarrow 0; CW \Leftarrow CW_{min}$
  Listen: Free_channel
  if channel is not idle **then**
    $attempt \Leftarrow attempt + 1$
    goto Listen
  end if
  Wait DIFS
  if $attempt \neq 1$ **then**
    if $backoff = 0$ **then**
      $backoff \Leftarrow Random\_value(0, CW)$
    end if
    Counting_down_backoff
    while $backoff \neq 0$ **do**
      $backoff \Leftarrow backoff - 1$
      if channel is not idle **then**
        goto Listen
      end if
    end while
  end if
  if channel is not idle **then**
    goto Listen
  end if
  $attempt \Leftarrow attempt + 1$
  Transmitting_packet
  Start ACK_timer
  if ACK_received = false **then**
    Collision
    $CW \Leftarrow CW \times 2$
    if $CW \geqslant CW_{max}$ **then**
      $CW \Leftarrow CW_{max}$
    end if
    if Exceeding_retransmission_number = true **then**
      Print "Error of transmission"
    else
      goto Listen
    end if
  else
    Print "Successful transmission"
    $CW \Leftarrow CW_{min}$
  end if

Backoff (B-off)

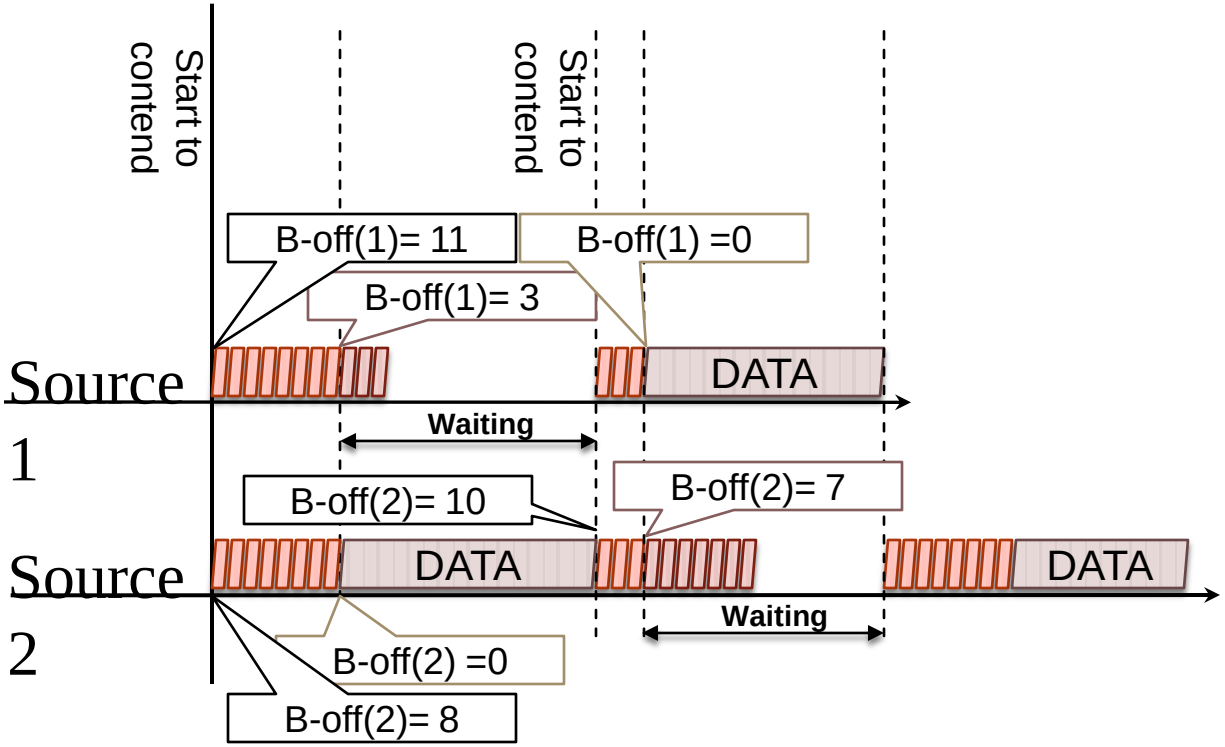
- **Decrease the possibility of contention/collision**
- **Backoff window**
  - Choosing a random number withen a window [0,CW]
  - CW is a contention Window
- **Random backoff number**
  - This number is chosen from the period [0,CW]
- **Random backoff time**
  - **= Backoff number x slot time**
  - Time to wait to avoid collision
  - Waiting time to contend access channel

Node A send to Node B

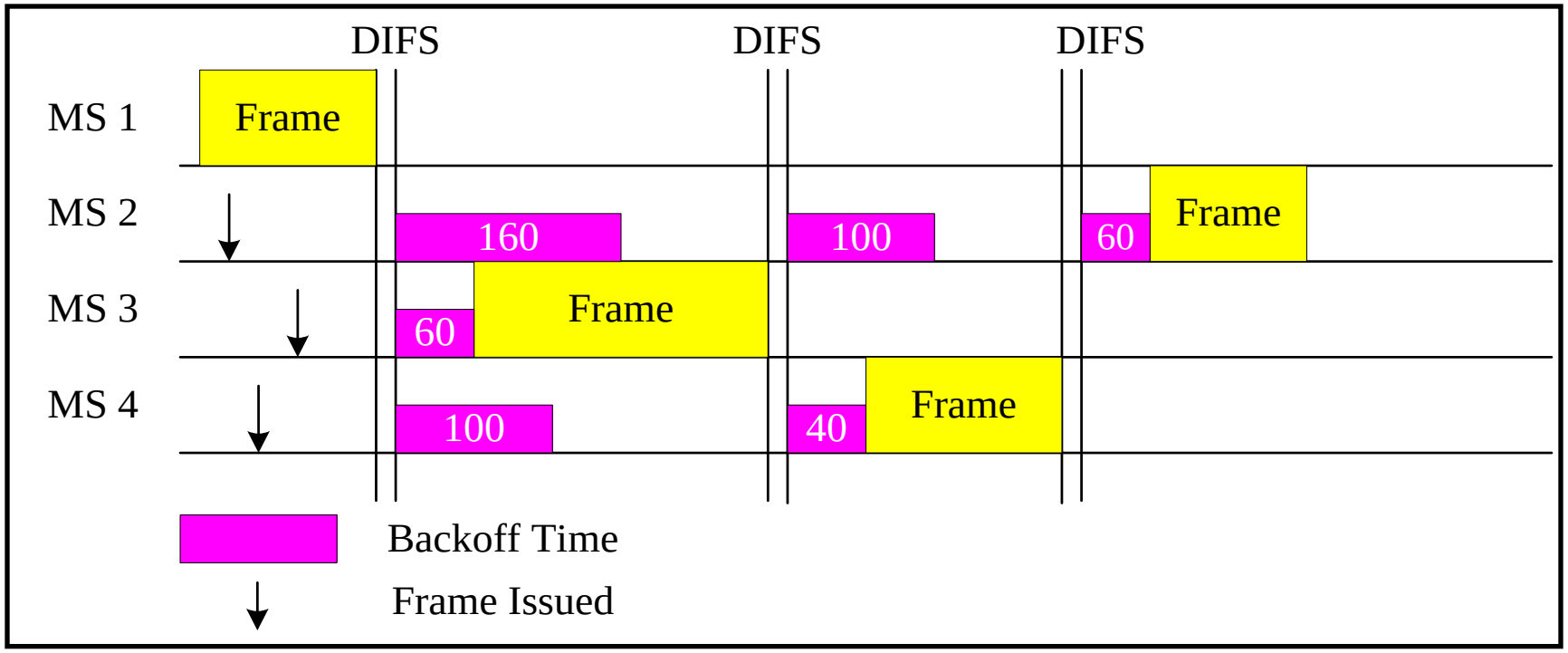


- CW – Contention Window. Starts only after DIFS.
- Random number ‘r’ picked form range (0-CW)
- CW_{min} minimum value of CW
- CW_{max} maximum value the CW can grow to after collisions
- ‘r’ can be decremented *only* in CW
- CW doubles after every collision

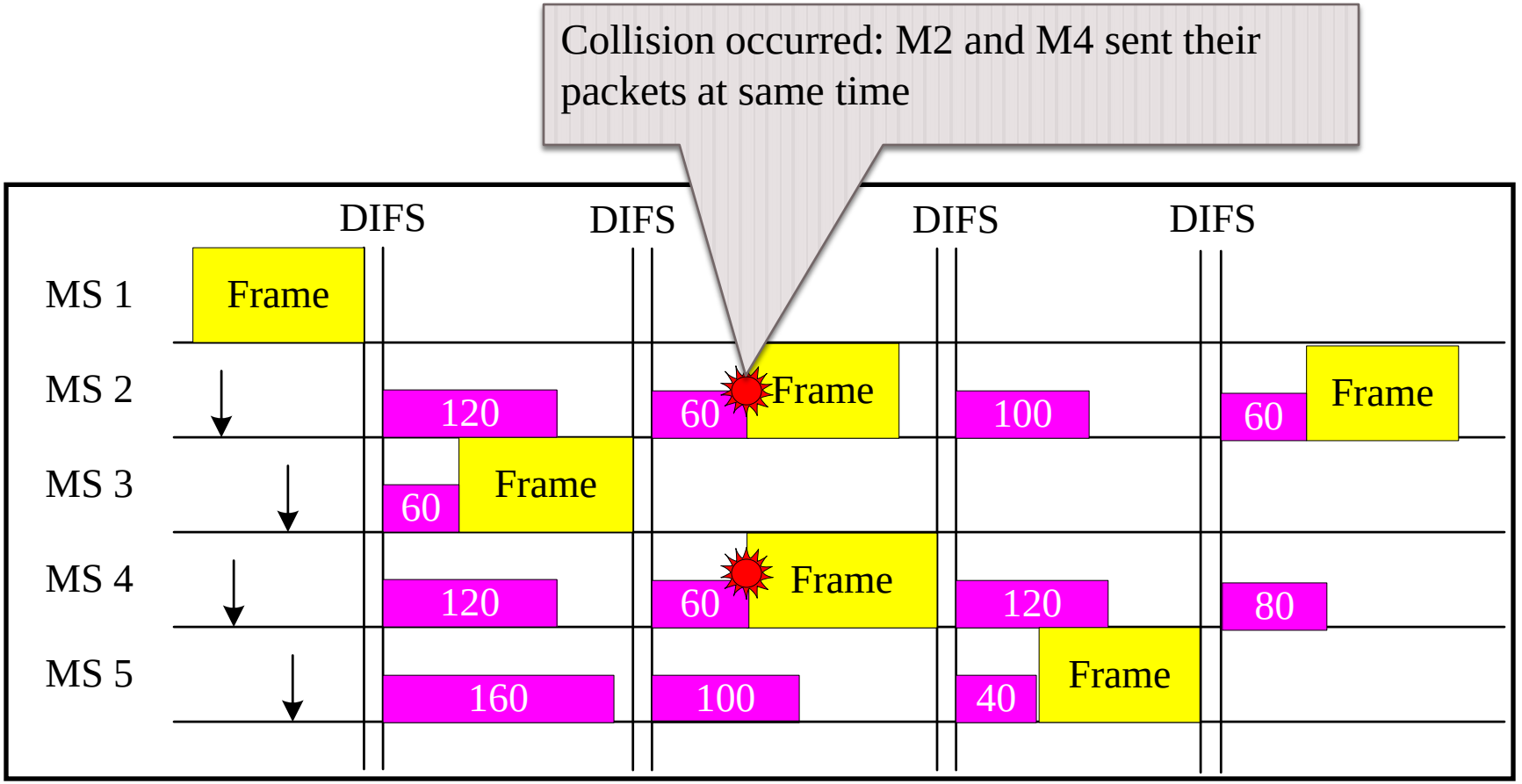
Back-off counter



Example of Backoff Mechanism (without collision)

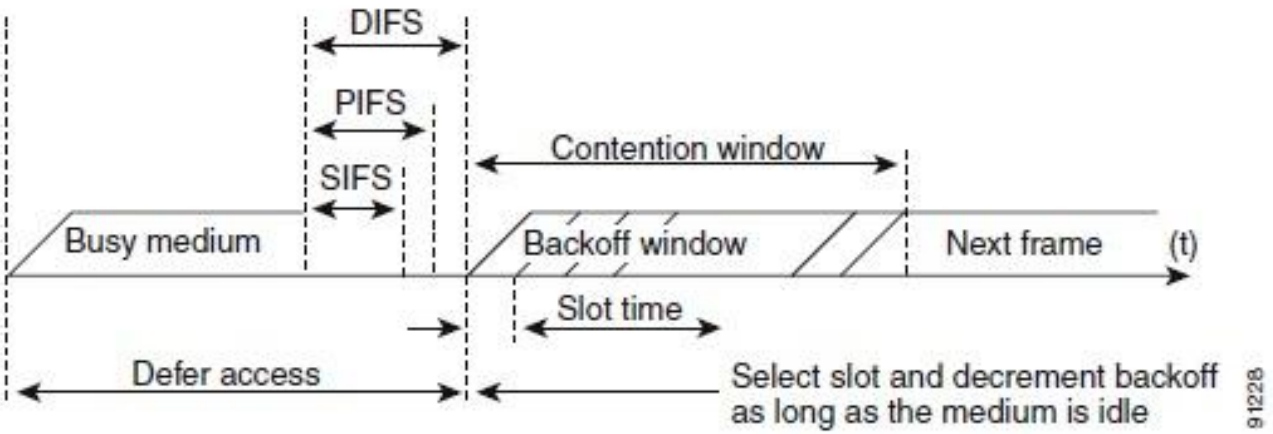


Example of Backoff Mechanism (with existance of collision)



IFS	802.11b	802.11g	802.11a	802.11n 2.4GHz	802.11n 5GHz
SIFS	10µs	10µs	16µs	10µs	16µs
Slot Time	20µs	Long = 20µs Short = 9µs	9µs	Long = 20µs Short = 9µs	9µs
DIFS	50µs	Long = 50µs Short = 28µs	34µs	Long = 50µs Short = 28µs	34µs

Figure 2-3 Interframe Spaces



802.11 - Congestion Control

- Contention window (cw) in DCF: Congestion control achieved by dynamically choosing cw
- *large* cw leads to larger backoff intervals
- *small* cw leads to larger number of collisions

- Binary Exponential Backoff in DCF:
  - When a node fails to receive CTS in response to its RTS, it increases the contention window
    - cw is doubled (up to a bound cwmax =1023)
  - Upon successful completion data transfer, restore cw to cWmin=31

The DCF Protocol

- As it stands, CSMA/CA doesn't help to solve the hidden transmitter problem.
- The Distributed Coordination Function (DCF) helps to overcome this limitation. DCF uses the following control frames:
  - RTS (request to send): if station A wants to send to B it waits for no traffic then sends RTS to B. The RTS contains a duration value covering the whole time of the remaining steps of the transaction (SIFS+CTS time+SIFS+data frame time+SIFS+ACK time) so other stations will set their NAVs. After sending an RTS, the station waits.
  - CTS (clear to send): if B accepts the request it sends CTS back to A, it also sends the NAV duration for the remaining time (same as RTS NAV minus time the CTS takes: SIFS+data frame time+SIFS+ACK time).
  - When A receives the CTS from B it will send the data to B,.
  - ACK: when the data arrives successfully at B it will send an acknowledgment ACK back to A. The transfer is complete.
  - Between each message there is a SIFS delay so no other stations can interrupt.

The DCF Protocol

- If any station hears an RTS from another station it will wait for a time long enough to allow the message to finish before attempting to send.
- If a station hears a CTS from another station it will wait for a suitable length of time. This will *avoid* collisions.
- If collisions occur when two stations send RTS they will not know, because they don't try to detect it, but the intended receiver(s) will fail to receive the RTS because of the collision so it/they will not send a CTS. Consequently the original senders of the RTS will know it failed and they must retry.
- Now consider how this deals with the problems of the "hidden station" above. If A sends RTS to B it will not be detected by C, but C will detect the CTS that B sends back to A, and will therefore set its NAV and wait until the transfer is over.

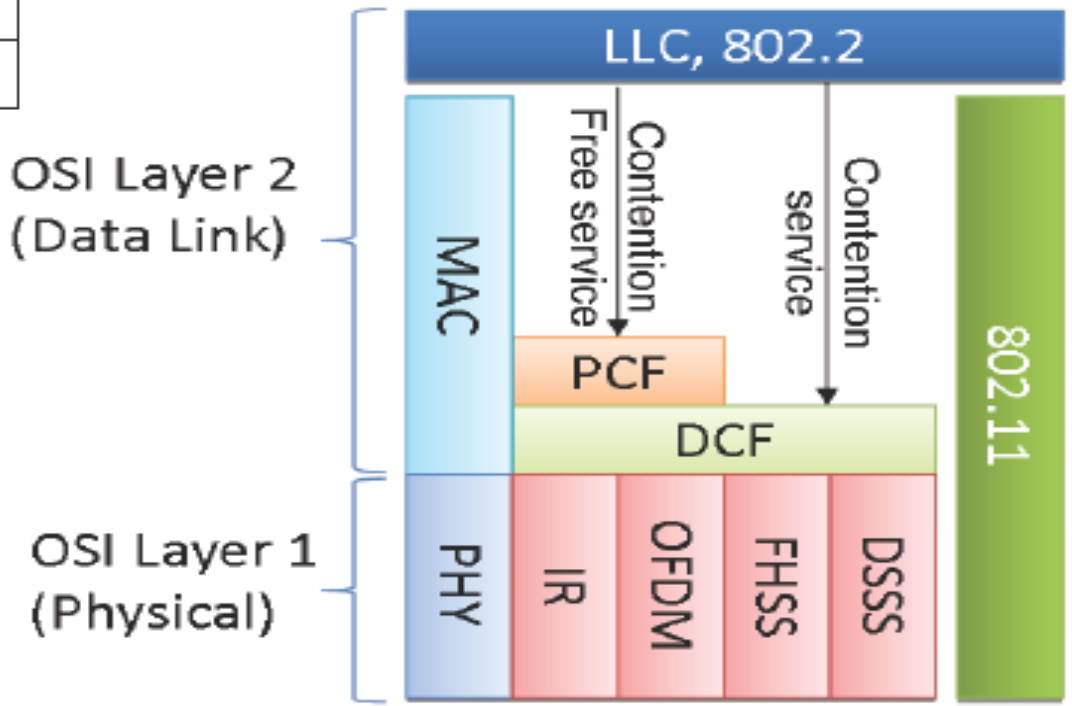
PCF:

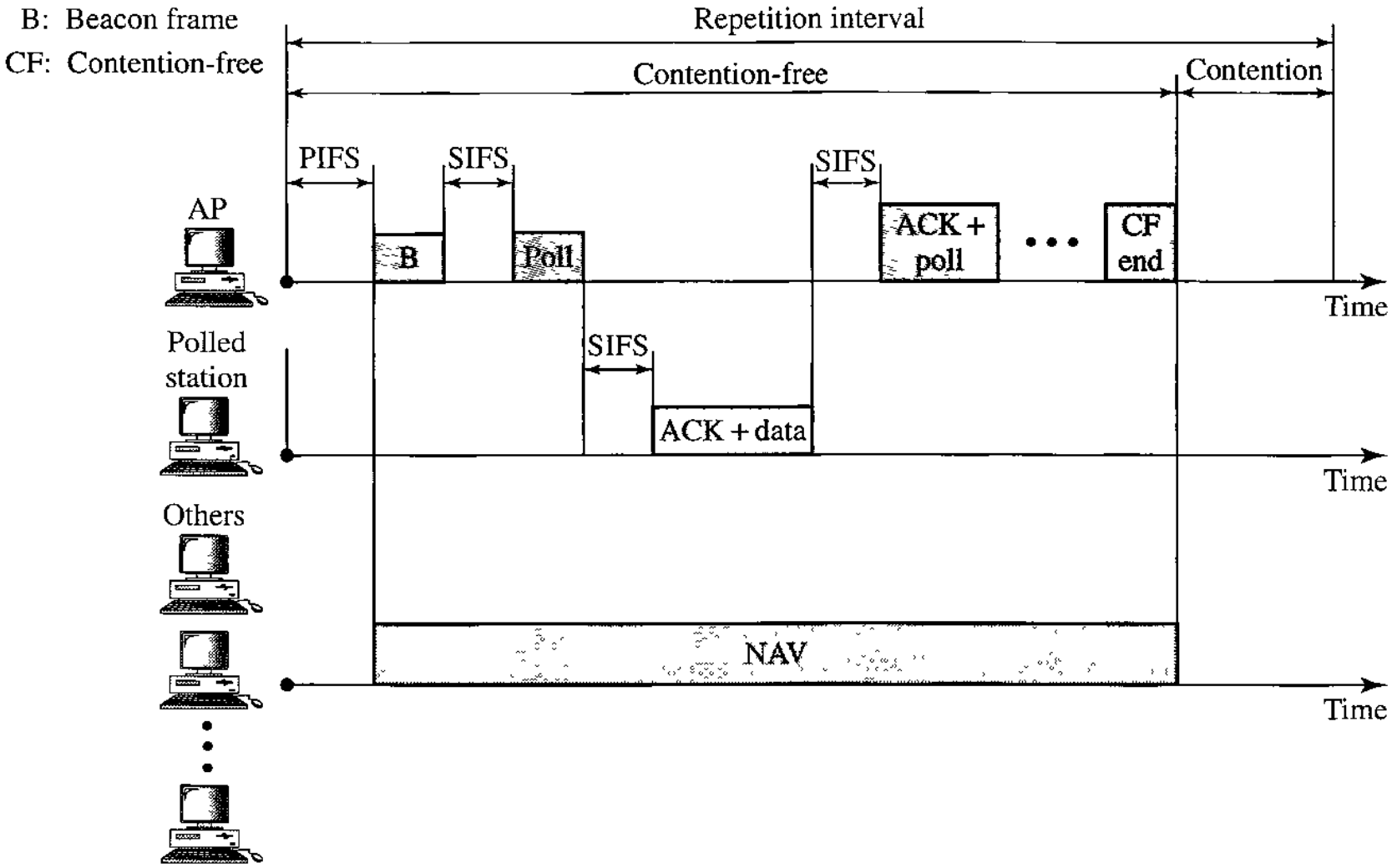
- ***Point Coordination Function (PCF)***
- The point coordination function (PCF) is an optional access method that can be implemented in an infrastructure network (not in an ad hoc network). It is implemented on top of the DCF and is used mostly for time-sensitive transmission. PCF has a centralized, contention-free polling access method. The AP performs polling for stations that are capable of being polled. The stations are polled one after another, sending any data they have to the AP. To give priority to PCF over DCF, another set of interframe spaces has been defined: PIFS and SIFS. The SIFS is the same as that in DCF, but the PIFS (PCF IFS) is shorter than the DIFS. This means that if, at the same time, a station wants to use only DCF and an AP wants to use PCF, the AP has priority.
- Due to the priority of PCF over DCF, stations that only use DCF may not gain access to the medium. To prevent this, a repetition interval has been designed to cover both contention-free (PCF) and contention-based (DCF) traffic. The repetition interval, which is repeated continuously, starts with a special control frame, called a beacon frame. When the stations hear the beacon frame, they start their NAV for the duration of the contention-free period of the repetition interval. The figure shows an example of a repetition interval.

IEEE 802.11 Modes of Operation

Media Access Control modes (PCF)

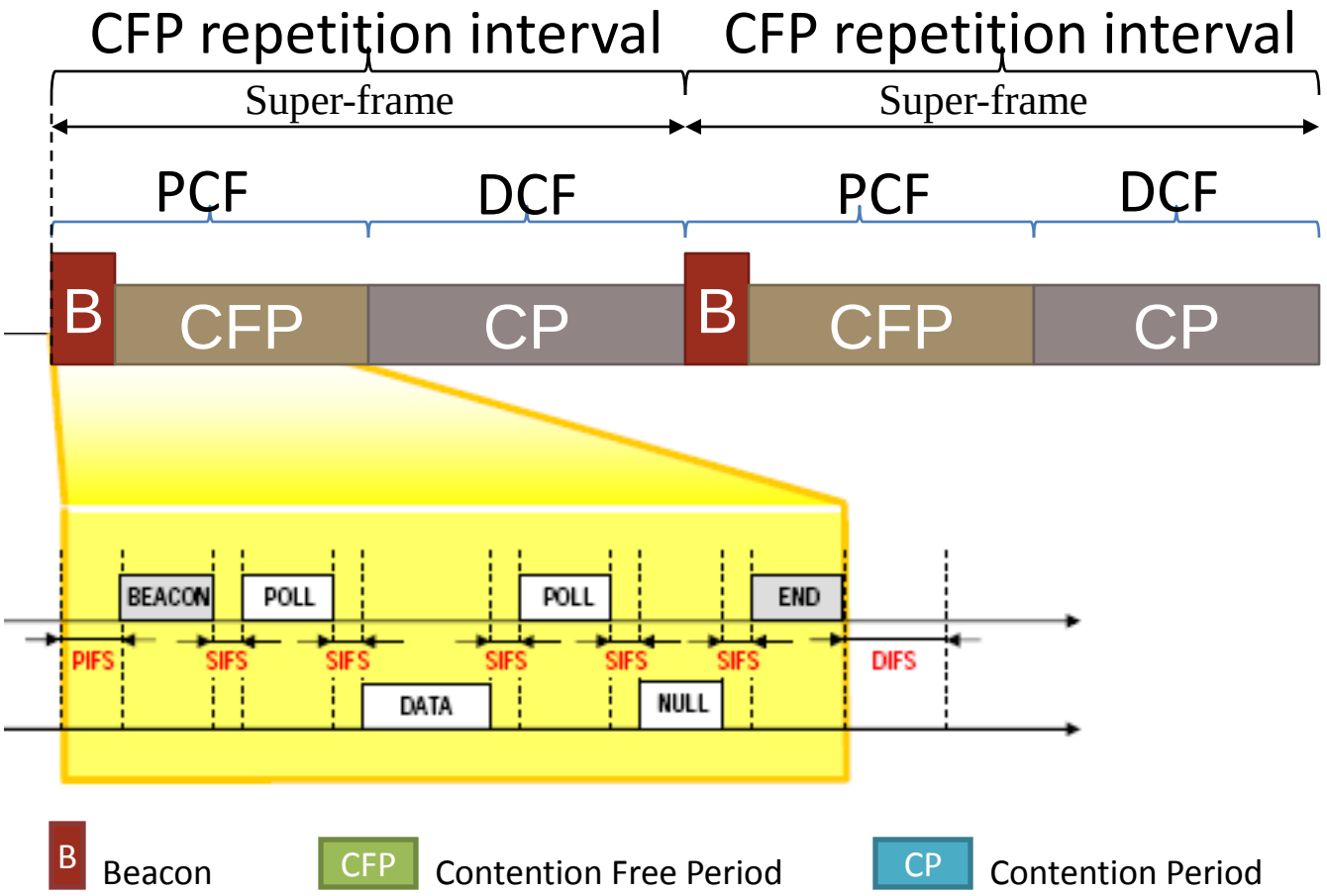
Standard	802.11b	802.11a	802.11g
Slot time	$20\mu s$	$9\mu s$	$9\mu s$
SIFS	$10\mu s$	$16\mu s$	$10\mu s$
PIFS	$30\mu s$	$25\mu s$	$19\mu s$
DIFS	$50\mu s$	$34\mu s$	$28\mu s$
CW_{min}	31	15	16
CW_{max}	1023	1023	1024




B: Beacon frame
CF: Contention-free
Repetition interval
Contention-free
Contention
PIFS
SIFS
SIFS
AP
B
Poll
ACK + poll
CF end
Time
Polled station
SIFS
ACK + data
Time
Others
NAV
Time

Point Coordinated Function (PCF)

- PCF uses a base station to poll other stations to see if they have frames to send.
- No collisions occur.
- Base station sends ***beacon frame*** periodically.
- Base station can tell another station to ***sleep*** to save on batteries and base stations holds frames for sleeping station.


CFP repetition interval
CFP repetition interval
Super-frame
Super-frame
PCF
DCF
PCF
DCF
B
CFP
CP
B
CFP
CP
BEACON
POLL
POLL
END
PIFS
SIFS
SIFS
SIFS
SIFS
SIFS
DIFS
DATA
NULL
B
Beacon
CFP
Contention Free Period
CP
Contention Period

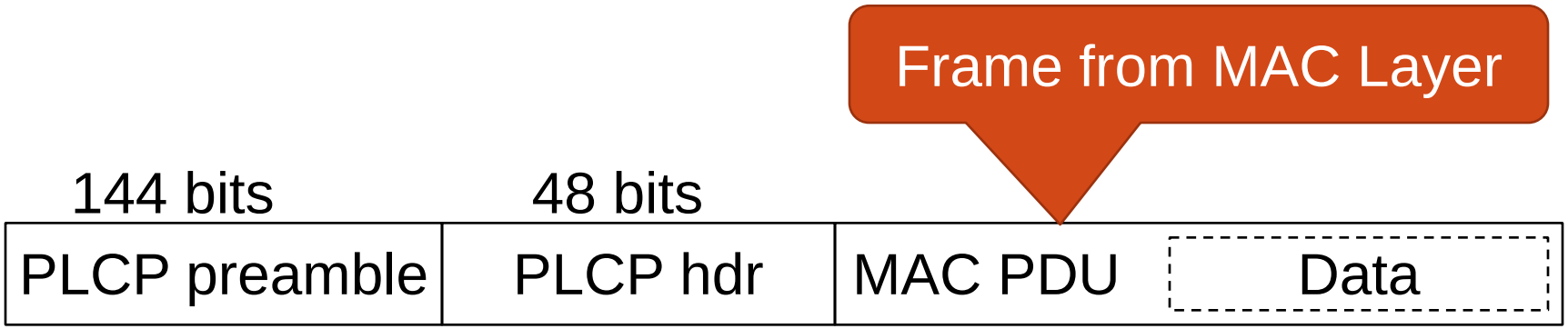
802.11 Data Frames and Addressing

In Physical Layer & MAC layer

WLAN doesn't use 802.3 Ethernet frames

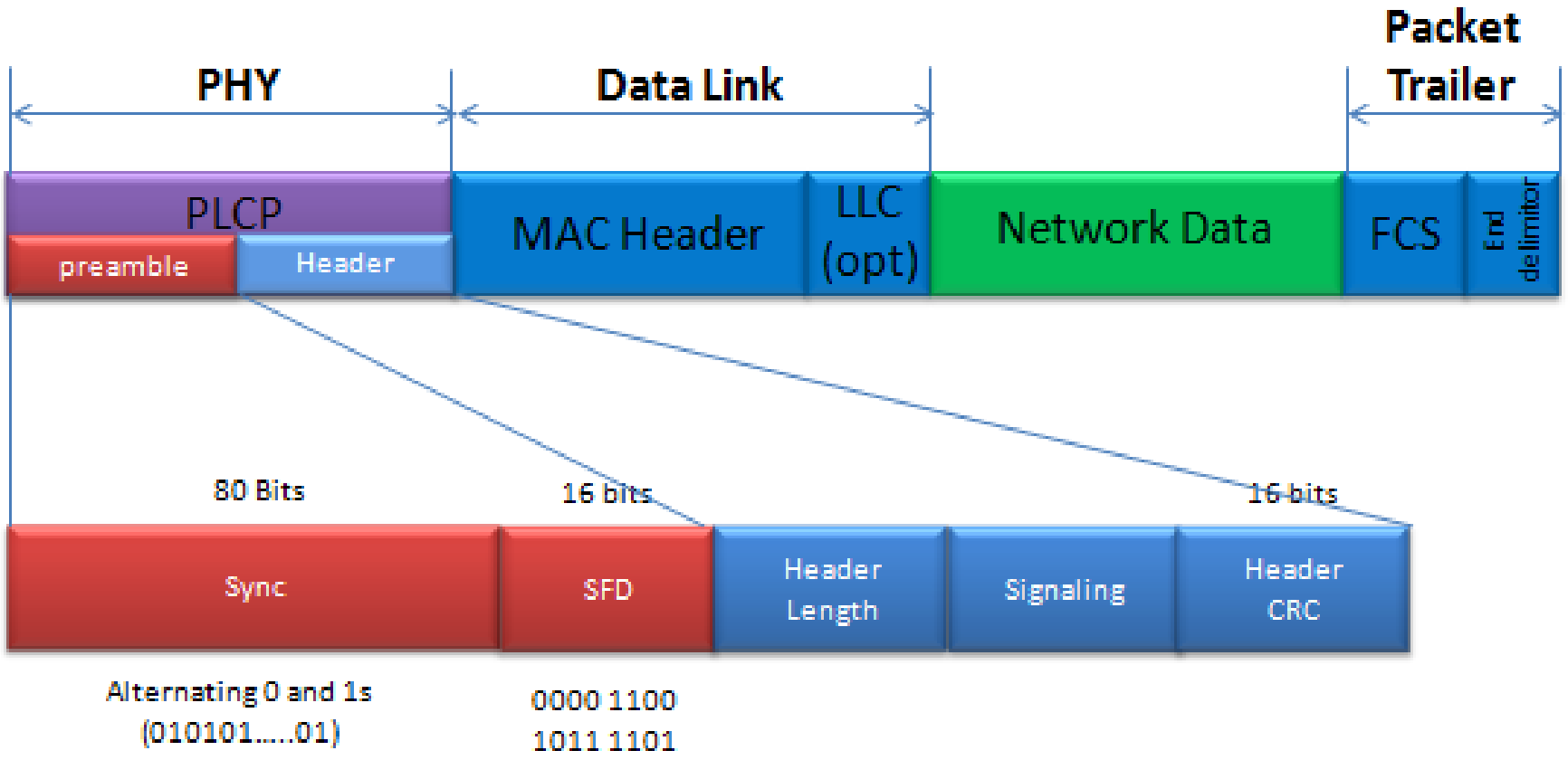
There three different types of WLAN frame named Control, Management and Data frame.

PLCP (Physical Layer Convergence Protocol) Structure



To enable sharing the media among many nodes:

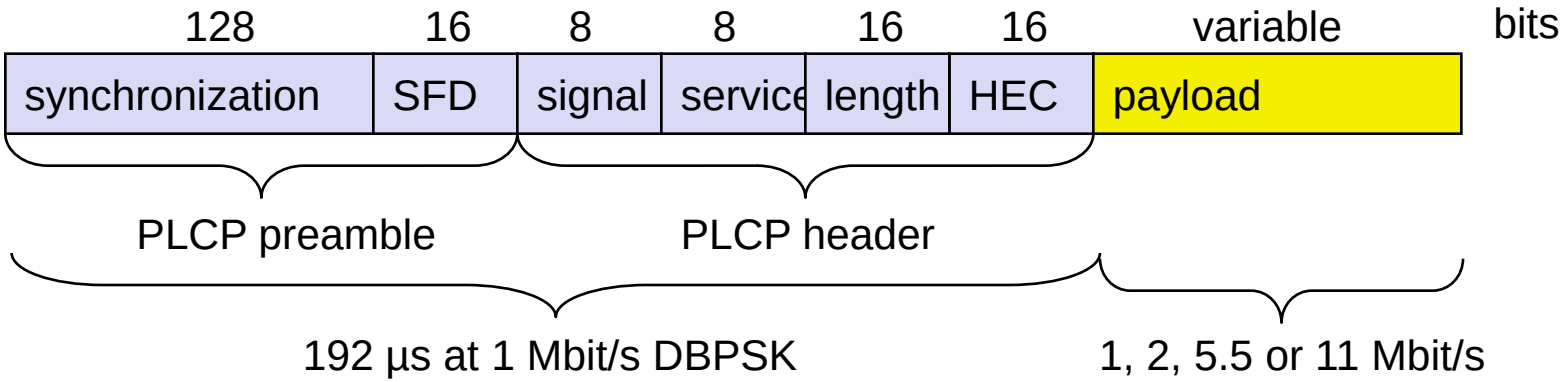
- All control information must be transmitted at rate understood by all stations
- After control information, transceivers change to rate agreed on by sender and receiver
- Preamble and header sent at lowest coding rate
  - 1 Mbps in .11b/g



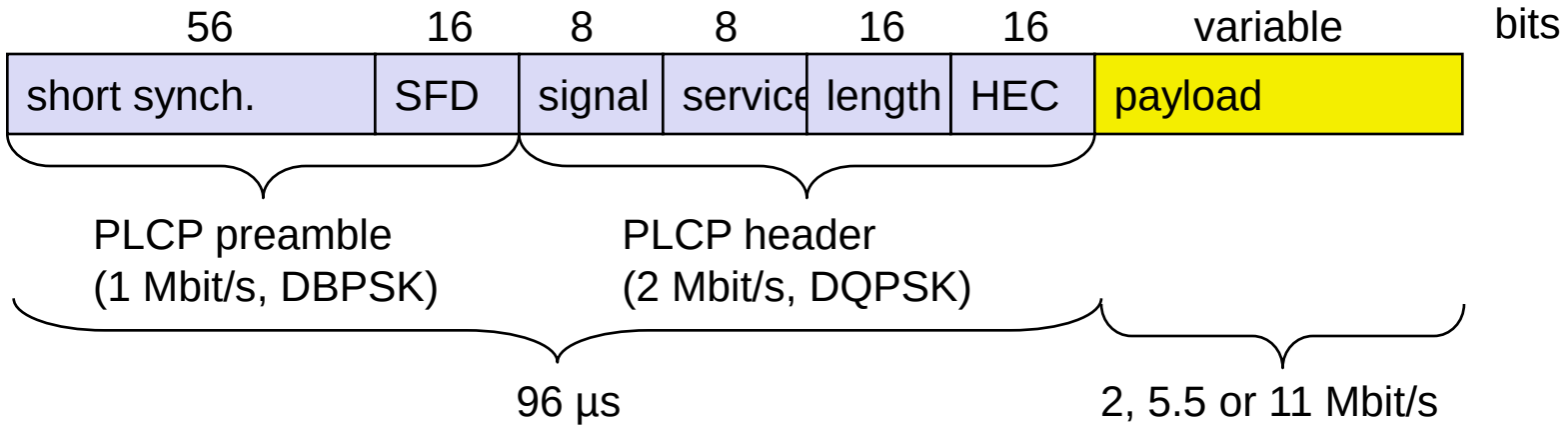
The first part of PLCP is for 'Sync' (Synchronization). This is a part made of 80 bits of alternation 0 and 1s.
The next portion is SFD (Start Frame Delimiter). This is a kind of tag indicating the start of physical frame and it is a specifically determined 16 bit sequence (0000110010111101).

IEEE 802.11b – PHY frame formats

Long PLCP PPDU format



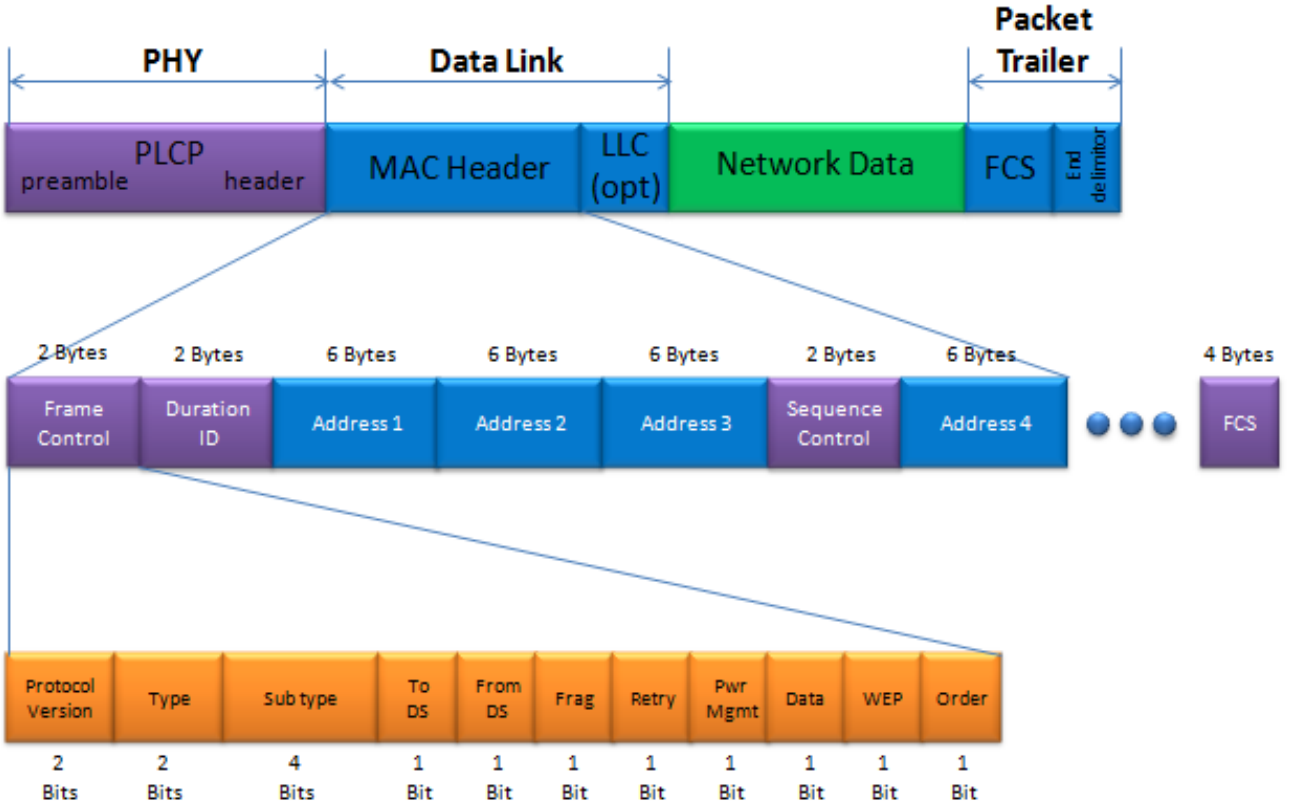
Short PLCP PPDU format (optional)



MAC Header Structure

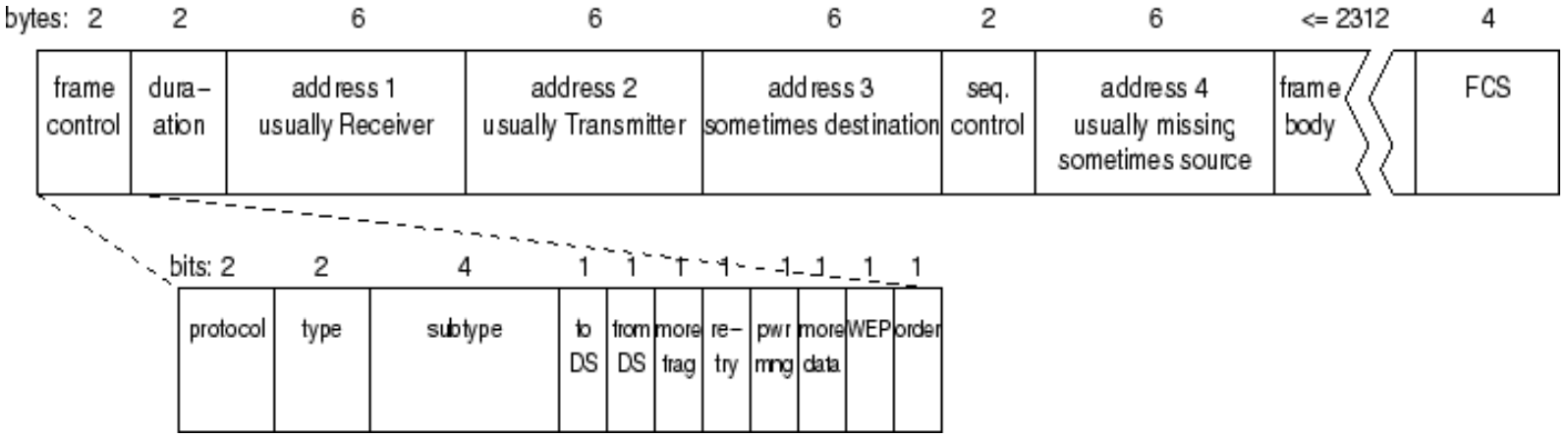
MAC Header would be a most complicated structure of the frame. The most important information contained in the MAC header would be as follows.

- What is the type of frame ?
- What are the source and destination address for the frame.



MAC frame format for 802.11

- There is more than one frame format for 802.11, as the protocol needs mechanisms for stations to associate with an Access Point, and for setting up frame encryption.
- However, the basic 802.11 frame format looks like this:



- The top frame is the most general form of frame; data frames are like this. The lower part of the picture is an expansion of the *frame control* field. Note the following:
- No preamble is shown. Each 802.11 technology deals with frame synchronization its own way, and so it is not shown as part of the frame.

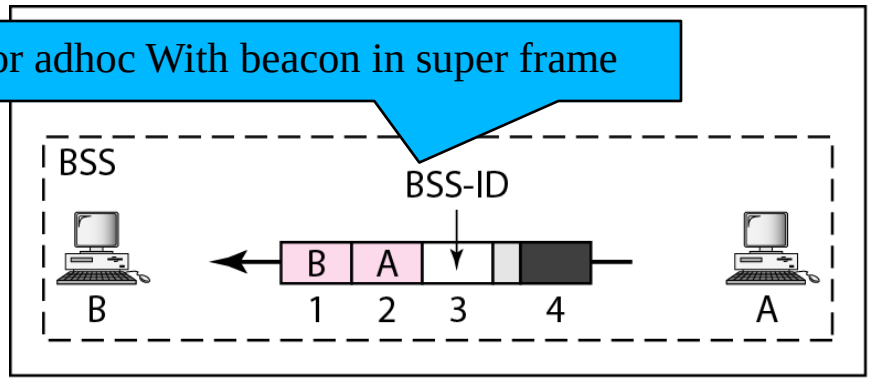
Address Field Description

- Addr 1 = All stations filter on this address.
- Addr 2 = Transmitter Address (TA)
  - Identifies transmitter to address the ACK frame to
- Addr 3 = Dependent on To and From DS bits
- Addr 4 = needed to identify the original source of WDS (Wireless Distribution System) frames

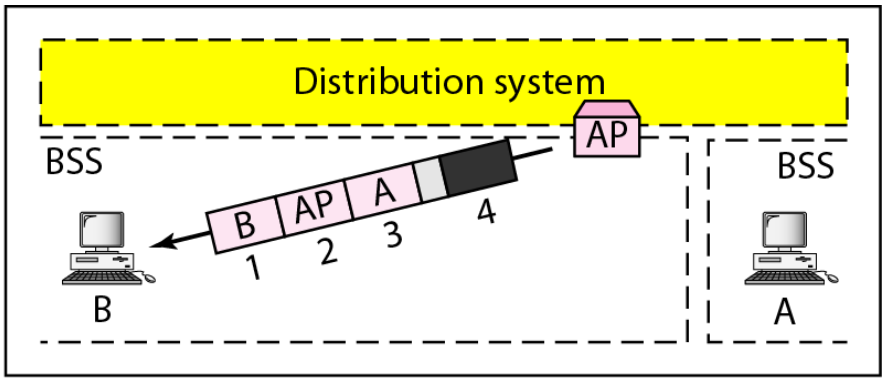
To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destination	Source	BSSID	N/A
0	1	Destination	BSSID	Source	N/A
1	0	BSSID	Source	Destination	N/A
1	1	Reciever	Transmitter	Destination	Source

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

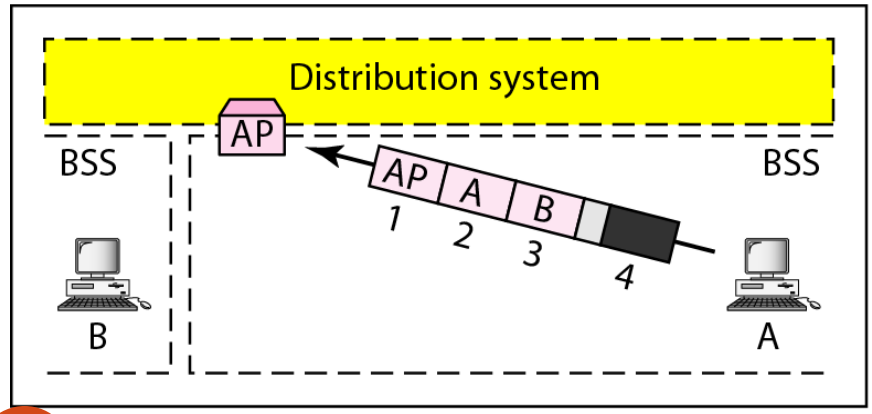
For adhoc With beacon in super frame



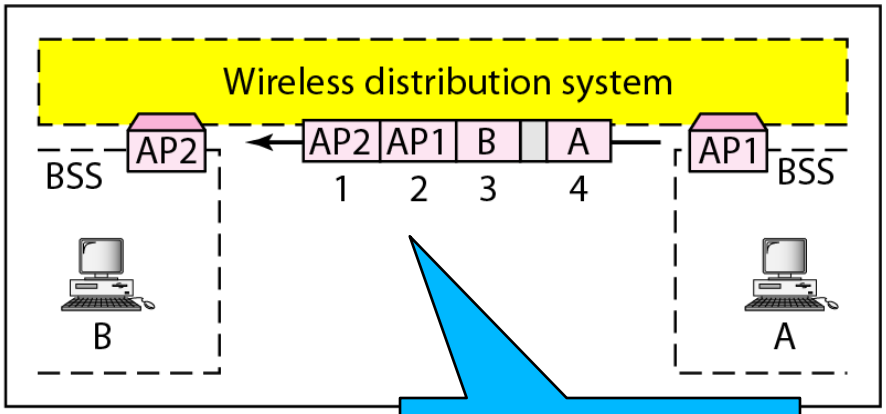
a. Case 1



b. Case 2



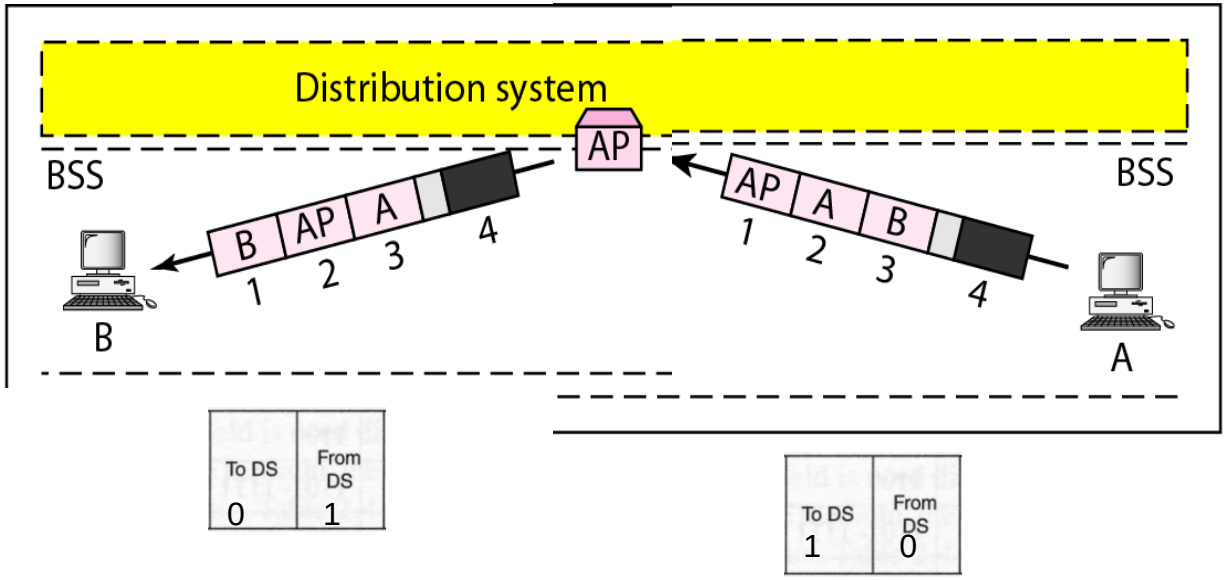
Case 3



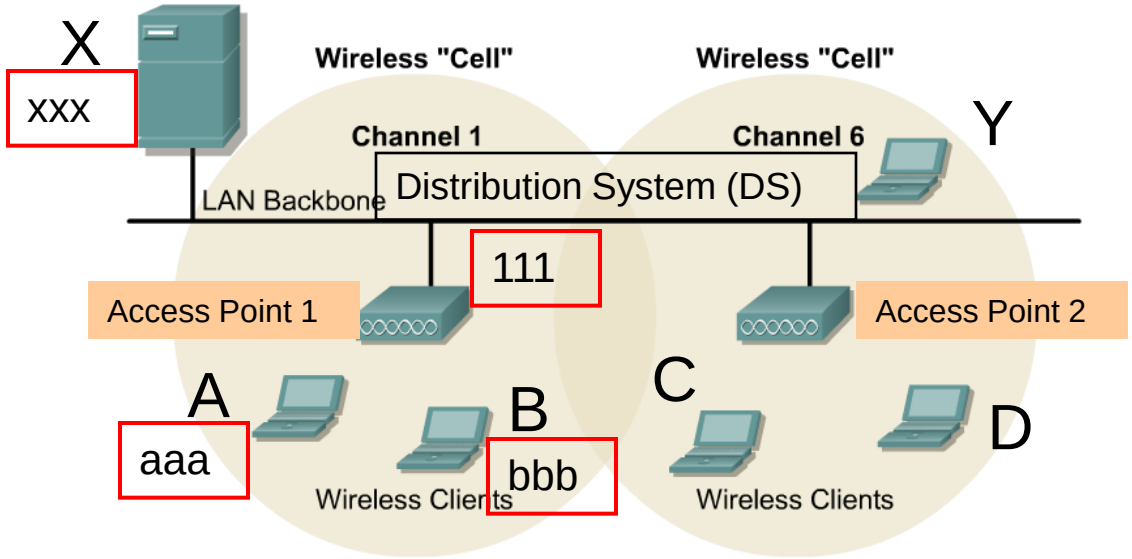
d. Case 4

For WDS & adhoc

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



802.11 MAC Addressing

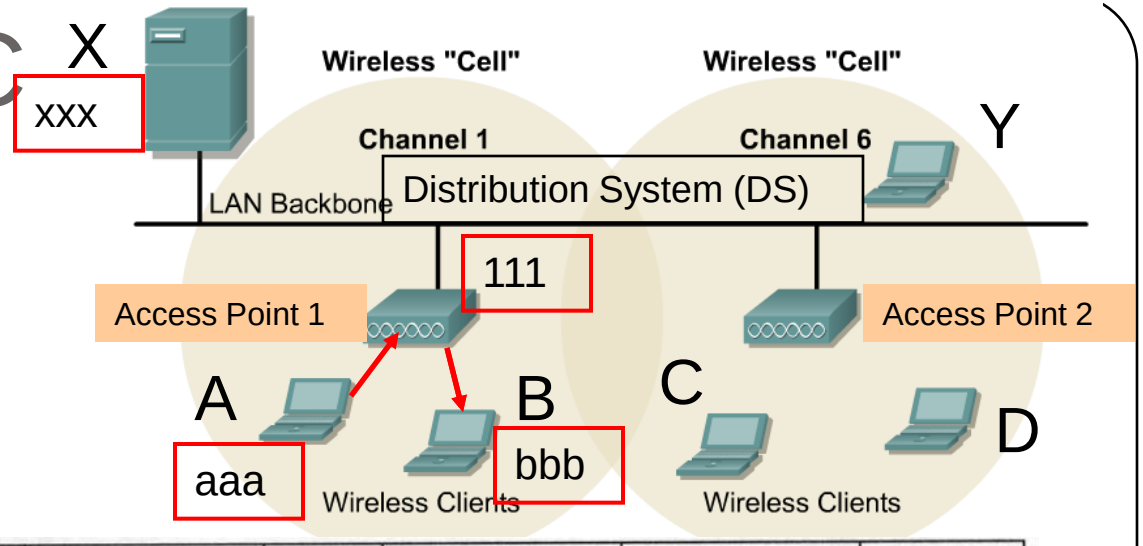


aaa bbb 111 ← Pseudo MAC address of hosts and AP1

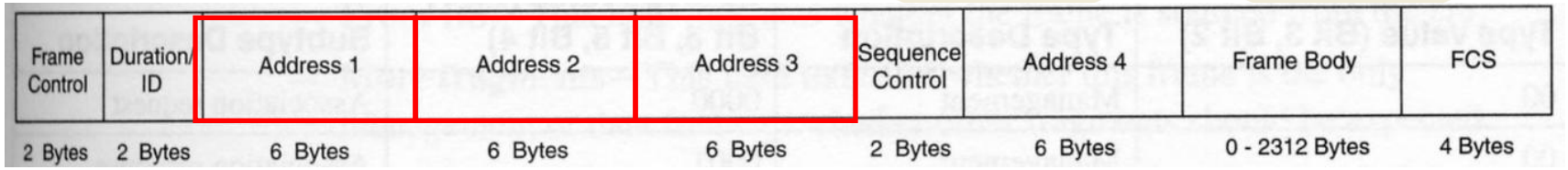
- Let's look at these options:
  - Host A to Host B
  - Host A to Host X
  - Host X to Host A
- Frames to and from a BSS must go via the access point.
- The access point is a layer 2 bridge (translation bridge) between the 802.11 network and the 802.3 network.

802.11 MAC Addressing

The BSSID



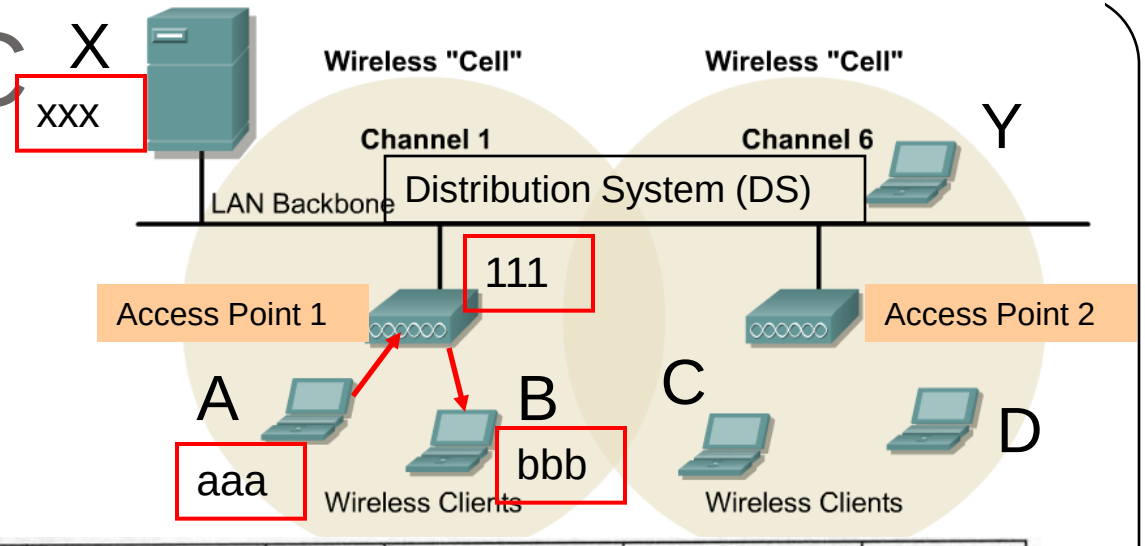
General 802.11 Frame



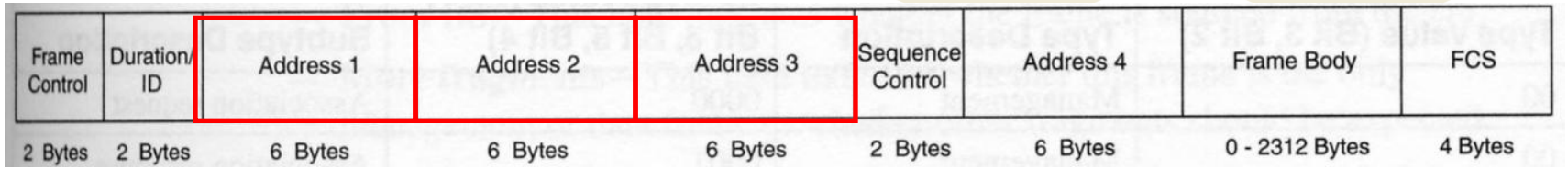
- Each BSS is assigned a **BSSID**.
  - Not to be confused with SSID or ESSID.
- BSSID – 48 bit identifier which distinguishes it from other BSSs in the network.
- Some BSSs may overlap and the APs need to know which AP the frame is for.
- In a BSS, the **BSSID is the MAC address of the wireless interface**, I.e. **the MAC address of the AP - wireless (translating) bridge**.
- *Remember, normal switches (bridges) may have MAC addresses, but these addresses are only used for management purposes and not for layer 2 frame forwarding (addressing).*

802.11 MAC Addressing

Host A to Host B



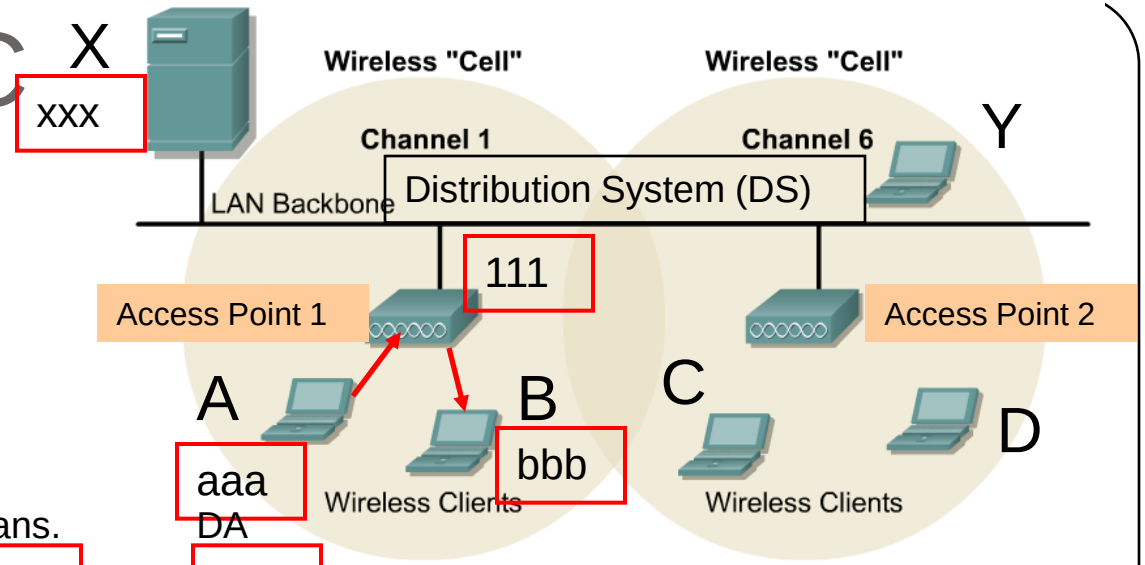
General 802.11 Frame



- Address 1 – Receiver address
- Address 2 – Transmitter address
- Address 3 – Ethernet SA, Ethernet DA, or BSSID

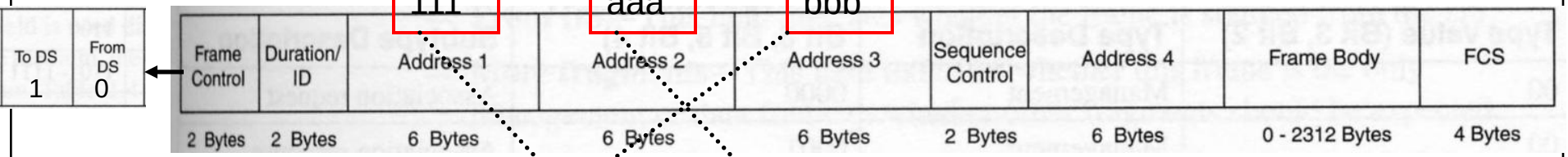
- **Transmitter**: Sends a frame on to the wireless medium, but doesn't necessarily create the frame.
- **Receiver**: Receives a frame on the wireless medium, but may not be the destination, i.e. may be the access point.

802.11 MAC Addressing

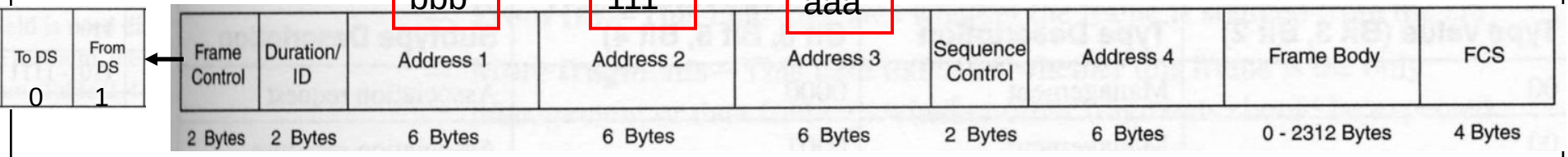


Host A to Host B

Host A to AP 1



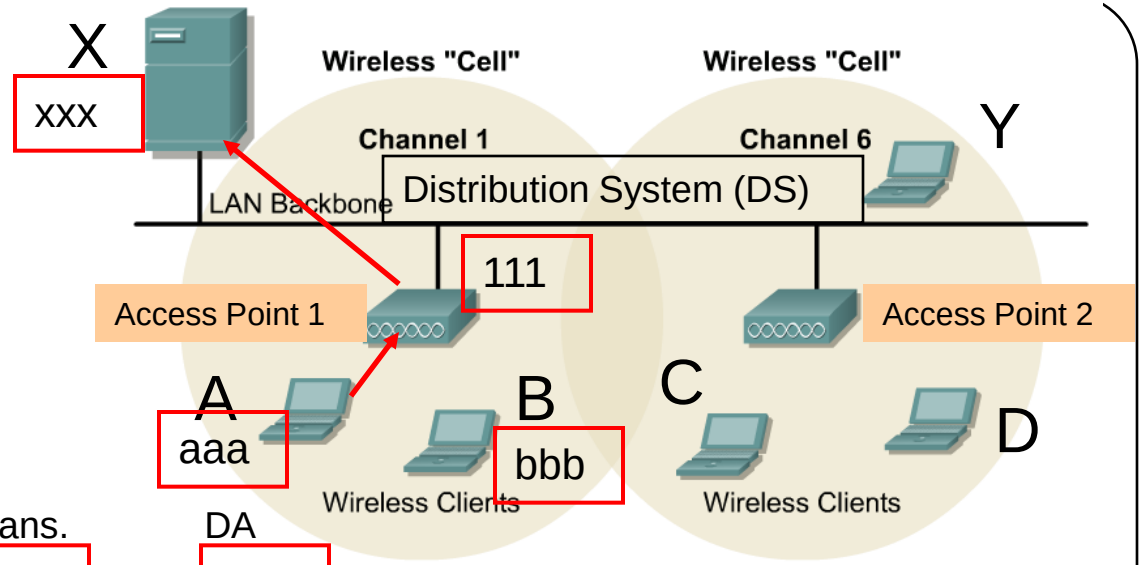
AP1 to Host B



- Address 1 – Receiver address
- Address 2 – Transmitter address
- Address 3 – Ethernet SA, Ethernet DA, or BSSID

802.11 MAC Addressing

Host A to Host X



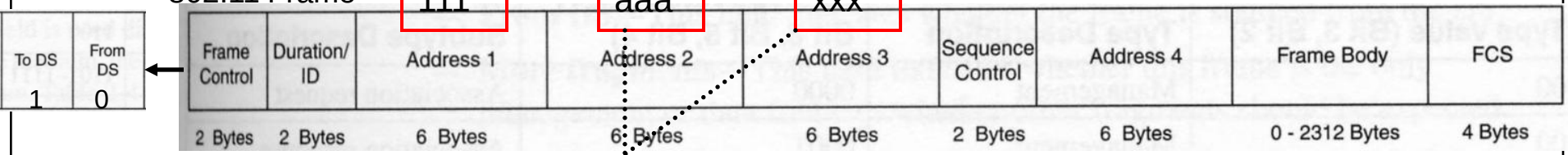
Host A to AP 1

802.11 Frame

Rec. 111

Trans. aaa

DA xxx

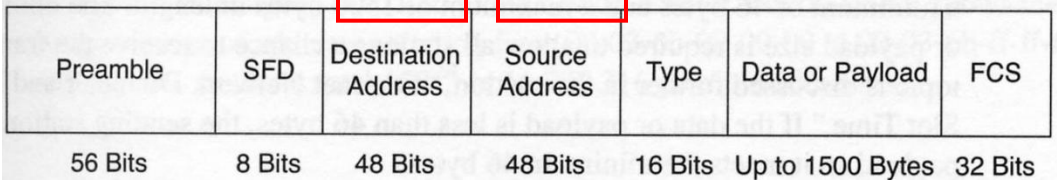


copied

Host A to AP 1

The Ethernet Frame

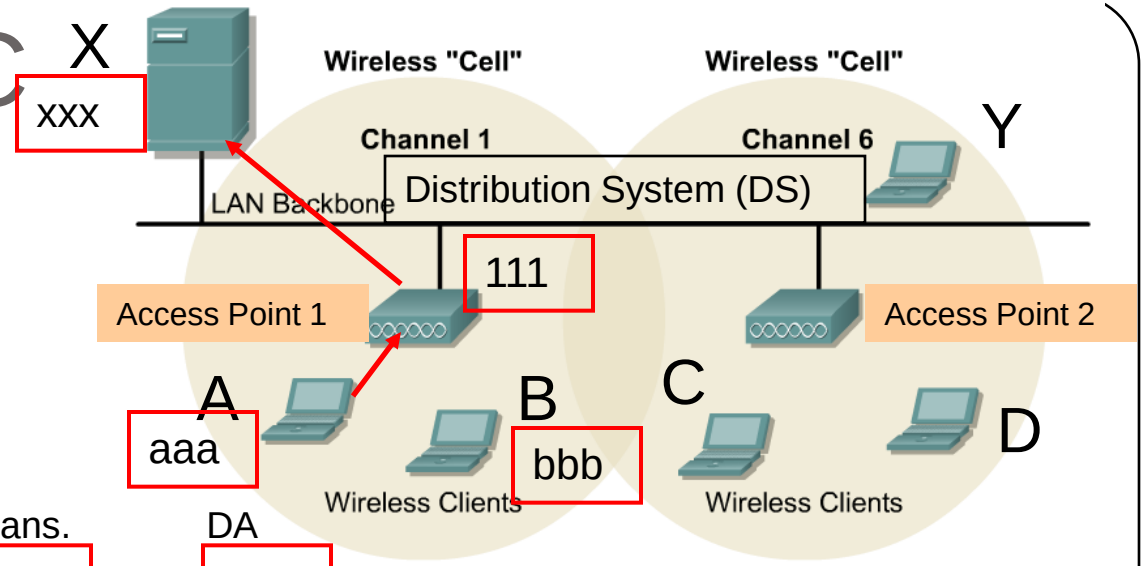
xxx aaa



- The Ethernet DA and SA are the source and destination addresses just like on traditional Ethernet networks.
  - Destination Address – Host X
  - Source Address – Host A

802.11 MAC Addressing

Host A to Host X



Host A to AP 1

802.11 Frame

Rec. 111 Trans. aaa DA xxx

To DS	From DS	Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS
1	0	2 Bytes	2 Bytes	6 Bytes	6 Bytes	6 Bytes	2 Bytes	6 Bytes	0 - 2312 Bytes	4 Bytes

copied

The Ethernet Frame

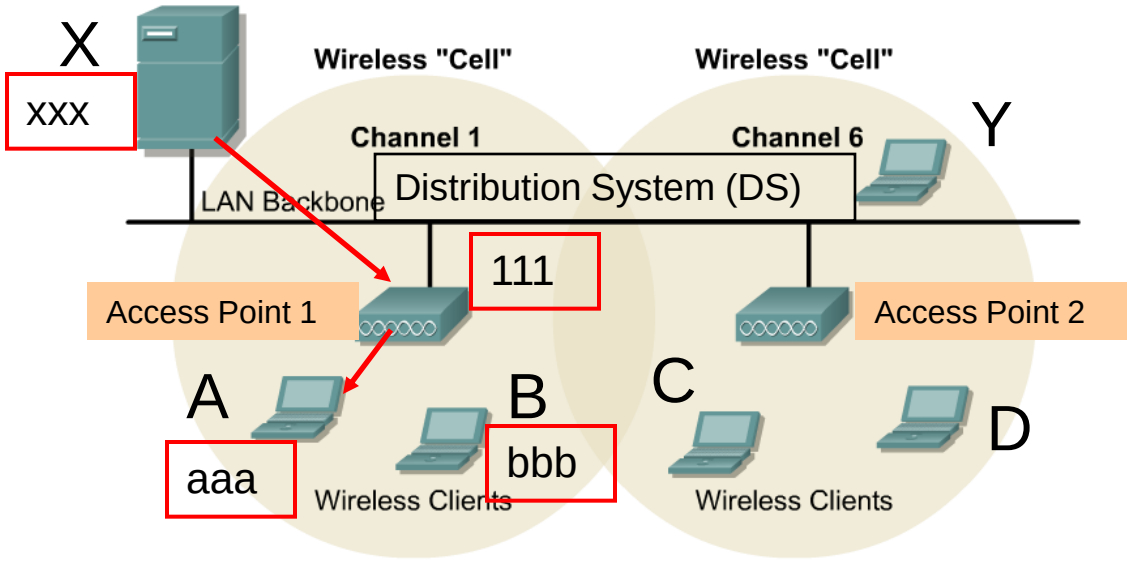
xxx aaa Host A to AP 1

Preamble	SFD	Destination Address	Source Address	Type	Data or Payload	FCS
56 Bits	8 Bits	48 Bits	48 Bits	16 Bits	Up to 1500 Bytes	32 Bits

- The AP (bridge) knows which MAC address on on its wireless interface and maintains a table with those MAC addresses. (from the Association process – later)
- When the AP receives an 802.11 frame, it examines the Address 3 address.
- If Address 3 is not in its table of wireless MACs it knows it needs to translate the frame to an Ethernet frame.
- The AP copies the Address 3 address to the Ethernet Destination Address, and Address 2 (Transmitter address) is copied to the Ethernet Source Address.

802.11 MAC Addressing

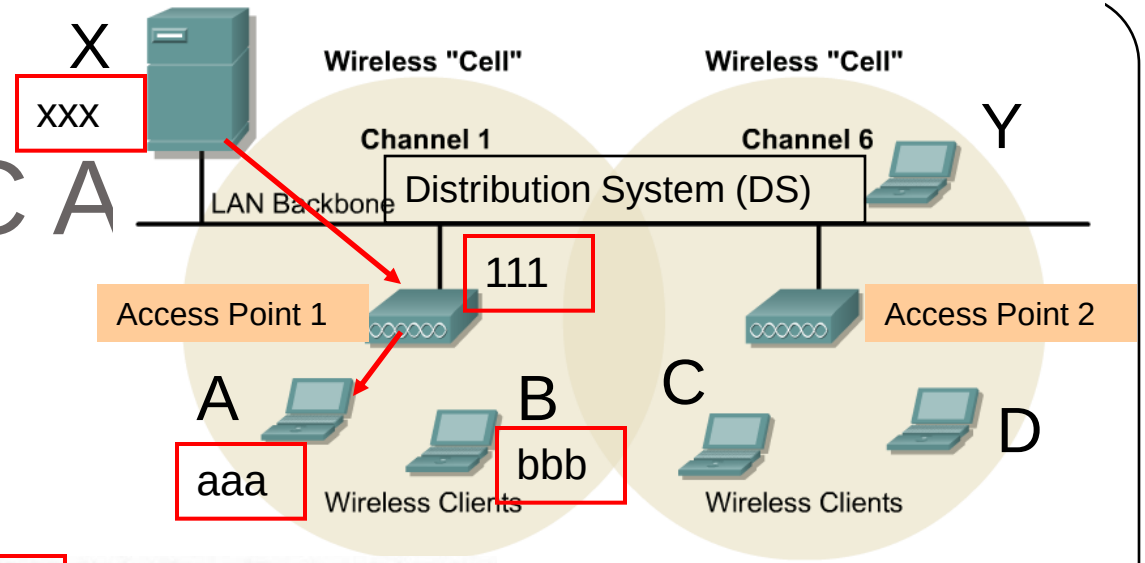
Host X to Host A



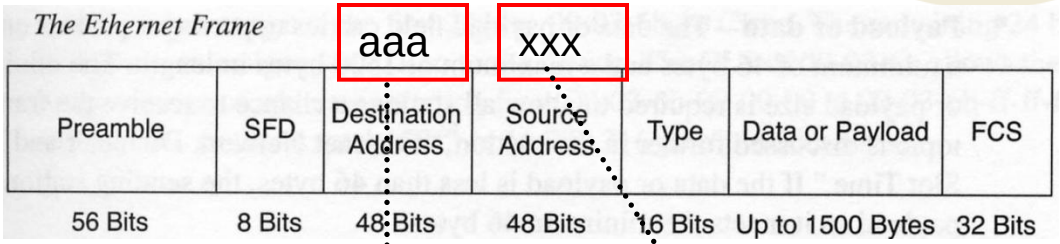
- Host X send ACK or data frames to Host A

802.11 MAC A

Host X to Host A



Host X to AP 1



copied

Destination Address – Host X

Source Address – Host A

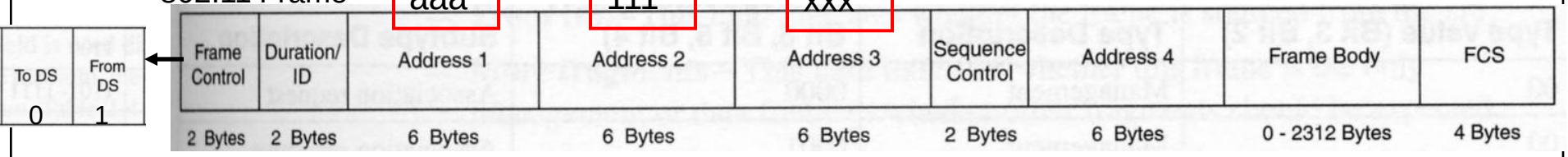
AP 1 to Host A

802.11 Frame

Rec.

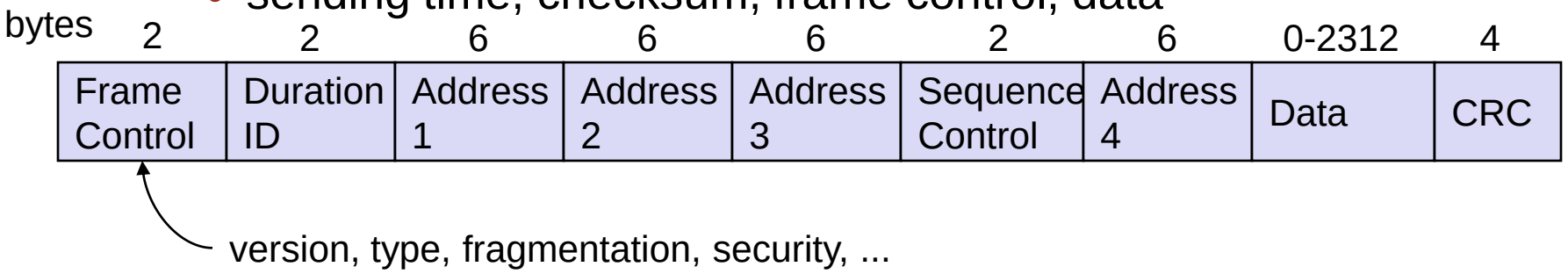
Trans.

SA



802.11 - Frame format

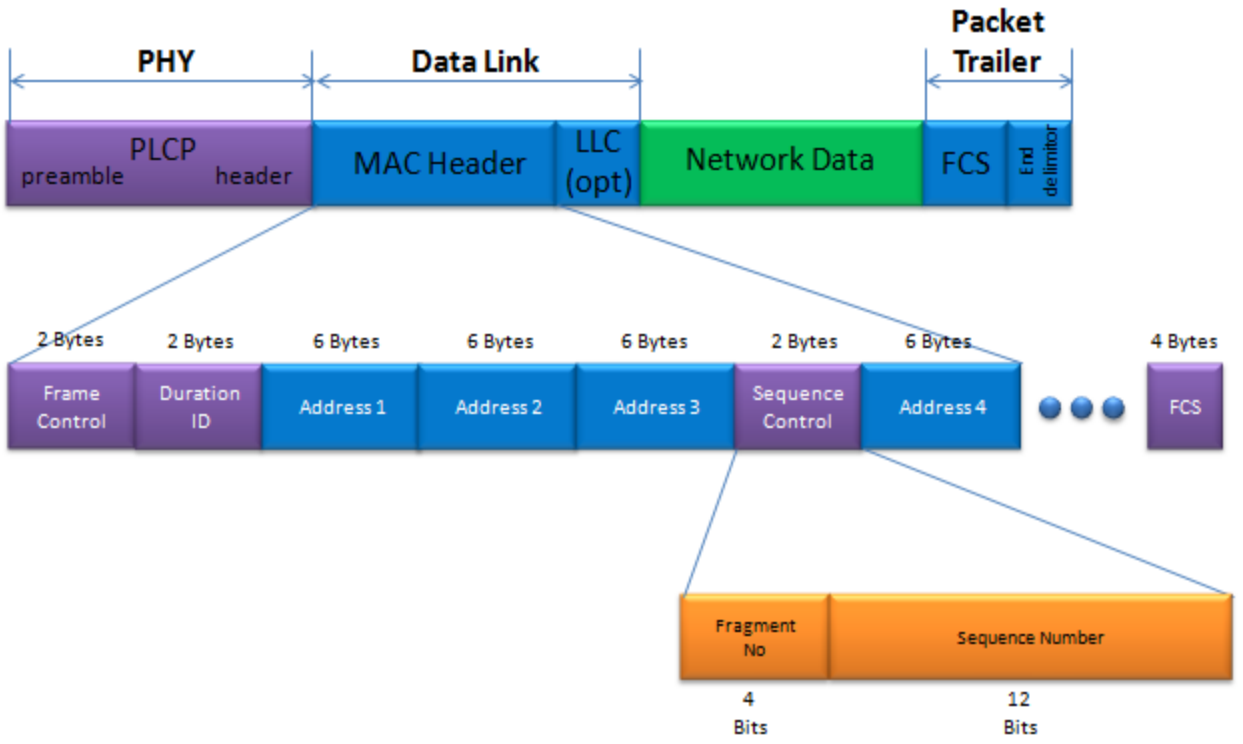
- Types
  - control frames, management frames, data frames
- Sequence numbers
  - important against duplicated frames due to lost ACKs
- Addresses
  - receiver, transmitter (physical), BSS identifier, sender (logical)
- Miscellaneous
  - sending time, checksum, frame control, data



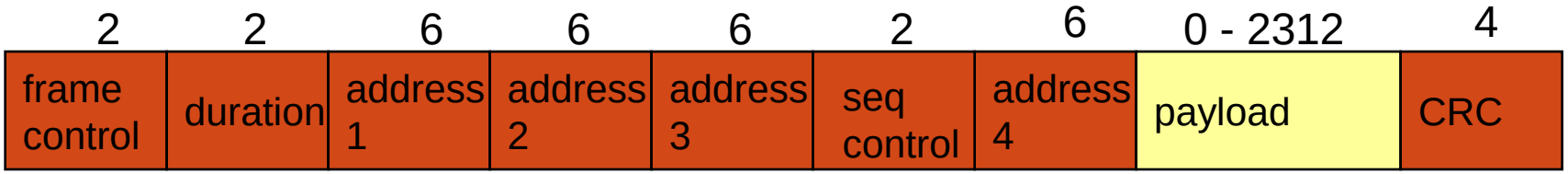
Type	Type Description	Sub Type	Sub Type Description
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Reassociation Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	0100-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Dissociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101-1111	Reserved
01	Control	0000-1001	Reserved
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF End
01	Control	1111	CF End + CF ACK
01	Control	1010	PS-Poll
10	Data	0000	Data
10	Data	0001	Data + CF ACK
10	Data	0010	Data + CF Poll
10	Data	0011	Data + CF ACK + CF Poll
10	Data	0100	Null Function(No Data)
10	Data	0101	CF ACK(no Data)
10	Data	0110	CF Poll(no Data)
10	Data	0111	CF ACK + CF Poll(no Data)
10	Data	1000-1111	Reserved
11	Reserved	0000-1111	Reserved

Sequence Control Field Structure

- When a packet comes into the MAC layer from higher layer, a sequence number is assigned at 'Sequence Number' field. If the incoming packet is too big for a single MAC frame, it be splitted into multiple fragment.



802.11 frame: addressing



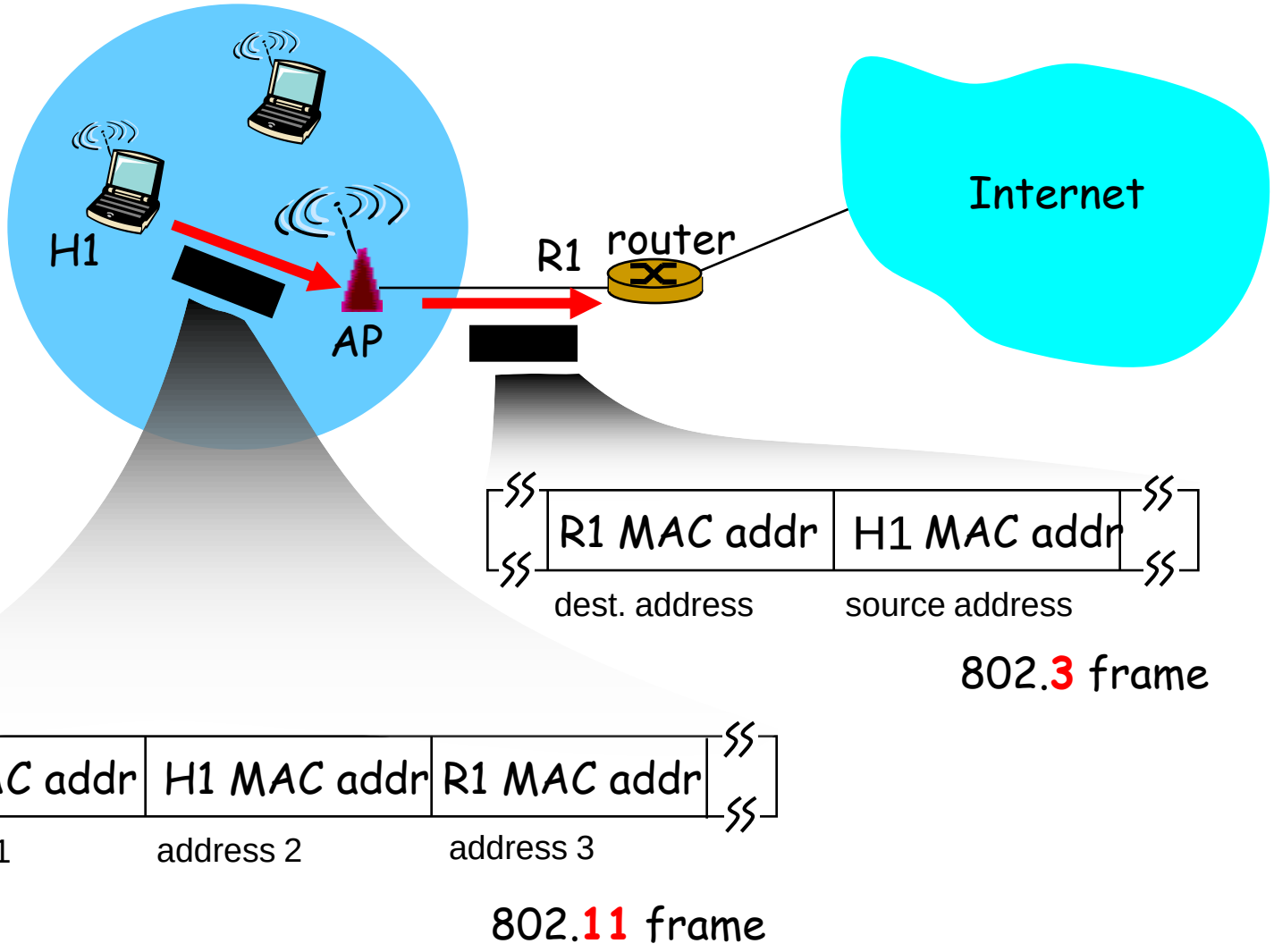
Address 1: Destination MAC address of wireless host or AP to receive this frame

Address 2: Source MAC address of wireless host or AP transmitting this frame

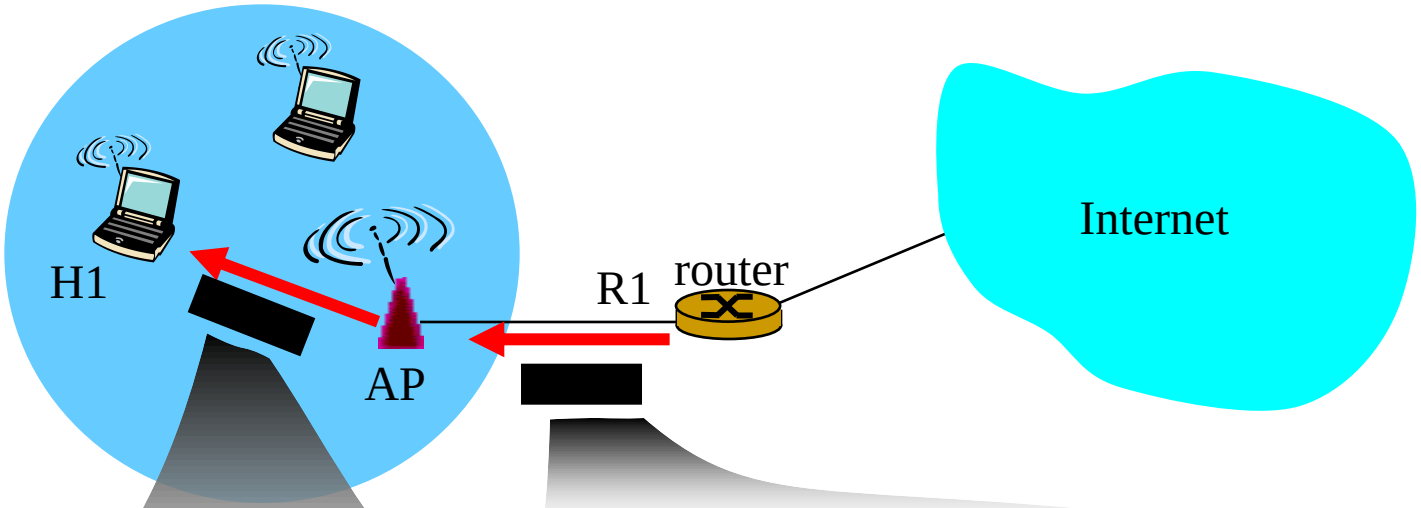
Address 3: MAC address of router (routed by) interface to which AP is attached

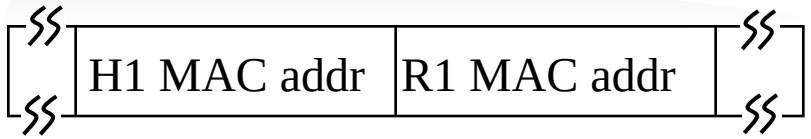
Address 3: used for WDS or in ad hoc mode

802.11 frame: addressing

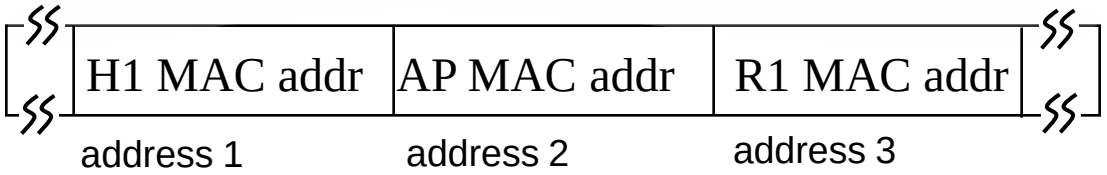


802.11 frame: addressing



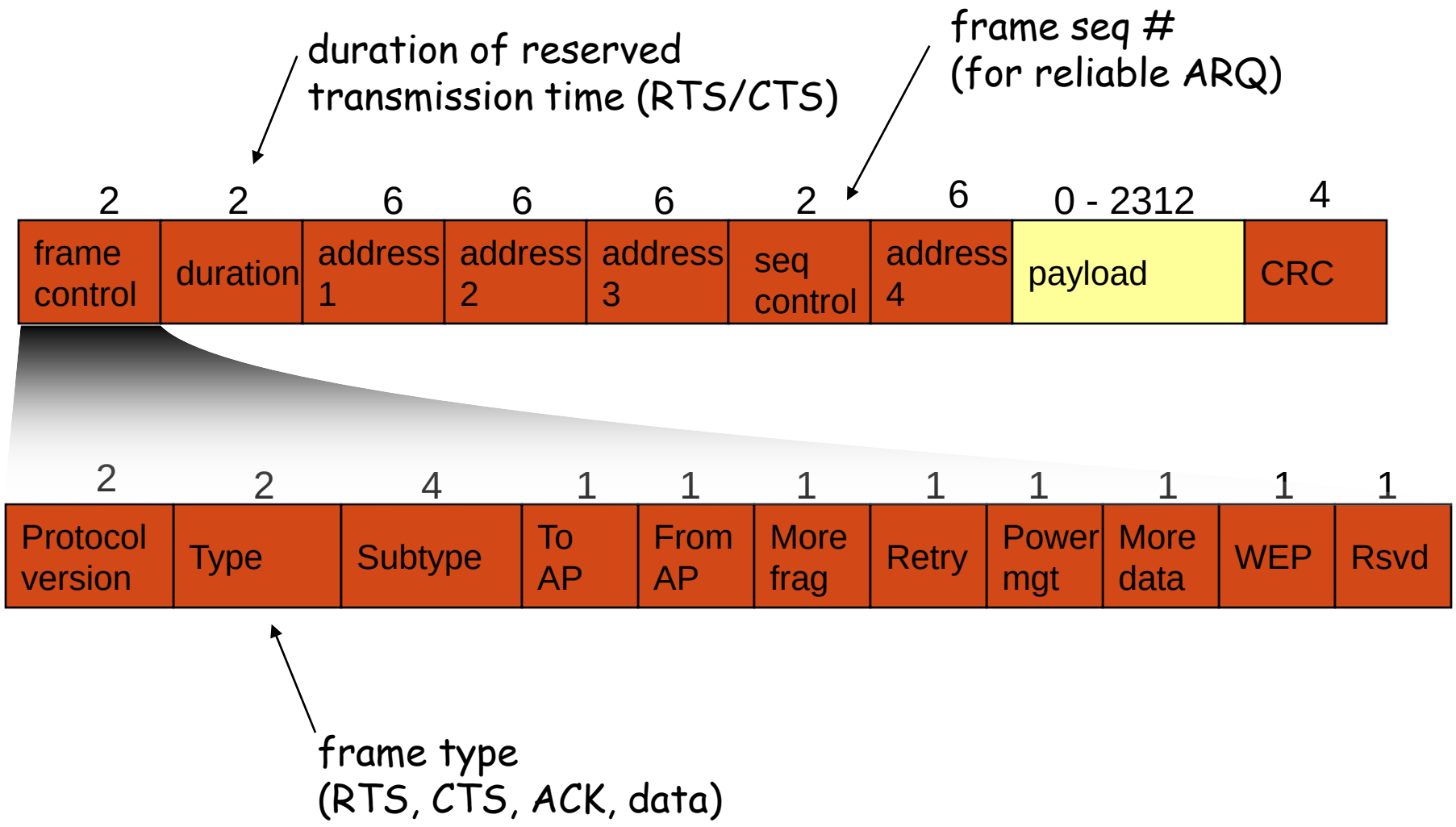


802.3 frame



802.11 frame

802.11 frame: more



Types of Frames

- Control Frames
  - RTS/CTS/ACK
  - CF-Poll/CF-End
  - Signaling packets for avoiding Exposed/Hidden terminal problems, and for reservation
    - Medium is reserved for the duration of the transmission
    - RTS-CTS in DCF
    - Polls in PCF
- Management Frames
  - Beacons
  - Probe Request/Response
  - Association Request/Response
  - Dissociation/Reassociation
  - Authentication/Deauthentication
  - ATIM
- Data Frames

802.11 Frames – This isn't Ethernet!

802.11 Frames

- Data Frames (most are PCF)
  - Data
  - Null data
  - Data+Ack
  - Data+CF+Ack
  - Data+CF+Poll
  - Data+CF+Ac+CF+Poll
  - CF-Ack
  - CF-Poll
  - CF-Cak+CF-Poll
- Control Frames
  - RTS
  - CTS
  - ACK
  - CF-End
  - CF-End+CF-Ack
- Management Frames
  - Beacon
  - Probe Request
  - Probe Response
  - Authentication
  - Deauthentication
  - Association Request
  - Association Response
  - Reassociation Request
  - Reassociation Response
  - Disassociation
  - Announcement Traffic Indication

Distribution Services

- The information required for the Distribution service to operate is provided by the Association services.
- Before a data message can be handled by the Distribution service, a STA must be "Associated".
- Mobility types:
  - No-transition
    - Static - no motion
    - Local movement - movement within a Basic Service Area
  - BSS-transition: movement from one BSS in one ESS to another BSS within the same ESS (Roaming same LAN).
  - ESS-transition: movement from one BSS in one ESS to another BSS in an independent ESS (Roaming other LAN).
- Different Association services support the different categories of mobility.

Distribution Services

- Association:
  - The service which establishes an initial Association between a station and an access point.
- Before a STA is allowed to send via an AP, it must first become associated with the AP.
- At any given time, a mobile STA may be associated with no more than one AP. This ensures that the DS can determine which AP is serving a specified STA.
- An AP may be associated with many mobile STAs at one time.
- A station learns what APs are present and requests to establish an association by invoking the Association service.
- Association is always initiated by the mobile STA.
- Association is sufficient to support no-transition mobility.
- Association is necessary, but not sufficient, to support BSS-transition mobility.

Channels, beacon frames & association

- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies; 3 non-overlapping
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!
- AP regularly sends *beacon frame*
  - Includes SSID, beacon interval (often 0.1 sec)
- host: must *associate* with an AP
  - scans channels, listening for beacon frames
  - selects AP to associate with; initiates association protocol
  - may perform authentication
  - After association, host will typically run DHCP to get IP address in AP's subnet

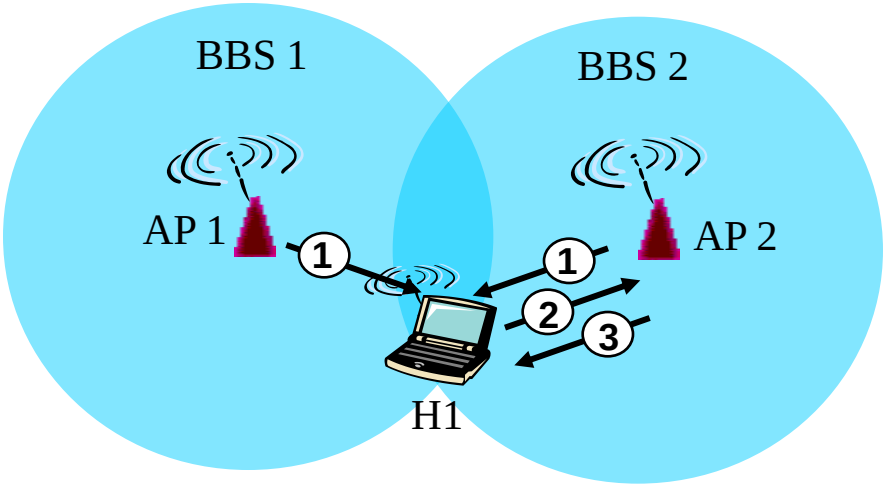
Distribution Services

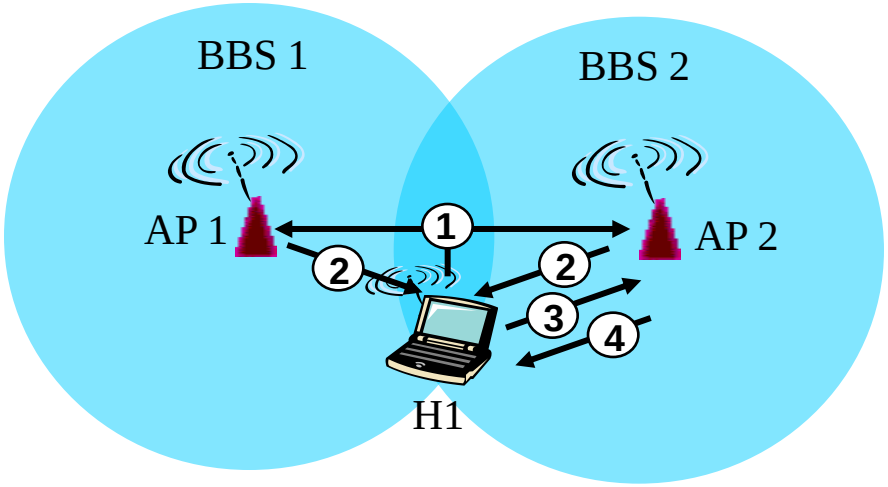
- Reassociation:
  - The service which enables an established Association (of a STA) to be transferred from one AP to another AP (within an ESS).
- The Reassociation Service is invoked to "move" a current association from one AP to another. This keeps the DS informed of the current mapping between AP and STA as the station moves from BSS to BSS within an ESS.
- Reassociation also enables changing association attributes of an established association while the STA remains associated with the same AP.
- Reassociation is always initiated by the mobile STA.

Distribution Services

- Disassociation:
  - The service which deletes an existing Association.
- The Disassociation Service is invoked whenever an existing Association must be terminated, and can be invoked by either party to an Association (mobile STA or AP).
- Disassociation is a notification (not a request) and can not be refused by either party to the association.
- APs might need to disassociate STAs to enable the AP to be removed from a network for service or for other reasons.
- STAs are encouraged to Disassociate whenever they leave a network.

802.11: passive/active scanning





Passive Scanning:

(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent: AP to H1

Active Scanning:

(1) Probe Request frame broadcast from H1
(2) Probes response frame sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent: AP to H1

802.11 - MAC management

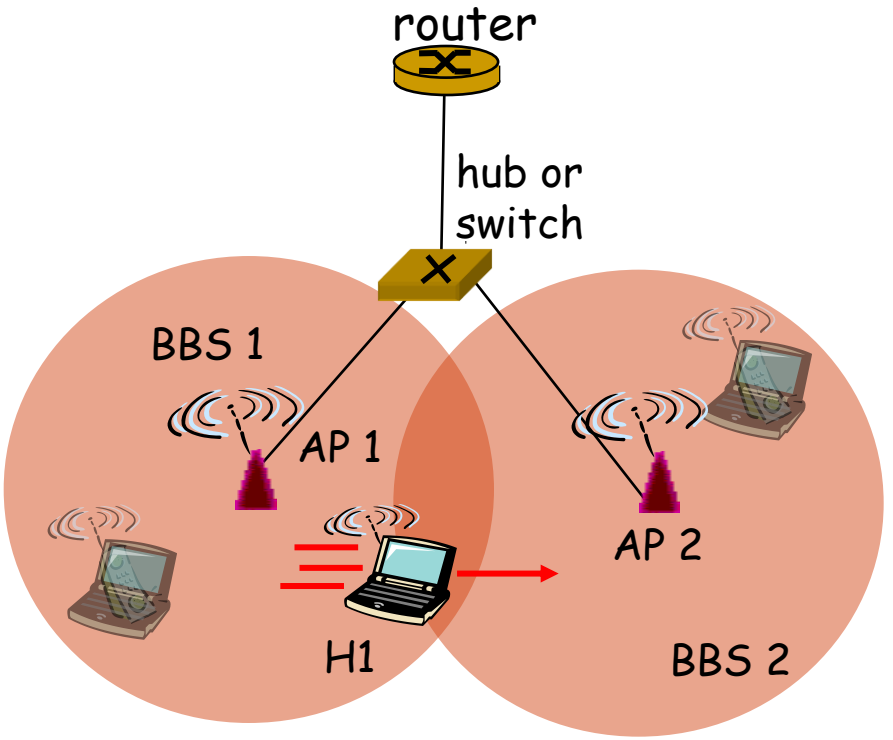
- Synchronization
  - try to find a LAN, try to stay within a LAN
  - timer etc.
- Power management
  - sleep-mode without missing a message
  - periodic sleep, frame buffering, traffic measurements
- Association/Reassociation
  - integration into a LAN
  - roaming, i.e. change networks by changing access points
  - scanning, i.e. active search for a network
- MIB - Management Information Base
  - managing, read, write

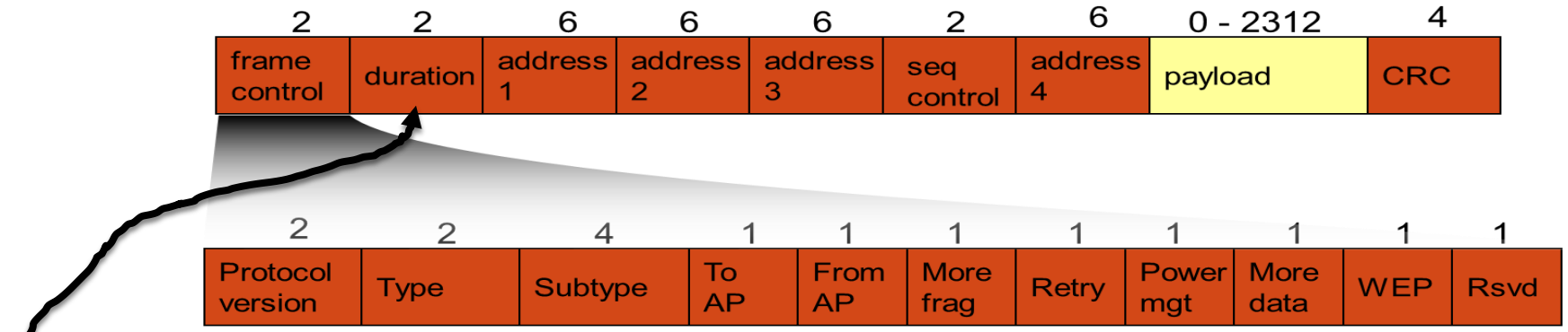
802.11 - Roaming

- Bad connection in Infrastructure mode? Perform:
- scanning of environment
  - listen into the medium for beacon signals or send probes into the medium and wait for an answer
- send Reassociation Request
  - station sends a request to a new AP(s)
- receive Reassociation Response
  - success: AP has answered, station can now participate
  - failure: continue scanning
- AP accepts Reassociation Request and
  - signals the new station to the distribution system
  - the distribution system updates its data base (i.e., location information)
  - typically, the distribution system now informs the old AP so it can release resources

802.11 - Roaming within same subnet

- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
  - self-learning
  - switch will see frame from H1 and "remember" which switch port can be used to reach H1





- The frame format is given by the *type* field in the *frame control* field. Frame types include:
  - Management frames, these are normally used for communication with the Access Point: there are frames for new stations to *associate* with the network, and for *authentication*,
- Control frames, these are used during data transfers but don't contain data, these include *acknowledgments* and the RTS and CTS messages of DCF.
- Data frames.
- The duration field in each frame "reserves" the carrier for the length of time to transmit the frame, and sometimes subsequent frames in a transaction.
- There are four address fields. The other two are needed when 802.11 is used to bridge two wired LANs. We discussed the use of these extra fields in slide(50).

Operational processes

Association

- To establish relationship with Access-Point
- Stations scan frequency band to and select Access-Point with best communications quality
  - Active Scan (sending a “Probe request” on specific channels and assess response)
  - Passive Scan (assessing communications quality from beacon message)
- Access-Point maintains list of associate stations in MAC FW
  - Record station capability (data-rate)
  - To allow inter-BSS relay
- Station’s MAC address is also maintained in bridge learn table associated with the port it is located on

Operational processes

Authentication

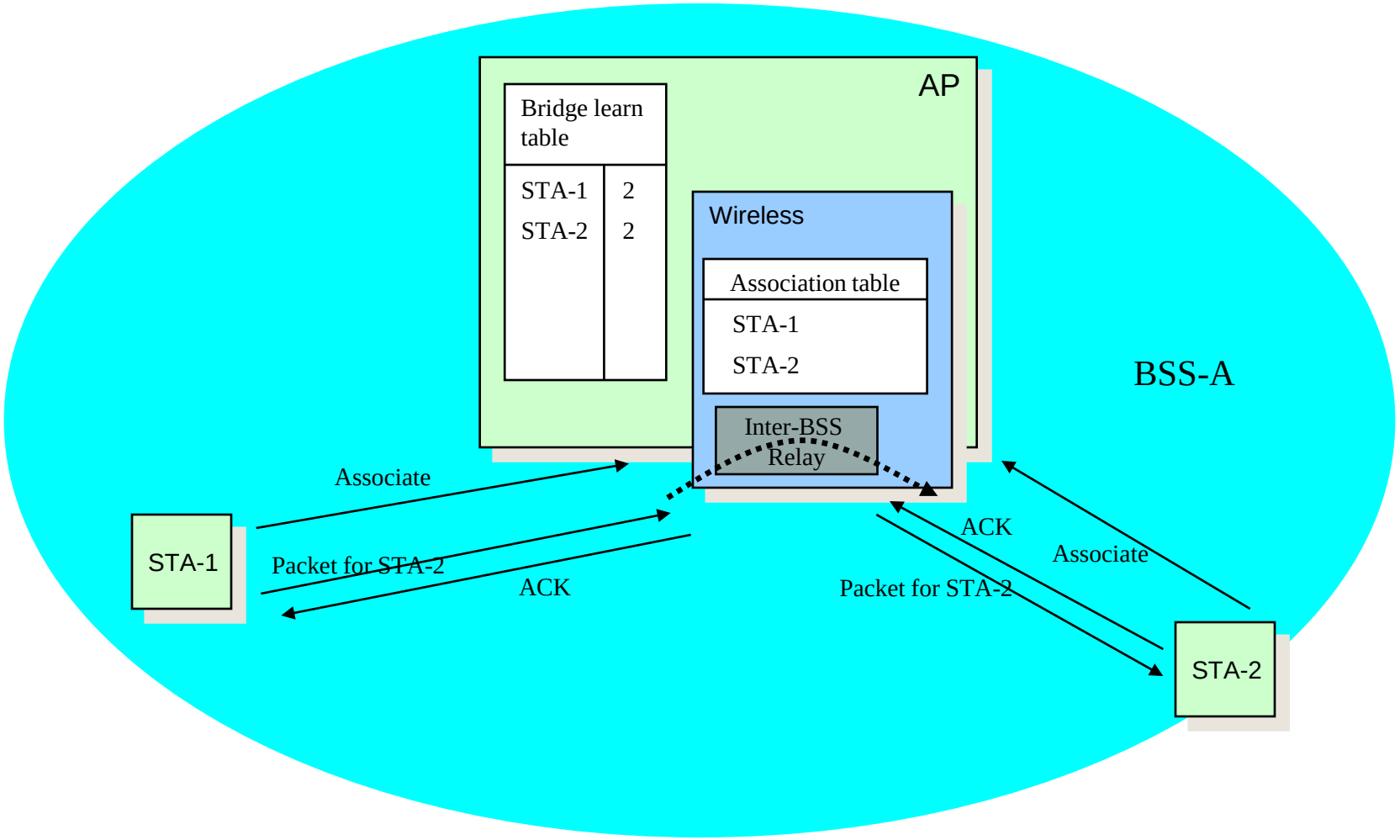
- To control access to the infrastructure via an authentication
- Stations identify themselves to other stations (or Access-Points) prior to data traffic or association
- Open System Authentication
  - Uses null authentication algorithm
  - Default
- Shared Key Authentication
  - Uses WEP privacy algorithm
  - Optional

Operational processes

- The infrastructure network is identified by its SSID
- All Access-Points will have been set according to this SSID
- Wireless stations will be configured to set their desired SSID
- On power up stations will issue Probe Requests and will locate the Access-Point that they will associate with:
  - “best” Access-Point with matching SSID
  - “best” Access-Point if the “desired SSID” has been set to “ANY”

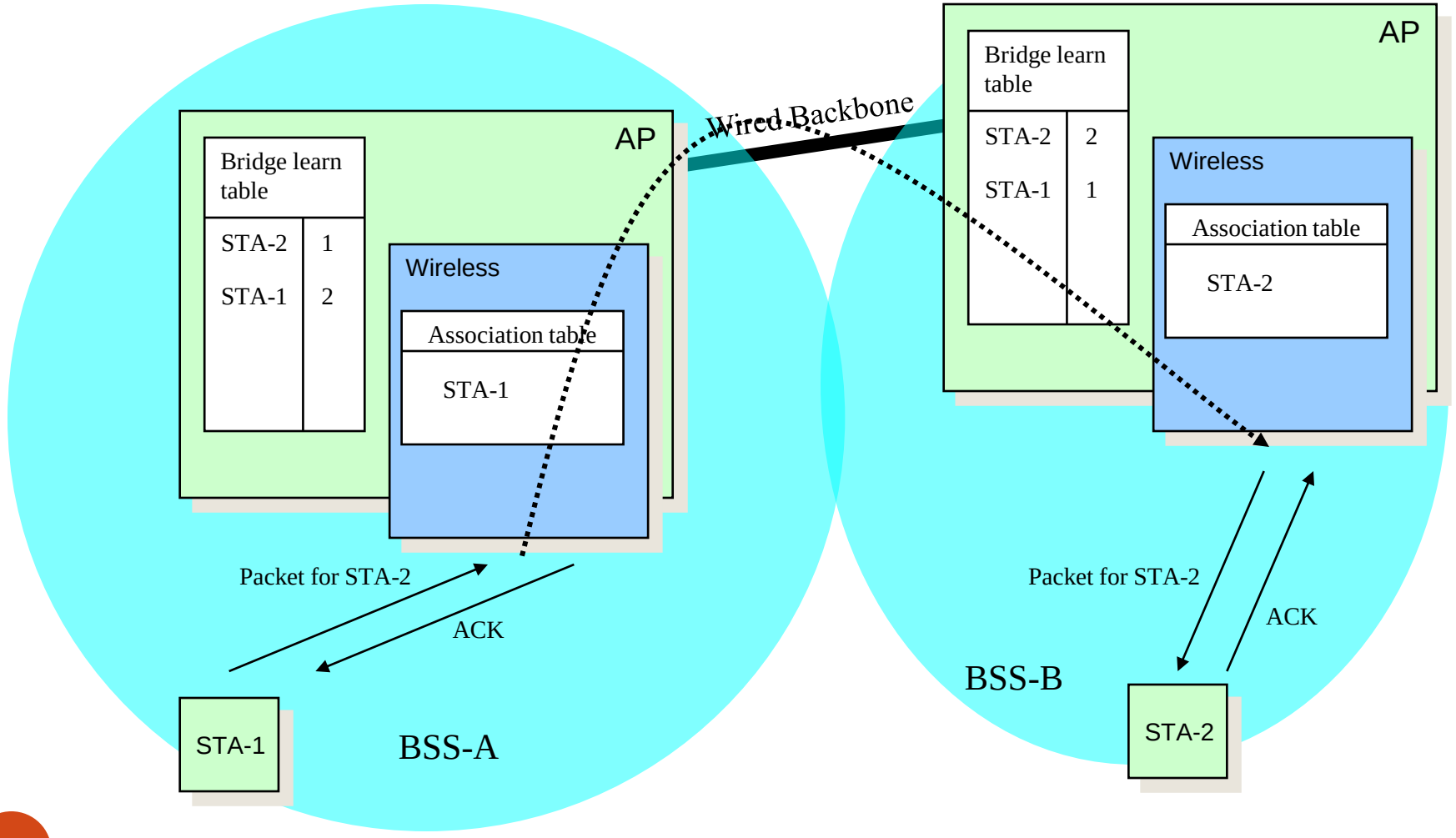
Operational processes

Traffic flow - Inter-BSS



Operational processes

Traffic flow - ESS operation



Operational processes

Traffic flow - WDS operation