Mobile Computing
Media Access

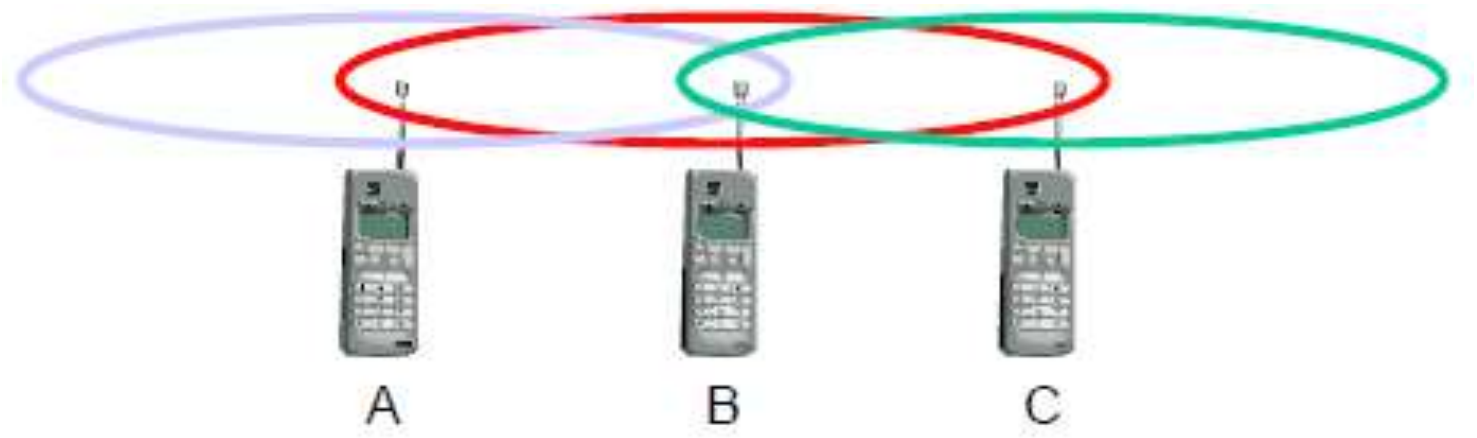
Mayank Pandey, MNNIT, Allahabad, India

Motivation

- Can we apply media access methods from fixed networks?
- Example CSMA/CD
  - **C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection
  - send when medium is free, listen to medium if collision occurs (IEEE 802.3)
- Problems in wireless networks
  - signal strength decreases with distance
  - sender applies CS and CD, but collisions happen at receiver
  - sender may not “hear” collision, i.e., CD does not work
  - Hidden terminal: CS might not work

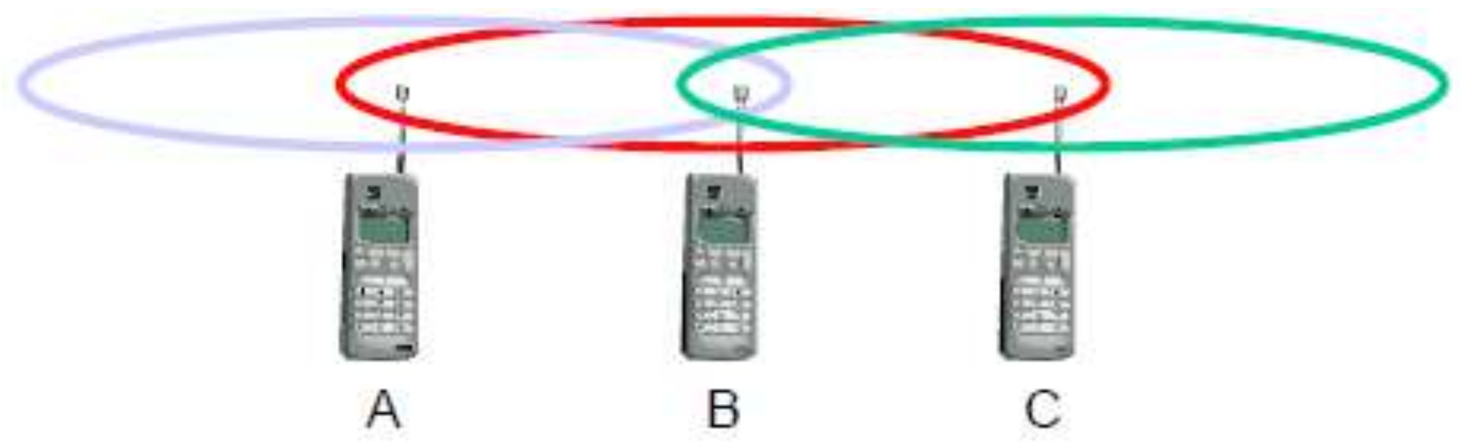
Motivation: Hidden Terminals

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



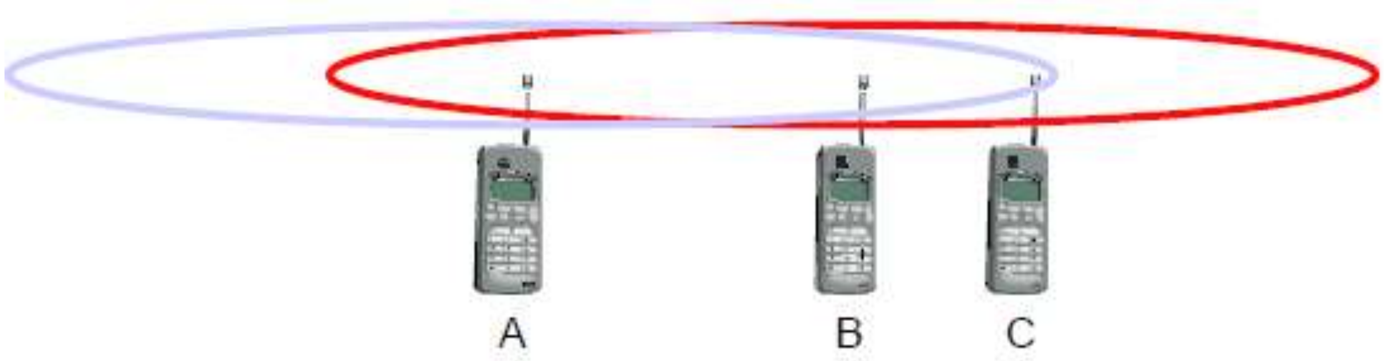
Motivation: Exposed Terminals

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



Motivation: Near & Far Terminals

- Terminals A and B send, C receives
  - signal strength decreases proportional to the square of the distance
  - B’s signal drowns out A’s signal
  - C cannot receive A

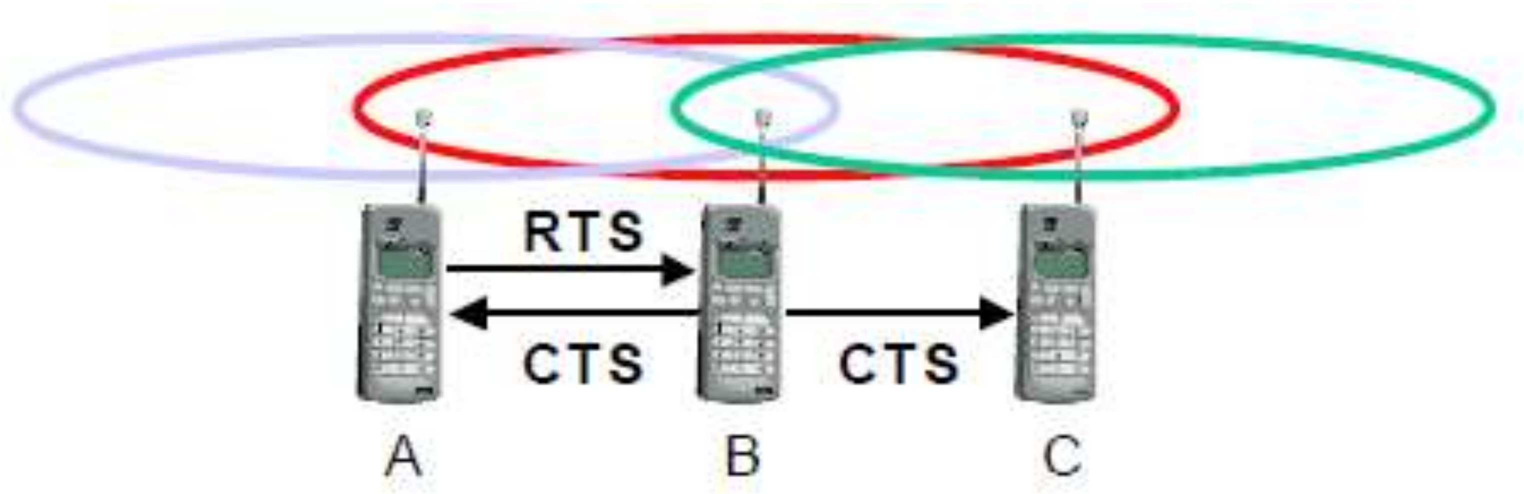


MACA: Collision Avoidance

- MACA (Multiple Access with Collision Avoidance) uses short signaling packets for collision avoidance
  - RTS (request to send): a sender uses RTS packet to request right to send before it sends a data packet
  - CTS (clear to send): the receiver grants the right to send as soon as it is ready to receive
- Signaling packets contain
  - sender address
  - receiver address
  - packet size
- Variants of this method can be found in IEEE802.11 as DFWMAC (Distributed Foundation Wireless MAC)

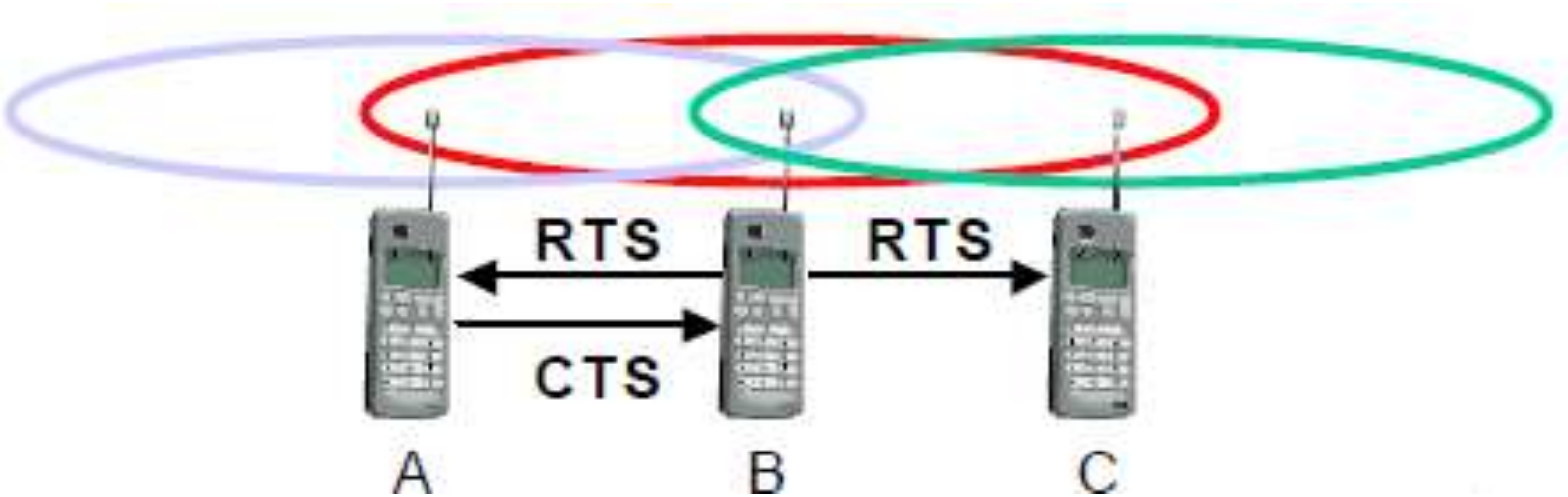
MACA: Hidden terminal

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



MACA: Exposed Terminal

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



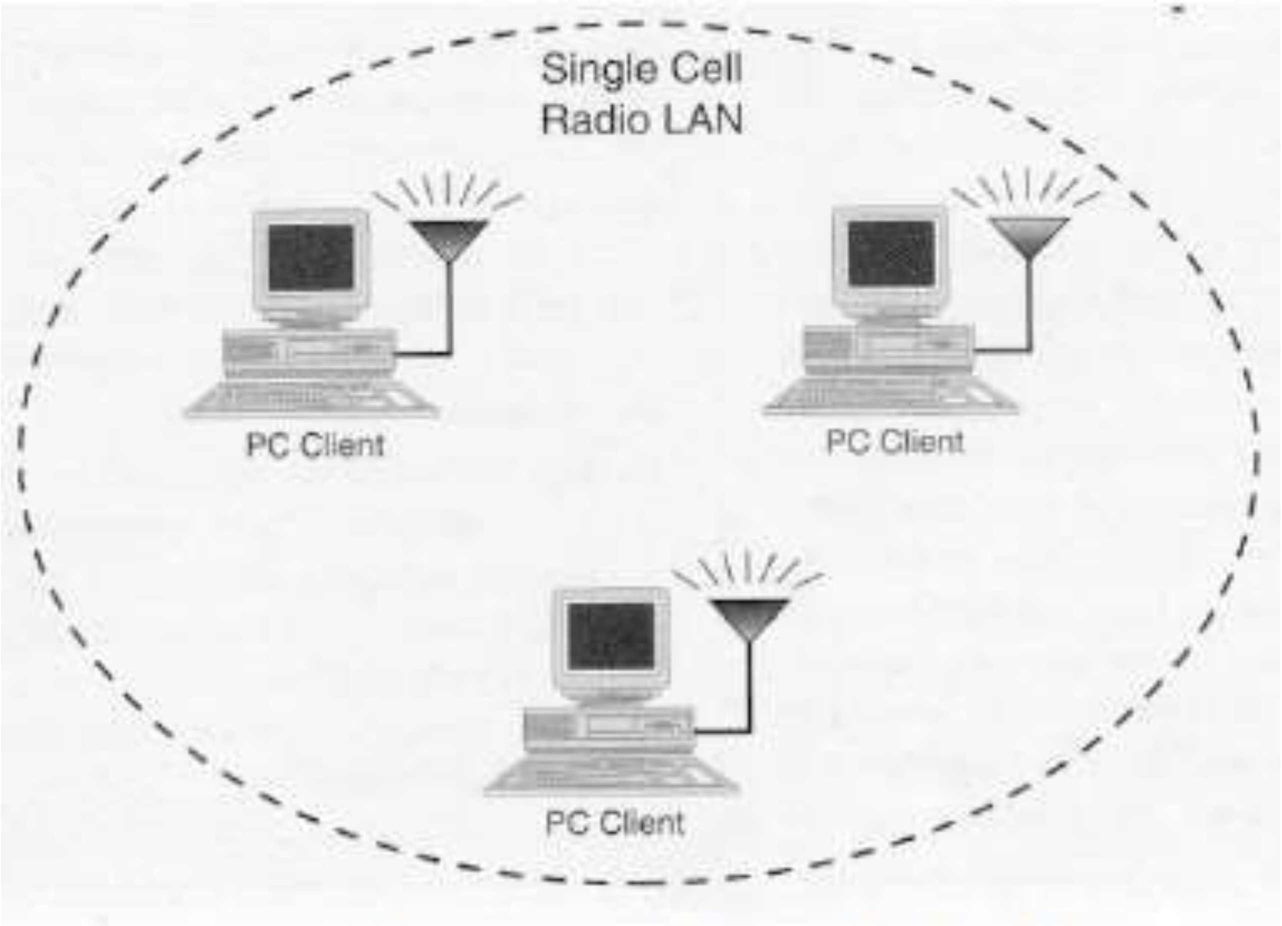
Introduction: WLAN

- A wireless LAN (WLAN) is a :
  - flexible data communication system implemented as
    - an alternative for a wired LAN within a building or campus.
- WLANs :
  - combine data connectivity with user mobility.
  - a network client can migrate between different physical locations within the LAN environment without losing connectivity.
- Flexible:
  - reconfigure /add more nodes to the network
    - without much planning effort and cost of re-cabling.

WLANs: Topologies

- Two types of network topologies:
  - ad hoc and infrastructure.
- An adhoc topology supports p2p connectivity :
  - mobile nodes communicate directly with each other using wireless adapters.
    - ideal for meetings or setting up of temporary workgroups.
      - However, it has disadvantage of limited coverage area

WLAN: Ad-hoc

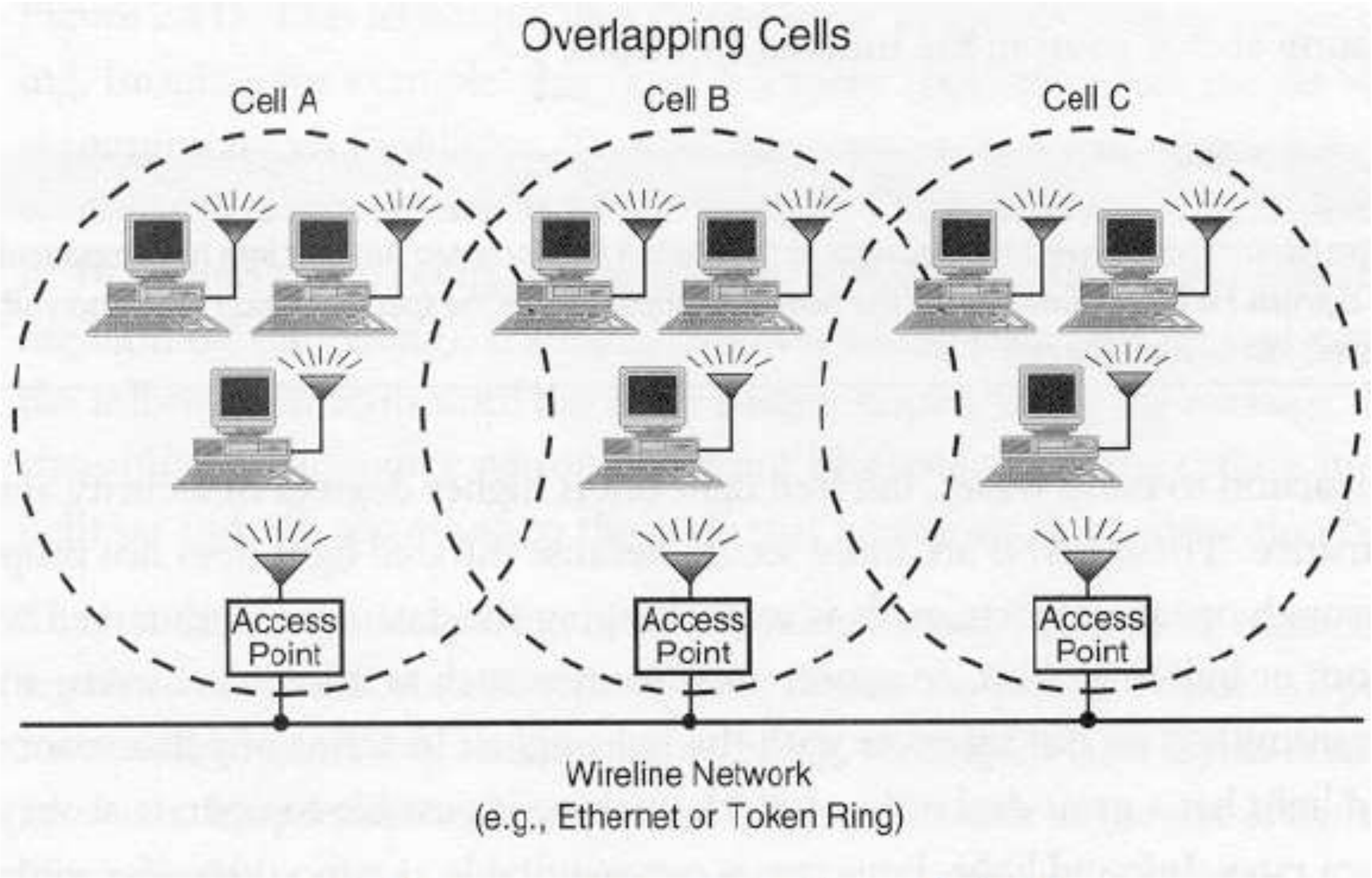


Ad hoc wireless LAN

Infrastructure wireless LANs

- Use an access point that controls :
  - transmission and assigns priority levels
  - monitors network load and
  - allows mobile stations to roam from cell to cell.
- Also:
  - to handle traffic from a mobile station to another mobile station
    - within the coverage area or to the wired backbone.

WLAN: Infrastructure



Infrastructure wireless LAN

IEEE 802.11

- Wireless LAN standard defined in the unlicensed spectrum (2.4 GHz and 5 GHz U-NII bands)

Region	Allocated Spectrum
US	2.4000 – 2.4835 GHz
Europe	2.4000 – 2.4835 GHz
Japan	2.471 - 2.497 GHz
France	2.4465 - 2.4835 GHz
Spain	2.445 - 2.475 GHz

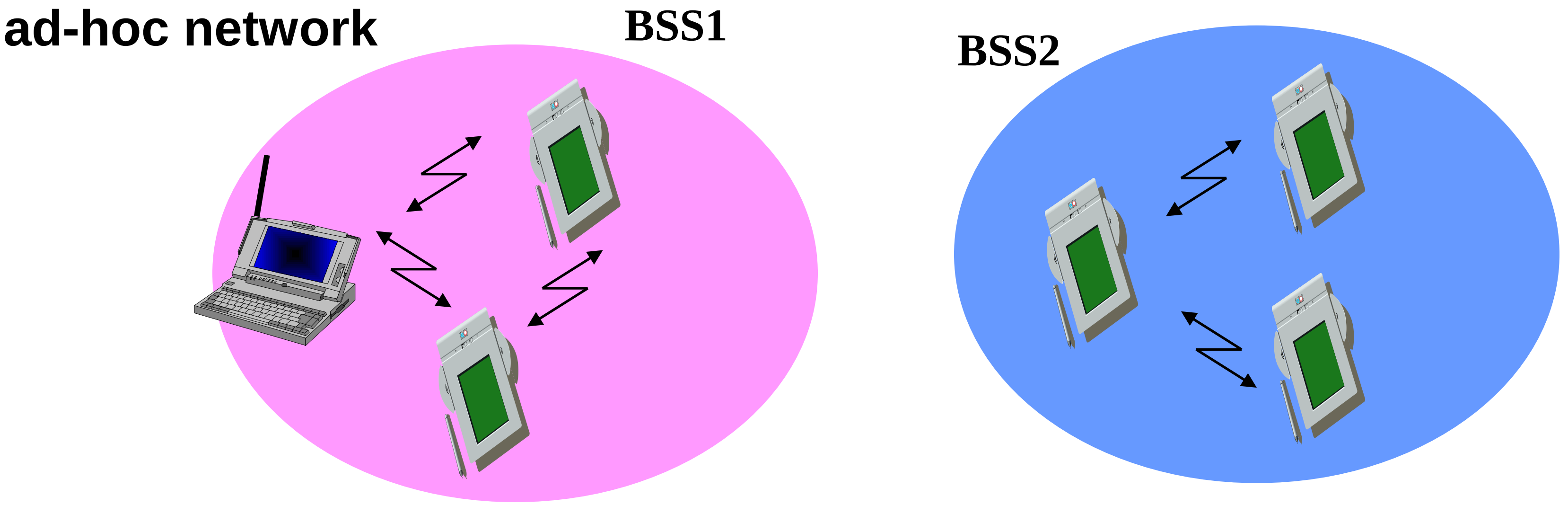
Table 1 Global Spectrum Allocation at 2.4 GHz

802.11 (contd.)

- Standards covers the MAC sublayer and PHY layers
- Three different physical layers in the 2.4 GHz band
  - FHSS, DSSS and IR
- OFDM based PHY layer in the 5 GHz band

802.11 architecture

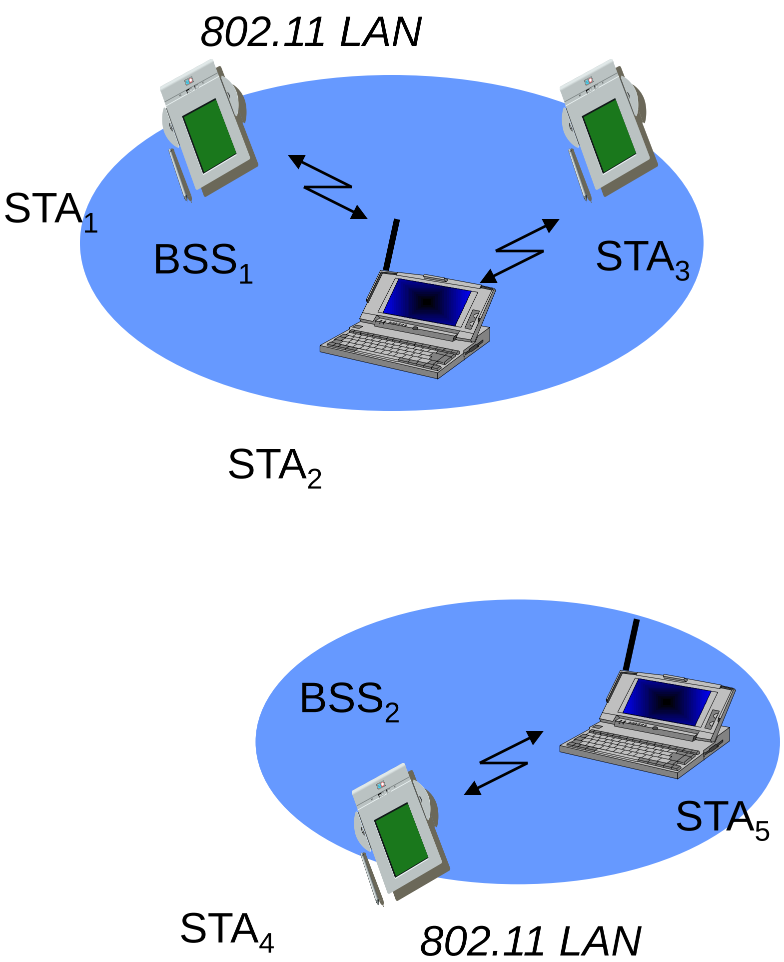
- The basic service set (BSS) is the basic building block of an IEEE 802.11 LAN



802.11 architecture (contd.)

- The ovals can be thought of as the coverage area within which member stations can directly communicate
- The Independent BSS (IBSS) is the simplest LAN. It may consist of as few as two stations
- IBSS is also called the ad hoc mode or DCF mode in 802.11

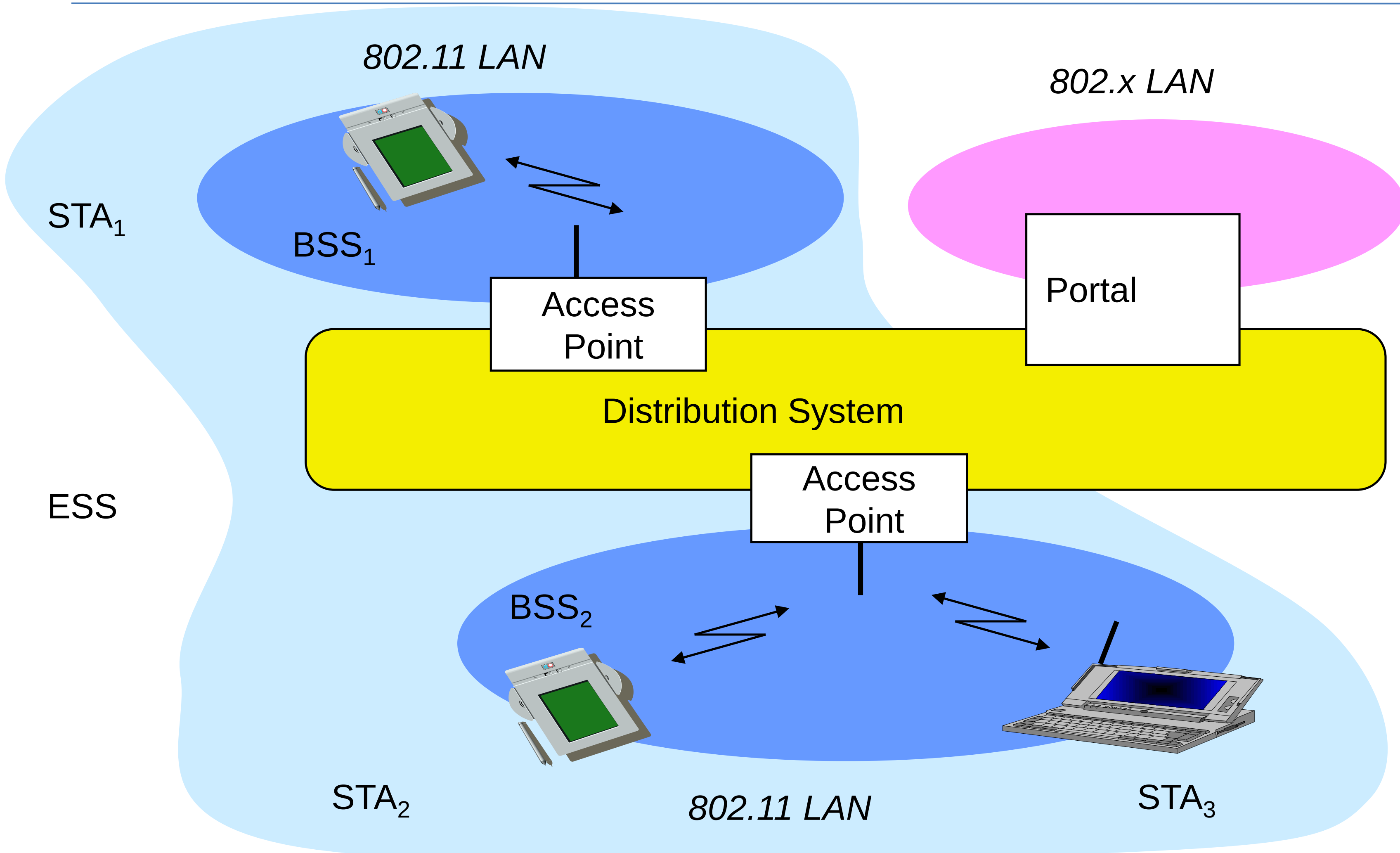
802.11 - ad-hoc network



- Direct communication within a limited range
  - Station (STA): terminal with access mechanisms to the wireless medium
  - Basic Service Set (BSS): group of stations using the same radio frequency

Source: Schiller

802.11 - infrastructure



Source: Schiller

Infrastructure 802.11 components

- Station (STA): terminal with access mechanisms to the wireless medium and radio contact to the access point
- Basic Service Set (BSS): group of stations using the same radio frequency
- Access Point: station integrated into the wireless LAN and the distribution system
- Portal: bridge to other (wired) networks
- Distribution System: interconnection network to form one logical network (ESS: Extended Service Set) based on several BSS

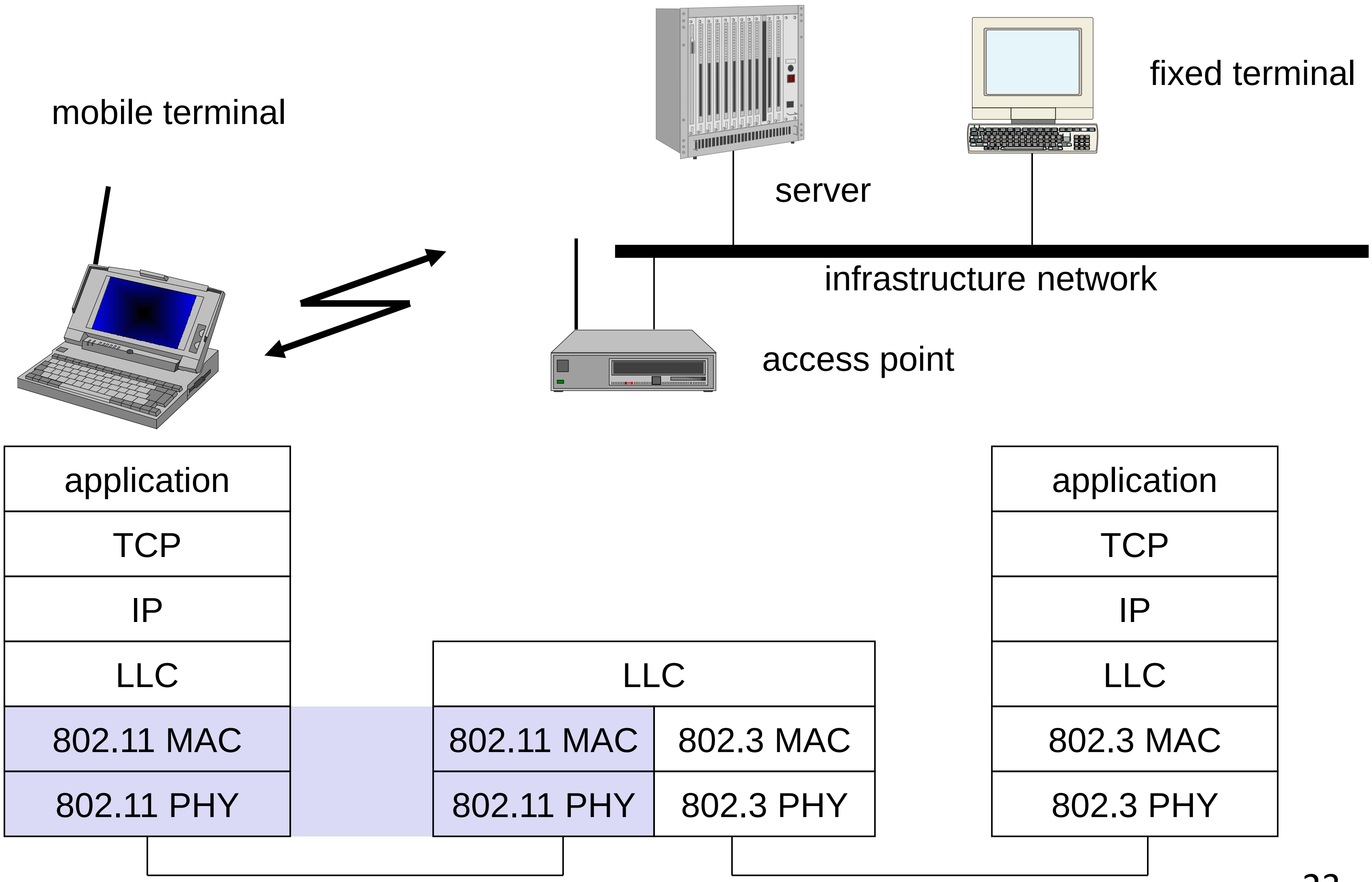
Distribution System (DS)

- The Distribution system interconnects multiple BSSs
- 802.11 standard logically separates the wireless medium from the distribution system
  - it does not preclude, nor demand, that the multiple media be same or different

DS (contd.)

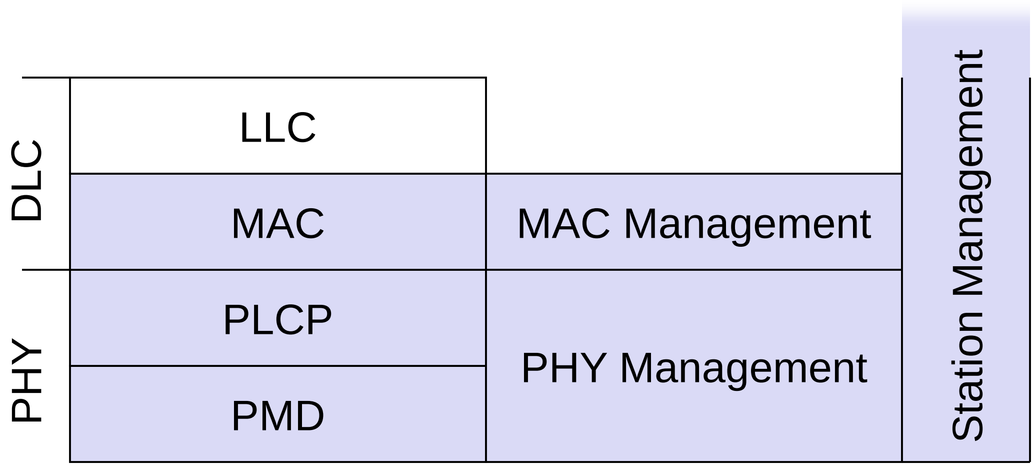
- An Access Point (AP) is a STA that provides access to the DS by providing DS services in addition to acting as a STA.
- Data moves between BSS and the DS via an AP
- The DS and BSSs allow 802.11 to create a wireless network of arbitrary size and complexity called the Extended Service Set network (ESS)

802.11- in the TCP/IP stack



802.11 - Layers and functions

- MAC
  - access mechanisms, fragmentation, encryption
- MAC Management
  - synchronization, roaming, MIB, power management



- PLCP Physical Layer Convergence Protocol
  - clear channel assessment signal (carrier sense)
- PMD Physical Medium Dependent
  - modulation, coding
- PHY Management
  - channel selection, MIB
- Station Management
  - coordination of all management functions

802.11 - MAC layer

- Traffic services
  - Asynchronous Data Service (mandatory) – DCF
  - Time-Bounded Service (optional) - PCF

- Access methods
  - DCF CSMA/CA (mandatory)
    - collision avoidance via randomized back-off mechanism
    - ACK packet for acknowledgements (not for broadcasts)

802.11 access methods

- DCF CSMA/CA (mandatory)
- DCF with RTS/CTS (optional)
  - avoids hidden terminal problem
- PCF (optional)
  - access point polls terminals according to a list

802.11 - Carrier Sensing

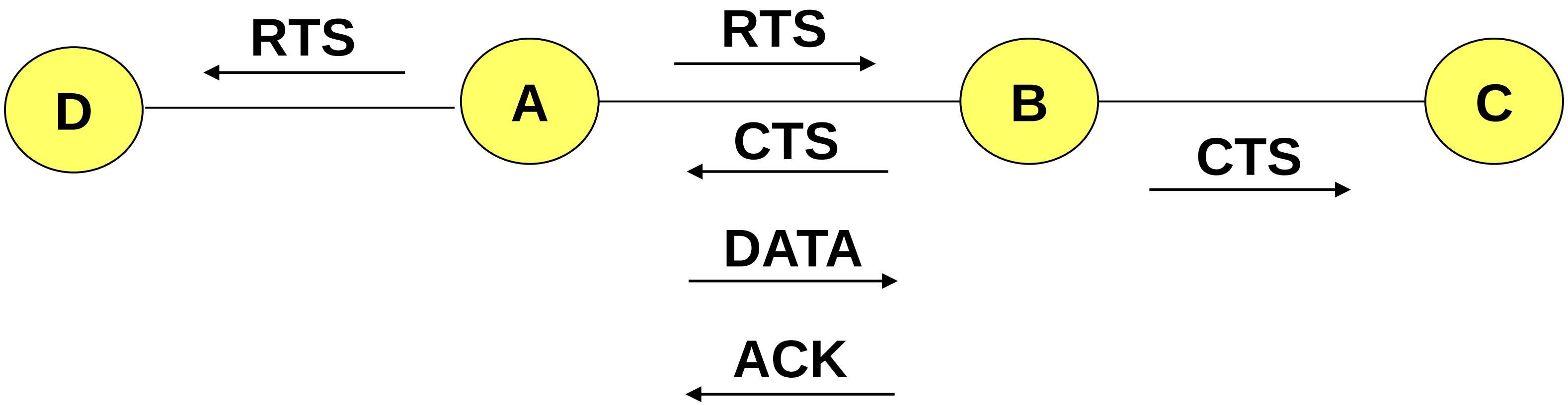
- **In IEEE 802.11, carrier sensing is performed**
  - at the air interface (*physical carrier sensing*), and
  - at the MAC layer (*virtual carrier sensing*)
- **Physical carrier sensing**
  - detects presence of other users by analyzing all detected packets
  - Detects activity in the channel via relative signal strength from other sources

802.11 virtual carrier sensing

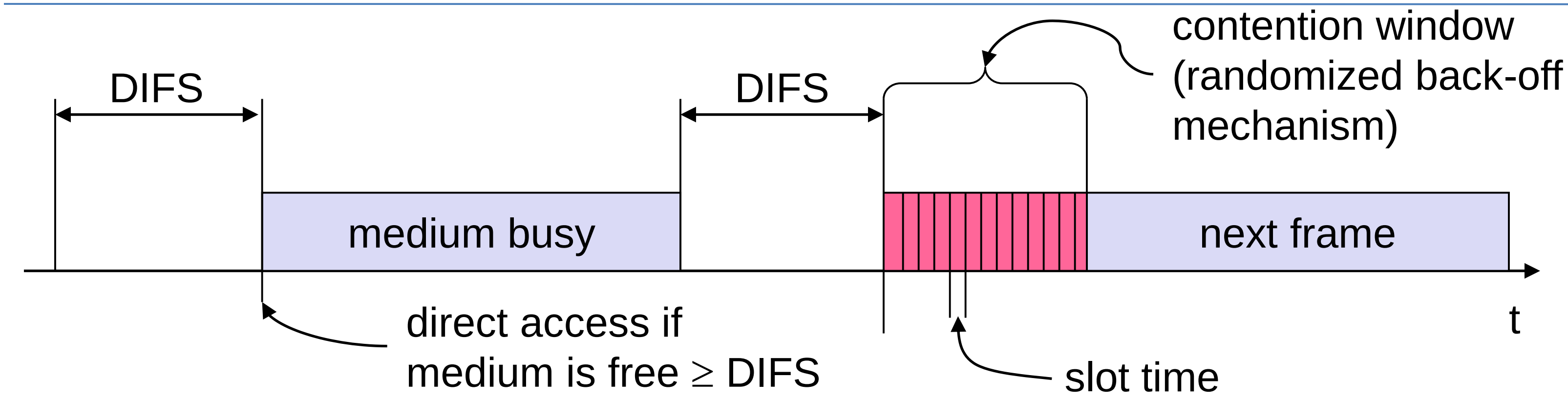
- **Virtual carrier sensing** is done by sending MPDU duration information in the header of RTS/CTS and data frames
- Channel is busy if **either** mechanisms indicate it to be
  - Duration field indicates the amount of time (in microseconds) required to complete frame transmission
  - Stations in the BSS use the information in the duration field to adjust their network allocation vector (NAV)

802.11 – Reliability: ACKs

– When B receives DATA from A, B sends an ACK
– If A fails to receive an ACK, A retransmits the DATA
– Both C and D remain quiet until ACK (to prevent collision of ACK)
– Expected duration of transmission+ACK is included in RTS/CTS packets



802.11 - CSMA/CA



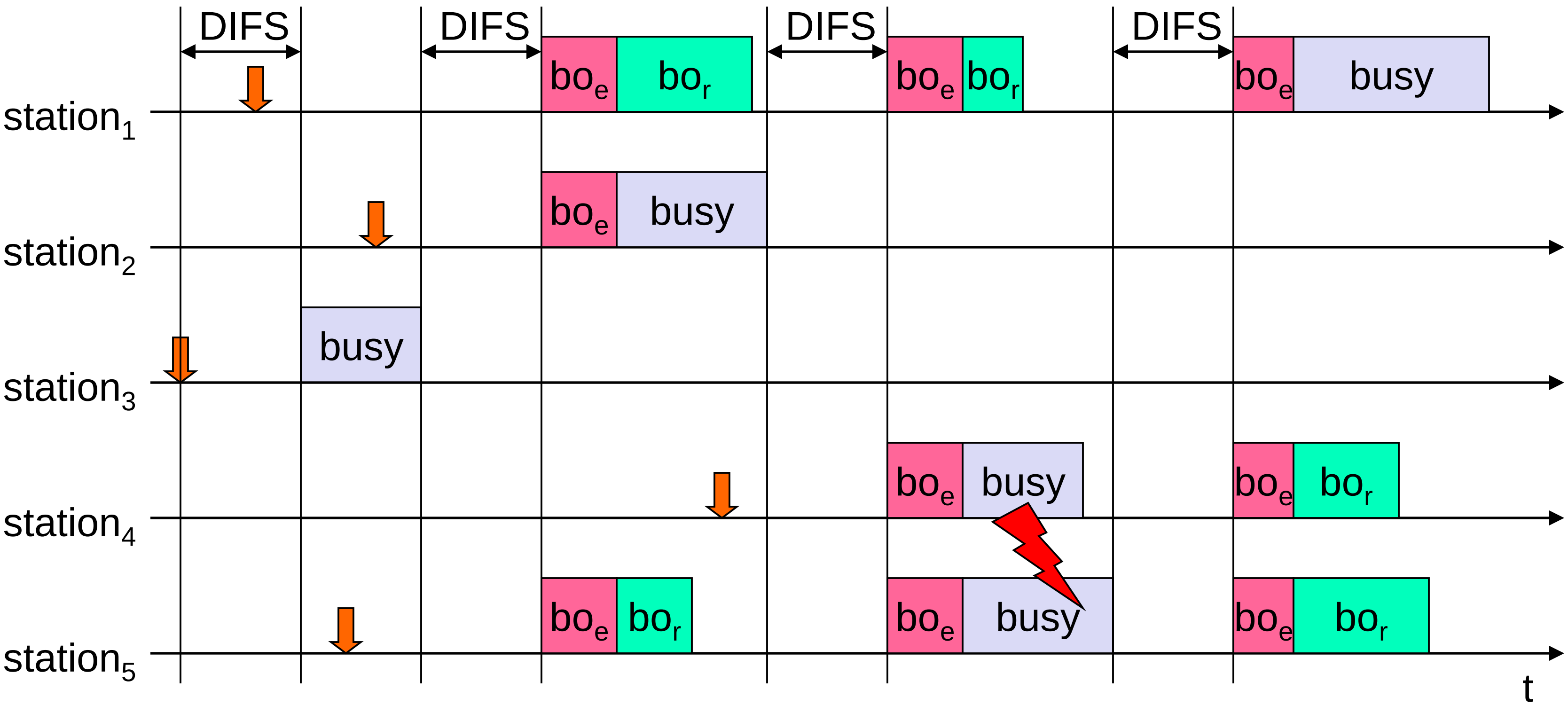
– station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)

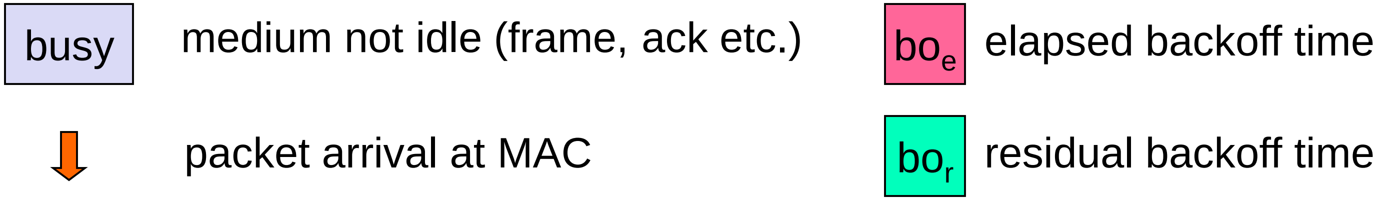
– if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)

802.11 – CSMA/CA

- if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)

802.11 –CSMA/CA example

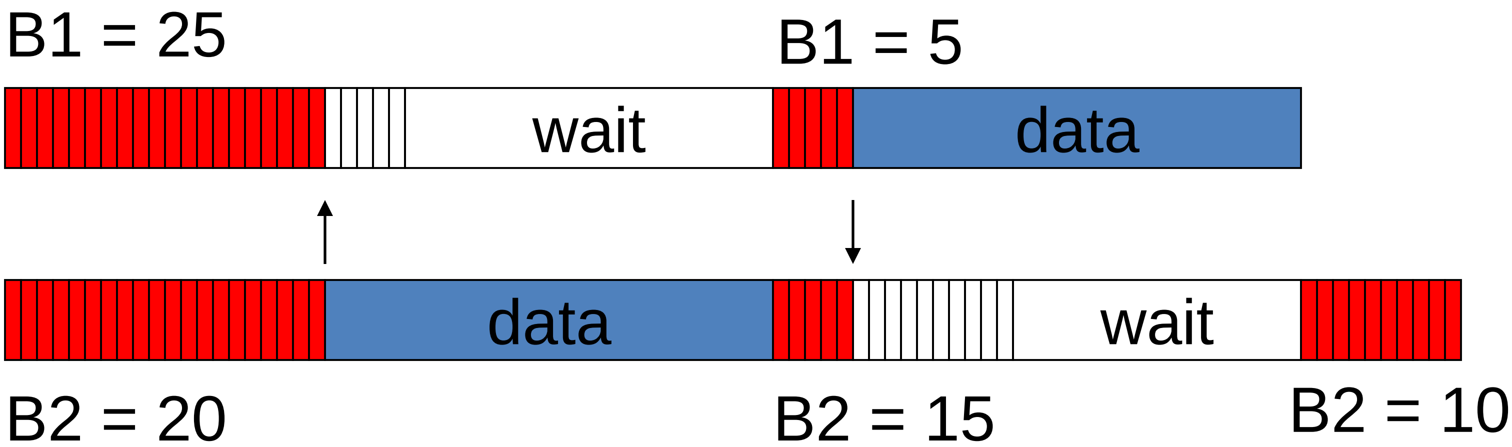




802.11 - Collision Avoidance

- Collision avoidance: Once channel becomes idle, the node waits for a randomly chosen duration before attempting to transmit
  - When transmitting a packet, choose a backoff interval in the range [0,cw]; cw is contention window
  - Count down the backoff interval when medium is idle
  - Count-down is suspended if medium becomes busy
  - When backoff interval reaches 0, transmit RTS

DCF Example



cw = 31

B1 and B2 are backoff intervals at nodes 1 and 2

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

Congestion control (contd.)

- 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)
  - Upon successful completion data transfer, restore cw to CWmin

802.11 - Priorities

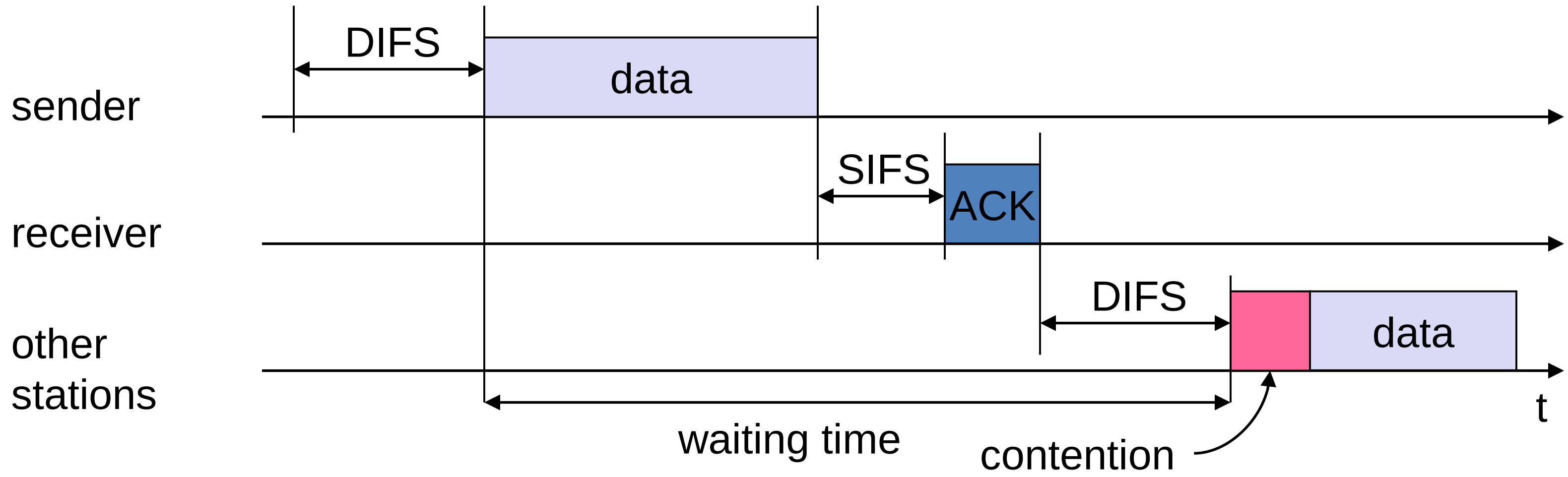
- Defined through different inter frame spaces
  - mandatory idle time intervals between the transmission of frames
- SIFS (Short Inter Frame Spacing)
  - highest priority, for ACK, CTS, polling response
  - SIFSTime and SlotTime are fixed per PHY layer
  - (10 µs and 20 µs respectively in DSSS)

802.11 – Priorities (contd.)

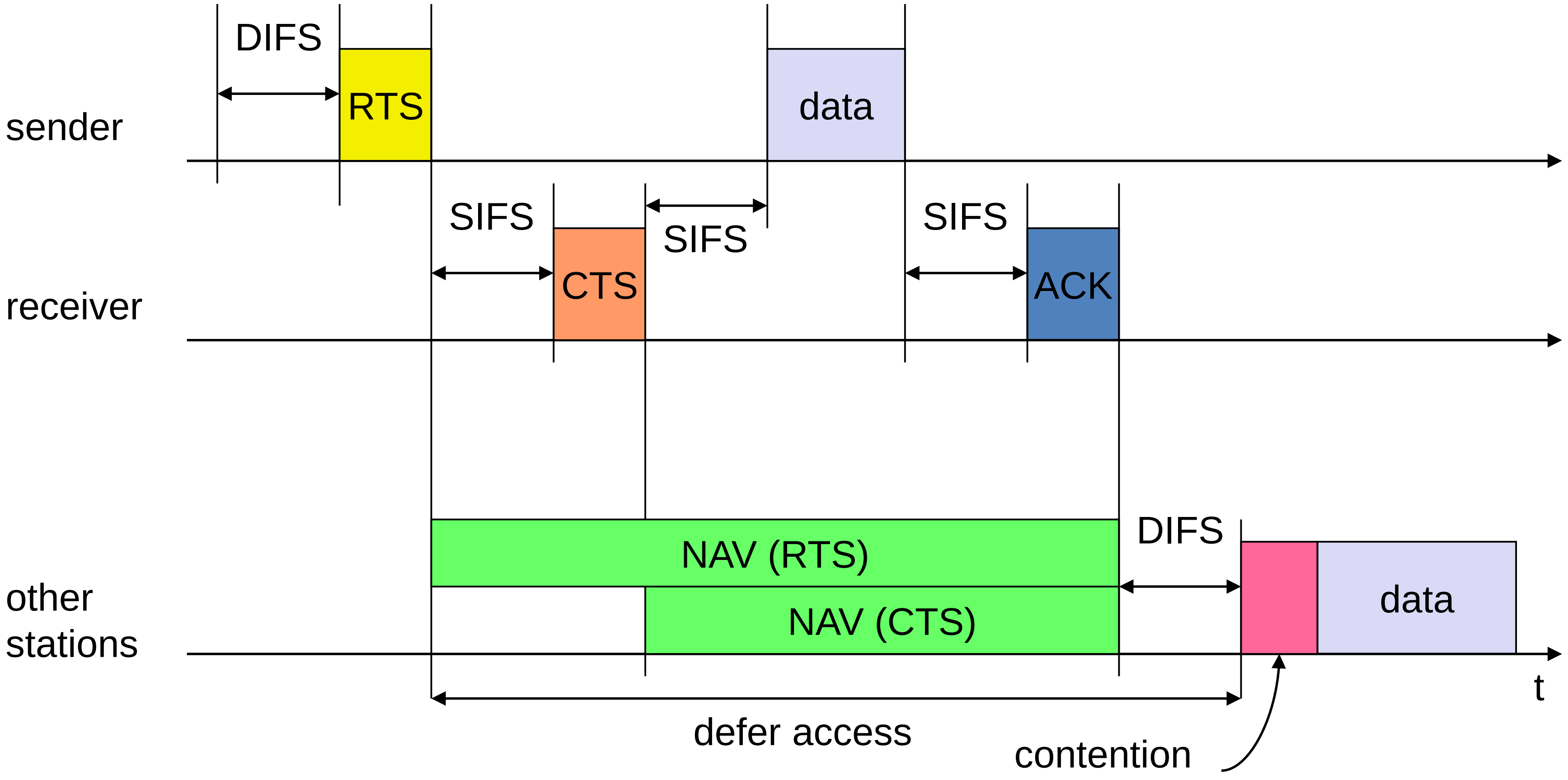
- PIFS (PCF IFS)
  - medium priority, for time-bounded service using PCF
  - PIFSTime = SIFSTime + SlotTime
- DIFS (DCF IFS)
  - lowest priority, for asynchronous data service
  - DCF-IFS (DIFS): DIFSTime = SIFSTime + 2xSlotTime

802.11 - CSMA/CA II

- station has to wait for DIFS before sending data
- receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
- automatic retransmission of data packets in case of transmission errors



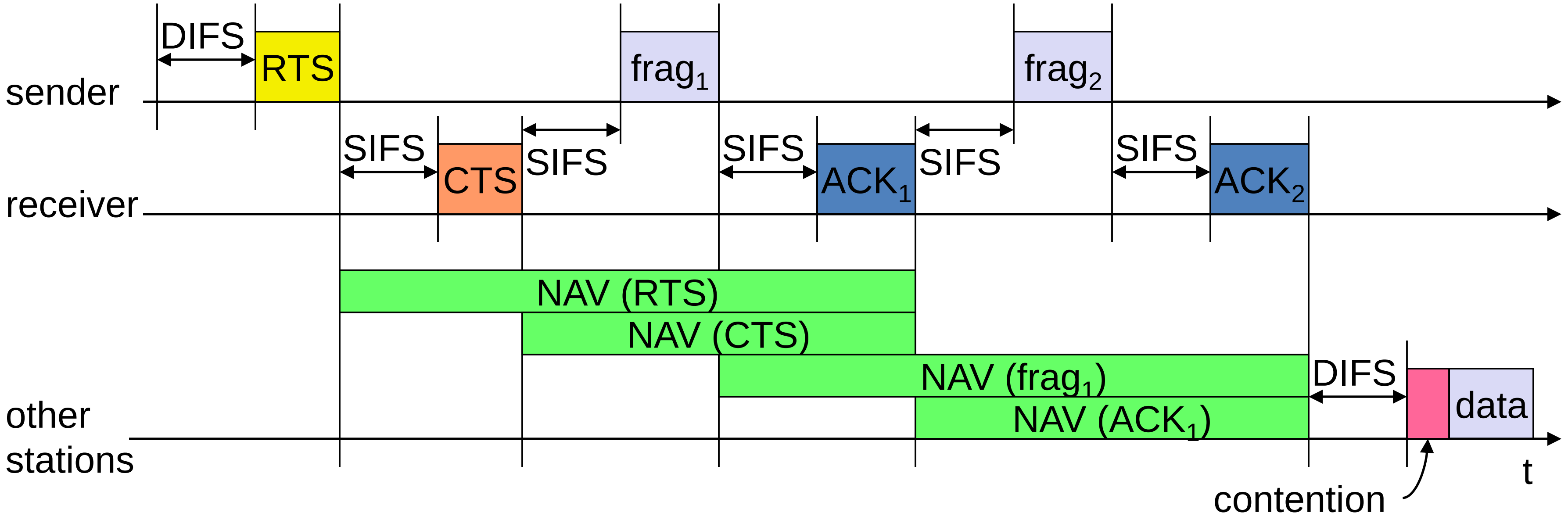
802.11 –RTS/CTS



802.11 –RTS/CTS

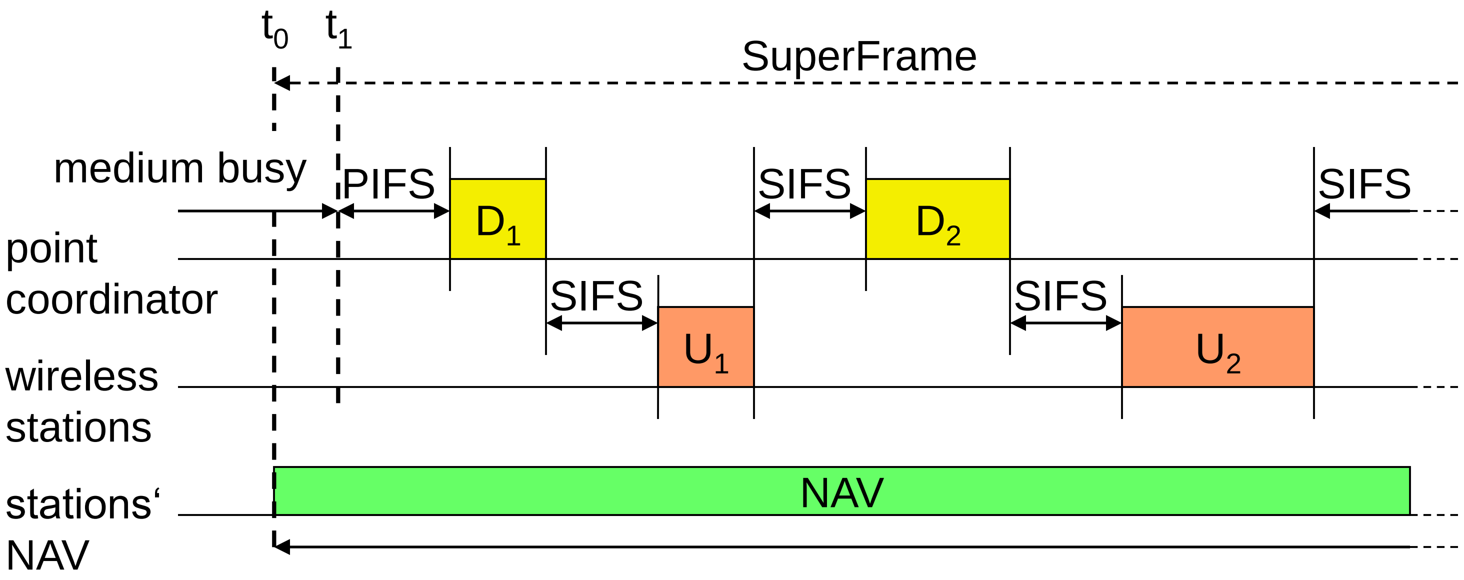
- station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
- acknowledgement via CTS after SIFS by receiver (if ready to receive)
- sender can now send data at once, acknowledgement via ACK
- other stations store medium reservations (NAV) distributed via RTS and CTS

Fragmentation



Done when the packet is very large->
Fragmentation is being performed
Sender will keep sending each frag after every sifs of receiver

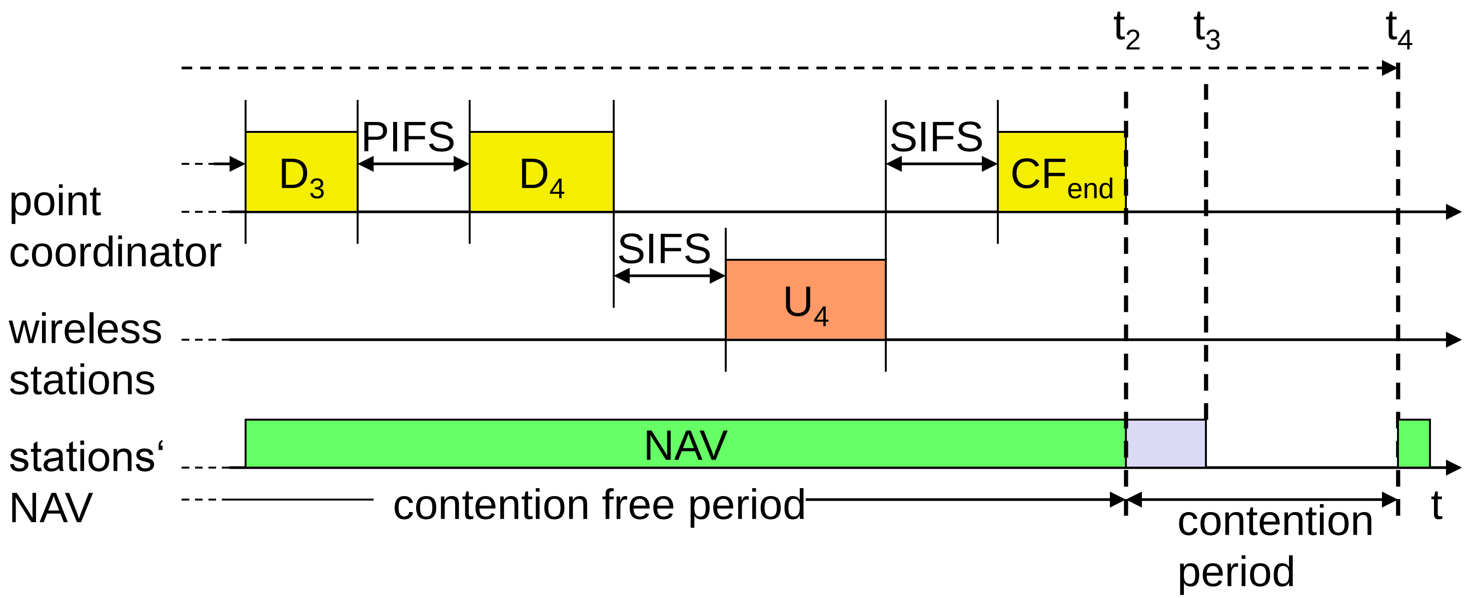
802.11 - PCF



t0 = time when the superframe should have started

t1 = time when it actually started due to contention in the prev period

802.11 - PCF



t2 = time when CFP actually finished

t3 = initial planned CFP (but PCF finished polling earlier than expected)

CFP

- The length of CFP is controlled by PC
  - CFPMaxDuration field is used for this
- When CFP is more than beacon interval
  - CFP_Dur_Remaining is included in beacons
  - CFP_Dur_Remaining is set to 0 for beacons in CP

Polling Mechanisms

- With DCF, there is no mechanism to guarantee minimum delay for time-bound services
- PCF wastes bandwidth (control overhead) when network load is light, but delays are bounded
- Implicit signaling mechanism for STAs to indicate when they have data to send improves performance

Coexistence of PCF and DCF

- PC controls frame transfers during a Contention Free Period (CFP).
  - CF-Poll control frame is used by the PC to invite a station to send data
  - CF-End is used to signal the end of the CFP
- CFPs are generated at the CFP repetition rate and each CFP begins with a beacon frame

PCF and DCF (contd.)

- The CFP alternates with a CP, when DCF controls frame transfers
  - The CP must be large enough to send at least one maximum-sized MPDU including RTS/CTS/ACK
- Superframe: One CFP + One CP. It repeats according to the CFP repetition rate and each CFP begins with a beacon frame

802.11 - Frame format

Field Name	FC	D/I	Address	Address	Address	SC	Address	Frame body	CRC
Bytes	2	2	6	6	6	2	6	0-2312	4

FC = Frame Control
D/I = Duration/Connection ID
SC = Sequence Control
CRC = Cyclic Redundancy Check

(a) MAC frame

FC Subfield	Protocol Version	Type	Subtype	To DS	From DS	MF	RT	PM	MD	WEP	O
Bits	2	2	4	1	1	1	1	1	1	1	1

DS = Distribution System
MF = More Fragments
RT = Retry
PM = Power Management
MD = More Data
WEP = Wired Equivalent Privacy
O = Order

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

Types of Frames

- Control Frames
  - RTS/CTS/ACK
  - CF-Poll/CF-End
- Data Frames
- Management Frames
  - Beacons
  - Probe Request
  - Probe Response
  - Association Request
  - Association Response
  - Dis/Reassociation
  - Authentication
  - Deauthentication
  - ATIM (Announcement TIM)

MAC address format

scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

DS: Distribution System

AP: Access Point

DA: Destination Address

SA: Source Address

BSSID: Basic Service Set Identifier

RA: Receiver Address

TA: Transmitter Address

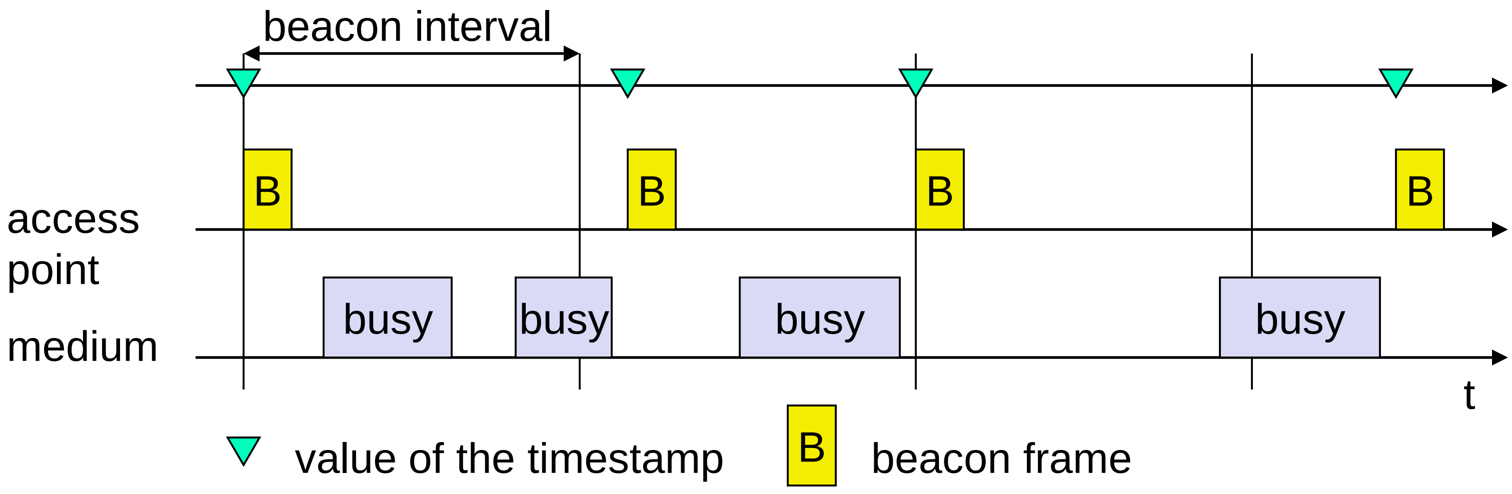
802.11 - MAC management

- Synchronization
  - try to find a LAN, try to stay within a LAN; timer etc.
- Power management
  - sleep-mode without missing a message
- Association/Reassociation
  - scanning, i.e. active search for a network
  - roaming, i.e. change networks by changing APs
- MIB - Management Information Base
  - managing, read, write

Synchronization using Beacon (infrastructure)

- Synchronized clocks are needed for PCF, Power saving and for frequency hopping
- Within a BSS timing is conveyed by a periodic beacon
- STAs use the timestamp in beacon to adjust its internal local clock
- AP always tries to send beacon at scheduled period (even if the prev beacon was delayed)

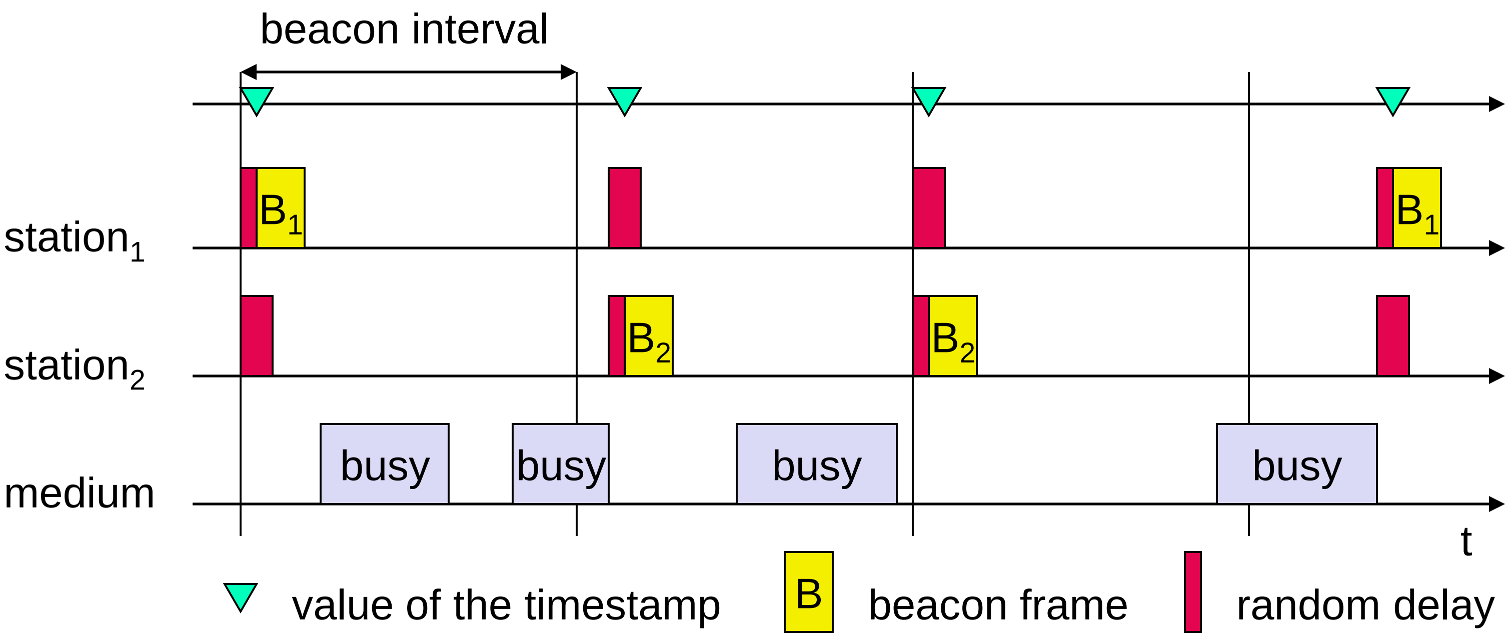
Synchronization using Beacon (infrastructure)



Synchronization using Beacon (ad-hoc)

- Synchronization in ad hoc mode is more difficult, since there is no AP for beacon transmission
- Each STA maintains its synchronization timer and starts transmission of a beacon periodically
- Standard random back off is applied to beacon frames so that only one STA wins transmitting beacon

Synchronization using Beacon (ad-hoc)



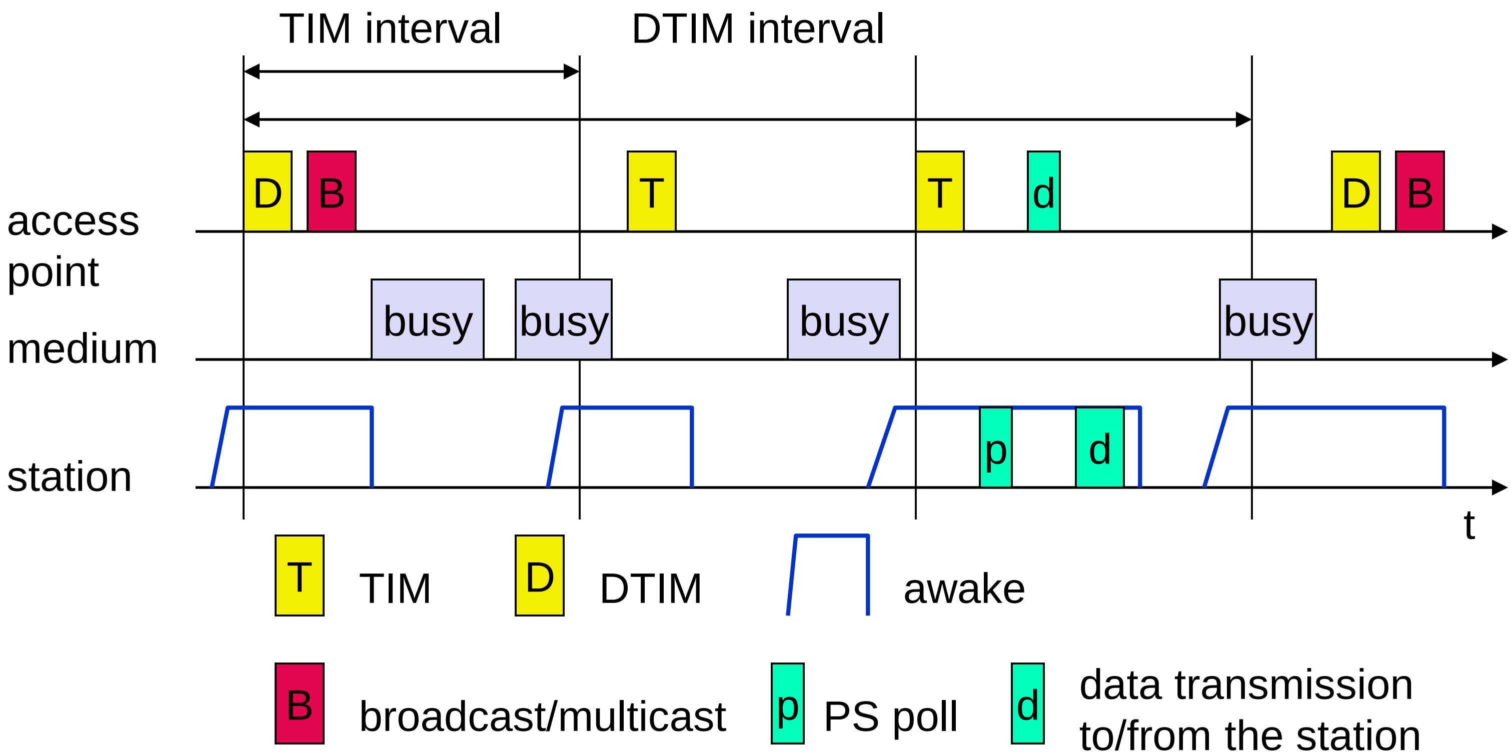
Power saving in 802.11

- Basic idea is to switch off transceiver when there is no communication
- Easy for sender since they know when to send data
- Receivers should wakeup periodically to check if it has to receive anything

Power saving :wake-up patterns (infra)

- All stations (one station shown) wake up prior to TIM or DTIM
  - With every beacon the AP sends TIM (Traffic Indication Map)
    - TIM contains a list of stations for which unicast data frames are waiting
    - DTIM (Delivery TIM) is for sending broadcast frames
  - PS (Power Saving) poll is sent by STA in response to TIM destined to the STA

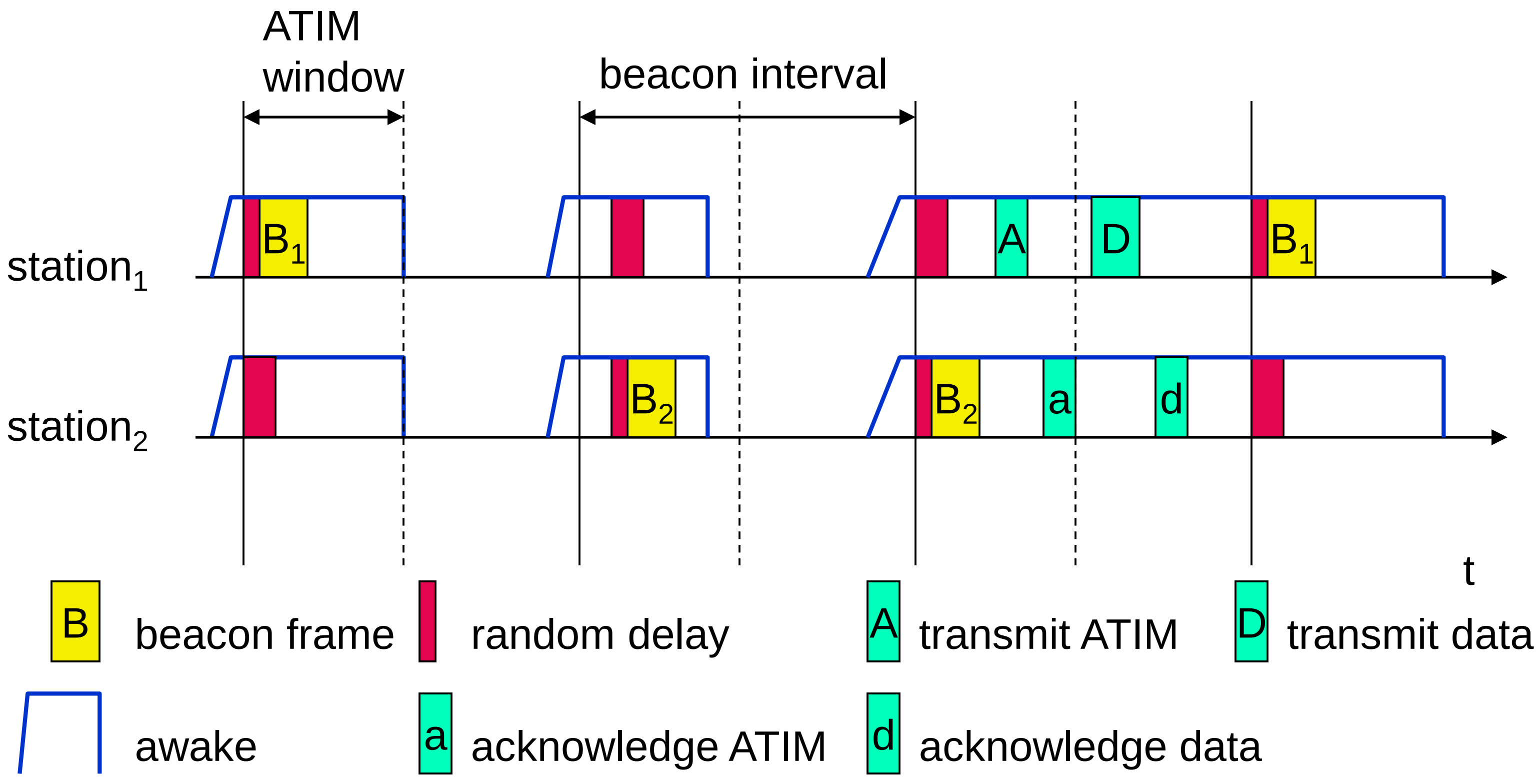
Power saving :wake-up patterns (infra)



Power saving:wakeup patterns (ad-hoc)

- PS in ad hoc mode is more complex (no central AP)
- All stations announce a list of buffered frames during a period when all of them are awake
  - Destinations are announced using ATIM (Adhoc TIM)

Power saving :wake-up patterns (ad-hoc)



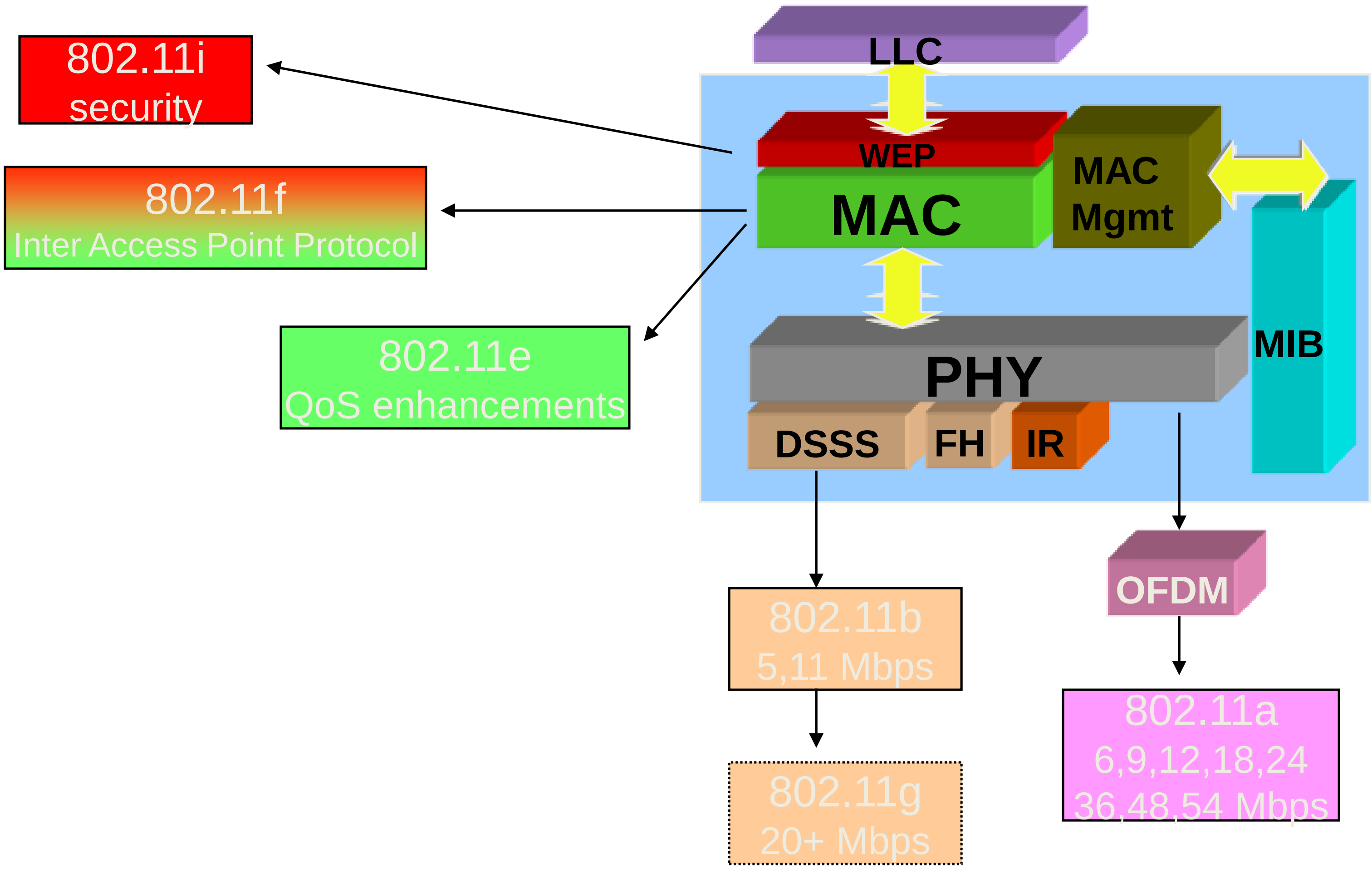
802.11 - Roaming

- Scanning
  - scan the environment, i.e.,
  - passive scanning
    - listen into the medium for beacon signals (to detect other network)
  - active scanning
    - send probes into the medium on each channel and wait for an answer
- Station then selects the best AP (e.g. based on signal strength)
  - sends association Request to the AP
- association Response
  - success: AP has answered, station is now associated with the new AP
  - failure: continue scanning

Roaming (contd.)

- AP accepts Association Request
  - signal 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 status



IEEE 802.11 Summary

- Infrastructure (PCF) and adhoc (DCF) modes
- Signaling packets for collision avoidance
  - Medium is reserved for the duration of the transmission
  - Beacons in PCF
  - RTS-CTS in DCF
- Acknowledgements for reliability
- Binary exponential backoff for congestion control
- Power save mode for energy conservation