A Brief Overview of 802.11 Wireless Networking

Alex C. Snoeren

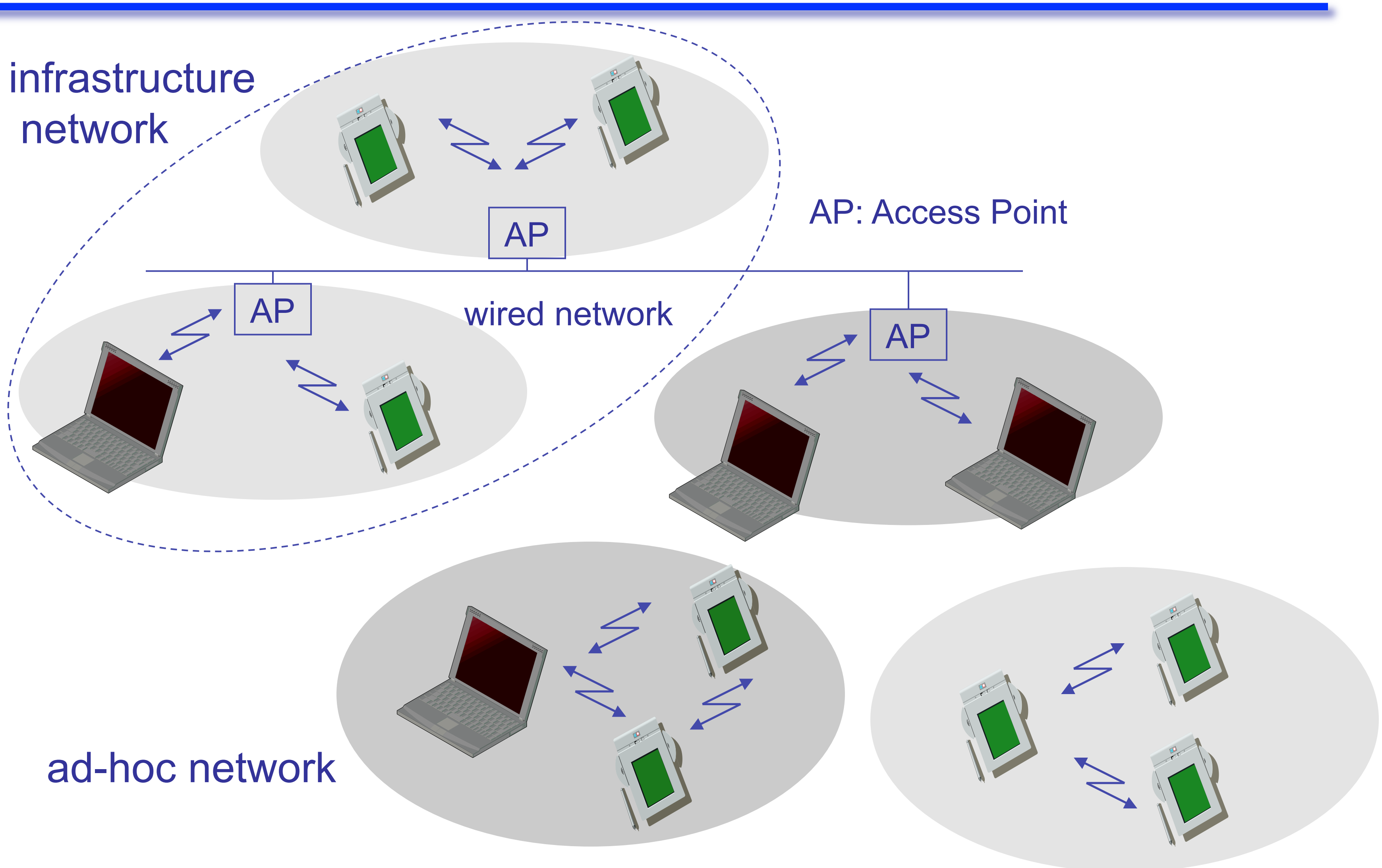
CS6250: Computer Networking

November 10, 2011

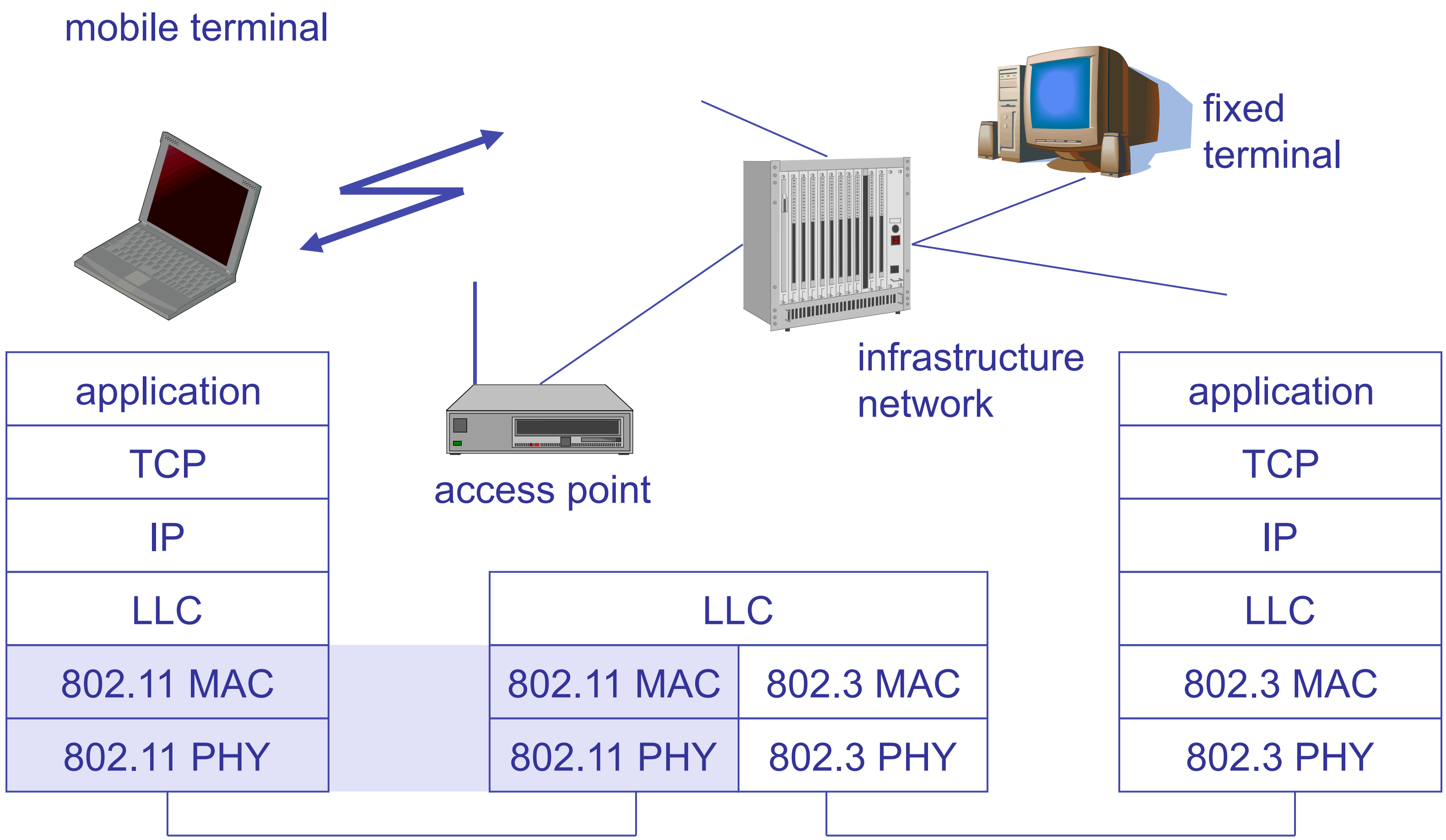
(Some slides curtesy Lili Qiu & Nitin Vaidya)

UCSDCSE
Computer Science and Engineering

Infrastructure vs. *Ad hoc*

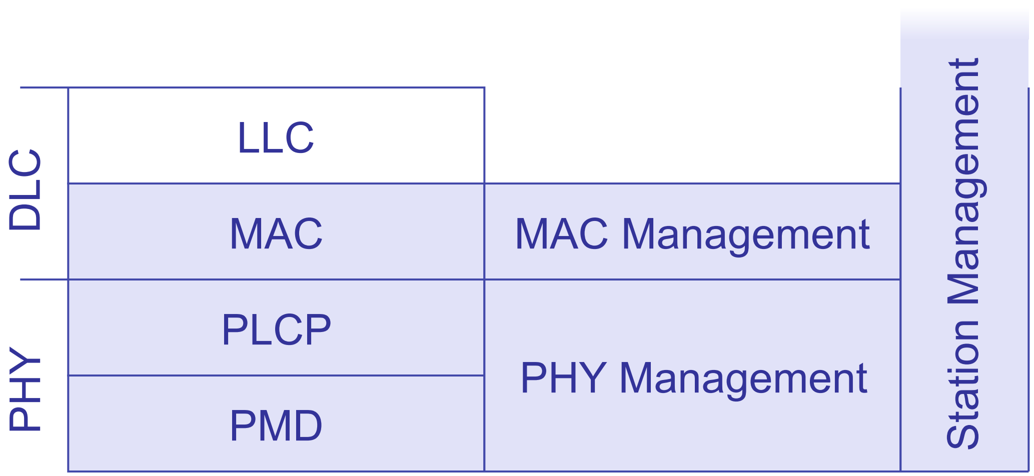


IEEE 802.11 Infrastructure



802.11 - Layers and functions

- MAC
  - access mechanisms, fragmentation, error control, 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 Physical Layers

- 802.11b - 2.4 GHz ISM band
  - FHSS (Frequency hopping spread spectrum); deprecated
  - DSSS (Direct sequence spread spectrum)
  - Up to 11 Mbps
- 802.11a/g - 2.4 GHz ISM band / 5.0 GHz UNII band
  - OFDM (Orthogonal frequency domain multiplexing)
  - Up to 54 Mbps
- 802.11n – 2.4/5.0 GHz bands
  - Adds MIMO and other tricks to 802.11g
  - Up to 300-500 Mbps!
- Each backwards compatible with the previous ones

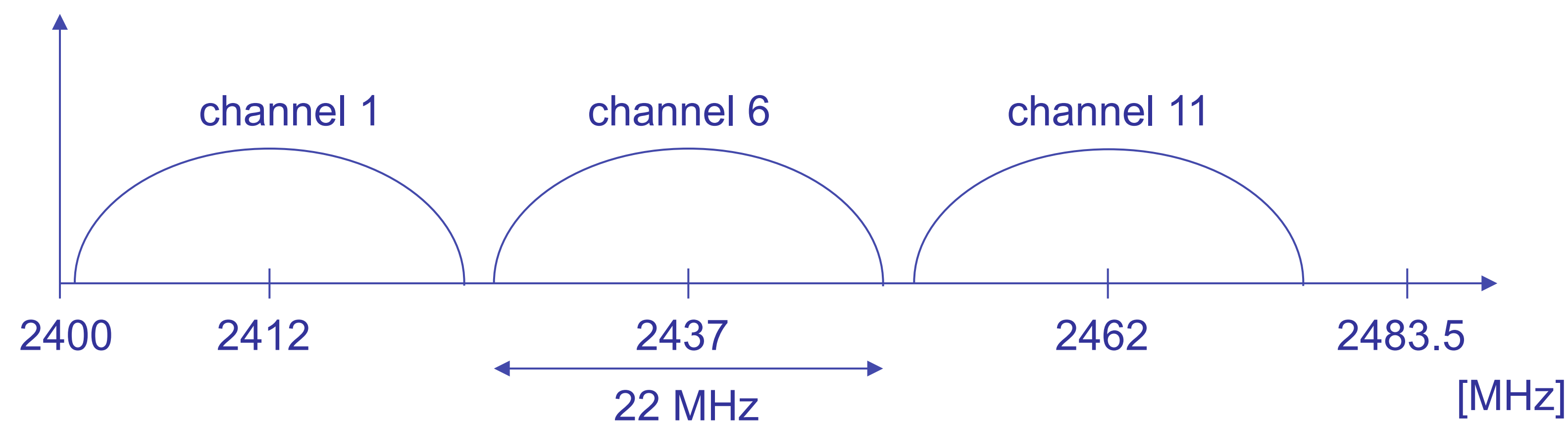
IEEE 802.11b

- Data rate
  - 1, 2, 5.5, 11 Mbit/s
  - User data rate max. approx. 6 Mbit/s
- Transmission range
  - 300m outdoor, 30m indoor
  - Max. data rate ~10m indoor
- Frequency
  - Free 2.4 GHz ISM-band

802.11b Physical Channels

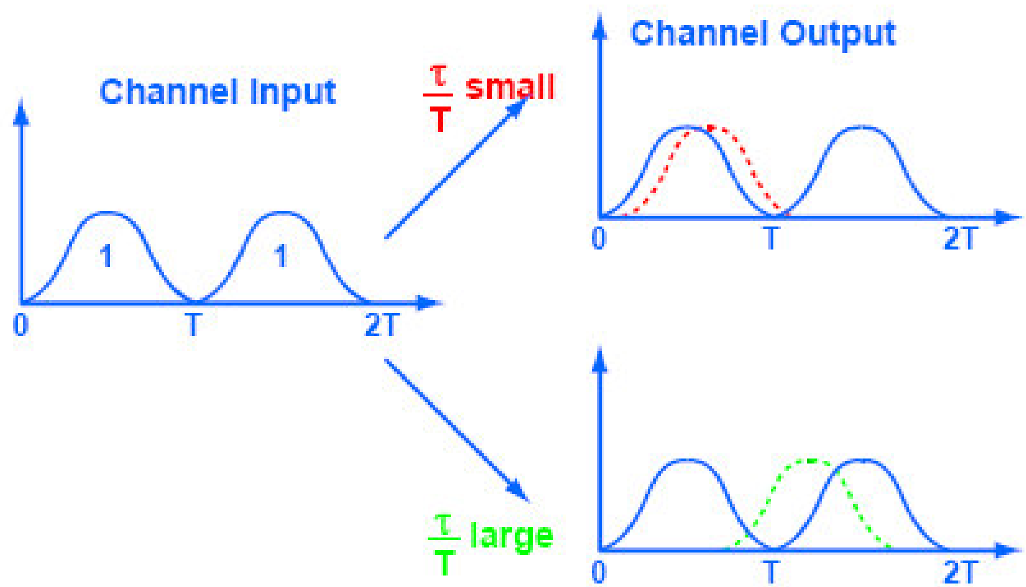
- 12 channels available for use in the US
  - Each channel is 20+2 MHz wide
  - Only 3 orthogonal channels
  - Using any others causes interference

US (FCC)/Canada (IC)



Multipath Interference

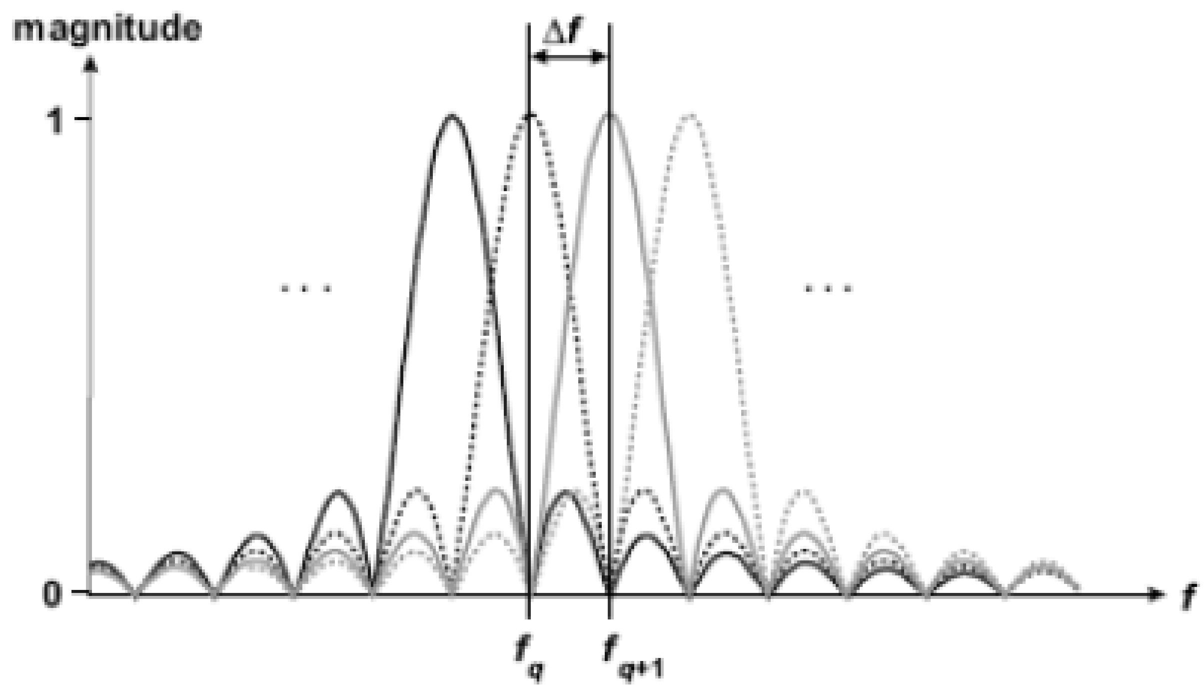
- RF signals bounce off of objects (e.g., walls)
  - Reflected signals travel different distances to receiver
  - Difference in distance leads to difference in delay



- Limits effective modulation rate in 802.11b

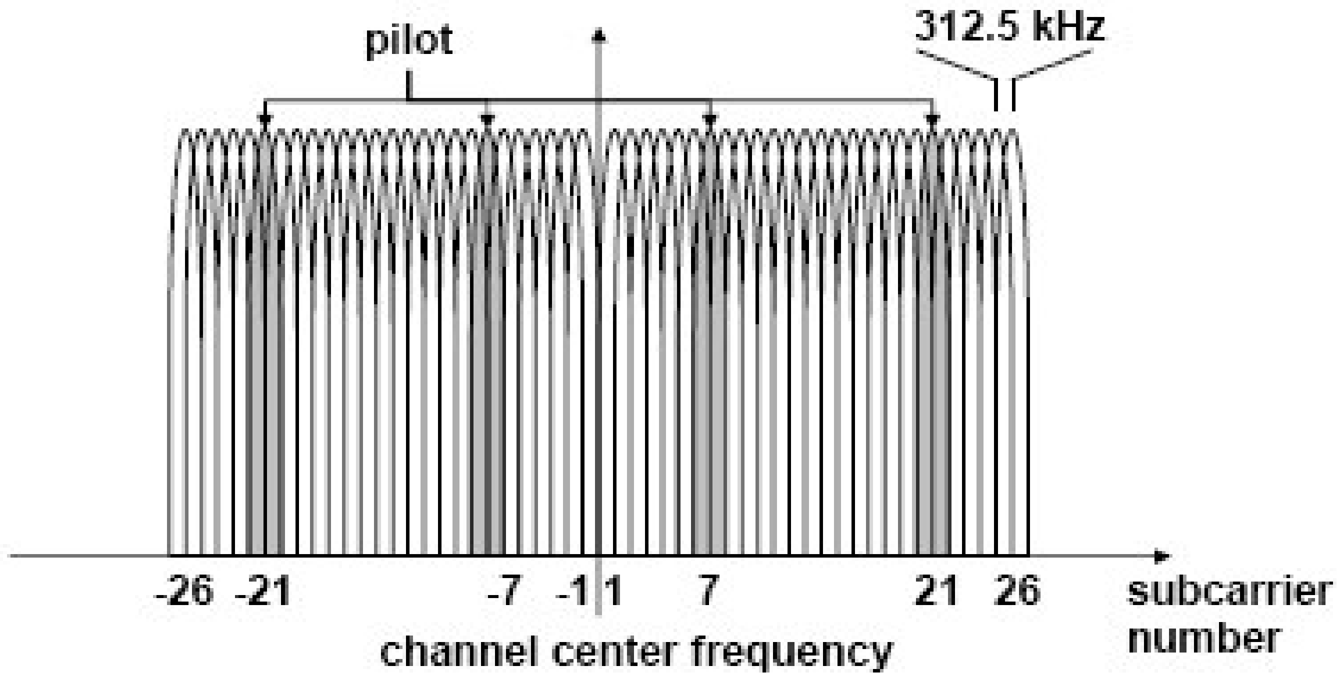
Avoiding ISI: OFDM

- Break data up into multiple separate streams
  - Transmit each stream independently on different frequency
  - Pack frequencies so that they are orthogonal



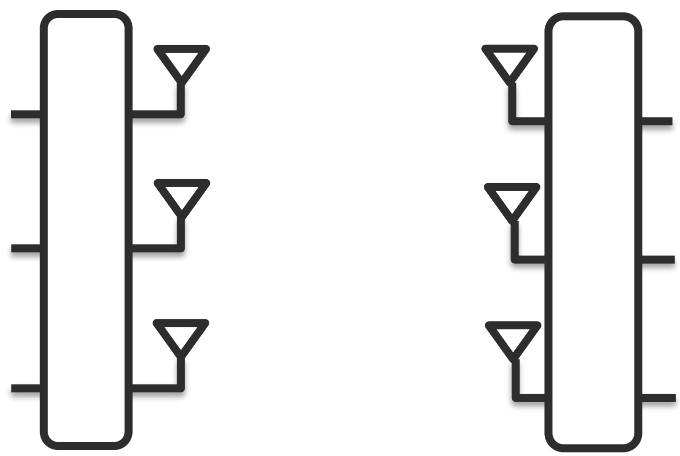
802.11a/g/n ODFM PHY

- Each 20-MHz channel divided into 50 subcarriers
  - Subcarriers spaced appropriately, 4 used as “pilots”



802.11n: MIMO

- Use multiple physical antennae simultaneously
  - Spatial multiplexing: split data cross antennae
  - Space-Time Block Coding: same data, encoded differently
  - Transmit beamforming: steer the signal toward the receiver



Carrier Sense Multiple Access

CSMA: listen before transmit

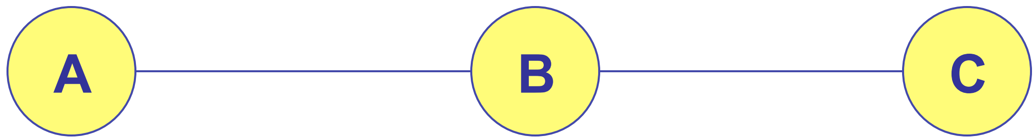
- If channel sensed idle: transmit entire packet
- If channel sensed busy, defer transmission
  - Persistent CSMA: retry immediately with probability *p* when channel becomes idle (may cause instability)
  - Non-persistent CSMA: retry after random interval

- But what about collisions?

CSMA/CA

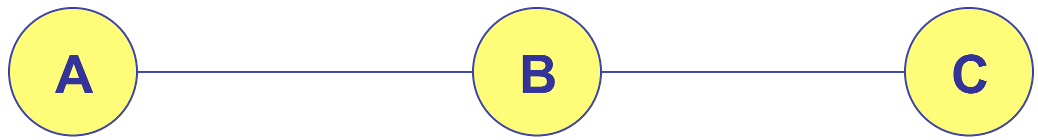
- Impossible to hear collision w/half-duplex radio
- Wireless MAC protocols often use collision avoidance techniques, in conjunction with a (physical or virtual) carrier sense mechanism
- Collision avoidance
  - Nodes negotiate to reserve the channel.
  - Once channel becomes idle, the node waits for a randomly chosen duration before attempting to transmit.

Hidden Terminal Problem



- B can communicate with both A and C
- A and C cannot hear each other
- Problem
  - When A transmits to B, C cannot detect the transmission using the carrier sense mechanism
  - If C transmits, collision will occur at node B
- Solution
  - Hidden sender C needs to defer

RTS/CTS (MACA)



- When A wants to send a packet to B, A first sends a Request-to-Send (RTS) to B
- On receiving RTS, B responds by sending Clear-to-Send (CTS), provided that A is able to receive the packet
- When C overhears a CTS, it keeps quiet for the duration of the transfer
  - Transfer duration is included in both RTS and CTS

Backoff Interval

- Problem: With many contending nodes, RTS packets will frequently collide
- Solution: When transmitting a packet, choose a backoff interval in the range [0, CW]
  - CW is contention window
- Wait the length of the interval when medium is idle
  - Count-down is suspended if medium becomes busy
  - Transmit when backoff interval reaches 0
- Need to adjust CW as contention varies

MILD Algorithm in MACAW

- MACAW uses exponential increase linear decrease to update CW
  - When a node successfully completes a transfer, reduces CW by 1
  - In 802.11 CW is restored to CW_{min}
  - In 802.11, CW reduces much faster than it increases
- MACAW can avoid wild oscillations of CW when many nodes contend for the channel

Cute Hack

- We can use CTS to reserve the channel for ourselves
  - Don’t use RTS/CTS handshake, just back half
  - Called a CTS-to-self, simply transmit CTS before our packet
- Doesn’t solve hidden terminal, but does squelch
  - Means stations don’t need to be able to decode data frame
- 802.11g uses CTS-to-self to operate w/802.11b
  - 11g stations always send a CTS before sending packets encoded in a way (ODFM) that 11b stations can’t decode
- Much more efficient that full RTS/CTS

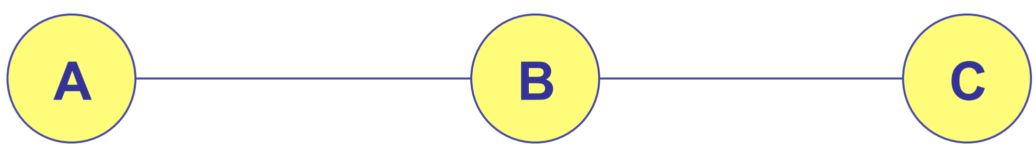
Challenge: Reliability

- Wireless links are prone to errors. High packet loss rate detrimental to transport-layer performance.

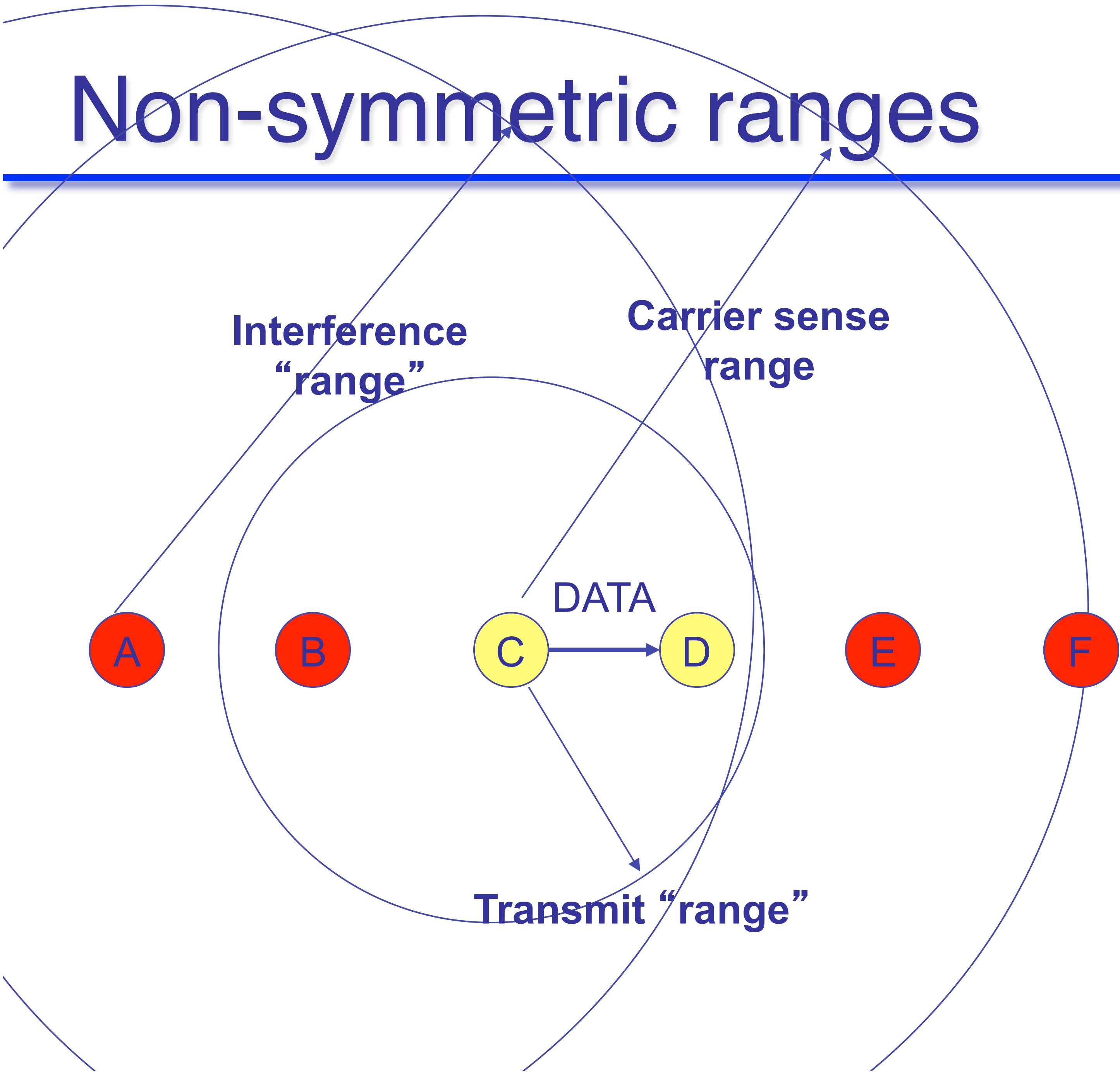
- Mechanisms needed to reduce packet loss rate experienced by upper layers

Link-layer ARQ

- When B receives a data packet from A, B sends an Acknowledgement (ACK) to A.
- If node A fails to receive an ACK, it will retransmit the packet



Non-symmetric ranges



Other MACAW Features

- Fairness: Normally, each node wins the channel with equal probability
  - Nodes with multiple streams should be more aggressive
  - Abandoned in 802.11. Why?
- Conservative collision avoidance
  - Use a Data Sending (DS) packet to reserve the channel
  - 802.11 uses different length intervals and the NAV
- Request-for-Request-to-Send
  - Assume carrier sense range far larger than transmission range

802.11 MAC Modes

- Disributed Coordination Function (DCF) CSMA/CA
  - collision avoidance via randomized “back-off“ mechanism
  - minimum distance between consecutive packets
  - ACK packet for acknowledgements (not for broadcasts)

- DCF w/ RTS/CTS
  - Distributed Foundation Wireless MAC
  - avoids hidden terminal problem

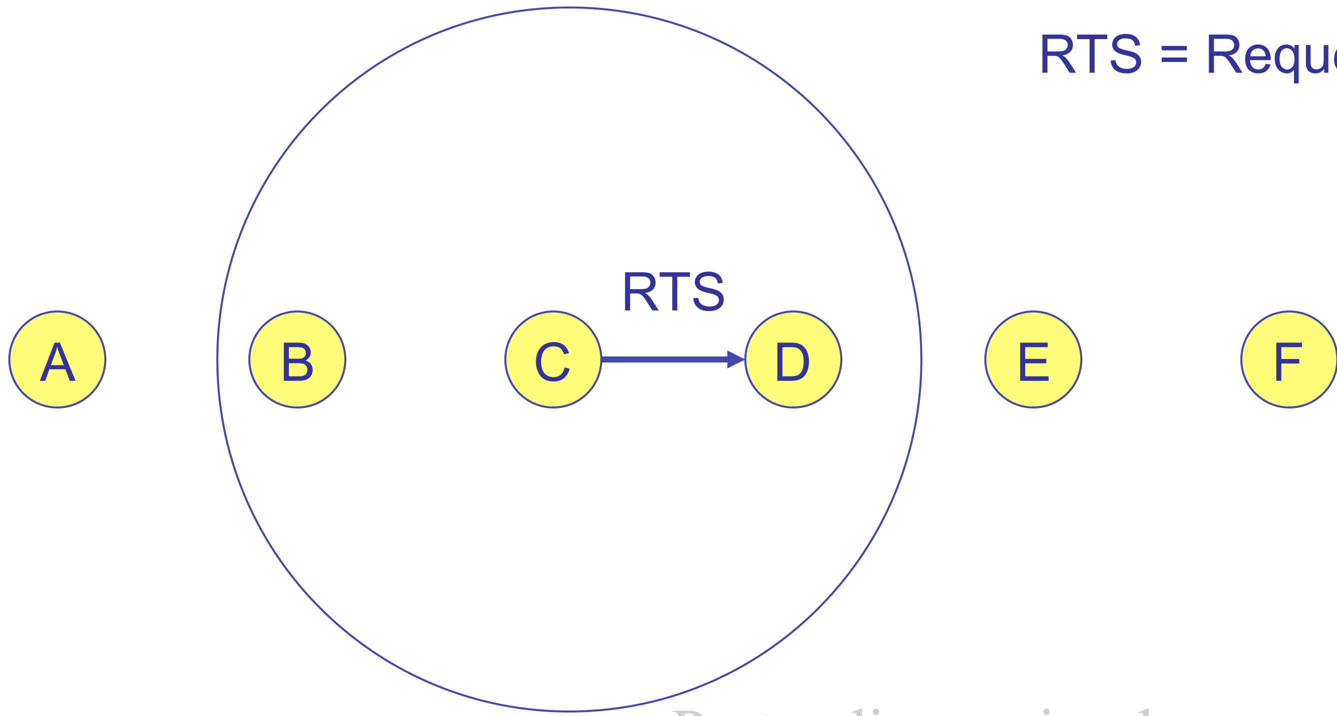
- Point Control Function (PCF) - *optional*
  - Access point polls terminals according to a list
  - We’re not going to discuss…

IEEE 802.11 DCF

- DCF is CSMA/CA protocol
  - Uses a Network Allocation Vector (NAV) to implement collision avoidance
- DCF suitable for multi-hop ad hoc networking
- Optionally uses RTS-CTS exchange to avoid hidden terminal problem
  - Any node overhearing a CTS cannot transmit for the duration of the transfer
- Uses ACK to provide reliability

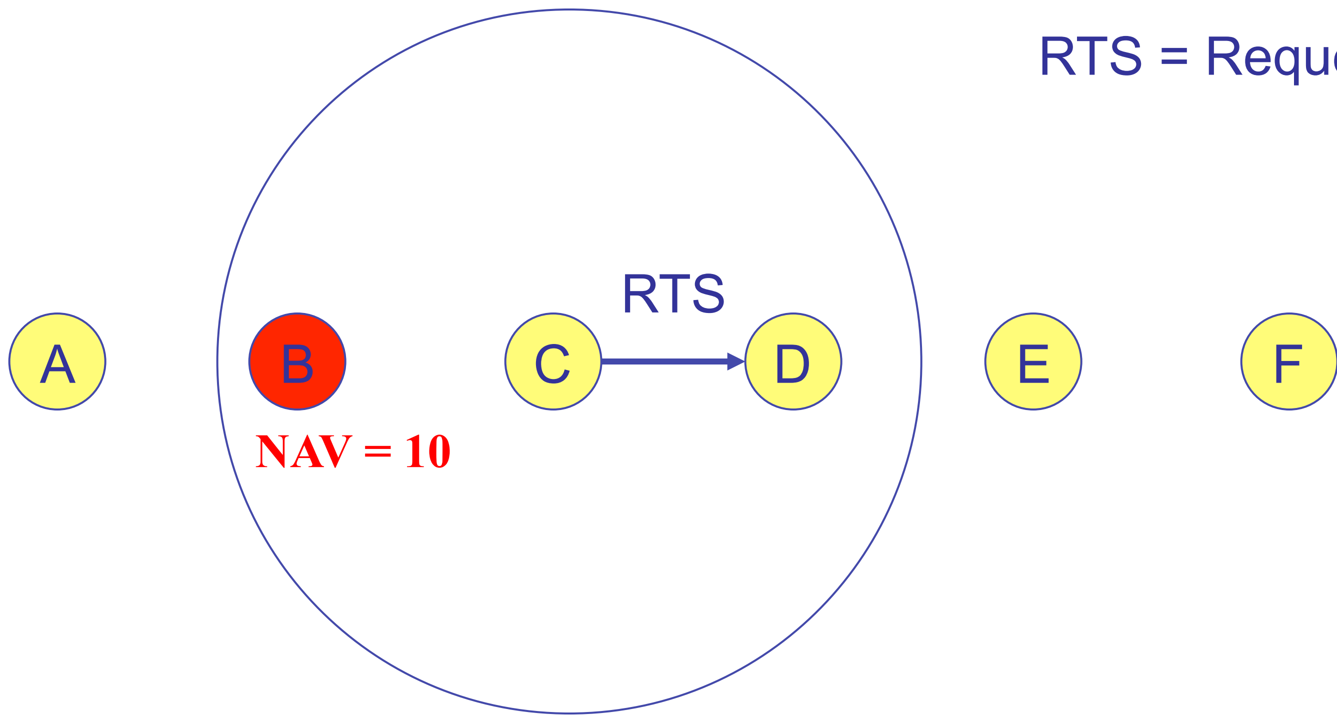
IEEE 802.11

RTS = Request-to-Send



Pretending a circular range

IEEE 802.11

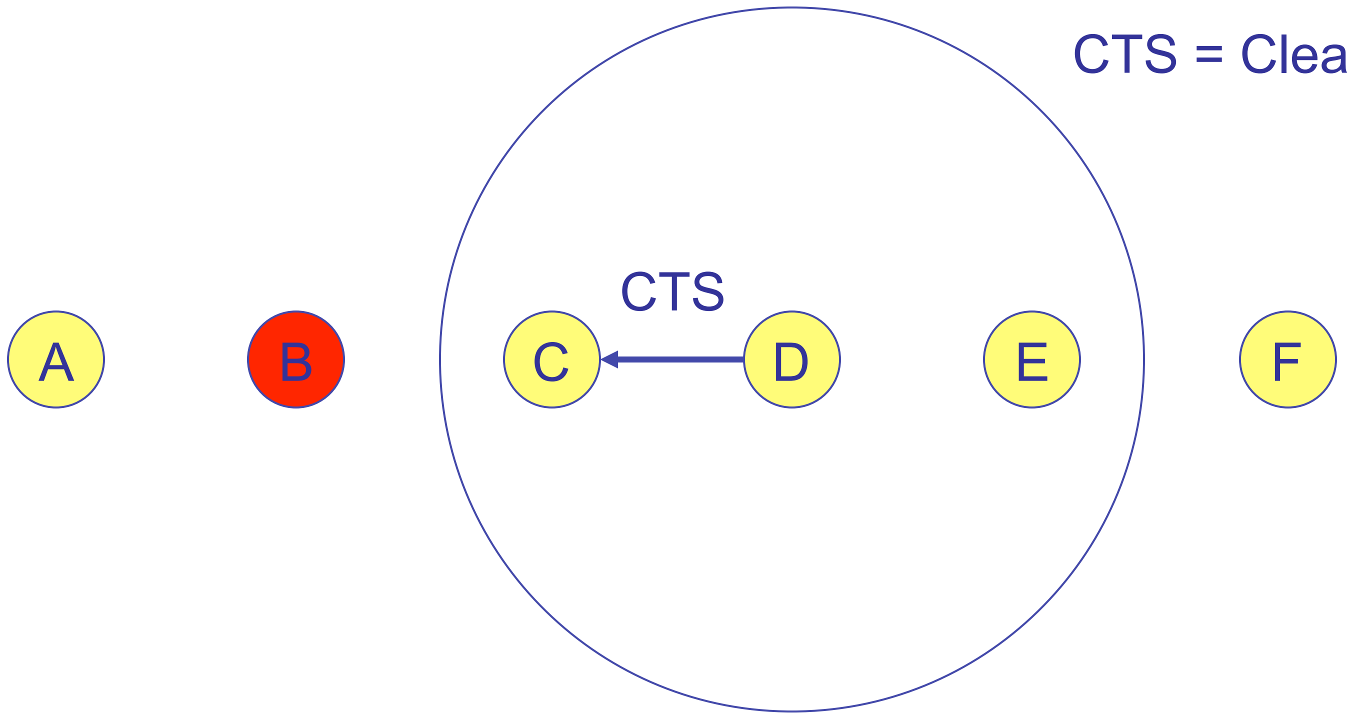


RTS = Request-to-Send

NAV = remaining duration to keep quiet

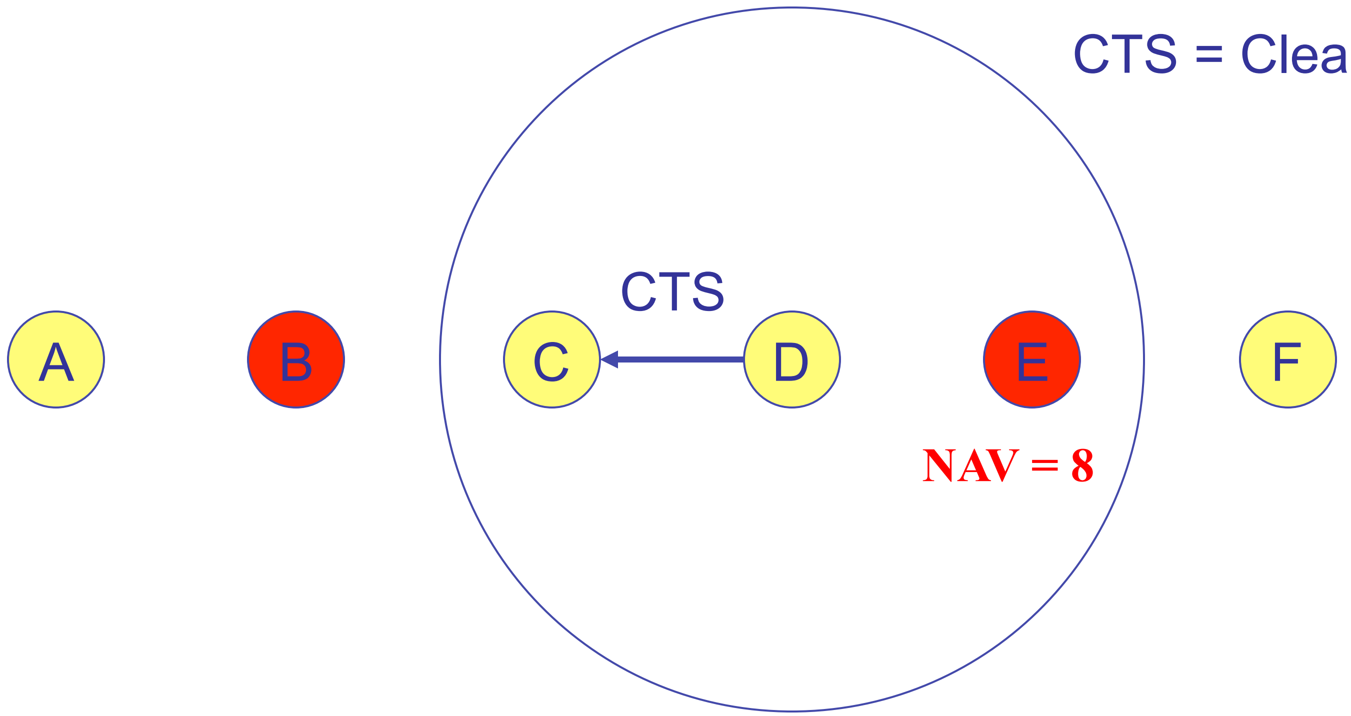
IEEE 802.11

CTS = Clear-to-Send



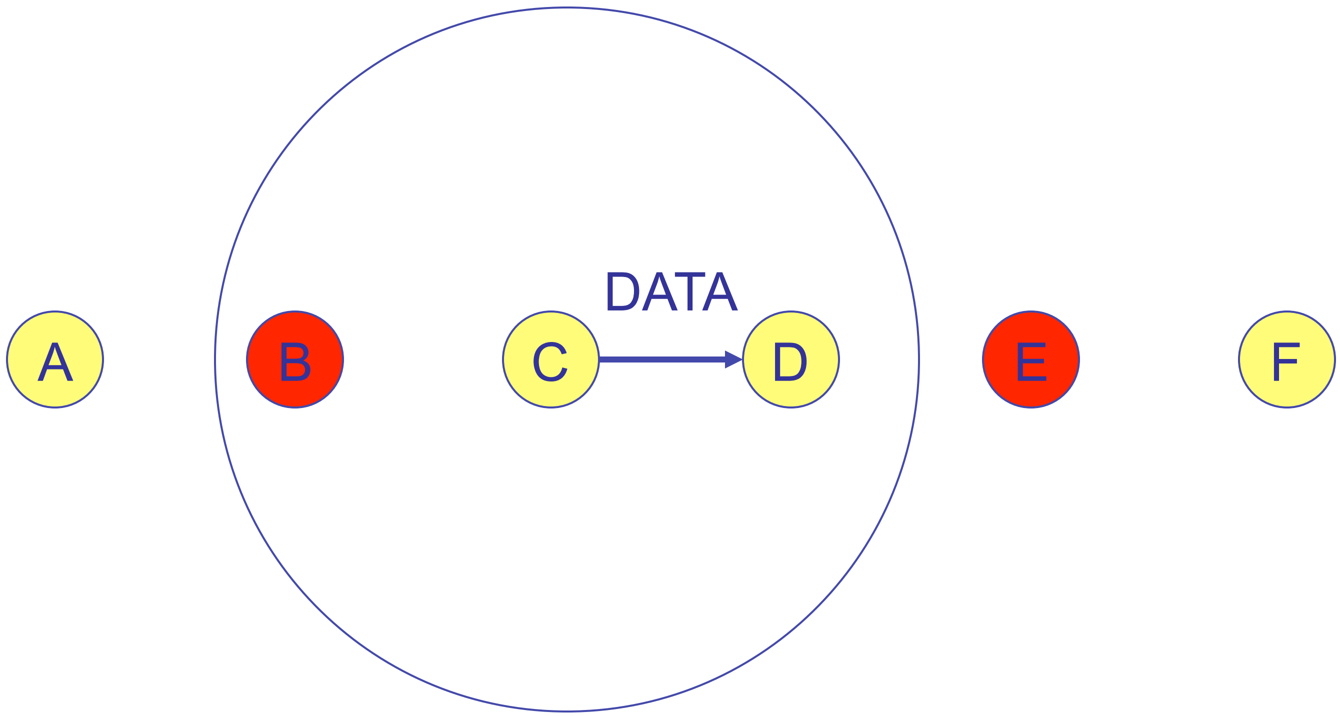
IEEE 802.11

CTS = Clear-to-Send

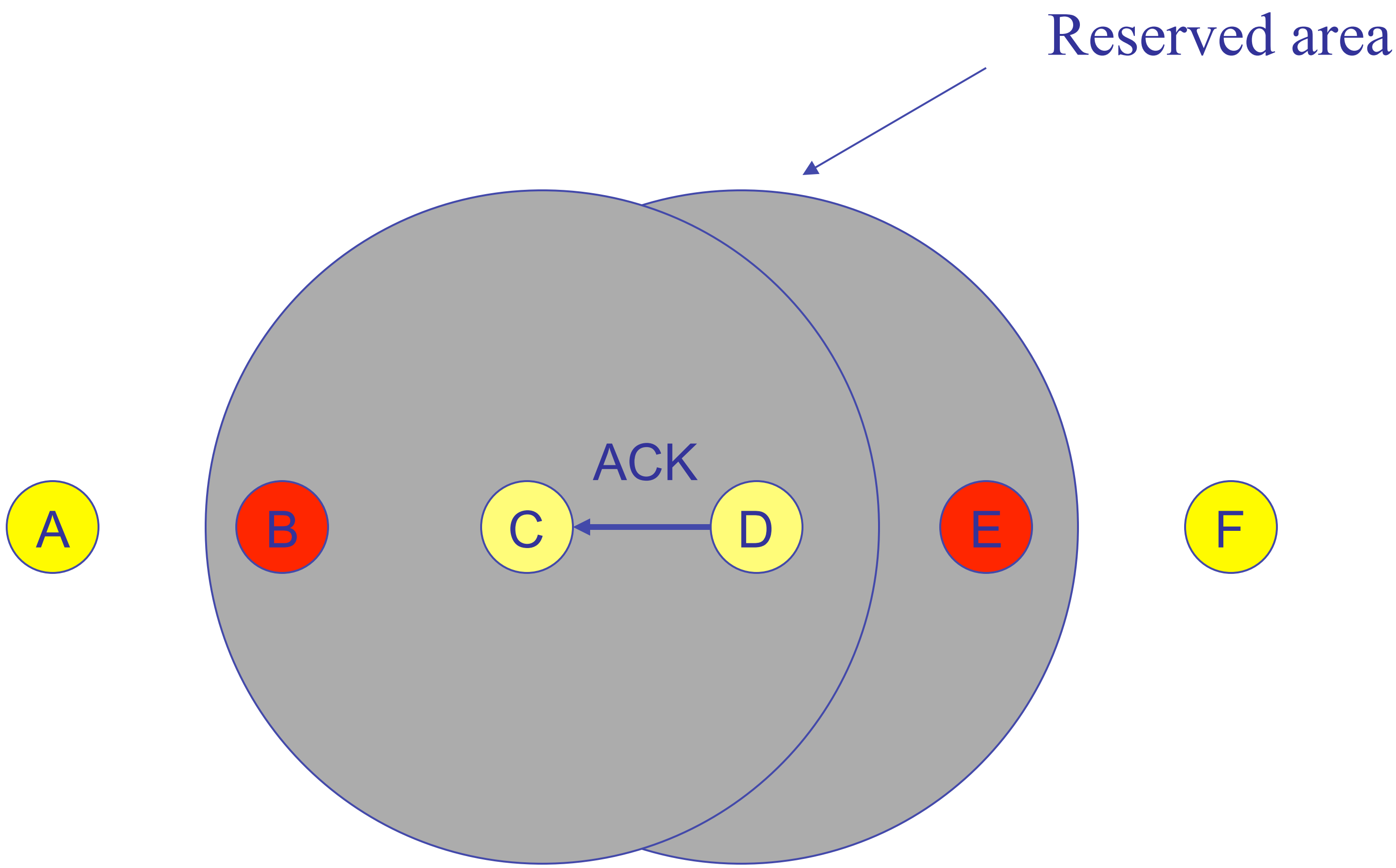


IEEE 802.11

- DATA packet follows CTS. Successful data reception acknowledged using ACK.



IEEE 802.11



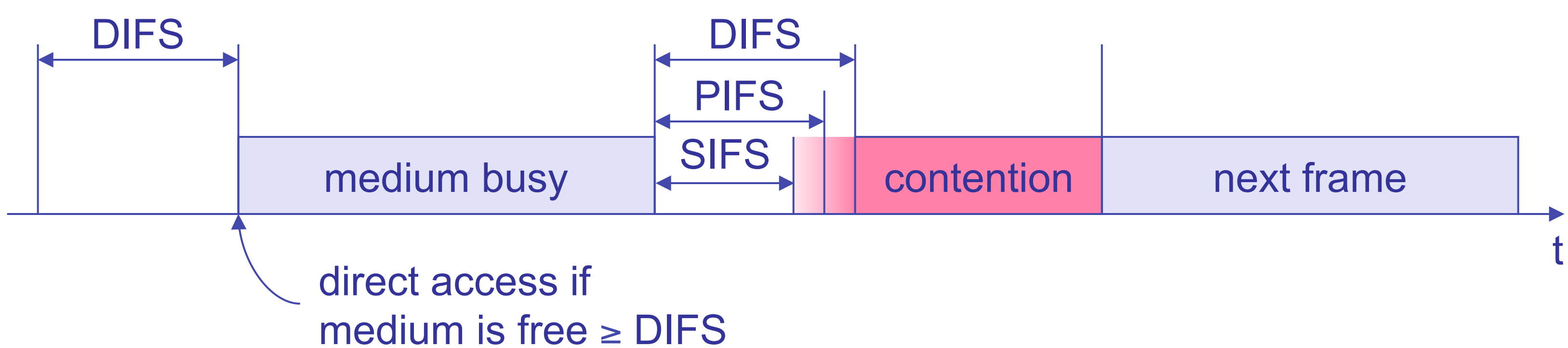
Binary Exponential Backoff in DCF

- When a node fails to receive CTS in response to its RTS, it increases the contention window
  - CW is doubled (up to an upper bound)
  - More collisions ➔ longer waiting time to reduce collision

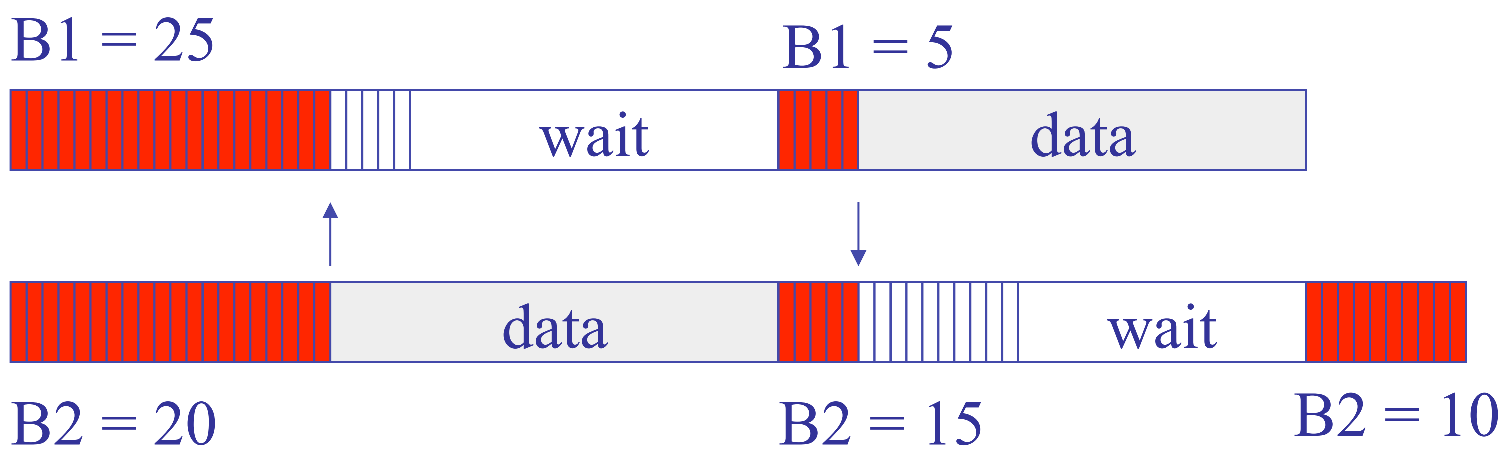
- When a node successfully completes a data transfer, it restores CW to CW_{min}

802.11 Backoffs

- SIFS (Short Inter Frame Spacing)
  - highest priority, for ACK, CTS, polling response
- PIFS (PCF IFS)
  - medium priority, for time-bounded service using PCF
- DIFS (DCF, Distributed Coordination Function IFS)
  - lowest priority, for asynchronous data service



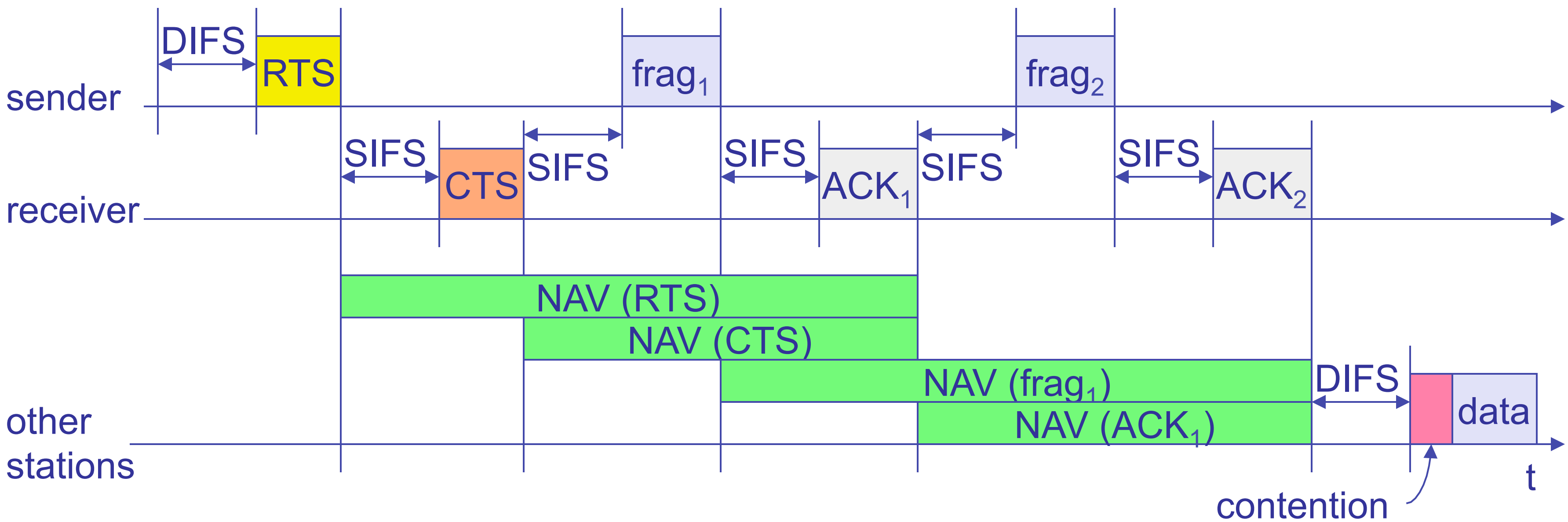
DCF Example



cw = 31

B1 and B2 are backoff intervals
at nodes 1 and 2

Fragmentation



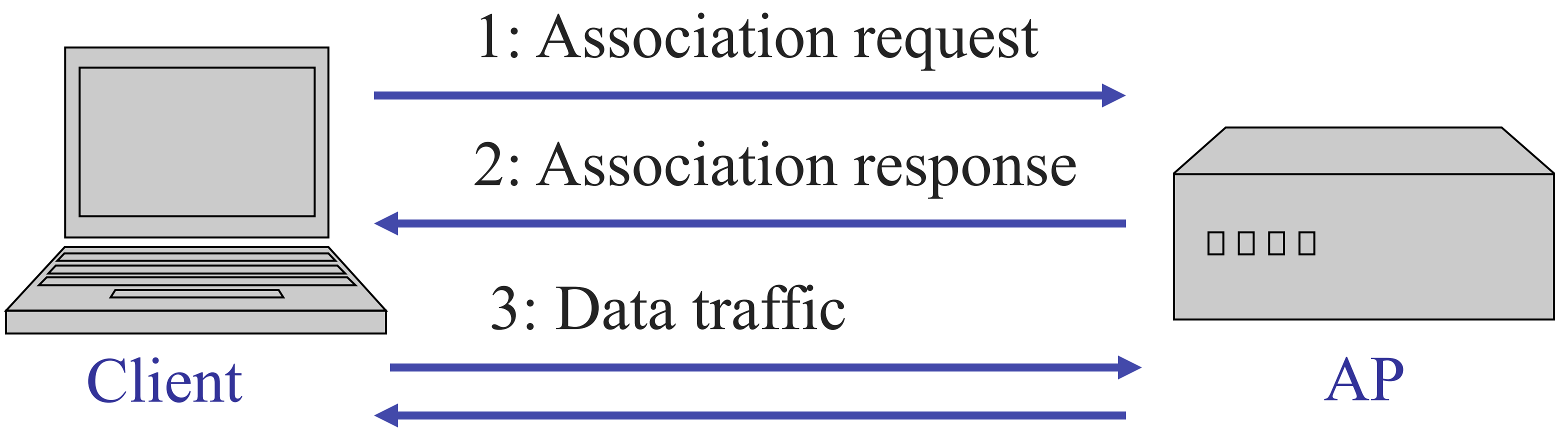
802.11 - MAC management

- Association/Reassociation
  - integration into a LAN
  - roaming, i.e. change networks by changing access points
  - scanning, i.e. active search for a network
- Power management
  - sleep-mode without missing a message
  - periodic sleep, frame buffering, traffic measurements

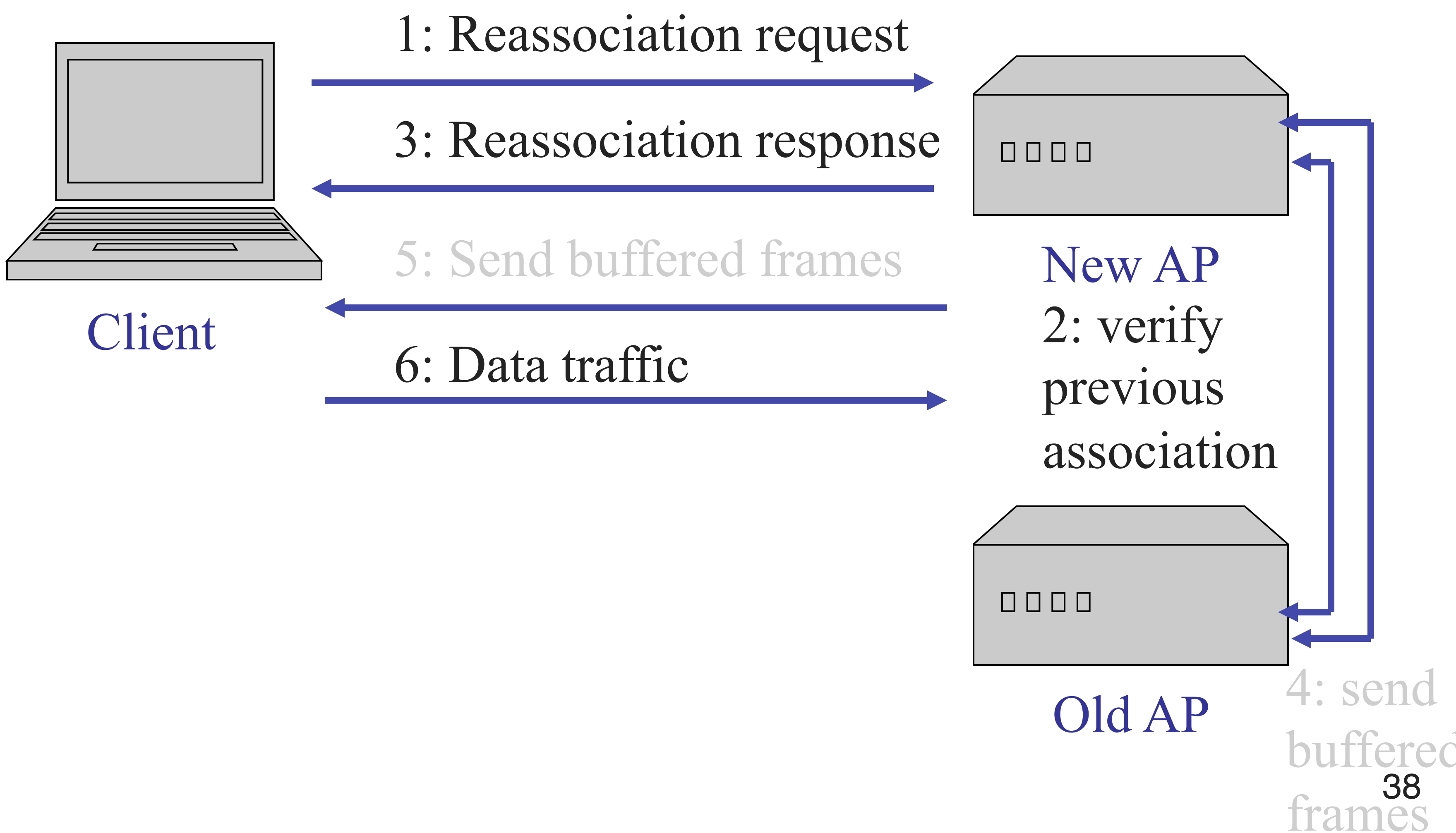
Scanning

- Goal: Find a network to connect
- Passive scanning
  - Not require transmission
  - Move to each channel, and listen for Beacon frames
- Active scanning
  - Require transmission
  - Move to each channel, and send Probe Request frames to solicit Probe Responses from a network

Association in 802.11



Reassociation in 802.11



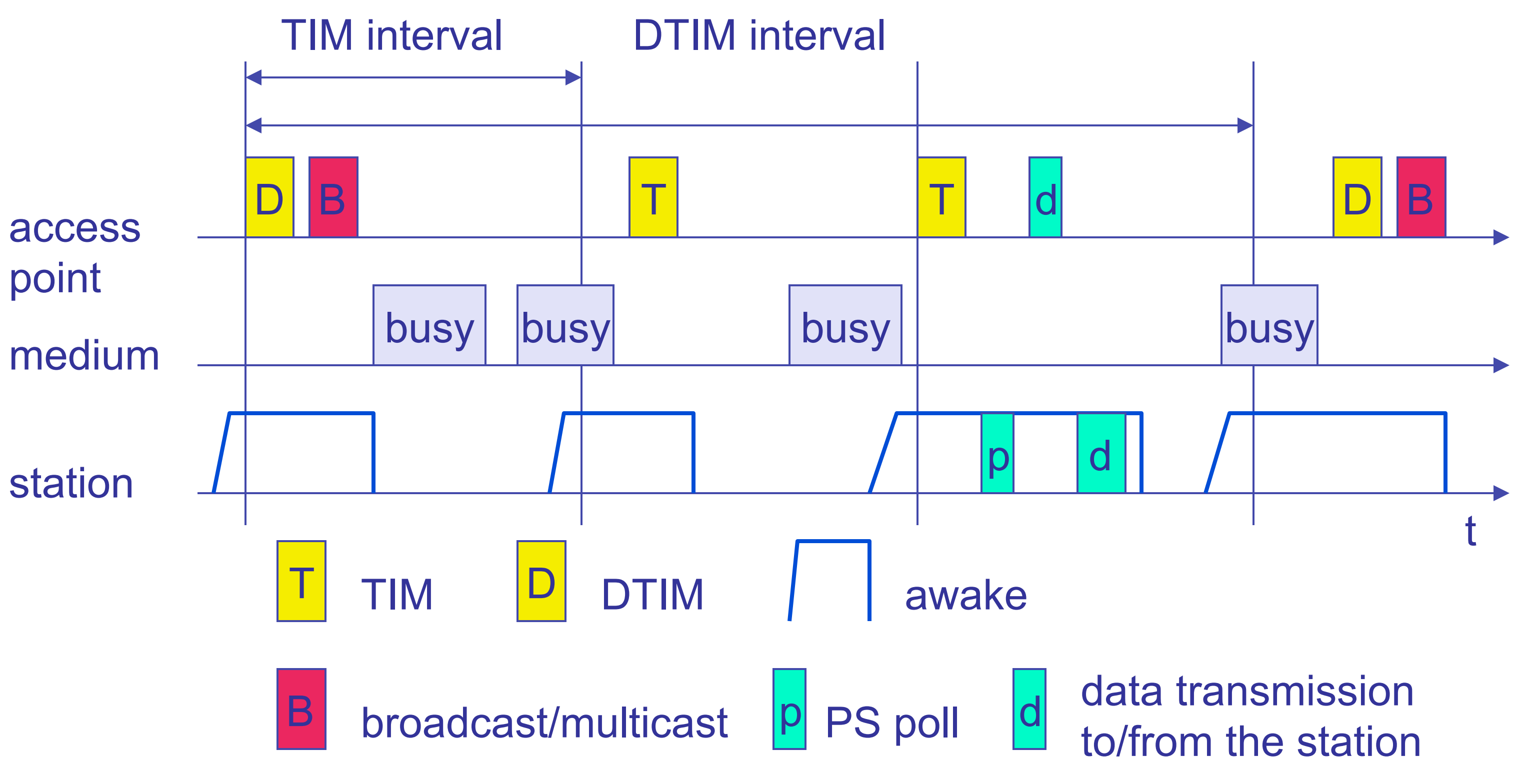
802.11 - Roaming

- No or bad connection? Then perform:
- Scanning
  - scan the environment, i.e., listen into the medium for beacon signals or send probes into the medium and wait for an answer
- Reassociation Request
  - station sends a request to one or several AP(s)
- Reassociation Response
  - success: AP has answered, station can now participate
  - failure: continue scanning
- AP accepts Reassociation 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

Power management

- Idea: switch the transceiver off if not needed
- States of a station: sleep and awake
- Timing Synchronization Function (TSF)
  - stations wake up at the same time
- Infrastructure
  - Traffic Indication Map (TIM)
    - » list of unicast receivers transmitted by AP
  - Delivery Traffic Indication Map (DTIM)
    - » list of broadcast/multicast receivers transmitted by AP

802.11 PSM


TIM interval
DTIM interval
access point
medium
station
D
B
T
T
d
D
B
busy
busy
busy
busy
p
d
t
T
TIM
D
DTIM
awake
B
broadcast/multicast
p
PS poll
d
data transmission to/from the station