# Paper Reading Assignment II

(Due on October 1st)

- Tramarin, Federico, Aloysius K. Mok, and Song Han. "Real-Time and Reliable Industrial Control Over Wireless LANs: Algorithms, Protocols, and Future Directions." Proceedings of the IEEE 107, no. 6 (2019): 1027-1052.
- https://ieeexplore.ieee.org/abstract/document/8718787
- Bianchi, Giuseppe. "Performance analysis of the IEEE 802.11 distributed coordination function." IEEE Journal on selected areas in communications 18, no. 3 (2000): 535-547.
- http://ieeexplore.ieee.org/document/840210/?arnumber=840210&tag=1

# Introduction to IEEE 802.11

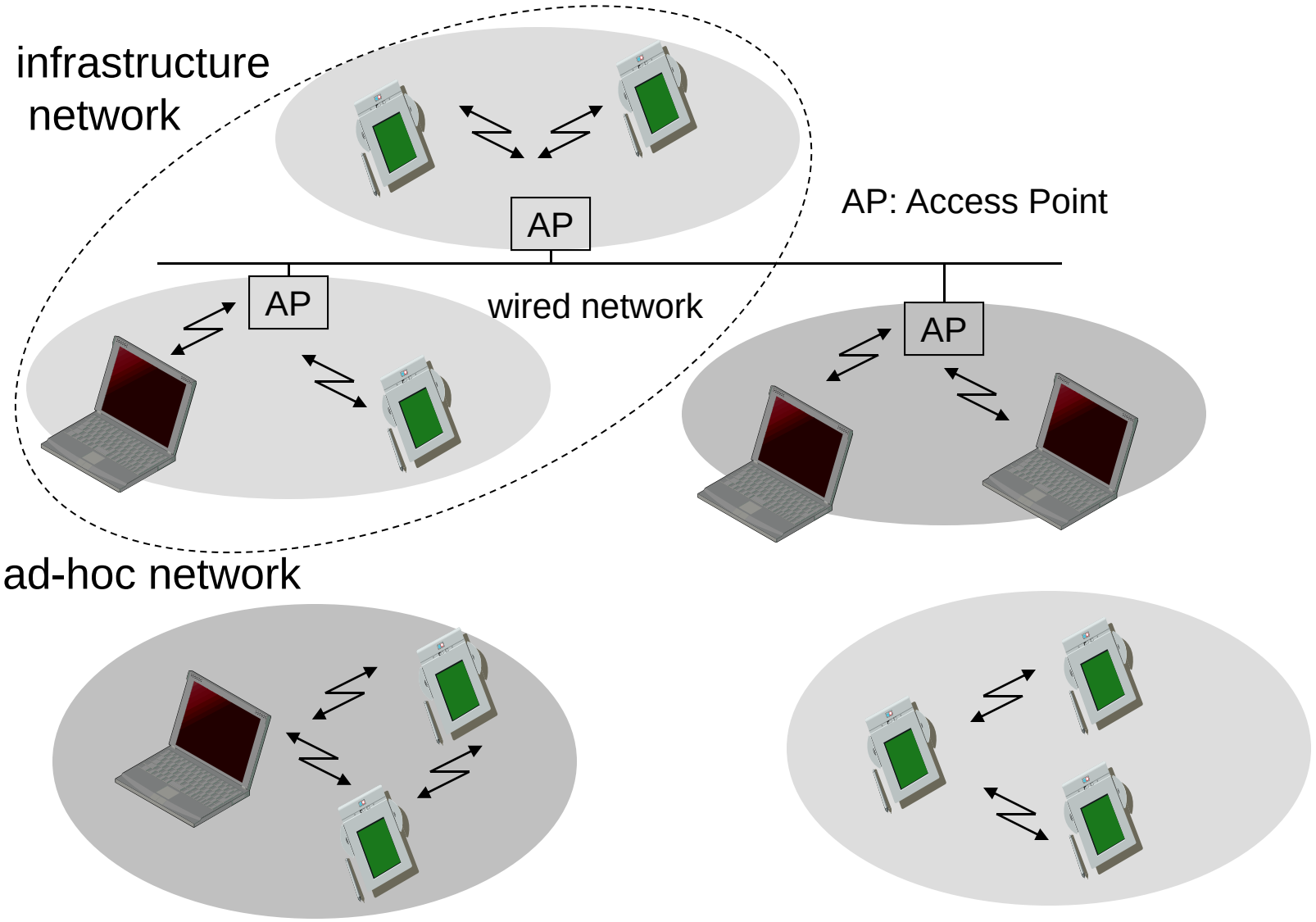
# Characteristics of wireless LANs

- Advantages
  - very flexible within the reception area
  - Ad-hoc networks without previous planning possible
  - (almost) no wiring difficulties
  - more robust against disasters
    - e.g., earthquakes, fire - or users pulling a plug...
- Disadvantages
  - typically low bandwidth compared to wired networks due to shared medium
  - Less reliable

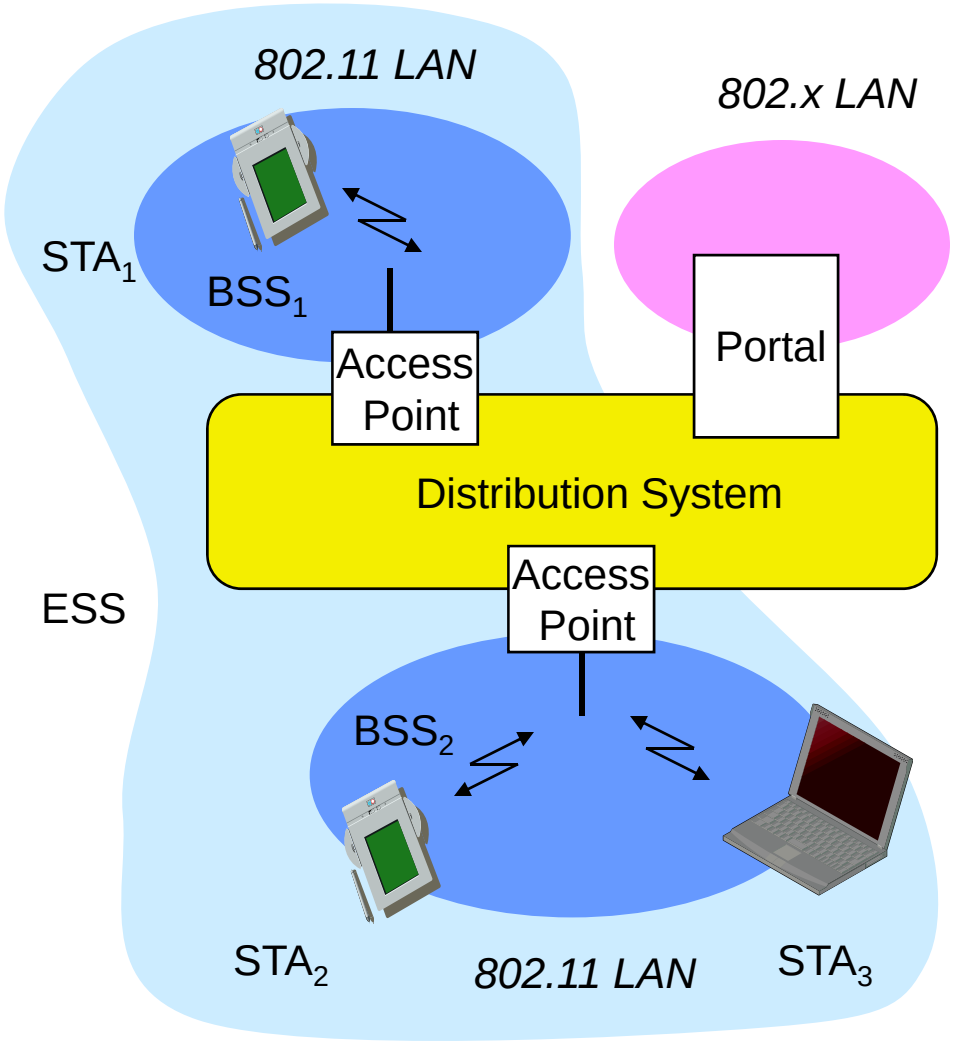
# Design Goals for Wireless LANs

- global, seamless operation
- low power for battery use
- no special licenses needed to use the LAN
- robust transmission technology
- easy to use for everyone, simple management
- security, privacy, safety
- transparent to applications and higher layer protocols
- location aware if necessary

# Infrastructure vs. ad-hoc networks

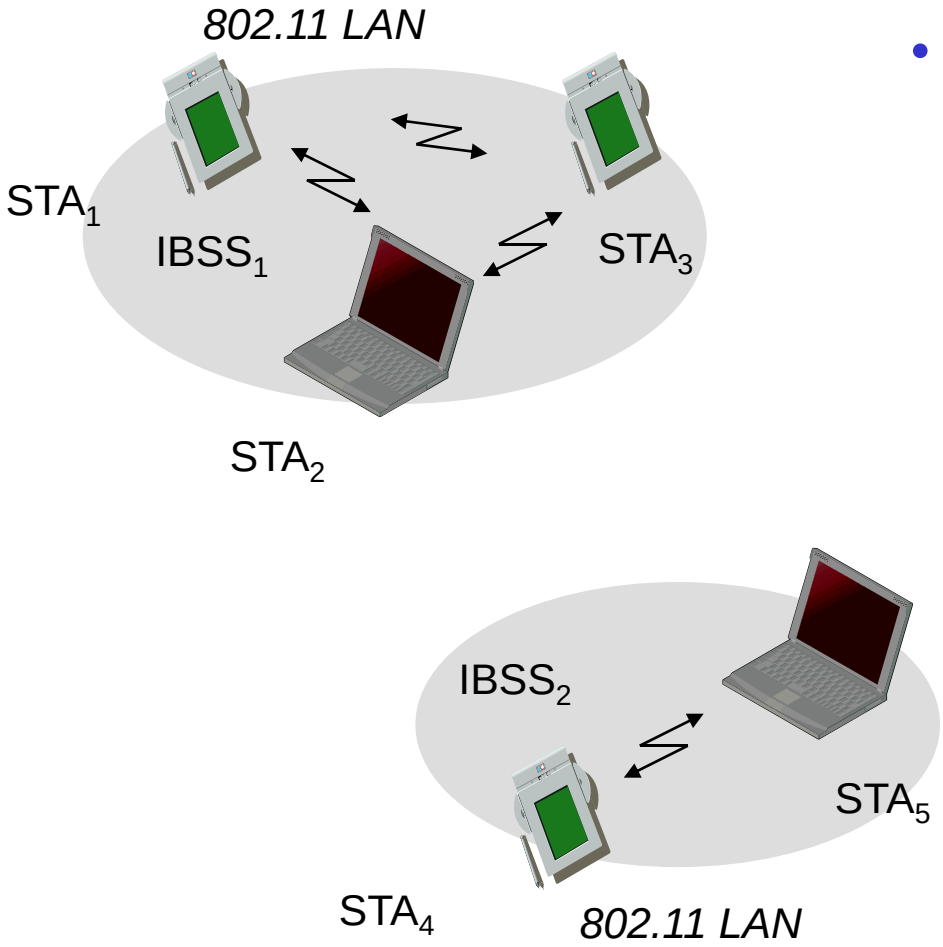


# 802.11: Infrastructure



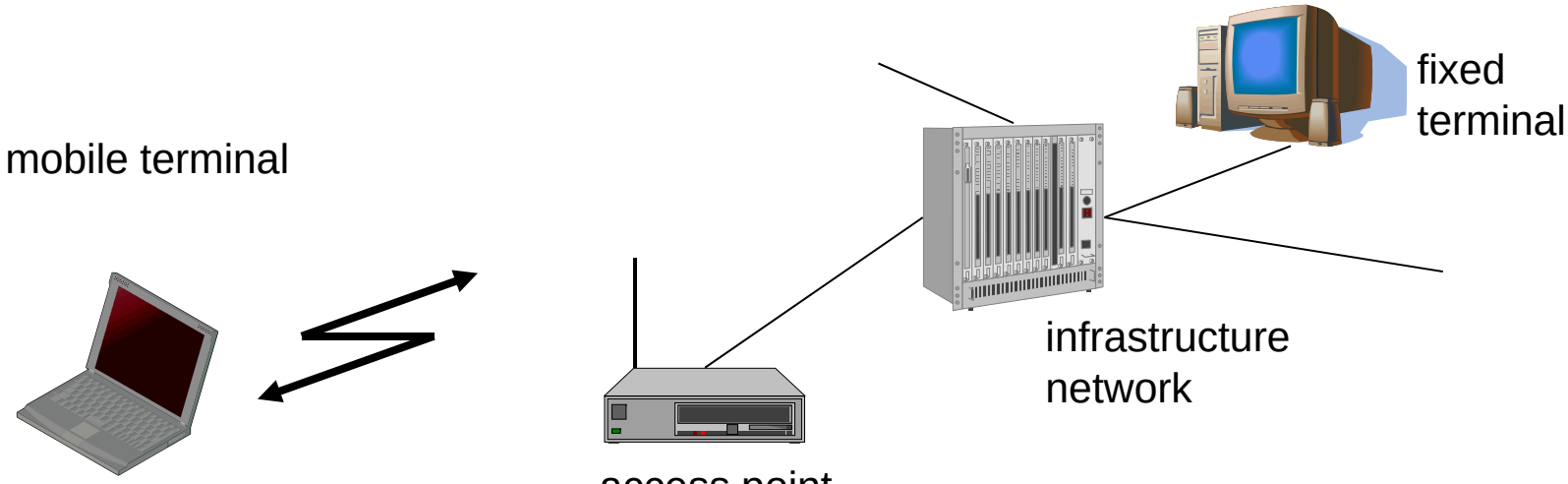

- Station (STA)
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- Access Point
  - station integrated into the wireless LAN and the distribution system
- Basic Service Set (BSS)
  - group of stations using the same AP
- Portal
  - bridge to other (wired)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

# 802.11: Ad hoc mode




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

# IEEE standard 802.11




| application | | | application |
|---|---|---|---|
| TCP | | | TCP |
| IP | | | IP |
| LLC | LLC | | LLC |
| 802.11 MAC | 802.11 MAC | 802.3 MAC | 802.3 MAC |
| 802.11 PHY | 802.11 PHY | 802.3 PHY | 802.3 PHY |

# Outline

- Introduction to MAC
- Introduction to IEEE 802.11
- 802.11 Physical layer
- 802.11 MAC layer
- 802.11 Management

# WLAN: IEEE 802.11b

- Data rate
  - 1, 2, 5.5, 11 Mbit/s, depending on SNR
  - 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
- Availability
  - Many products and vendors
- Quality of Service
  - Best effort, no guarantees (unless polling is used, limited support in products)
- Pros
  - Many installed systems and vendors
  - Available worldwide
  - Free ISM-band
- Cons
  - Heavy interference on ISM-band
  - No service guarantees
  - Relatively low data rate

# WLAN: IEEE 802.11a

- Data rate
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, depending on SNR
  - User throughput (1500 byte packets): 5.3 (6), 18 (24), 24 (36), 32 (54)
  - 6, 12, 24 Mbit/s mandatory
- Transmission range
  - 100m outdoor, 10m indoor
    - E.g., 54 Mbit/s up to 5 m, 48 up to 12 m, 36 up to 25 m, 24 up to 30m, 18 up to 40 m, 12 up to 60 m
- Frequency
  - Free 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz ISM-band
- Availability
  - Some products, some vendors
- Quality of Service
  - Best effort, no guarantees (same as all 802.11 products)
- Pros
  - Fits into 802.x standards
  - Free ISM-band
  - Available, simple system
  - Uses less crowded 5 GHz band
  - Higher data rates
- Cons
  - Shorter range

**Table 1** Roadmap of the Major IEEE 802.11 Standard Developments

| Protocol | | PHY Name | Max. Rate [Mbit/s] | Channel bandwidth [MHz] | Band [GHz] | Name |
|---|---|---|---|---|---|---|
| 802.11 | 1997 | DSSS | 2 | 22 | 2.4 | *(Wi–Fi 1)* |
| 802.11b | 1999 | HR/DSSS | 11 | 22 | 2.4 | *(Wi–Fi 2)* |
| 802.11a | 1999 | OFDM | 54 | 20 | 5 | — |
| 802.11g | 2003 | ERP-OFDM | 54 | 20 | 2.4 | *(Wi–Fi 3)* |
| 802.11n | 2009 | HT-MIMO | 600 | 20/40 | 2.4/5 | **Wi–Fi 4** |
| 802.11ac | 2013 | VHT-MIMO | 3466.8 | 20/40/80/160 | 5 | **Wi–Fi 5** |
| 802.11ax | 2019 | HE-OFDM | 10530 | 20/40 @2.4GHz<br>20/40/80/160 @5GHz | 2.4/5 | **Wi–Fi 6** |

# Other IEEE 802.11 developments

- 802.11i: Enhanced Security Mechanisms
  - Enhance the current 802.11 MAC to provide improvements in security.
  - TKIP enhances the insecure WEP, but remains compatible to older WEP systems
  - AES provides a secure encryption method and is based on new hardware
- 802.11j: Extensions for operations in Japan
  - Changes of 802.11a for operation at 5GHz in Japan using only half the channel width at larger range
- 802.11k: Methods for channel measurements
  - Devices and access points should be able to estimate channel quality in order to be able to choose a better access point of channel
- 802.11m: Updates of the 802.11 standards
- 802.11n: Higher data rates 600Mbit/s
  - Changes of PHY and MAC with the goal of 100Mbit/s at MAC SAP
  - MIMO antennas (Multiple Input Multiple Output), up to 600Mbit/s are currently feasible
  - However, still a large overhead due to protocol headers and inefficient mechanisms
- 802.11p: Inter car communications
  - Communication between cars/road side and cars/cars
  - Planned for relative speeds of min. 200km/h and ranges over 1000m
  - Usage of 5.850-5.925GHz band in North America

# Other IEEE 802.11 developments

- 802.11c: Bridge Support
  - Definition of MAC procedures to support bridges as extension to 802.1D
- 802.11d: Regulatory Domain Update
  - Support of additional regulations related to channel selection, hopping sequences
- 802.11e: MAC Enhancements – QoS
  - Enhance the current 802.11 MAC to expand support for applications with Quality of Service requirements, and in the capabilities and efficiency of the protocol
  - Definition of a data flow ("connection") with parameters like rate, burst, period…
  - Additional energy saving mechanisms and more efficient retransmission
- 802.11f: Inter-Access Point Protocol
  - Establish an Inter-Access Point Protocol for data exchange via the distribution system
  - Currently unclear to which extend manufacturers will follow this suggestion
- 802.11h: Spectrum Managed 802.11a
  - Extension for operation of 802.11a in Europe by mechanisms like channel measurement for dynamic channel selection (DFS, Dynamic Frequency Selection) and power control (TPC, Transmit Power Control)

# Other IEEE 802.11 developments

- 802.11r: Faster Handover between BSS
  - Secure, fast handover of a station from one AP to another within an ESS
  - Current mechanisms (even newer standards like 802.11i) plus incompatible devices from different vendors are massive problems for the use of, e.g., VoIP in WLANs
  - Handover should be feasible within 50ms in order to support multimedia applications efficiently
- 802.11s: Mesh Networking
  - Design of a self-configuring Wireless Distribution System (WDS) based on 802.11
  - Support of point-to-point and broadcast communication across several hops
- 802.11t: Performance evaluation of 802.11 networks
  - Standardization of performance measurement schemes
- 802.11u: Interworking with additional external networks
- 802.11v: Network management
  - Extensions of current management functions, channel measurements
  - Definition of a unified interface
- 802.11w: Securing of network control
  - Classical standards like 802.11, but also 802.11i protect only data frames, not the control frames. Thus, this standard should extend 802.11i in a way that, e.g., no control frames can be forged.

- Note: Not all "standards" will end in products, many ideas get stuck at working group
- Info: www.ieee802.org/11/, 802wirelessworld.com, standards.ieee.org/getieee802/

# Outline

- Introduction to MAC
- Introduction to IEEE 802.11
- 802.11 Physical layer
- 802.11 MAC layer
- 802.11 Management

# IEEE 802.11 Wireless MAC

- Distributed and centralized MAC components
  - Centralized – Point Coordination Function (PCF)
    - In infrastructure mode
    - Contention-free access protocol with a controller (AP) called a point coordinator within the BSS
  - Distributed – Distributed Coordination Function (DCF)
    - In ad-hoc mode
    - DCF is a Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol (distributed contention based protocol)
- Both the DCF and PCF can operate concurrently within the same BSS to provide alternative contention and contention-free periods

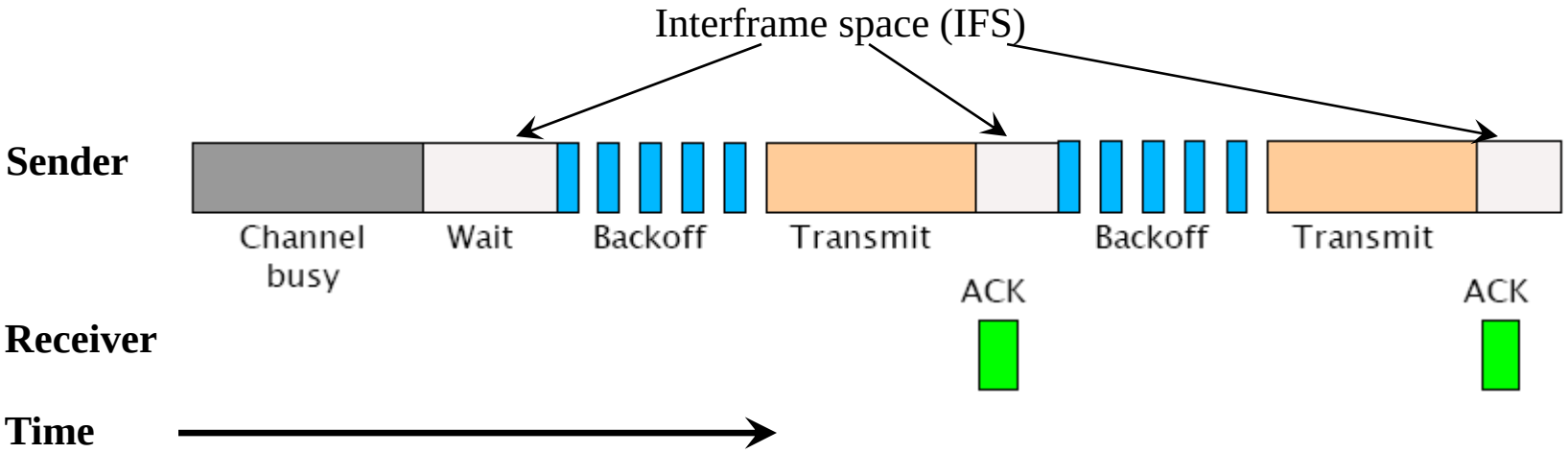
# PCF in 802.11 MAC

- Its objective is to provide QoS guarantees
  - E.g. bound the max access delay, bound the minimum guaranteed txmt rate
- Centralized MAC – infrastructure mode
- Key idea
  - The AP polls the nodes in its BSS
  - A PC (point coordinator) at the AP splits the access time into super frame periods
  - A super frame period consists of alternating contention free periods (CFPs) and contention periods (CPs)
  - The PC then determines which station transmits at any point in time

# DCF in 802.11 MAC

- The AP doesn't control the medium access
- Use *collision avoidance* techniques, in conjunction with a (physical or virtual) *carrier sense* mechanism
- Carrier sense:
  - When a node wishes to transmit a packet, it first waits until the channel is idle
- Collision avoidance:
  - Once channel becomes idle, the node waits for a randomly chosen duration before attempting to transmit
  - Nodes hearing RTS or CTS stay silent for the duration of the corresponding transmission

# DCF Illustration




- Before a node transmits, it listens for activity on the network
- If medium is busy, node waits to transmit
- After medium is clear, don't immediately start transmitting...
- *Otherwise all nodes would start talking at the same time!*
- Instead, delay a random amount of time (*random backoff*)

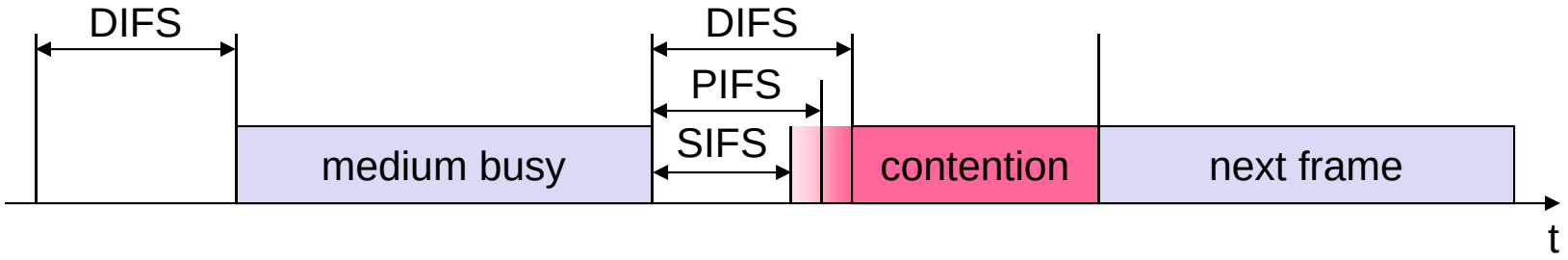
# 802.11 MAC Layer

- Distributed and centralized access methods
  - DCF CSMA/CA (mandatory)
    - collision avoidance via randomized "back-off" mechanism
    - minimum distance between consecutive packets
    - ACK packet for acknowledgements (not for broadcasts)
  - DCF w/ RTS/CTS (optional)
    - Distributed Foundation Wireless MAC
    - avoids hidden terminal problem
  - PCF (optional)
    - access point polls terminals according to a list

# How to prioritize frames?

# 802.11 - MAC layer II

- Priorities
  - defined through different inter frame spaces
  - no guarantee, hard priorities
  - 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



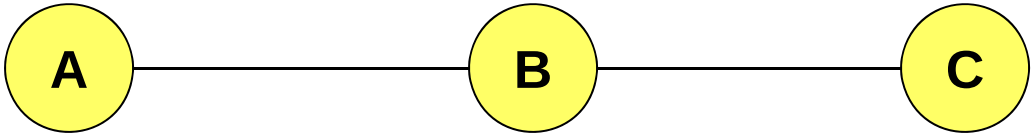
# IEEE 802.11 DCF

- DCF is *CSMA/CA* protocol
  - Why not CSMA/CD?
- 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

# CSMA/CA

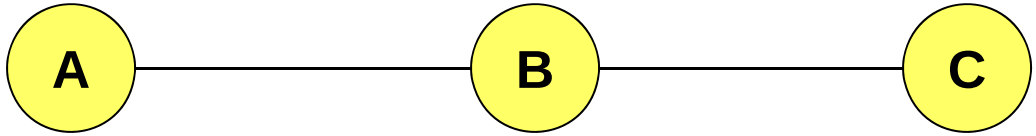
- Carrier sense
  - Nodes stay silent when carrier sensed (physical/virtual)
  - Physical carrier sense
    - Carrier sense threshold
  - Virtual carrier sense using Network Allocation Vector (NAV)
    - NAV is updated based on overheard RTS/CTS/DATA/ACK packets

# Hidden Terminal Problem



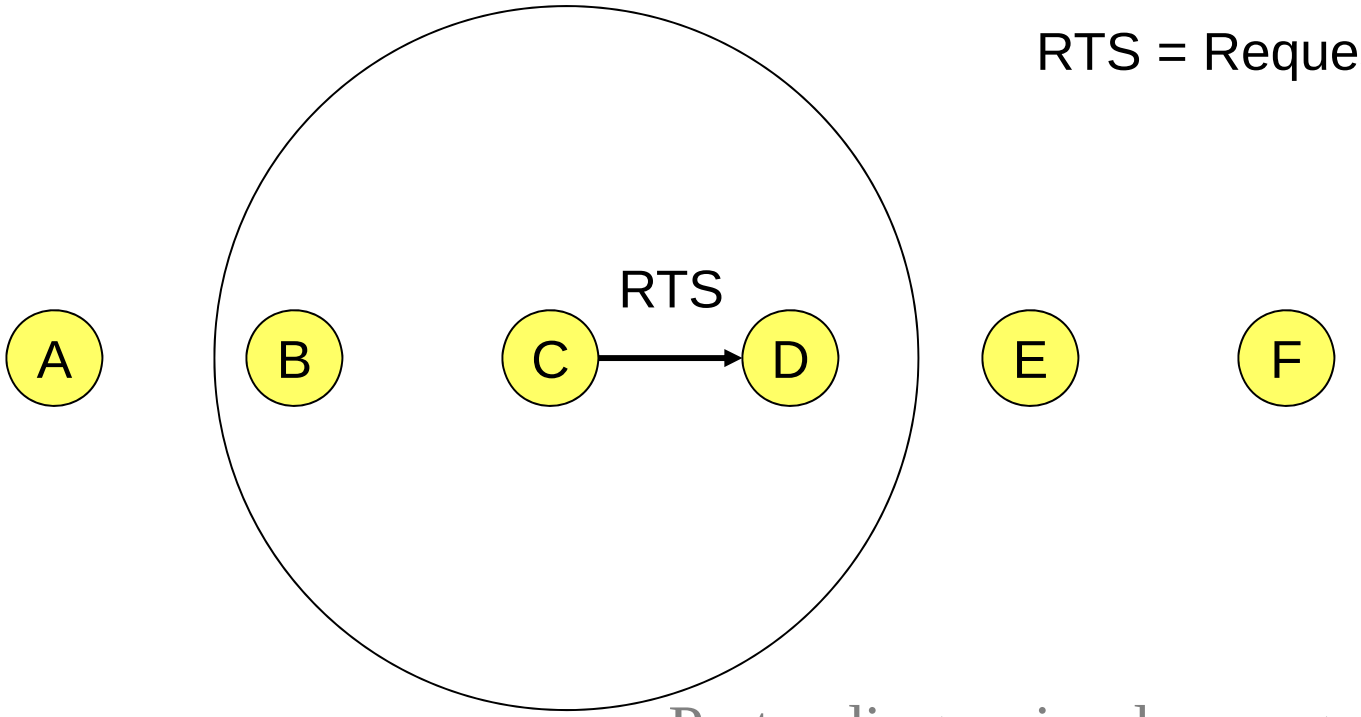

- B can communicate with both A and C
- A and C cannot hear each other
- Problem
  - When A transmits to B, C cannot detect the transmission using the carrier sense mechanism
  - If C transmits, collision will occur at node B
- Solution
  - Hidden sender C needs to defer

# Solution for Hidden Terminal Problem



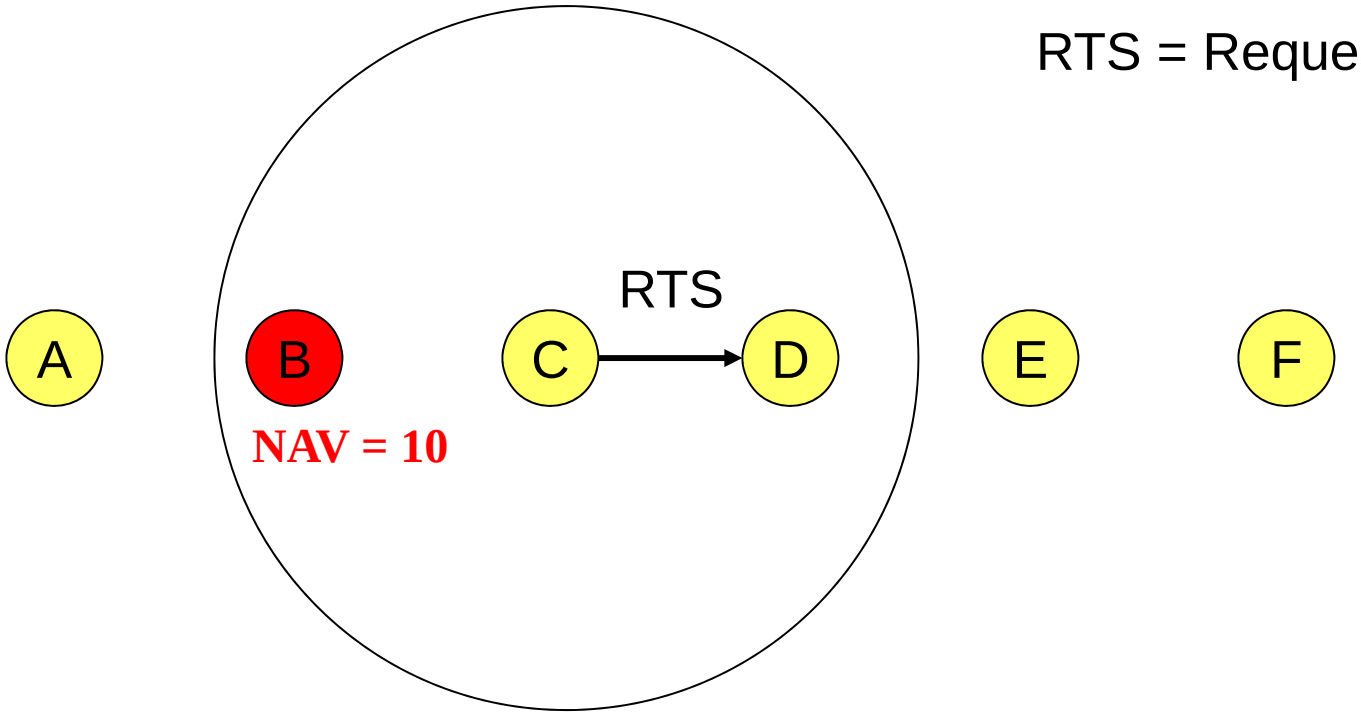

- When A wants to send a packet to B, A first sends a Request-to-Send (RTS) to B
- On receiving RTS, B responds by sending Clear-to-Send (CTS), provided that A is able to receive the packet
- When C overhears a CTS, it keeps quiet for the duration of the transfer
  - Transfer duration is included in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

# IEEE 802.11



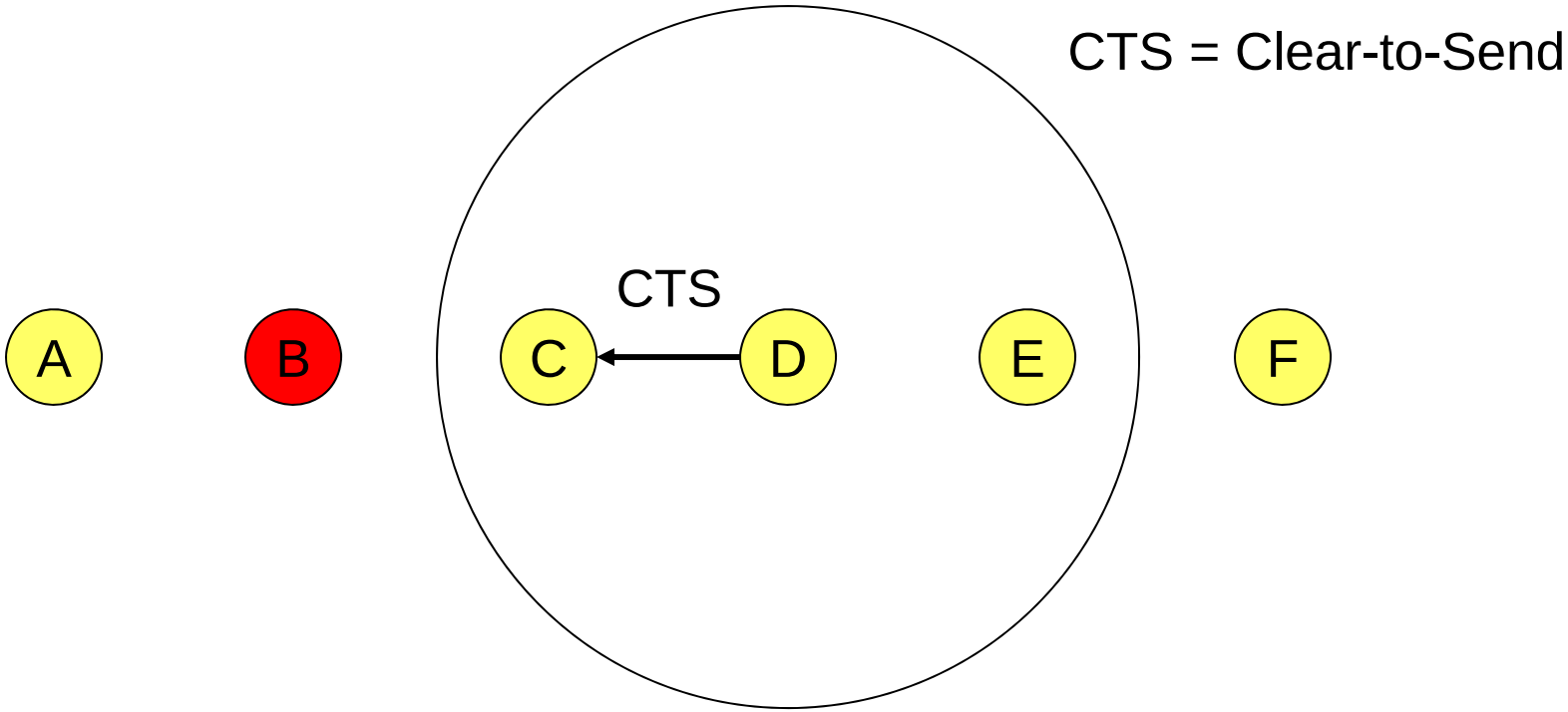

Pretending a circular range

# IEEE 802.11

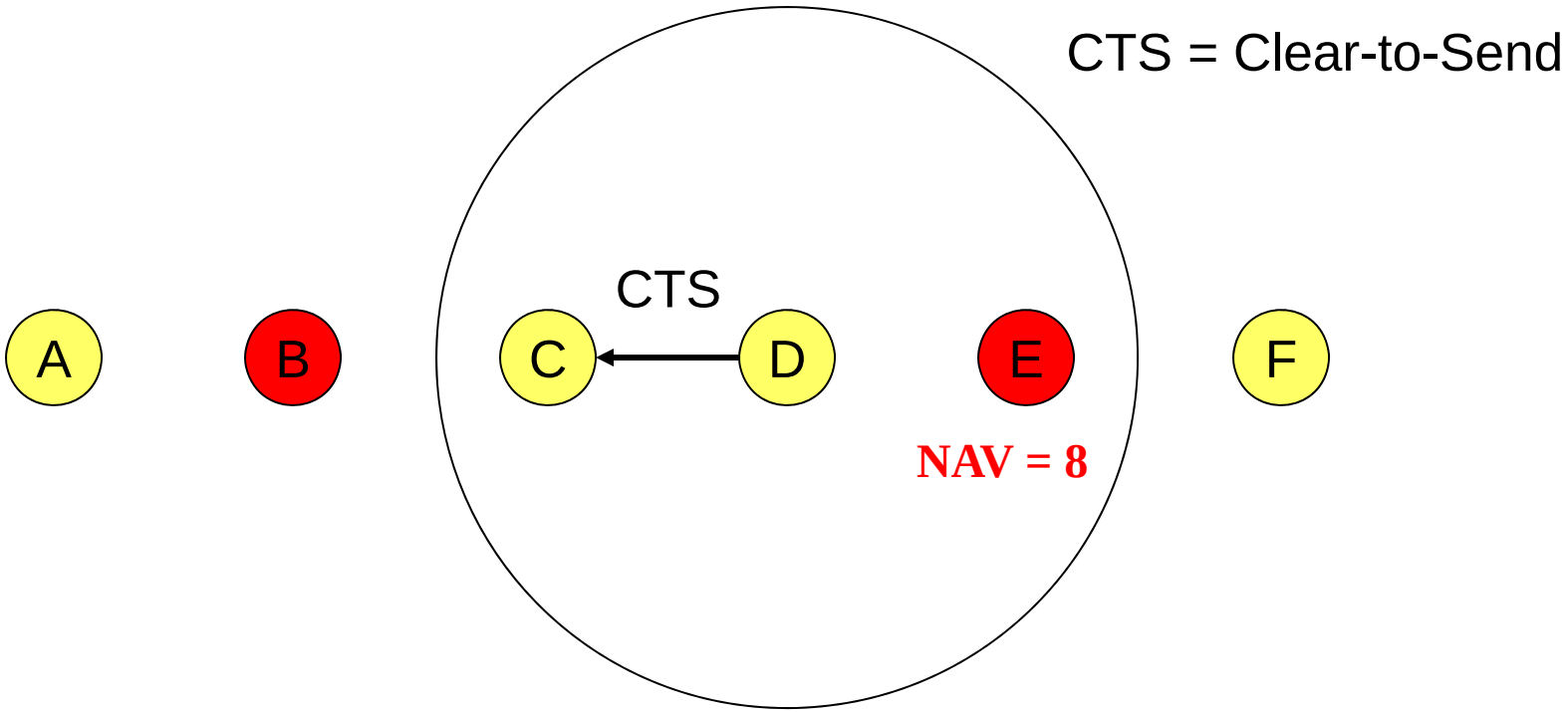



NAV = remaining duration to keep quiet

# IEEE 802.11

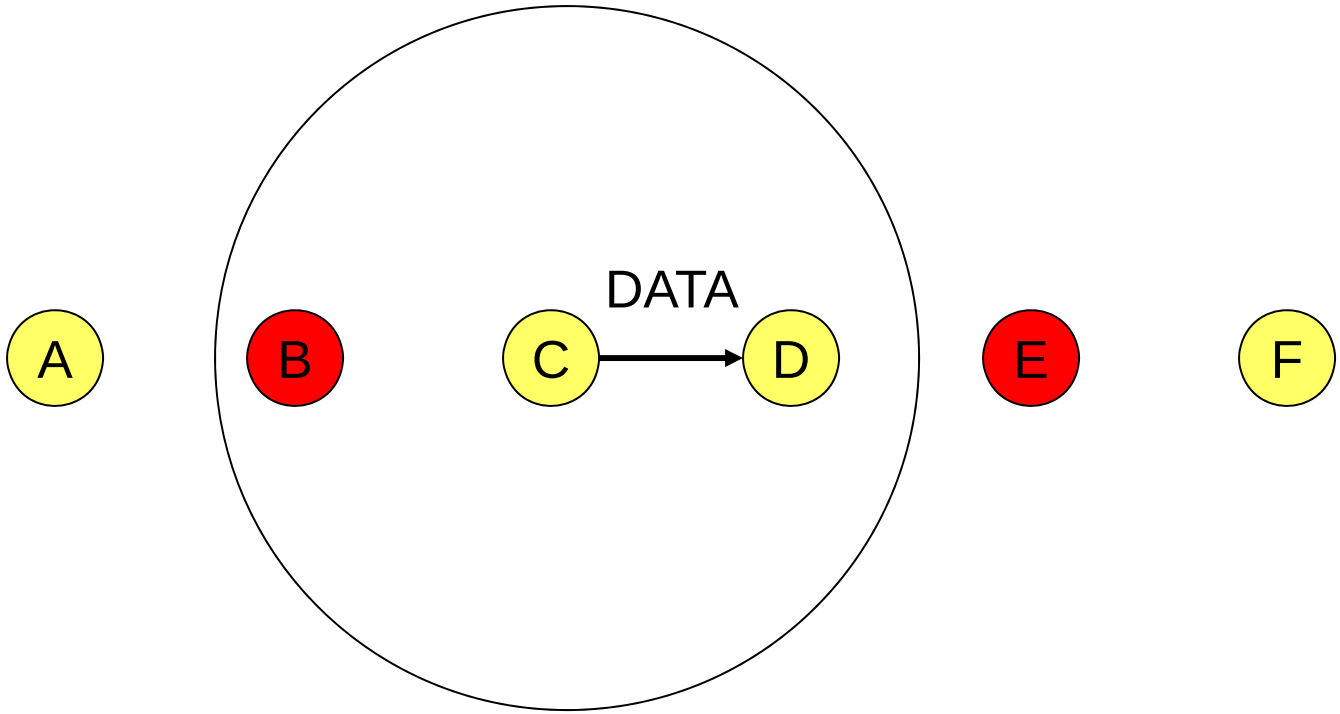


# IEEE 802.11

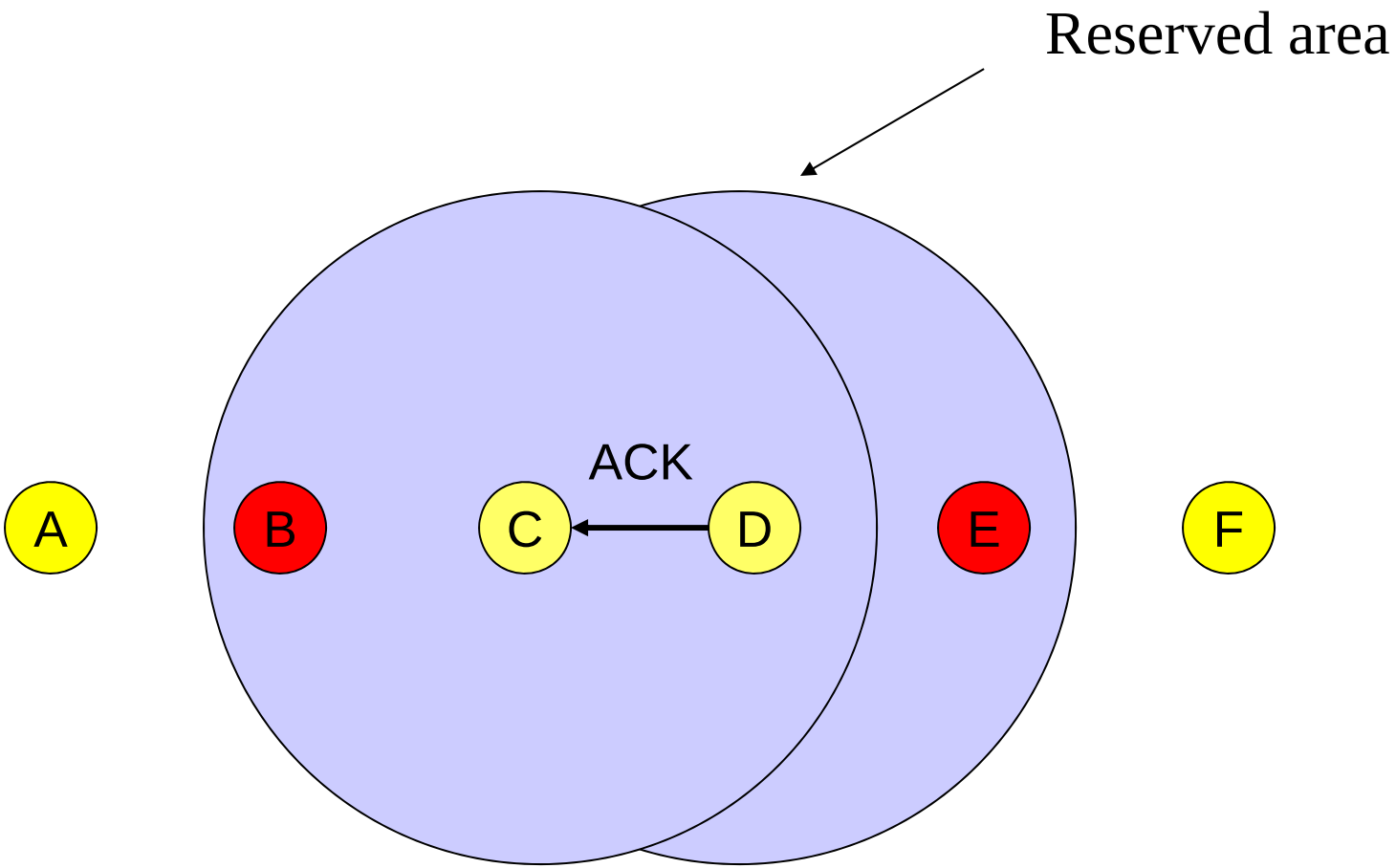


# IEEE 802.11

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



# IEEE 802.11



# Why do we need virtual carrier sense?

# Reliability

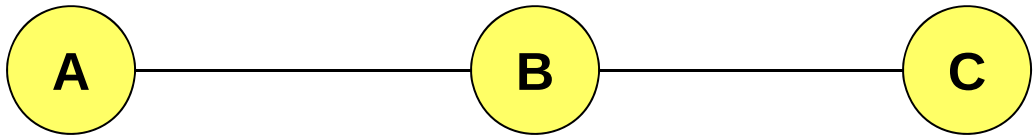
- Wireless links are prone to errors. High packet loss rate detrimental to transport-layer performance.

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

# A Simple Solution to Improve Reliability

- 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



Can RTS/CTS completely eliminate hidden terminals?

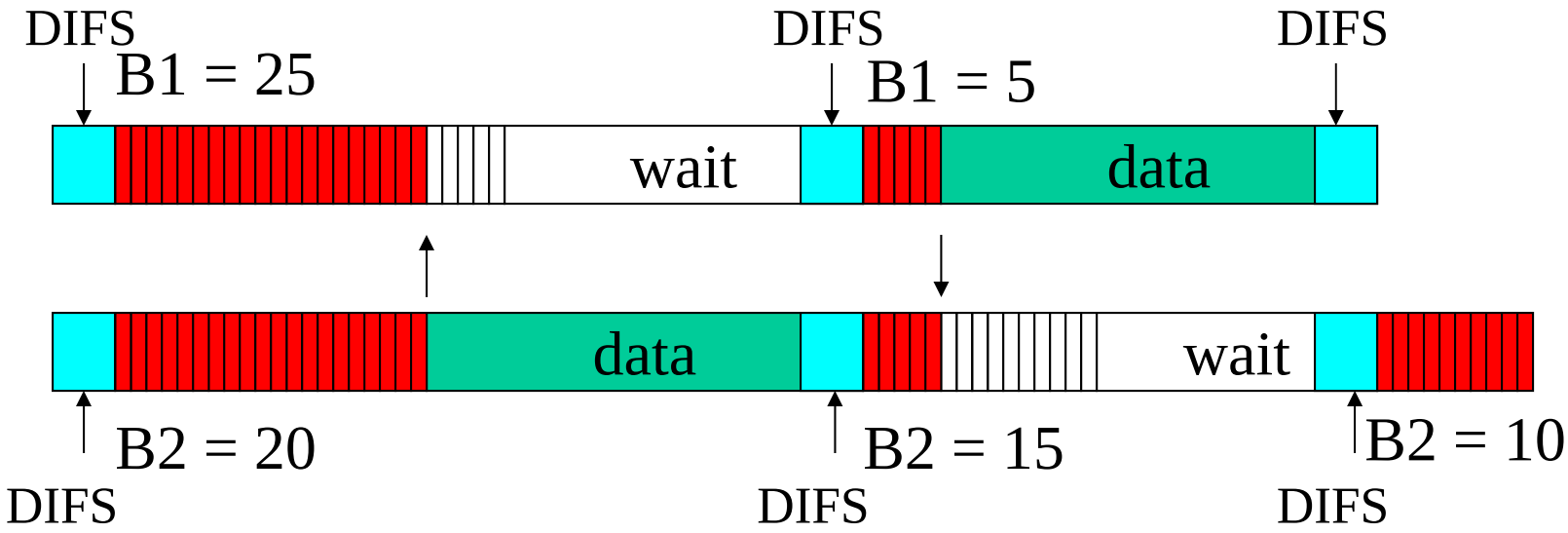
# Outline

- Introduction to MAC layer
- Introduction to IEEE 802.11
- 802.11 Physical layer
- 802.11 MAC layer
- 802.11 Management

# Backoff Interval

- Collision avoidance
  - Backoff intervals used to reduce collision probability
- 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
- Transmit when backoff interval reaches 0

# DCF Example




**cw = 31**

**B1 and B2 are backoff intervals at nodes 1 and 2**

# Backoff Interval

- The time spent counting down backoff intervals is a part of MAC overhead
- Important to choose CW appropriately
  - large CW → large overhead
  - small CW → may lead to many collisions (when two nodes count down to 0 simultaneously)
- How to choose an appropriate CW?

# Backoff Interval (Cont.)

- Since the number of nodes attempting to transmit simultaneously may change with time, some mechanism to manage contention is needed

- IEEE 802.11 DCF: contention window CW is chosen dynamically depending on collision occurrence

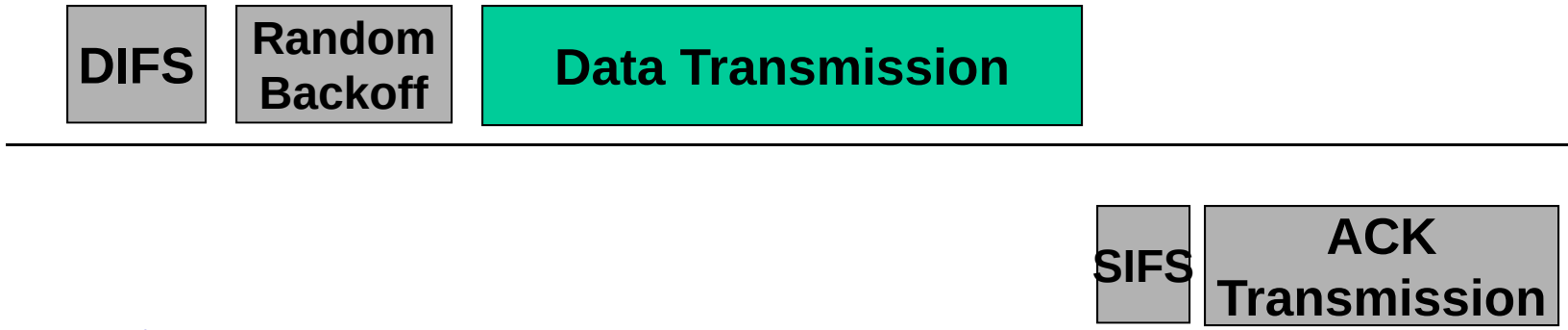
# Binary Exponential Backoff in DCF

- 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 $CW_{min}$

# MILD Algorithm in MACAW

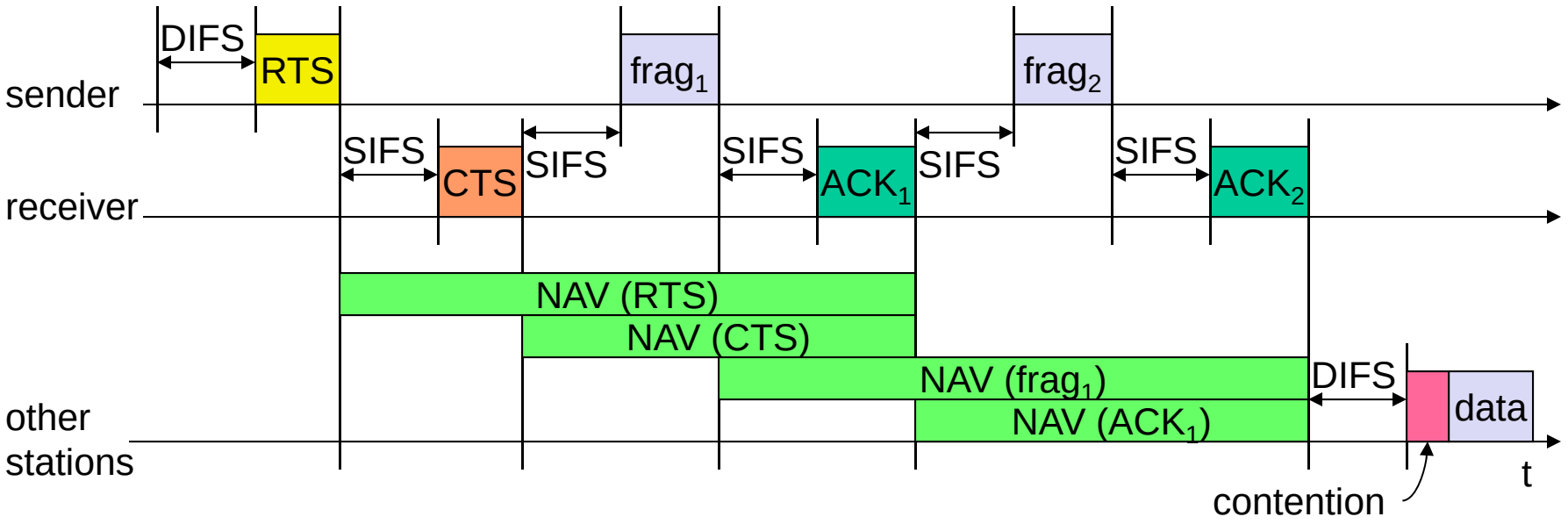
- MACAW uses exponential increase linear decrease to update CW
  - When a node successfully completes a transfer, reduces CW by 1
  - In 802.11, CW is restored to $CW_{min}$
  - In 802.11, CW reduces much faster than it increases
- MACAW can avoid wild oscillations of CW when many nodes contend for the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

# 802.11 Overhead




- Overhead:
  - DIFS
  - Random backoff
  - ACK/SIFS
  - Optional RTS/CTS handshake before transmission of data packet (often disabled due to its overhead)
  - Header overhead
- 802.11 has room for improvement. How?

# Fragmentation



# DFWMAC-PCF

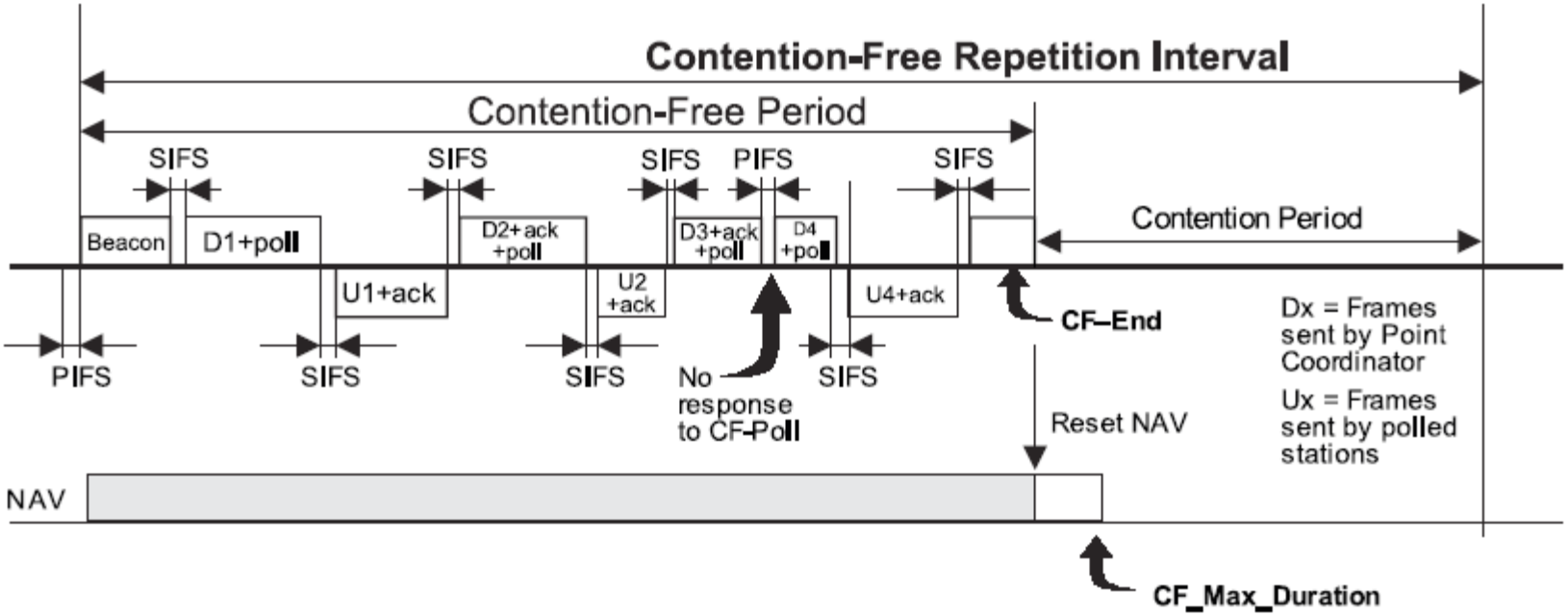
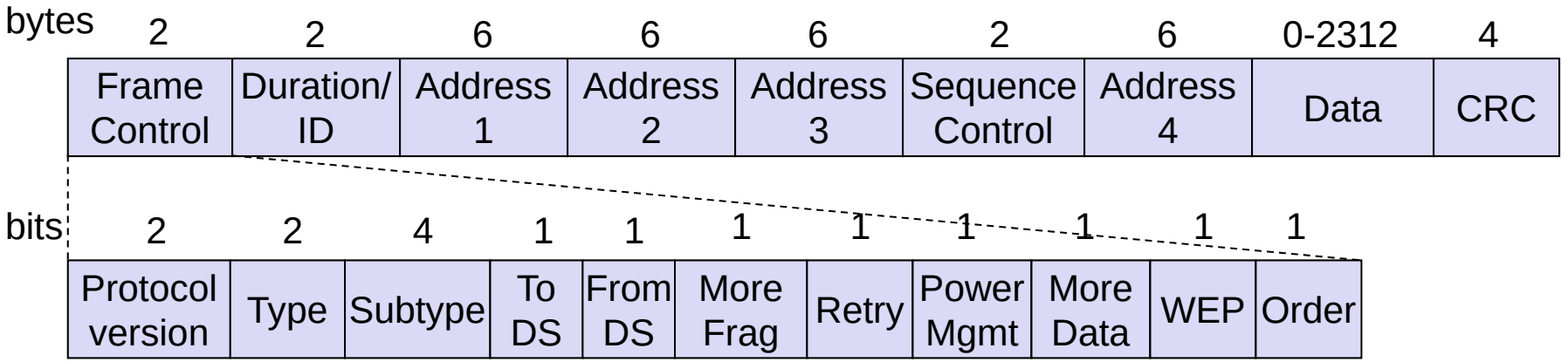



**Figure 62—Example of PCF frame transfer**

# 802.11 - Frame format

- Types
  - control frames, management frames, data frames
- Sequence numbers
  - important against duplicated frames due to lost ACKs
- Addresses
  - Sender, receiver, BSS identifier
- Miscellaneous
  - sending time, checksum, frame control, data



# MAC address format

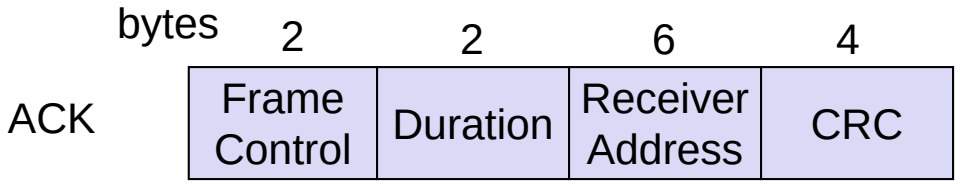
| scenario | to DS | from DS | address 1 | address 2 | address 3 | address 4 |
|---|---|---|---|---|---|---|
| ad-hoc network | 0 | 0 | DA | SA | BSSID | - |
| infrastructure network, from AP | 0 | 1 | DA | BSSID | SA | - |
| infrastructure network, to AP | 1 | 0 | BSSID | SA | DA | - |
| infrastructure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

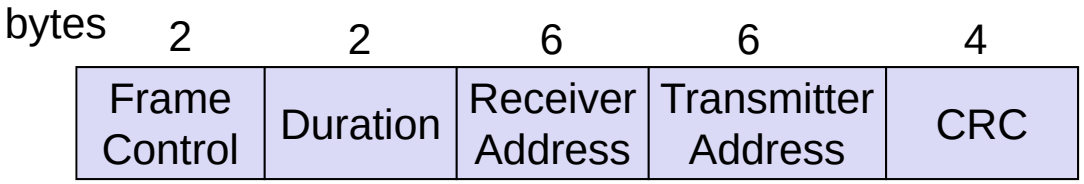
http://www.studioreti.it/slide/802-11-Frame_E_C.pdf

# Special Frames: ACK, RTS, CTS

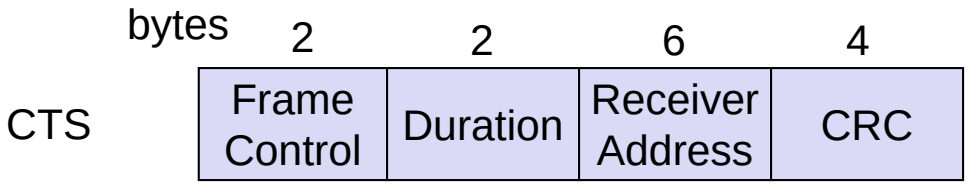
- Acknowledgement




- Request To Send




- Clear To Send



# Outline

- Introduction to MAC
- Introduction to IEEE 802.11
- 802.11 Physical layer
- 802.11 MAC layer
- 802.11 Management

# 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
- Synchronization
  - timing
- Power management
  - sleep-mode without missing a message
  - periodic sleep, frame buffering, traffic measurements
- MIB - Management Information Base
  - managing, read, write

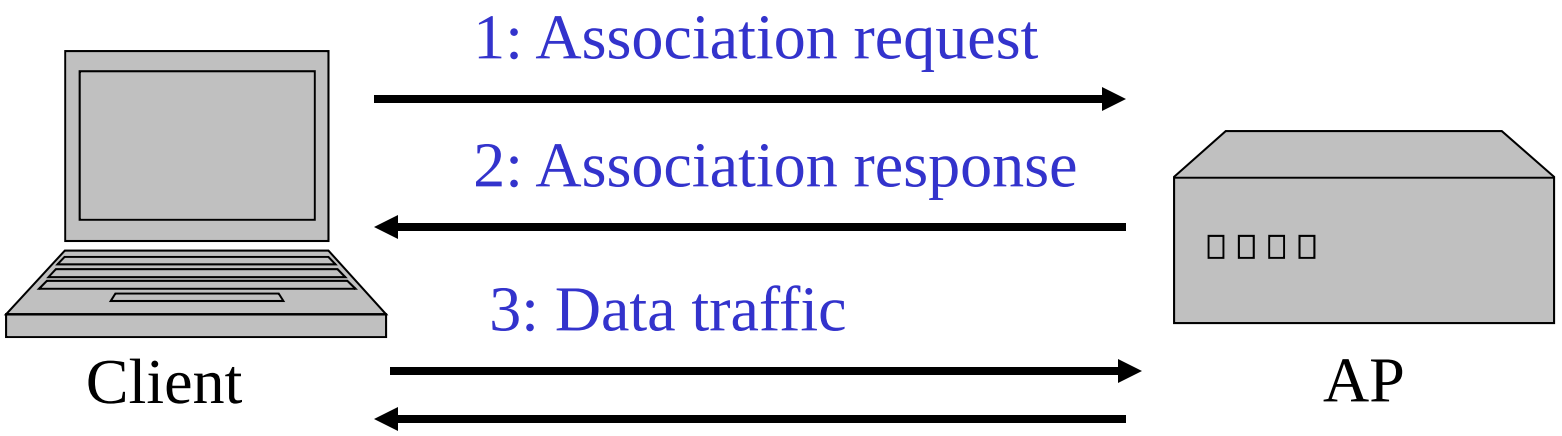
# Association and Reassociation

- Integration into a LAN
- Scanning: find a network to connect
- Roaming: change networks by changing access points

# 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

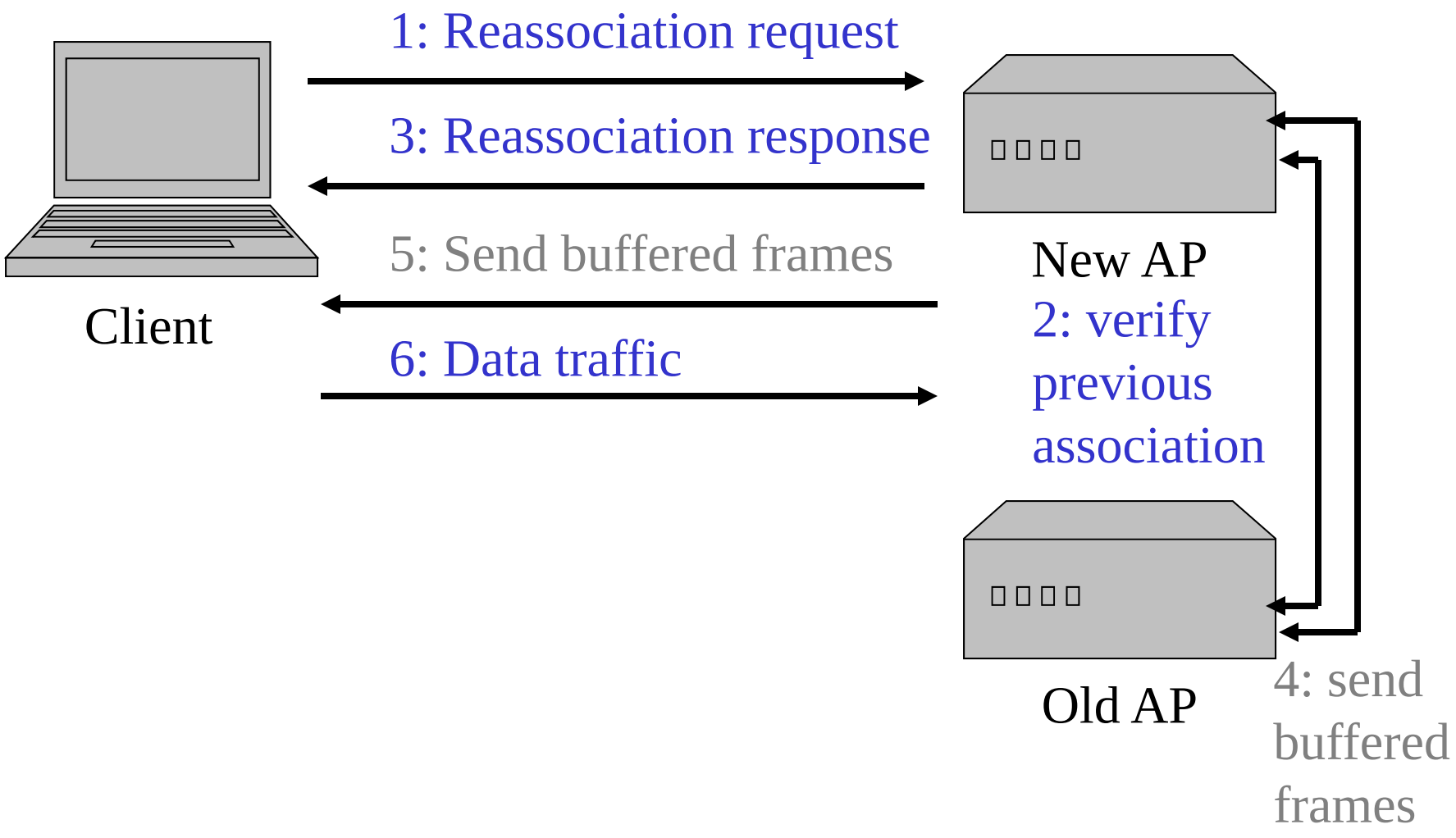
# Association in 802.11



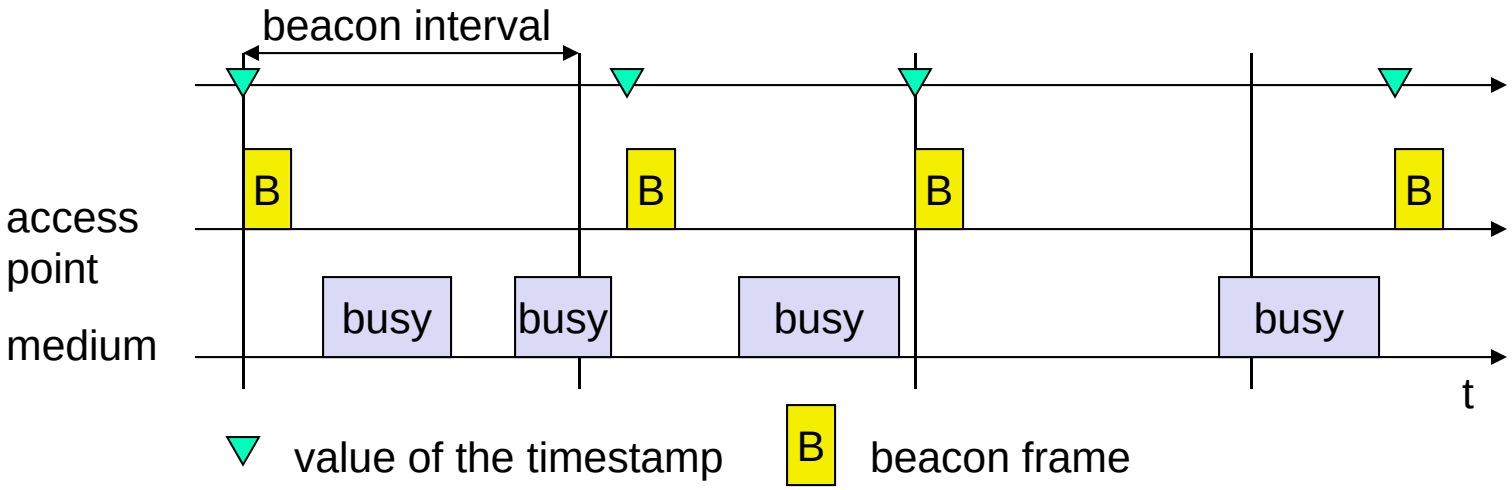
# 802.11 - Roaming

- No or bad connection? Then perform:
- Scanning
  - scan the environment, i.e., listen to the medium for beacon signals or send probes to 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

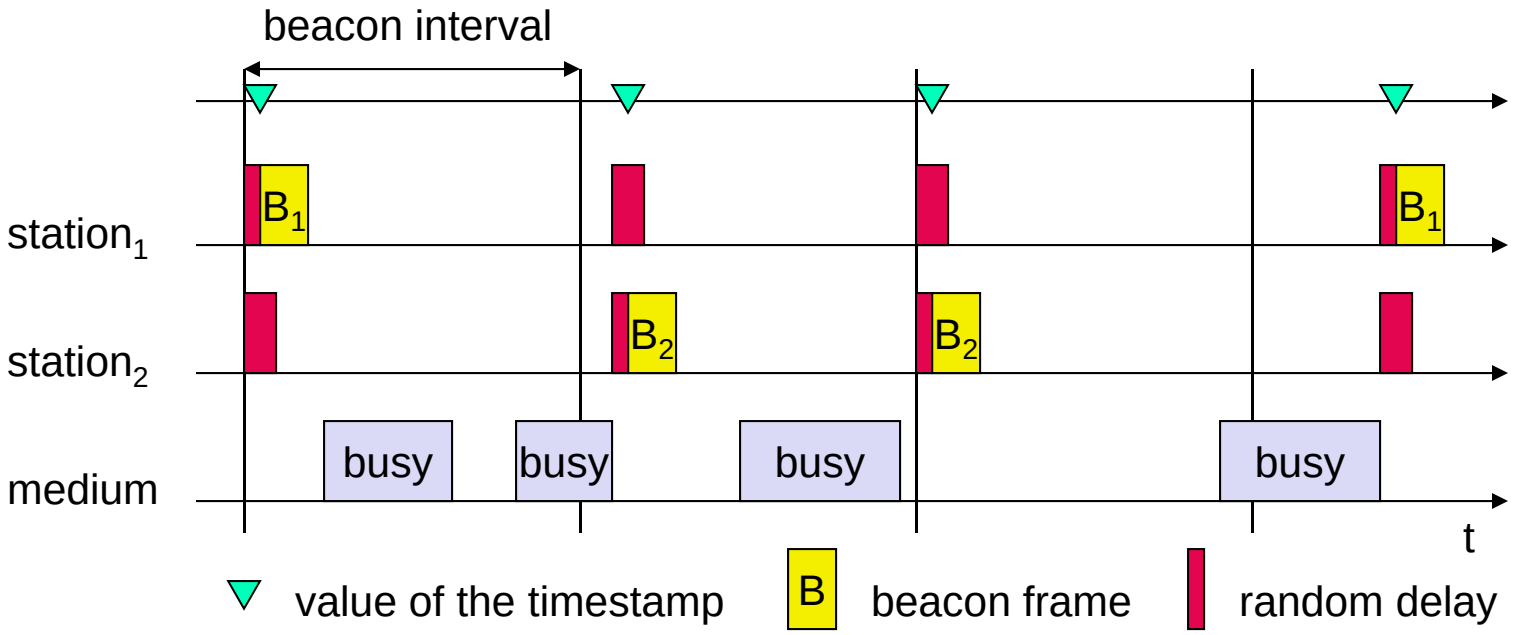
# Reassociation in 802.11



# Synchronization using a Beacon (infrastructure)



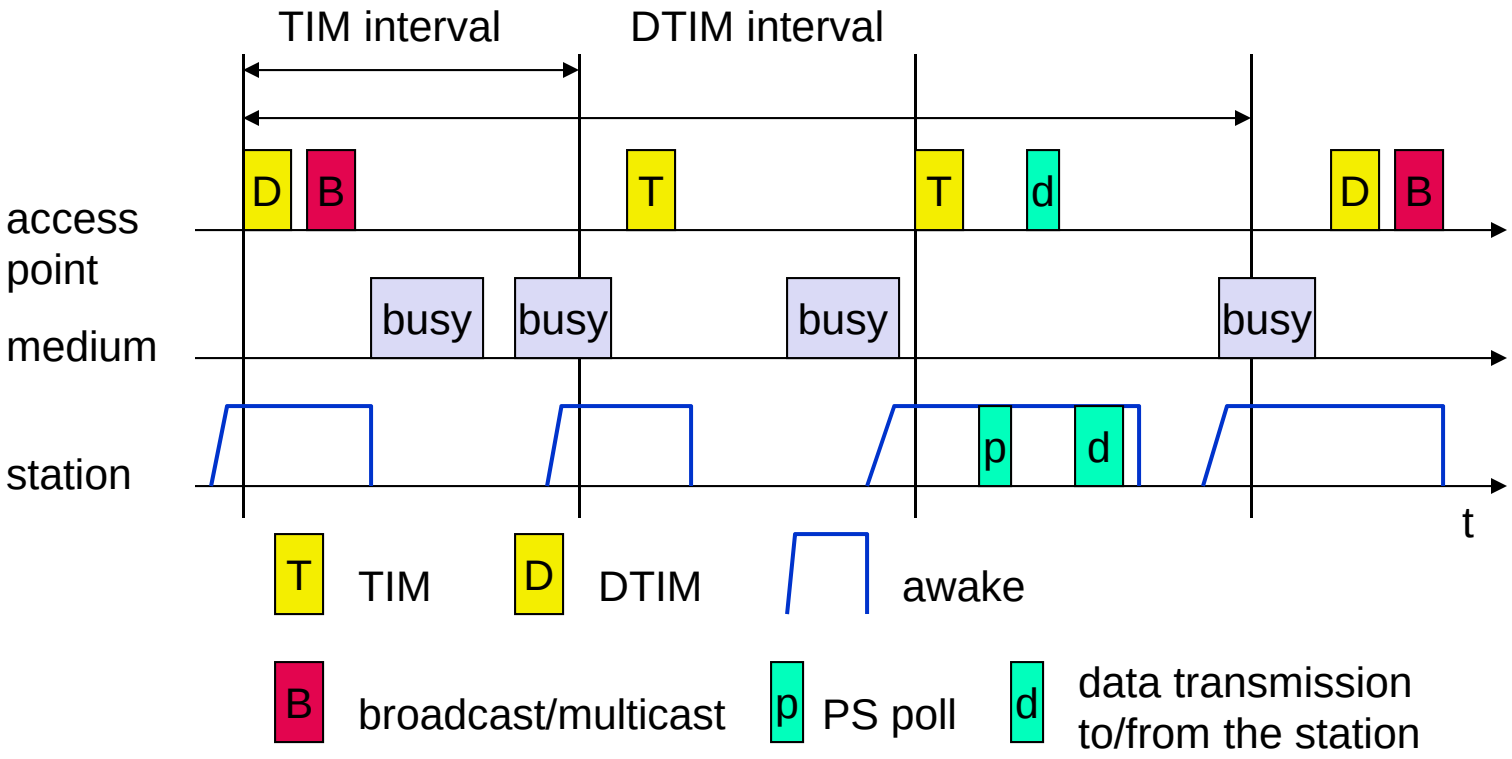
# Synchronization using a Beacon (ad-hoc)



# 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
- Ad-hoc
  - Ad-hoc Traffic Indication Map (ATIM)
    - announcement of receivers by stations buffering frames
    - more complicated - no central AP

# Power saving with wake-up patterns (infrastructure)



# Power saving with wake-up patterns (ad-hoc)