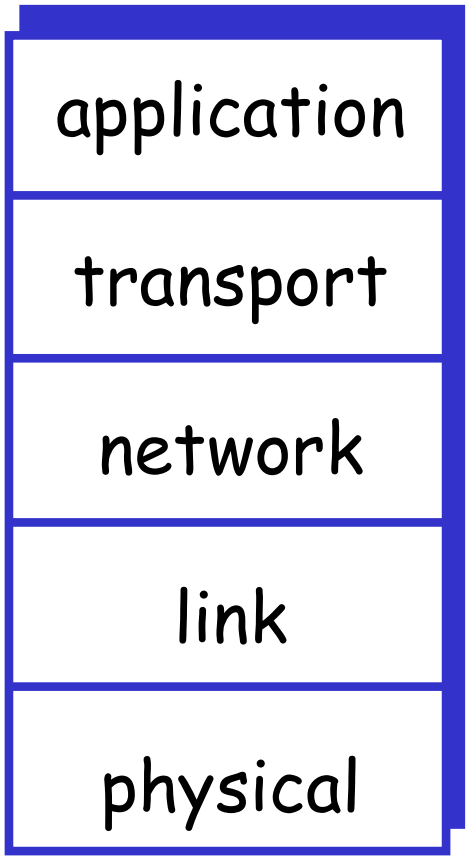
Internet Protocol Stack

- Application: supporting network applications
  - FTP, SMTP, HTTP
- Transport: data transfer between processes
  - TCP, UDP
- Network: routing of datagrams from source to destination
  - IP, routing protocols
- Link: data transfer between neighboring network elements
  - Ethernet, WiFi
- Physical: bits "on the wire"
  - Coaxial cable, optical fibers, radios



Introduction to Link Layer and IEEE 802.11 (WiFi)

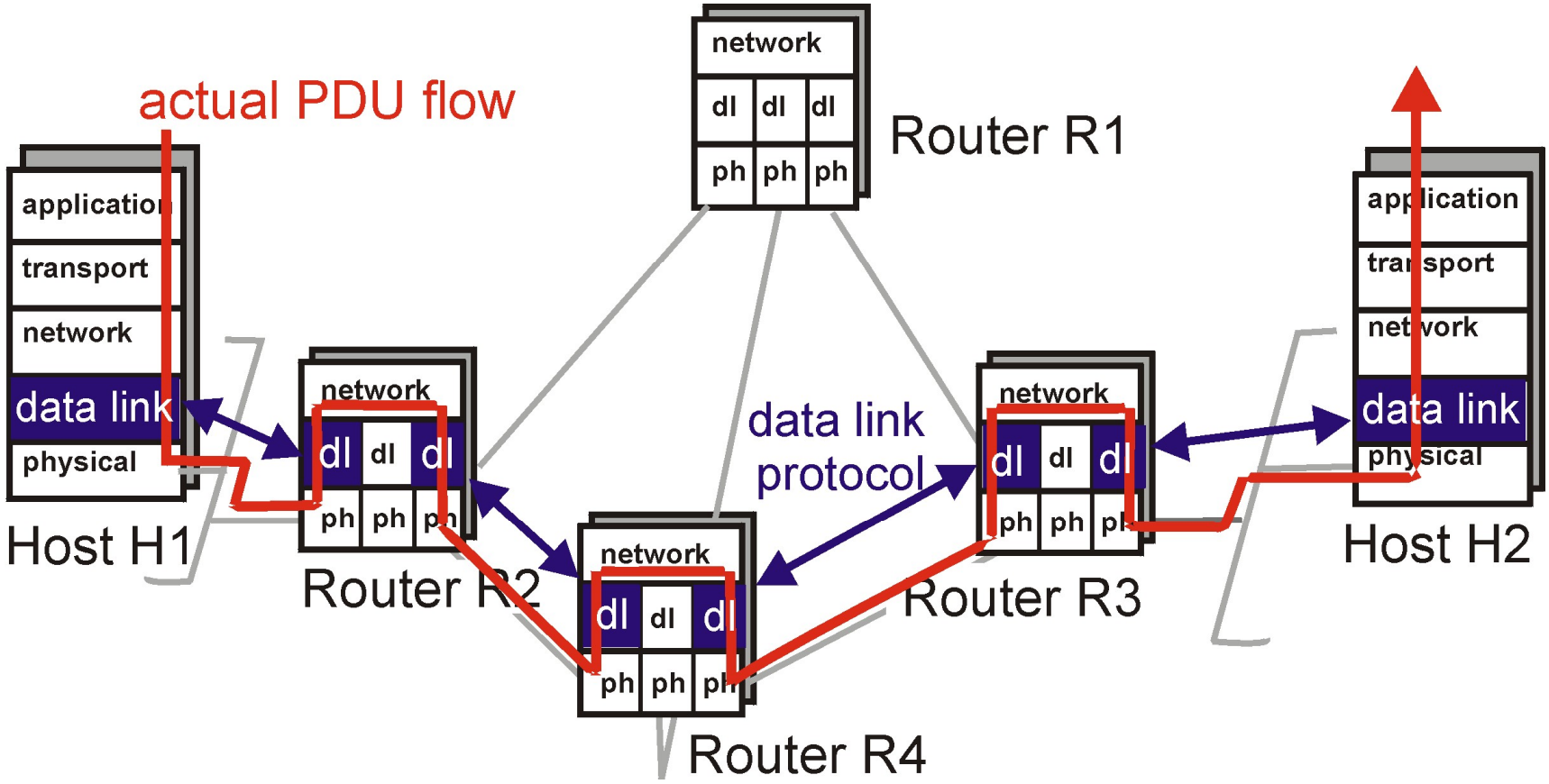
Outline

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

Link Layer Services

- Framing, link access:
  - encapsulate datagram into frame, adding header, trailer
  - implement channel access if shared medium (e.g., Ethernet)
  - 'physical addresses' used in frame headers to identify source, dest
    - different from IP address!
- coordinate access to a shared medium
- reliable delivery between two physically connected devices
- error detection/correction
- flow control

Link layer: setting the context



Experiment

Multiple Access Protocols

- Determine how stations share channel
  - single shared communication channel
  - two or more simultaneous transmissions by nodes: interference
    - only one node can send successfully at a time
- What to look for in MAC protocols
  - Synchronous vs. asynchoronous
  - Centralized vs. decentralized
  - Performance: efficiency and fairness

MAC Protocols: a taxonomy

- Channel Partitioning
  - divide channel into smaller "pieces" (time slots, frequency, code)
  - allocate piece to node for exclusive use
  - Examples
    - TDMA: partition time slots
    - FDMA: partition frequency
    - CDMA: partition code

MAC Protocols: a taxonomy

- Channel Partitioning
  - divide channel into smaller "pieces" (time slots, frequency, code)
  - allocate piece to node for exclusive use
  - Examples
    - TDMA: partition time slots
    - FDMA: partition frequency
    - CDMA: partition code
- Random Access
  - allow collisions
  - "recover" from collisions

MAC Protocols: a taxonomy

- Channel Partitioning
  - divide channel into smaller "pieces" (time slots, frequency, code)
  - allocate piece to node for exclusive use
  - Examples
    - TDMA: partition time slots
    - FDMA: partition frequency
    - CDMA: partition code
- Random Access
  - allow collisions
  - "recover" from collisions
- "Taking turns"
  - nodes take turns, but nodes with more to send can take longer turns

Random Access Protocols

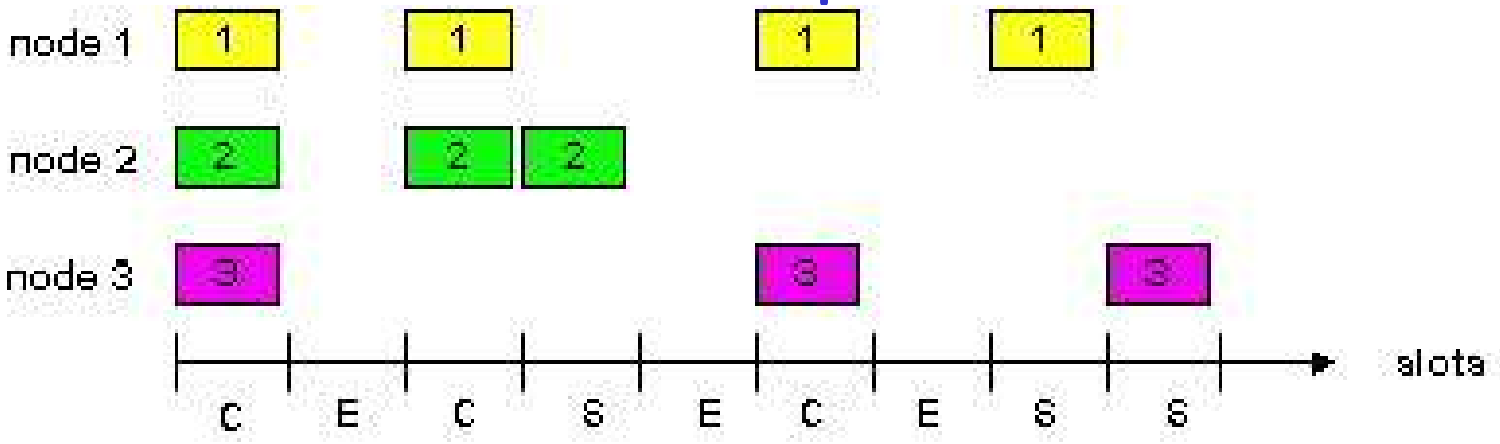
- When a node has a packet to send
  - transmit at full channel data rate R.
  - no *a priori* coordination among nodes
- two or more transmitting nodes -> "collision"
- random access MAC protocol specifies:
  - how to detect collisions
  - how to recover from collisions (e.g., via delayed retransmissions)
- Examples of random access MAC protocols:
  - Pure ALOHA
  - Slotted ALOHA
  - CSMA and CSMA/CD

Pure ALOHA

- Transmit whenever a message is ready
- Retransmit when there is a collision

Slotted Aloha

- time is divided into equal size slots (= pkt trans. time)
- node with new arriving pkt: transmit at beginning of next slot
- if collision: retransmit pkt in future slots



Success (S), Collision (C), Empty (E) slots

Slotted Aloha Efficiency

- Q: What is max efficiency?
- Suppose N stations have packets to send each with a probability p

Slotted Aloha Efficiency

- Q: What is max efficiency?
- Suppose N stations have packets to send each with a probability p

Slotted Aloha Efficiency

- Q: What is max efficiency?
- Suppose N stations have packets to send each with a probability p
- Succeed by a given node: $p(1-p)^{(N-1)}$
- Succeed by any of N nodes: $Np(1-p)^{(N-1)}$
- Optimal $p=1/e = 0.37$ as N-> infinity

What's the max efficiency of pure aloha?

Problems with Pure/Slotted ALOHA

- Pure ALOHA
  - Transmit whenever a message is ready
  - Retransmit when there is a collision

- Slotted ALOHA
  - Time is divided into equal time slots
  - Transmit only at the beginning of a time slot
  - Avoid partial collisions
  - Increase delay, and require synchronization

Problem: do not listen to the channel.

CSMA: Carrier Sense Multiple Access

CSMA: listen before transmit:

- If channel sensed idle: transmit entire pkt
- 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

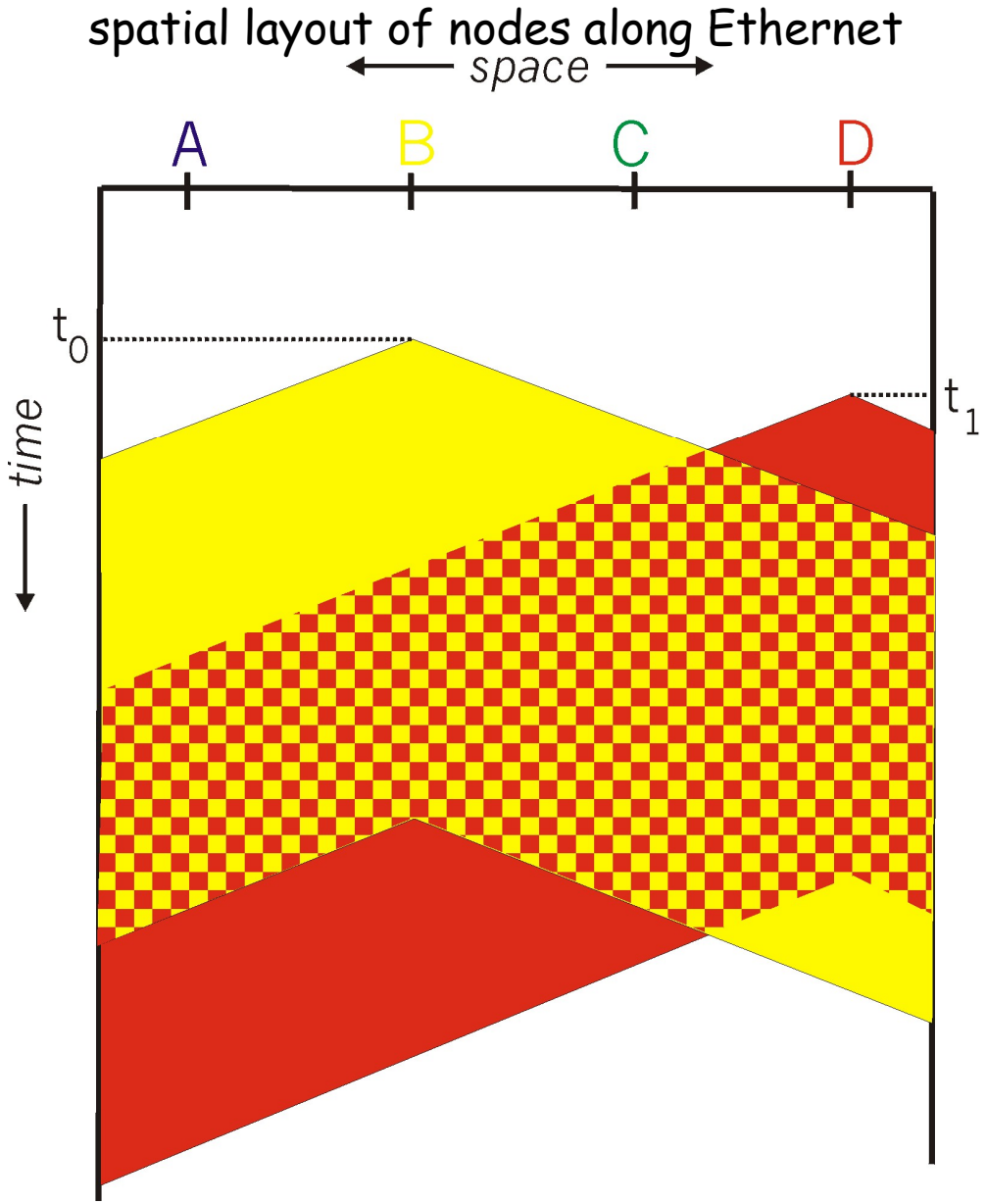
Does carrier sense eliminate collisions?

CSMA collisions

collisions *can* occur:
propagation delay means two nodes may not hear each other's transmission

collision:
entire packet transmission time wasted

note:
role of distance and propagation delay in determining collision prob.



How to reduce collision cost?

CSMA/CD (Collision Detection)

CSMA/CD: carrier sensing, deferral as in CSMA

- collisions *detected* within short time
- colliding transmissions aborted, reducing channel wastage
- persistent or non-persistent retransmission

- collision detection:
  - easy in wired LANs: measure signal strengths, compare transmitted, received signals
  - Can we do collision detection in wireless networks?

CSMA/CD (Collision Detection)

CSMA/CD: carrier sensing, deferral as in CSMA

- collisions *detected* within short time
- colliding transmissions aborted, reducing channel wastage
- persistent or non-persistent retransmission

- collision detection:
  - easy in wired LANs: measure signal strengths, compare transmitted, received signals
  - difficult in wireless LANs:
    - Most receivers cannot send and receive at the same time
    - receiver's channel condition is different from that of the sender

Introduction to IEEE 802.11

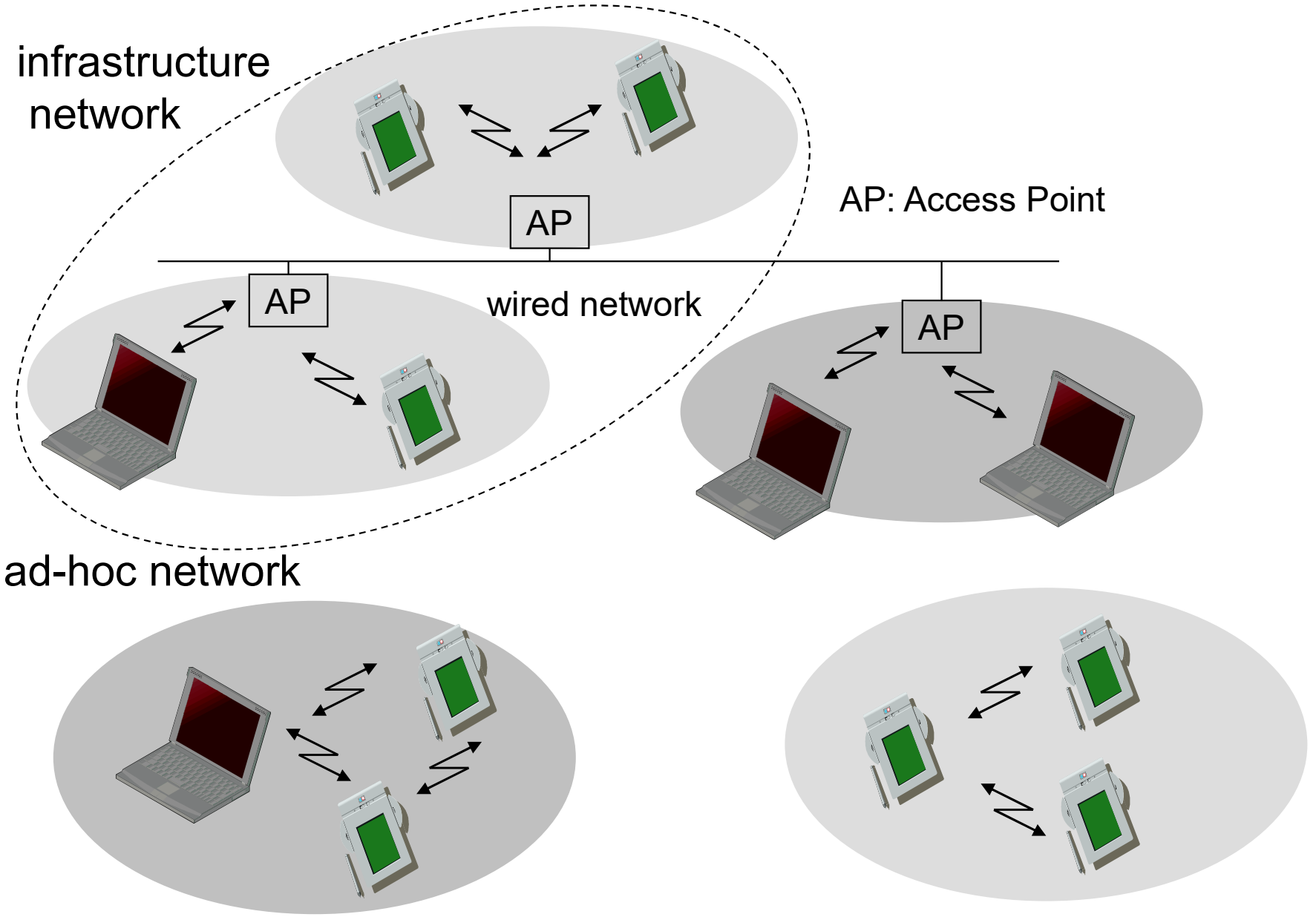
Characteristics of wireless LANs

- Advantages
  - very flexible within the reception area
  - Ad-hoc networks without previous planning possible
  - (almost) no wiring difficulties (e.g. historic buildings, firewalls)
  - more robust against disasters
    - e.g., earthquakes, fire - or users pulling a plug...
- Disadvantages
  - typically very low bandwidth compared to wired networks (1-10 Mbit/s) due to shared medium
  - Less reliable

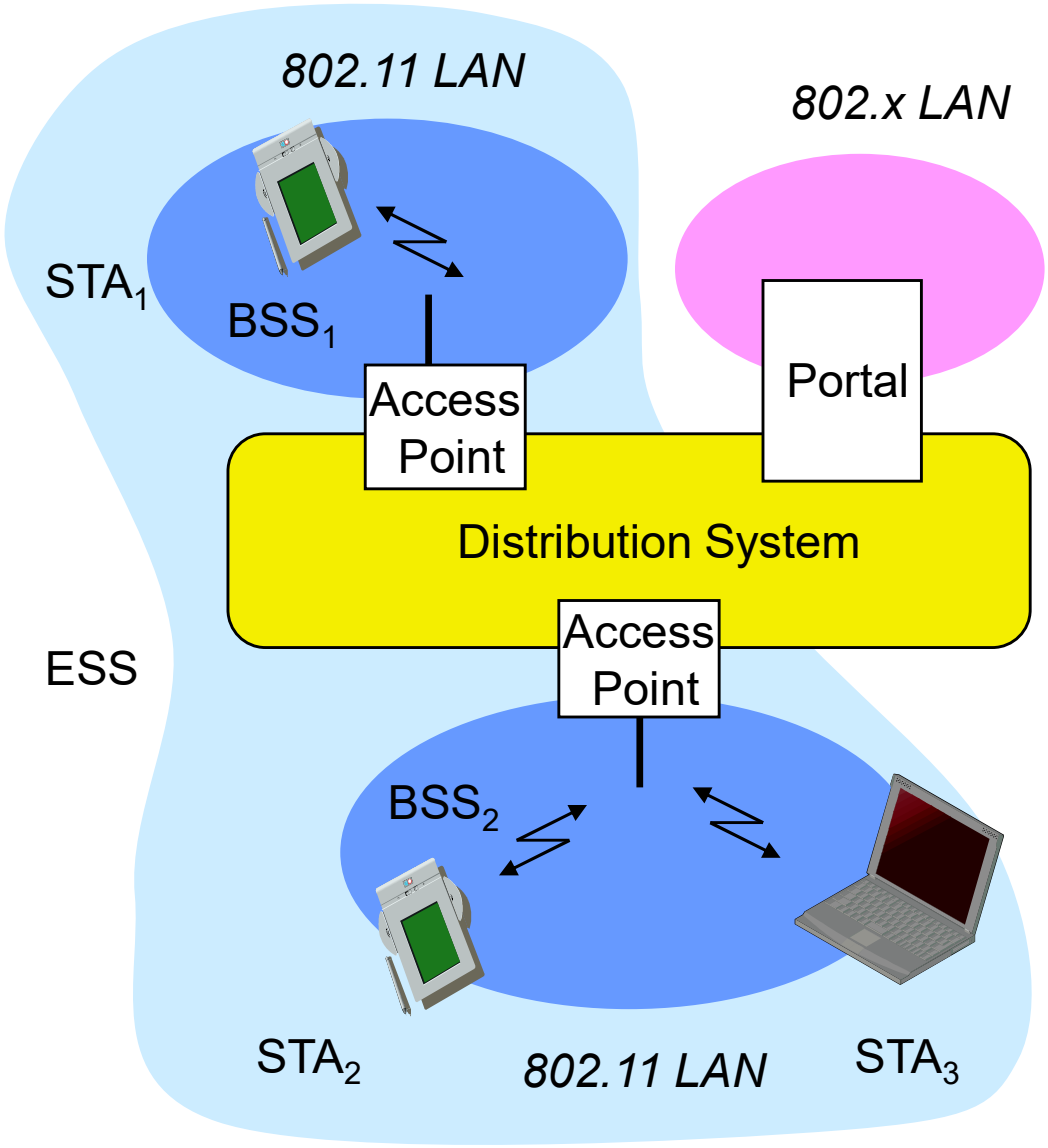
Design Goals for Wireless LANs

- global, seamless operation
- low power for battery use
- no special licenses needed to use the LAN
- robust transmission technology
- simplified spontaneous cooperation at meetings
- easy to use for everyone, simple management
- protection of investment in wired networks
- security, privacy, safety
- transparent to applications and higher layer protocols
- location aware if necessary

Infrastructure vs. ad-hoc networks

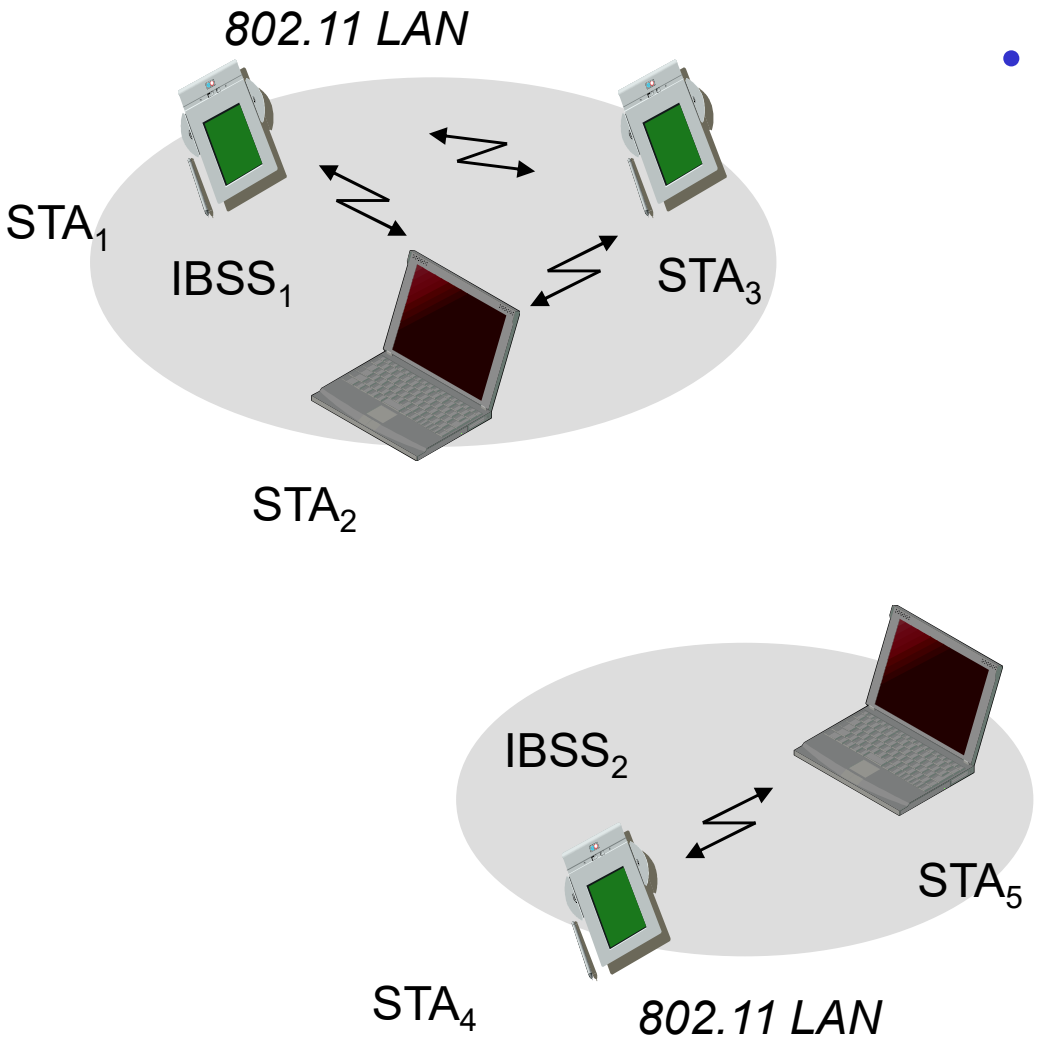


802.11: Infrastructure



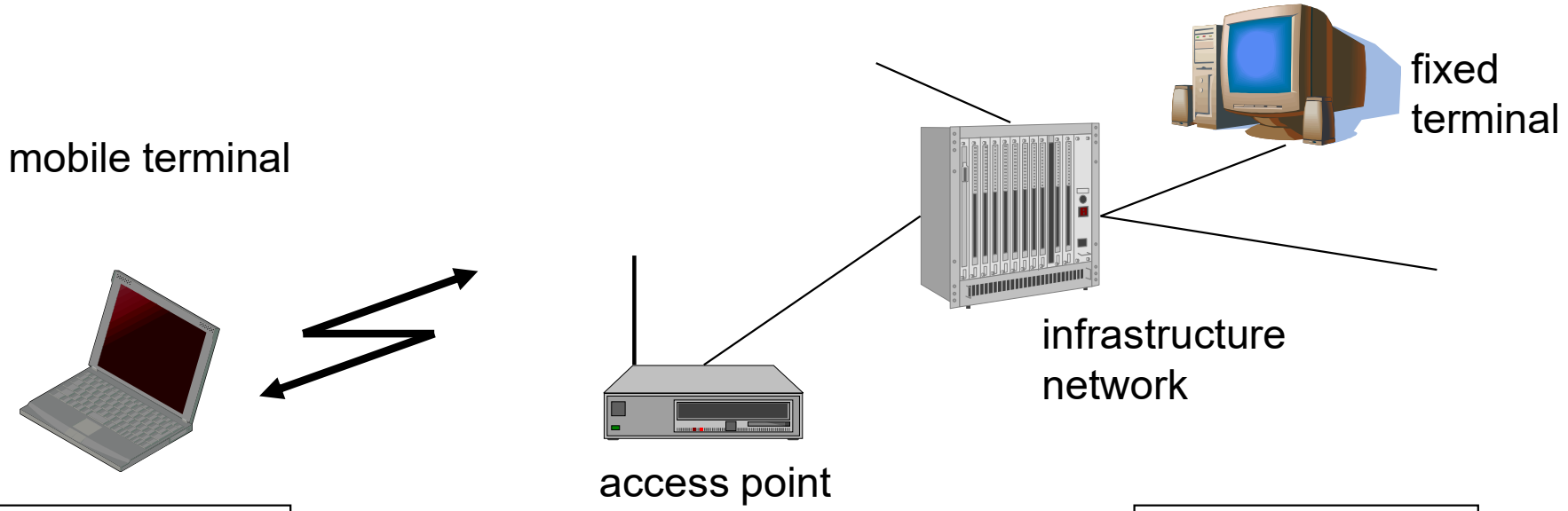
- Station (STA)
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- Access Point
  - station integrated into the wireless LAN and the distribution system
- Basic Service Set (BSS)
  - group of stations using the same AP
- Portal
  - bridge to other (wired)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

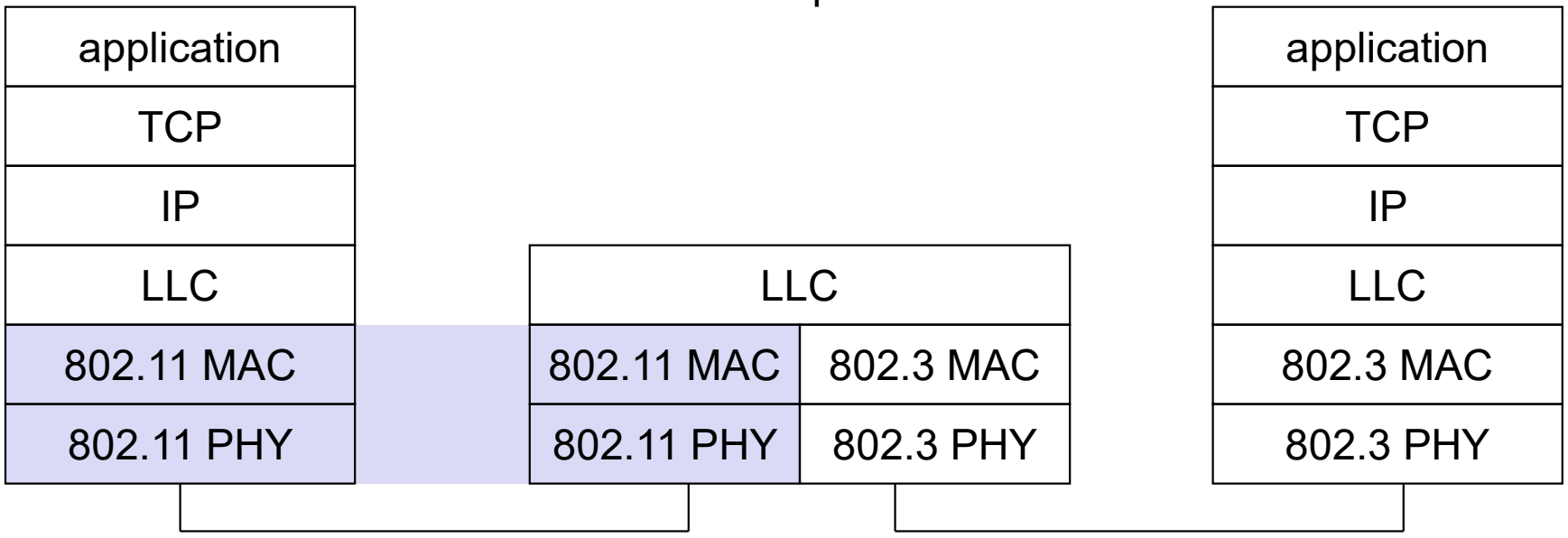
802.11: Ad hoc mode



- 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

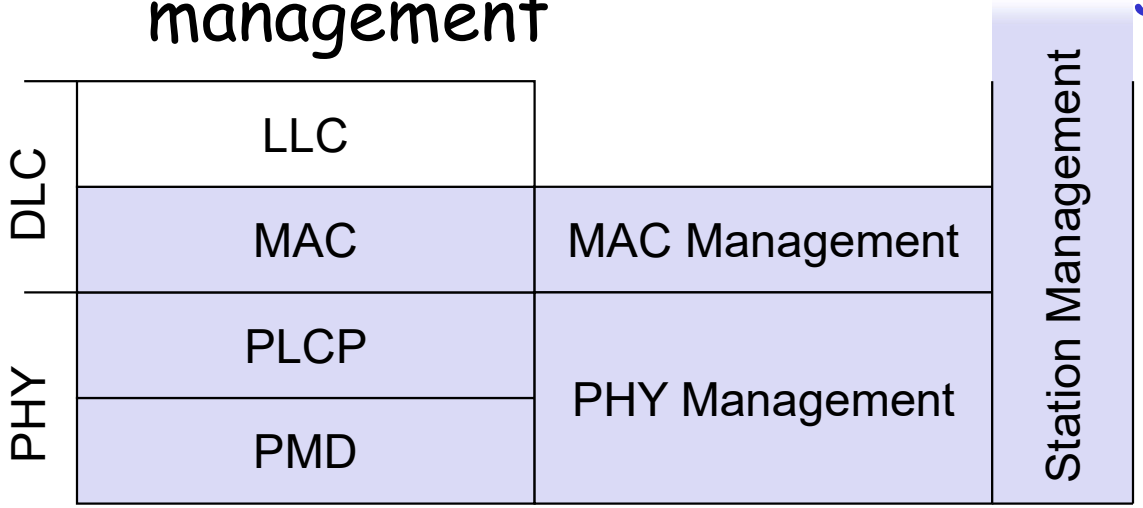
IEEE standard 802.11





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



Outline

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

WLAN: IEEE 802.11b (WiFi 1)

- 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
- Security
  - Limited, WEP insecure, SSID
- Availability
  - Many products and vendors
- Connection set-up time
  - Connectionless/always on
- Quality of Service
  - Best effort, no guarantees (unless polling is used, limited support in products)
- Manageability
  - Limited (no automated key distribution, sym. Encryption)
- 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 (WiFi 2)

- 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
- Security
  - Limited, WEP insecure, SSID
- Availability
  - Some products, some vendors
- Connection set-up time
  - Connectionless/always on
- Quality of Service
  - Best effort, no guarantees (same as all 802.11 products)
- Manageability
  - Limited (no automated key distribution, sym. Encryption)
- Pros
  - Fits into 802.x standards
  - Free ISM-band
  - Available, simple system
  - Uses less crowded 5 GHz band
  - Higher data rates
- Cons
  - Shorter range

WLAN: IEEE 802.11g (WiFi 3)

- Data rate
  - OFDM
  - BPSK / QPSK / 16-QAM / 64-QAM
- Transmission range
  - 300m outdoor, 30m indoor
  - Max. data rate ~10m indoor
- Frequency
  - Free 2.4 GHz ISM-band
- Security
  - Limited, WEP insecure, SSID
- Availability
  - Many products and vendors
- Connection set-up time
  - Connectionless/always on
- Quality of Service
  - Best effort, no guarantees (unless polling is used, limited support in products)
- Manageability
  - Limited (no automated key distribution, sym. Encryption)
- 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 802.11n (WiFi 4)

- Data rate
  - 7.2, 14.4, 21.7, 28.9, …, 72.2 Mbit/s, depending on SNR
- Multiple input multiple output (MIMO)
- 20MHz and 40MHz bands
- Transmission range
  - Increase range by several factors due to MIMO
- Frequency
  - Free 2.4GHz ISM-band
  - Free 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz ISM-band
- Security
  - Limited, WEP insecure, SSID
- Availability
  - Some products, some vendors
- Connection set-up time
  - Connectionless/always on
- Quality of Service
  - Best effort, no guarantees (same as all 802.11 products)
- Manageability
  - Limited (no automated key distribution, sym. Encryption)
- Pros
  - Fits into 802.x standards
  - Free ISM-band
  - Available, simple system
  - Uses dual band
  - Higher data rates
- Cons
  - Interference on ISM-band

WLAN: IEEE 802.11ac (WiFi 5)

- Data rate
  - 6.5 Bps – 3.466 Gps depending on SNR, channel width, # streams
- MIMO: up to 8 antennas
- 20, 40, 80, 160 MHz
- Transmission range
  - Increase range by several factors due to MIMO
- Dual bands
  - Free 2.4GHz ISM-band
  - Free 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz ISM-band
- Security
  - Limited, WEP insecure, SSID
- Availability
  - Some products, some vendors
- Connection set-up time
  - Connectionless/always on
- Quality of Service
  - Best effort, no guarantees (same as all 802.11 products)
- Manageability
  - Limited (no automated key distribution, sym. Encryption)
- Pros
  - Fits into 802.x standards
  - Free ISM-band
  - Available, simple system
  - Uses dual band
  - Higher data rates
- Cons
  - Interference on ISM-band

WLAN: IEEE 802.11ax (WiFi 6)

- Data rate
  - 6.5 Bps – 3.466 Gps depending on SNR, channel width, # streams
  - MAX QAM: 1024
  - OFMDA
- MIMO: up to 8 antennas
- 20, 40, 80, 160 MHz
- Transmission range
  - Increase range by several factors due to MIMO
- Dual bands
  - Free 2.4GHz ISM-band
  - Free 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz ISM-band
- Security
  - Limited, WEP insecure, SSID
- Availability
  - Some products, some vendors
- Connection set-up time
  - Connectionless/always on
- Quality of Service
  - Best effort, no guarantees (same as all 802.11 products)
- Manageability
  - Limited (no automated key distribution, sym. Encryption)
- Pros
  - Fits into 802.x standards
  - Free ISM-band
  - Available, simple system
  - Uses dual band
  - Higher data rates
- Cons
  - Interference on ISM-band

WLAN: IEEE 802.11be (WiFi 7)

- Data rate
  - 6.5 Bps – 3.466 Gps depending on SNR, channel width, # streams
  - MAX QAM: 4096
  - Enhanced OFDMA
- MIMO: up to 8 antennas
- 20, 40, 80, 160, 320 MHz
- Transmission range
  - Increase range by several factors due to MIMO
- Dual bands
  - Free 2.4GHz ISM-band
  - Free 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz ISM-band
- Security
  - Limited, WEP insecure, SSID
- Availability
  - Some products, some vendors
- Connection set-up time
  - Connectionless/always on
- Quality of Service
  - Best effort, no guarantees (same as all 802.11 products)
- Manageability
  - Limited (no automated key distribution, sym. Encryption)
- Pros
  - Fits into 802.x standards
  - Free ISM-band
  - Available, simple system
  - Uses dual band
  - Higher data rates
- Cons
  - Interference on ISM-band

Outline

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

802.11: MAC layer I - DFWMAC

Traffic services

- Asynchronous Data Service (mandatory)
  - exchange of data packets based on "best-effort"
  - support of broadcast and multicast
- Time-Bounded Service (optional)
  - implemented using PCF (Point Coordination Function)
- Broadcast, multicast, and unicast
  - Uses ACK and retransmission to achieve reliability for unicast frames
  - No ACK/retransmission for broadcast or multicast frames

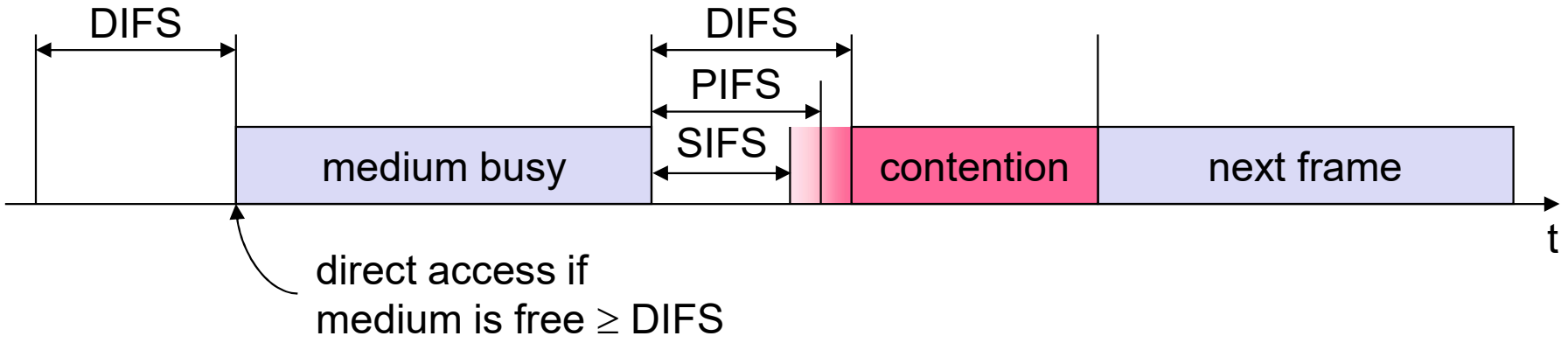
802.11 MAC Layer II

- Distributed and centralized access methods
  - DFWMAC-DCF CSMA/CA (mandatory)
    - collision avoidance via randomized "back-off" mechanism
    - minimum distance between consecutive packets
    - ACK packet for acknowledgements (not for broadcasts)
  - DFWMAC-DCF w/ RTS/CTS (optional)
    - Distributed Function Wireless MAC
    - avoids hidden terminal problem
  - DFWMAC- 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

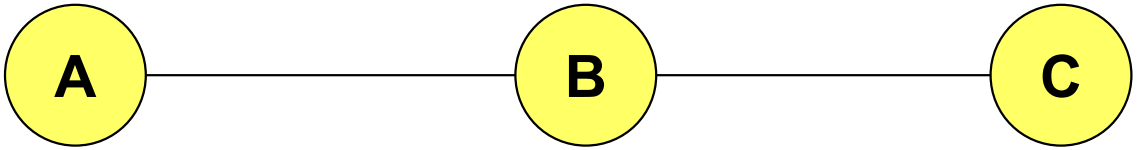
CSMA/CA

- CSMA/CA:
  - Wireless MAC protocols often use collision avoidance techniques, in conjunction with a (physical or virtual) carrier sense mechanism

CSMA/CA

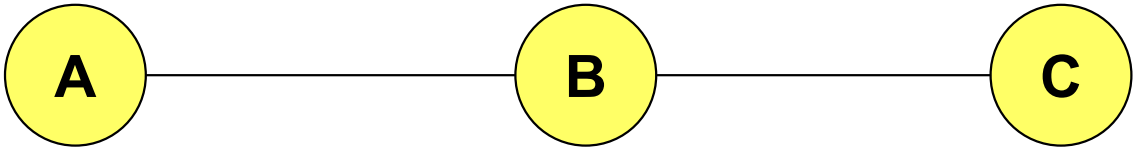
- Carrier sense
  - Nodes stay silent when carrier sensed (physical/virtual)
  - Physical carrier sense
    - Carrier sense threshold
  - Virtual carrier sense using Network Allocation Vector (NAV)
    - NAV is updated based on overheard RTS/CTS/DATA/ACK packets

Hidden Terminal Problem



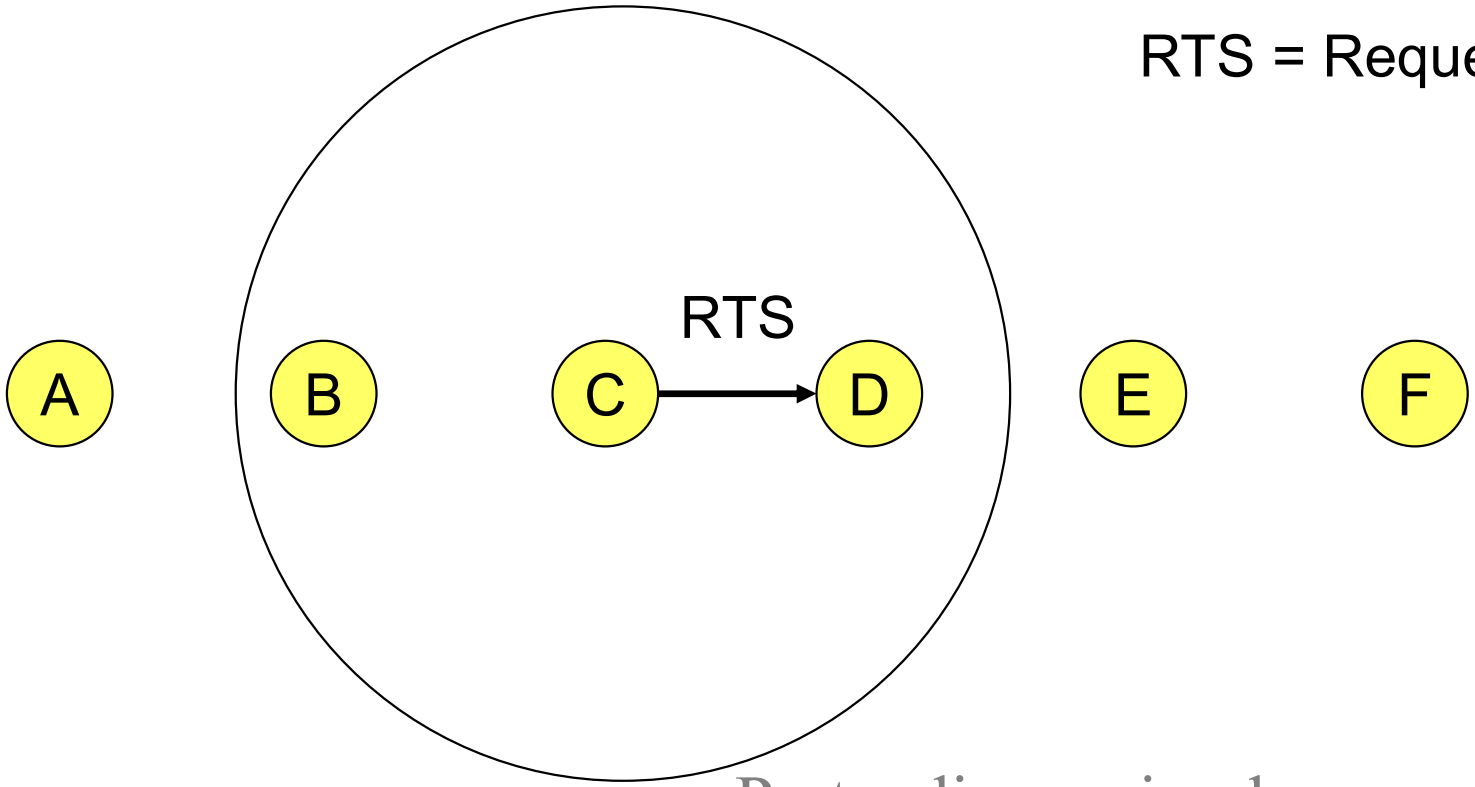
- B can communicate with both A and C
- A and C cannot hear each other
- Problem
  - When A transmits to B, C cannot detect the transmission using the carrier sense mechanism
  - If C transmits, collision will occur at node B
- Solution
  - Hidden sender C needs to defer

Solution for Hidden Terminal Problem: MACA



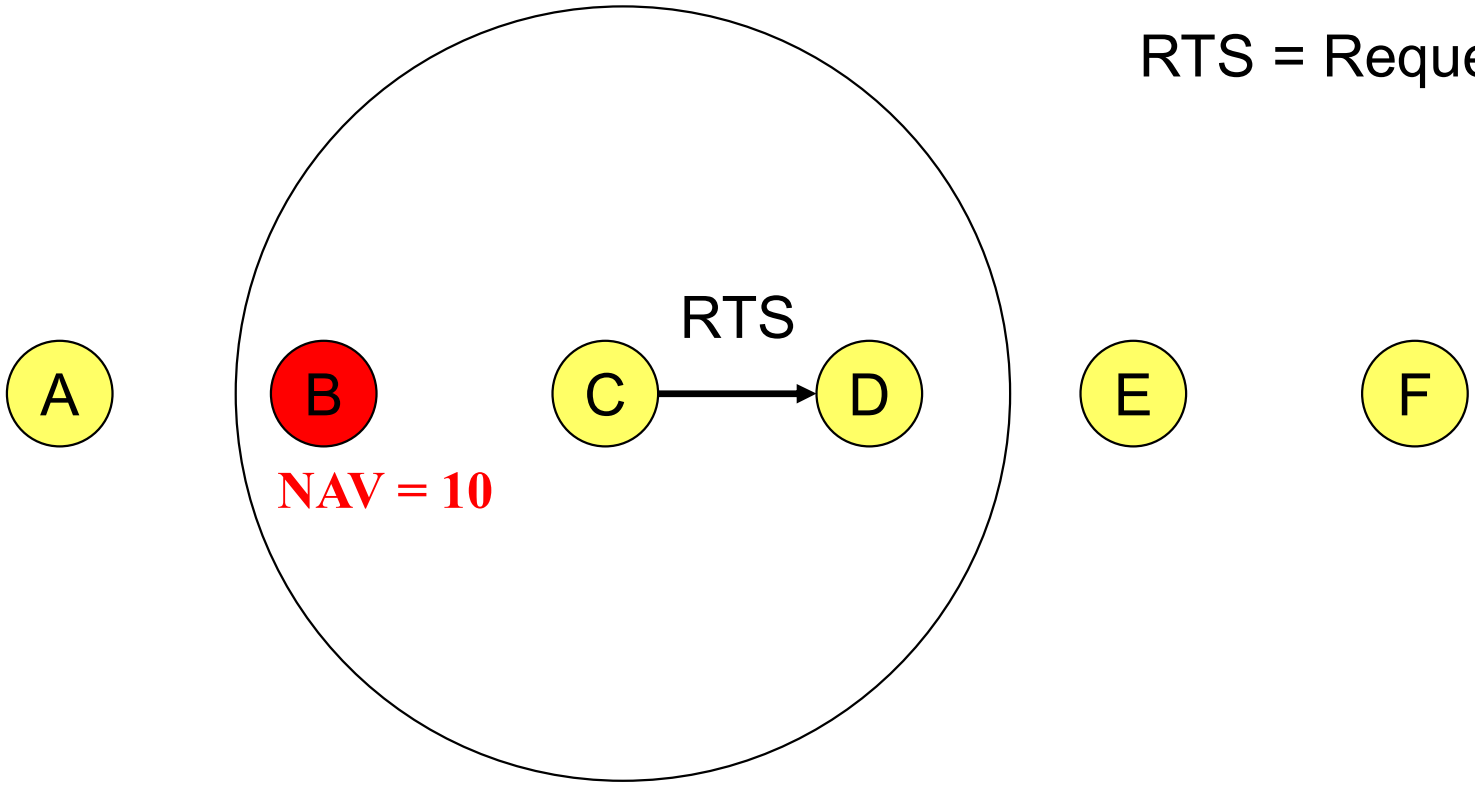
- When A wants to send a packet to B, A first sends a Request-to-Send (RTS) to B
- On receiving RTS, B responds by sending Clear-to-Send (CTS), provided that A is able to receive the packet
- When C overhears a CTS, it keeps quiet for the duration of the transfer
  - Transfer duration is included in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

IEEE 802.11



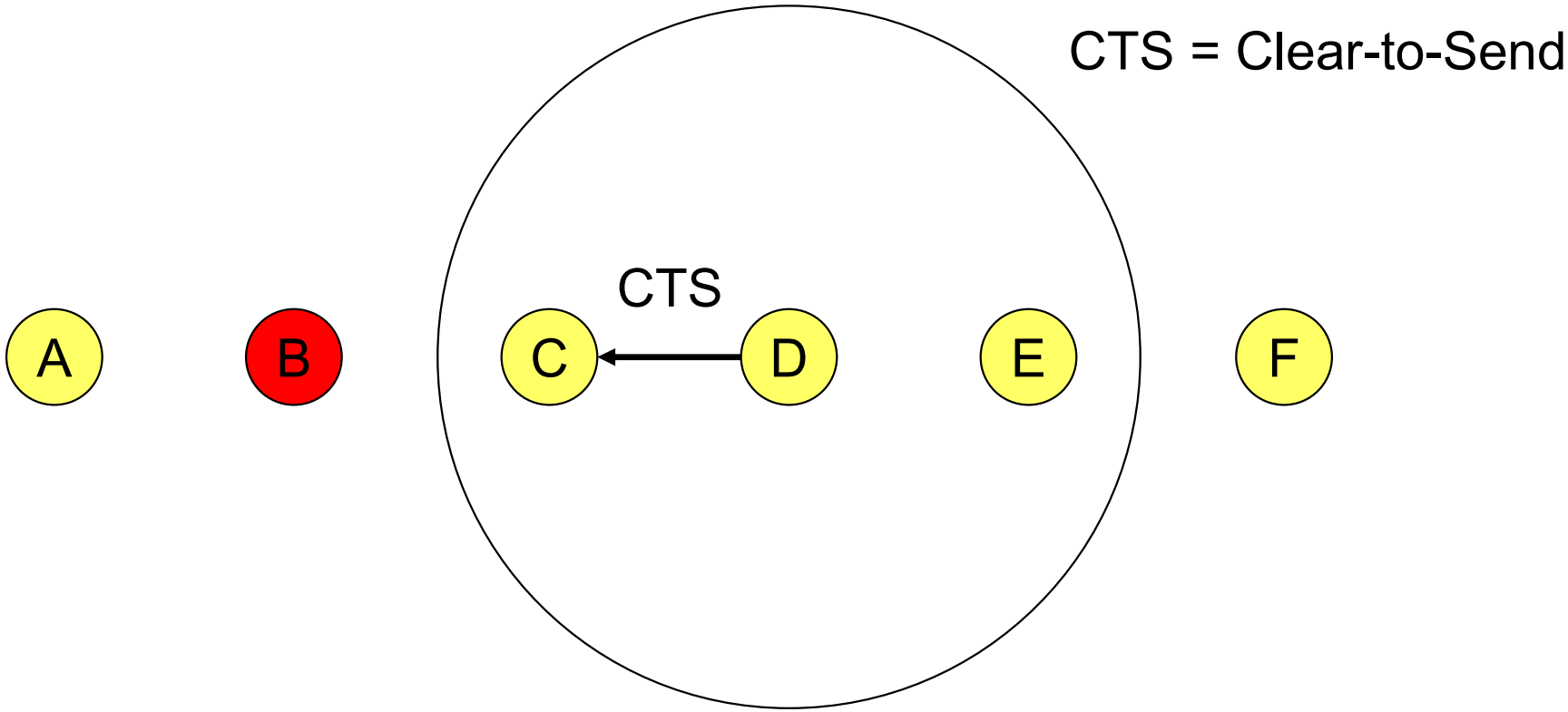
Pretending a circular range

IEEE 802.11

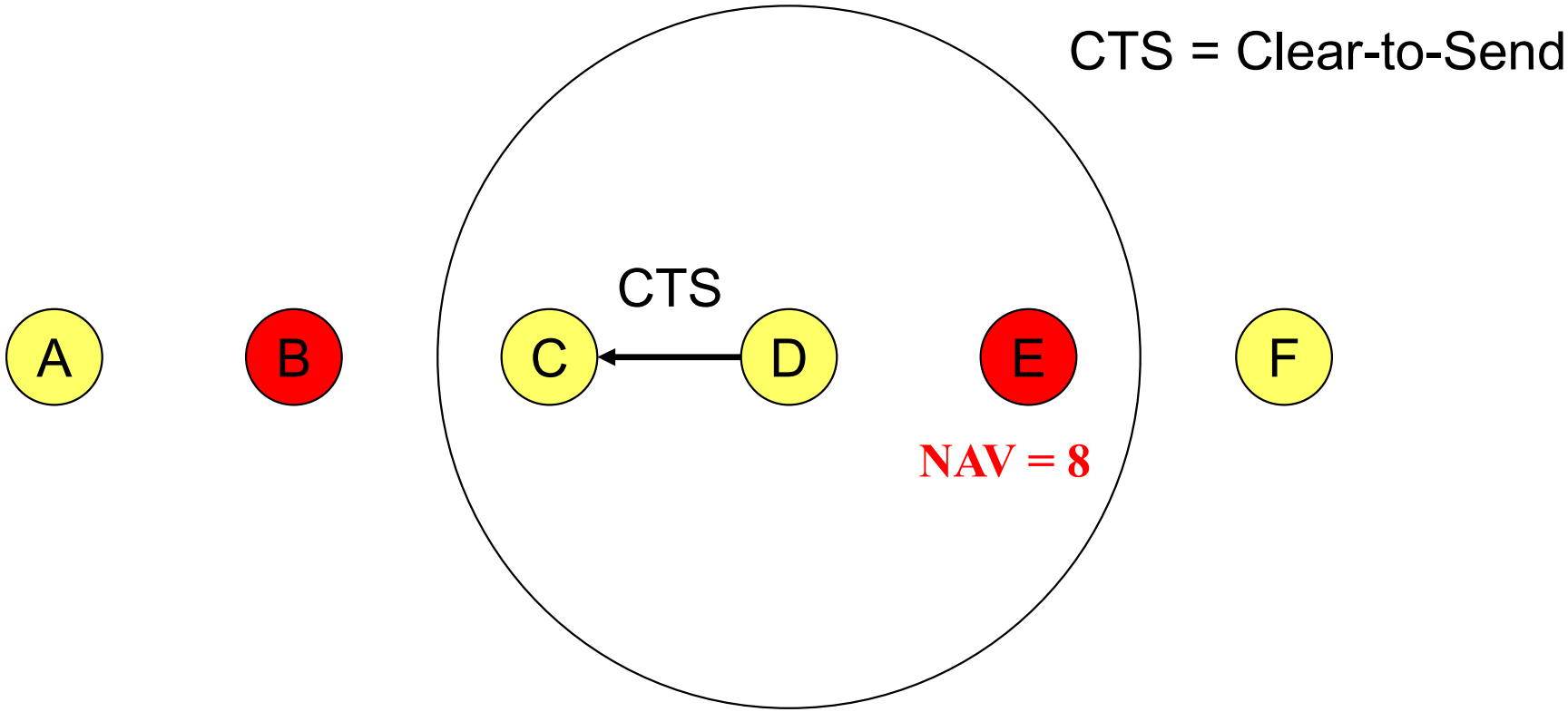


NAV = remaining duration to keep quiet

IEEE 802.11

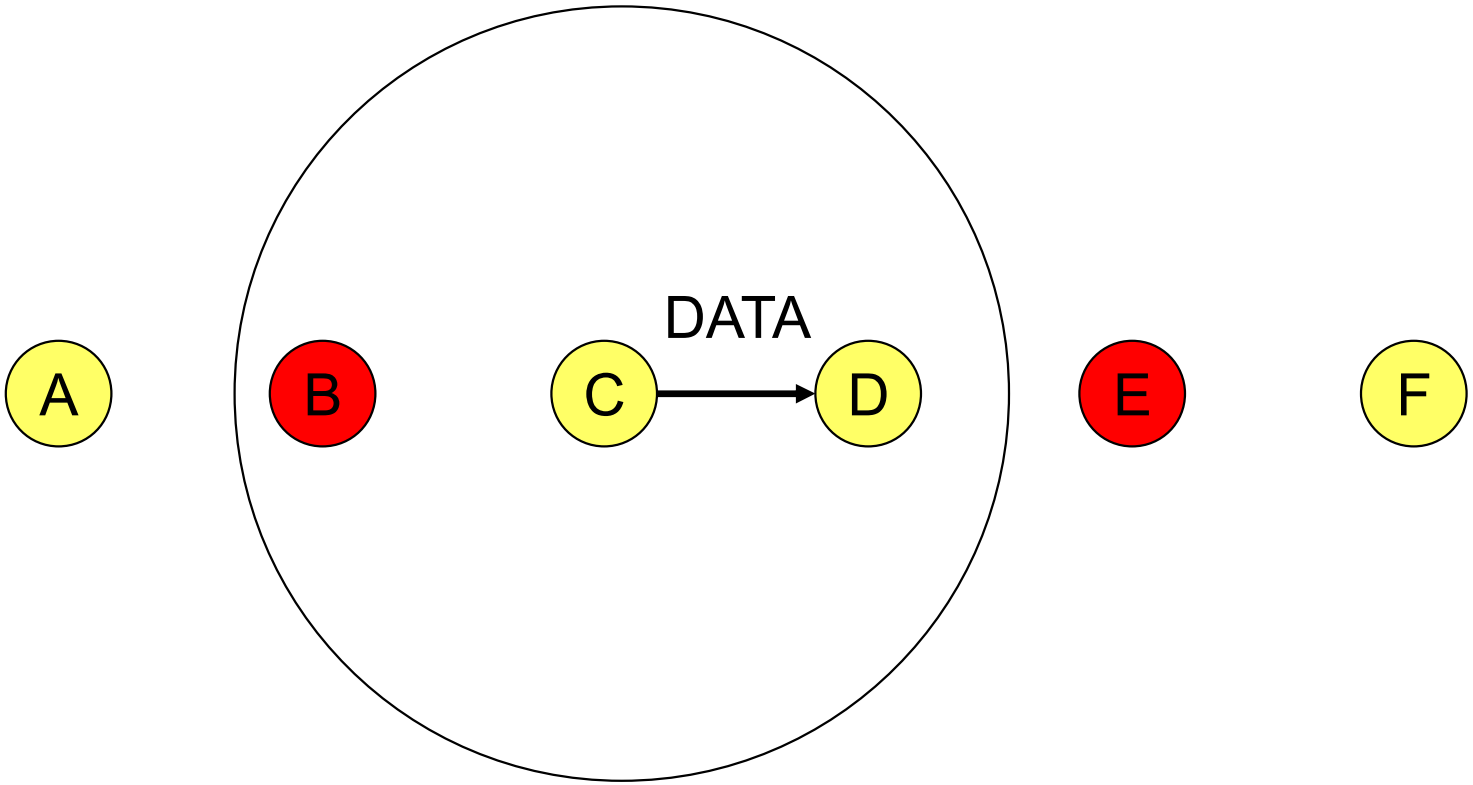


IEEE 802.11



IEEE 802.11

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



Why do we need virtual carrier sense?

- Which nodes defer to which transmissions and why?
- RTS/CTS optional

CSMA/CA

- Collision avoidance
  - Nodes hearing RTS or CTS stay silent for the duration of the corresponding transmission.
  - Once channel becomes idle, the node waits for a randomly chosen duration before attempting to transmit.

Reliability

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

- How to provide reliability?

Reliability

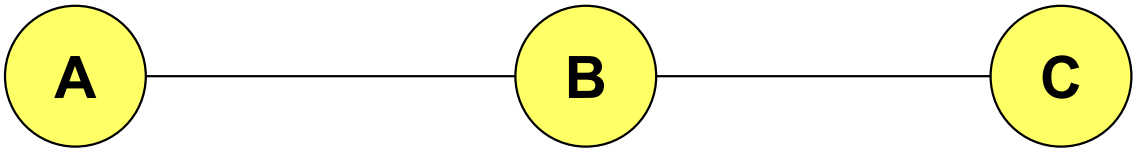
- Wireless links are prone to errors. High packet loss rate detrimental to transport-layer performance.

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

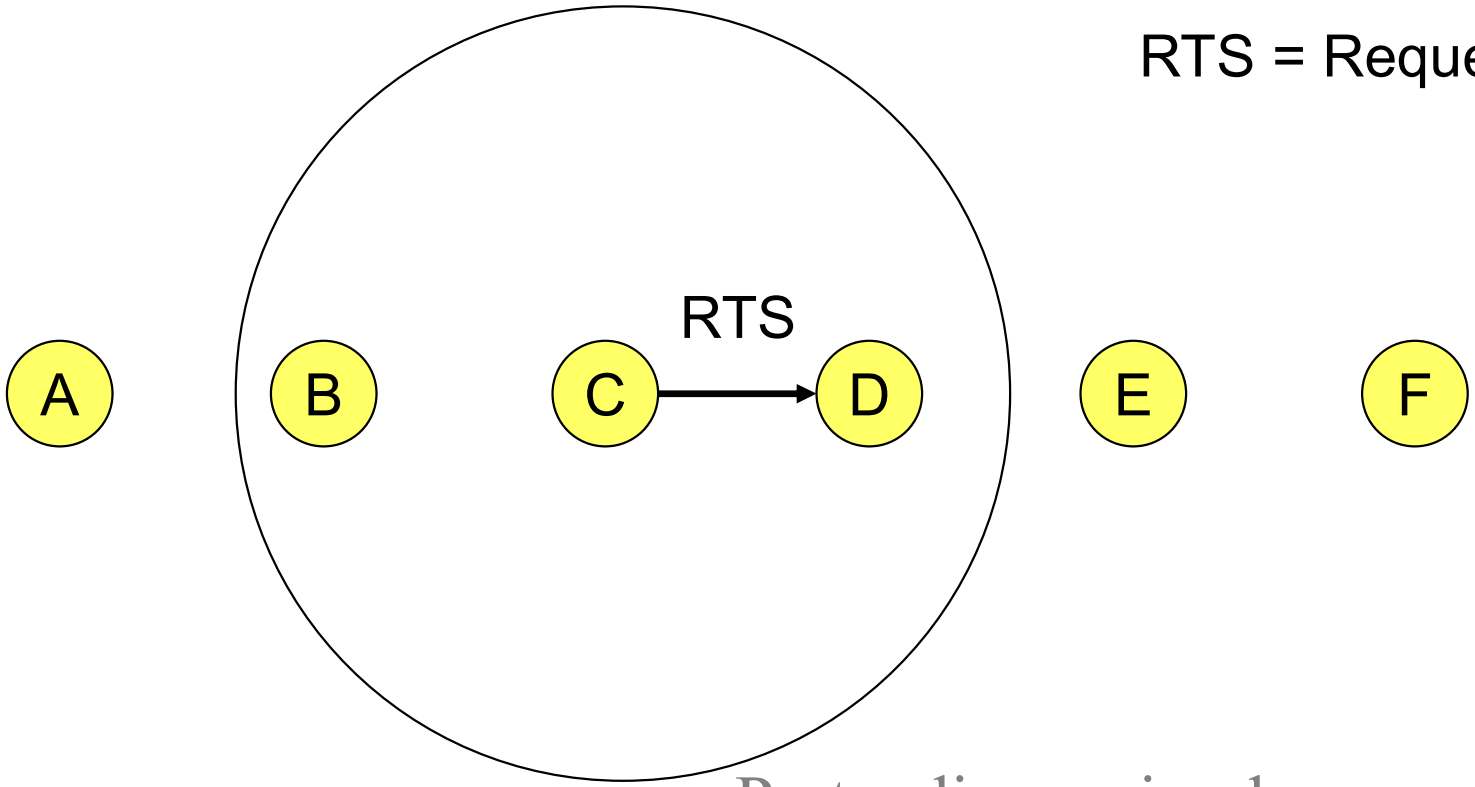
A Simple Solution to Improve Reliability

- 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

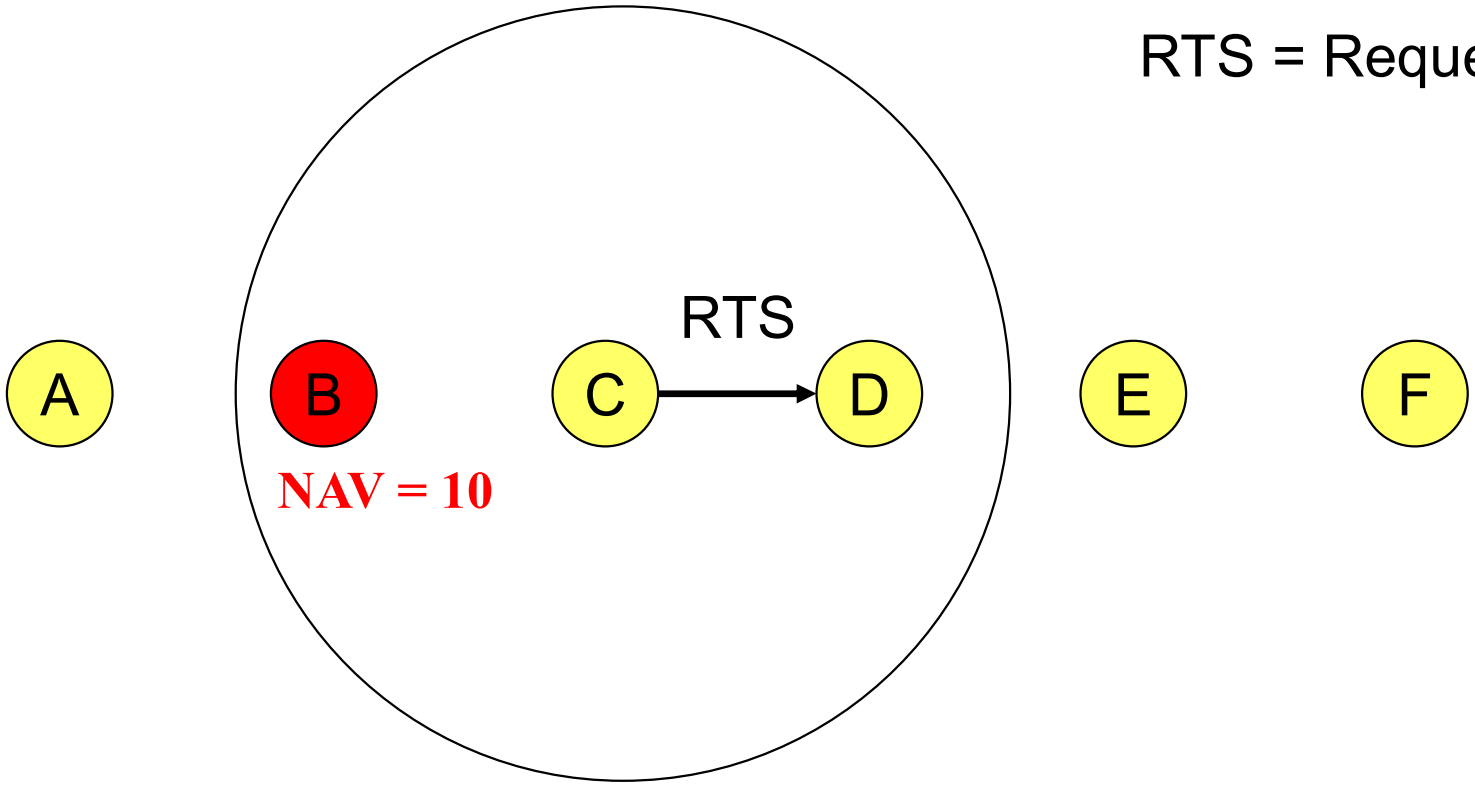


IEEE 802.11



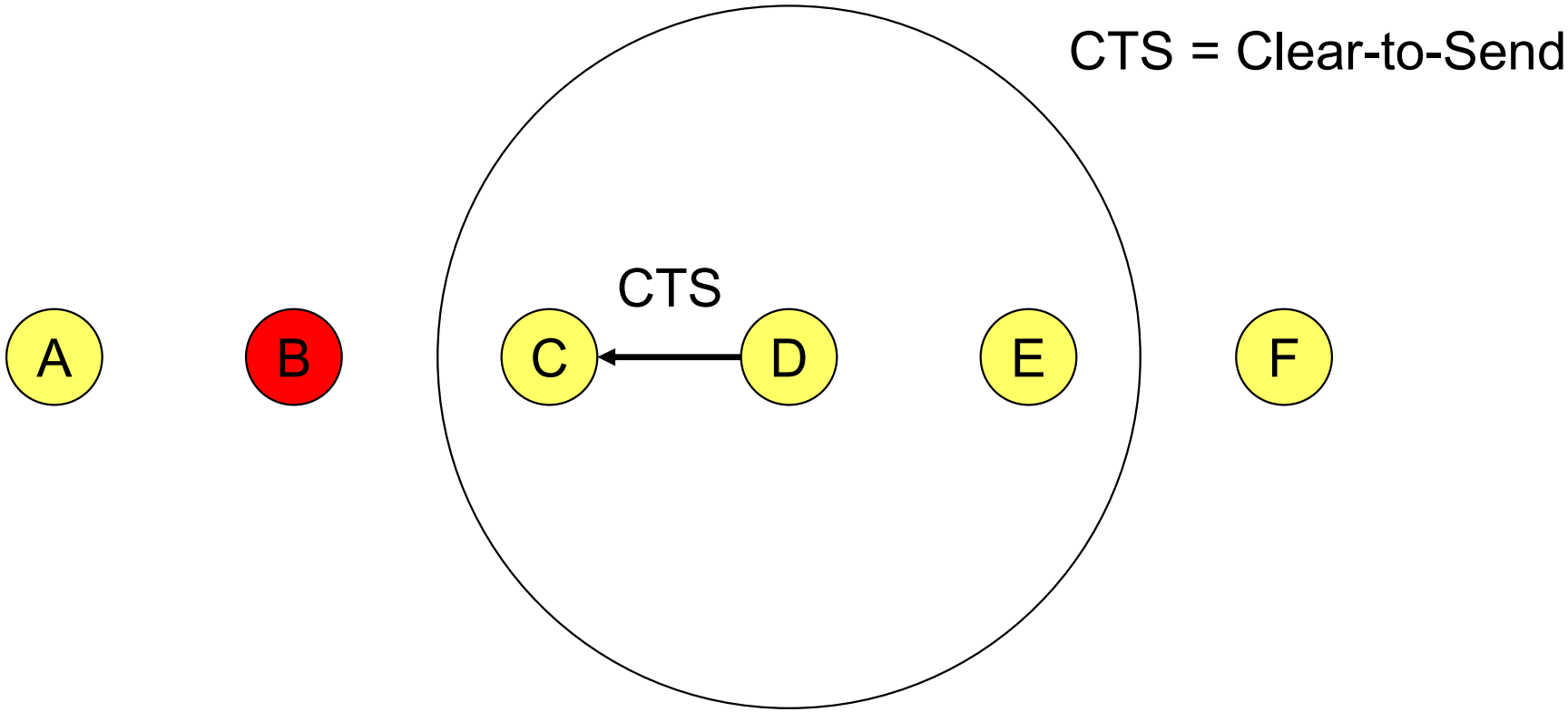
Pretending a circular range

IEEE 802.11

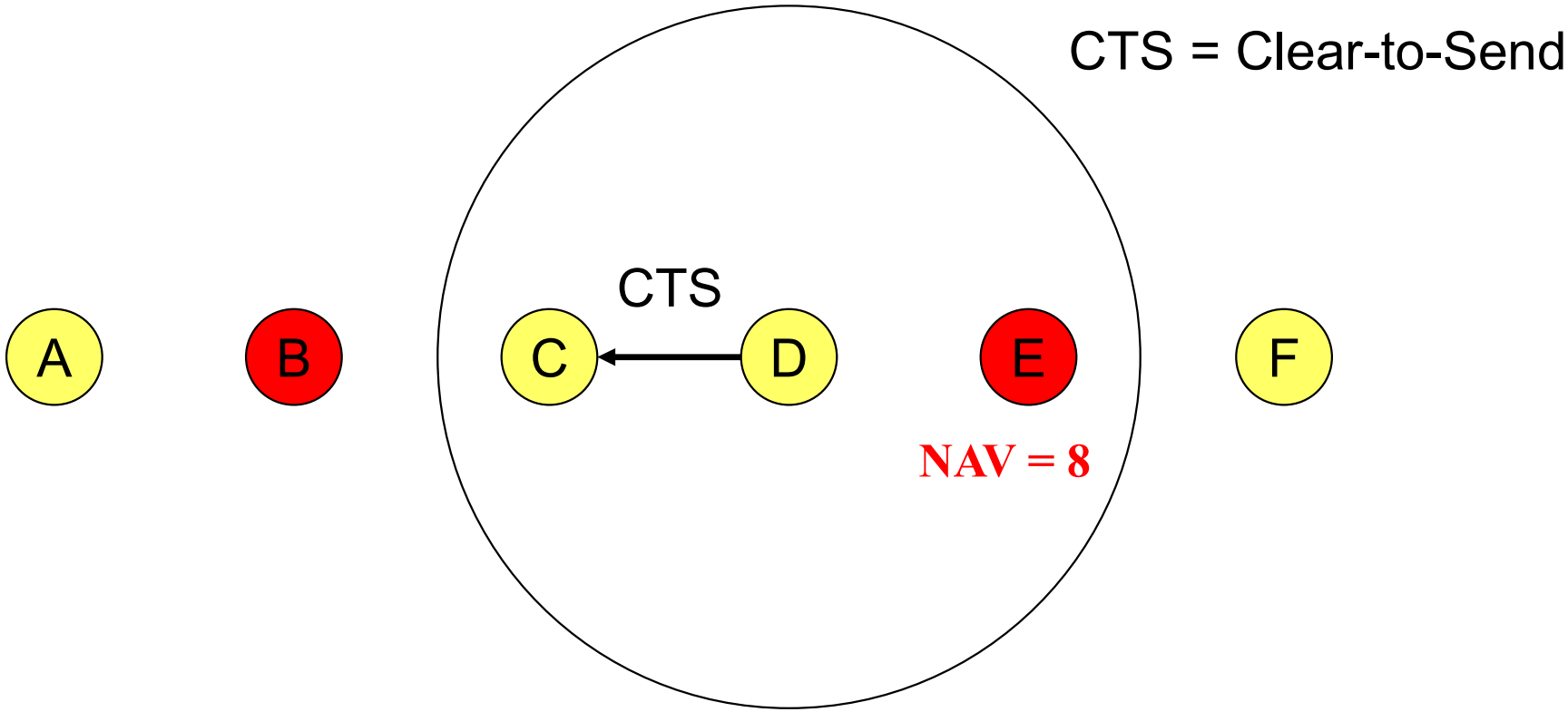


NAV = remaining duration to keep quiet

IEEE 802.11

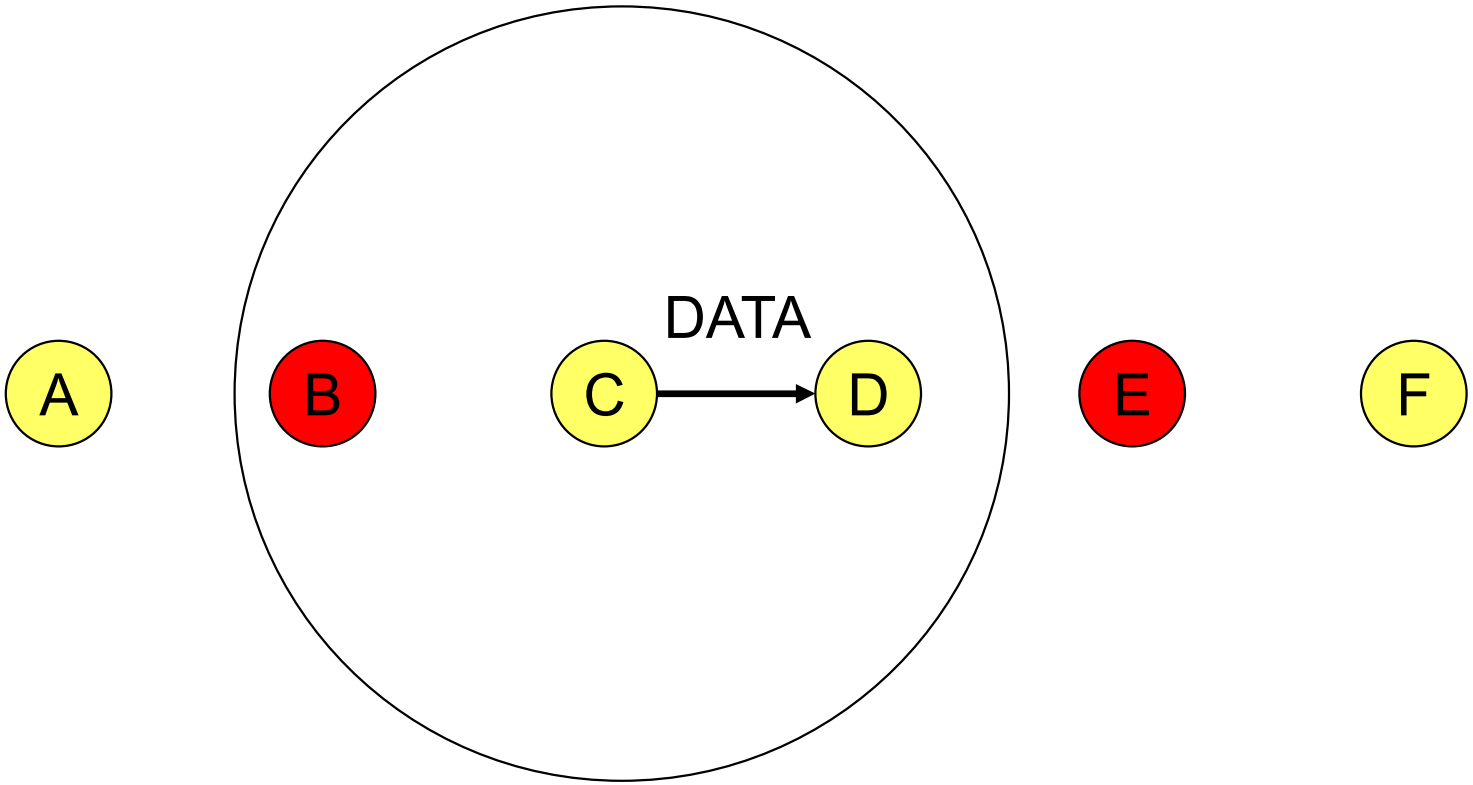


IEEE 802.11

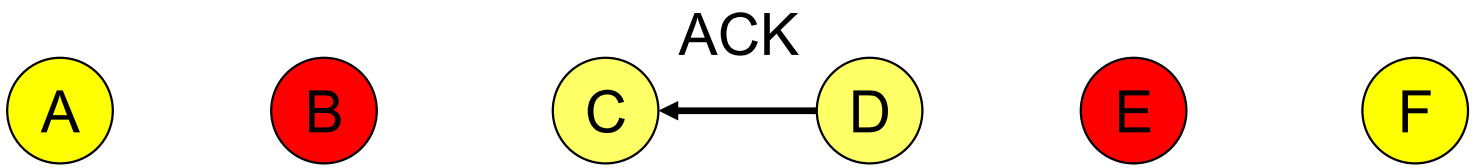


IEEE 802.11

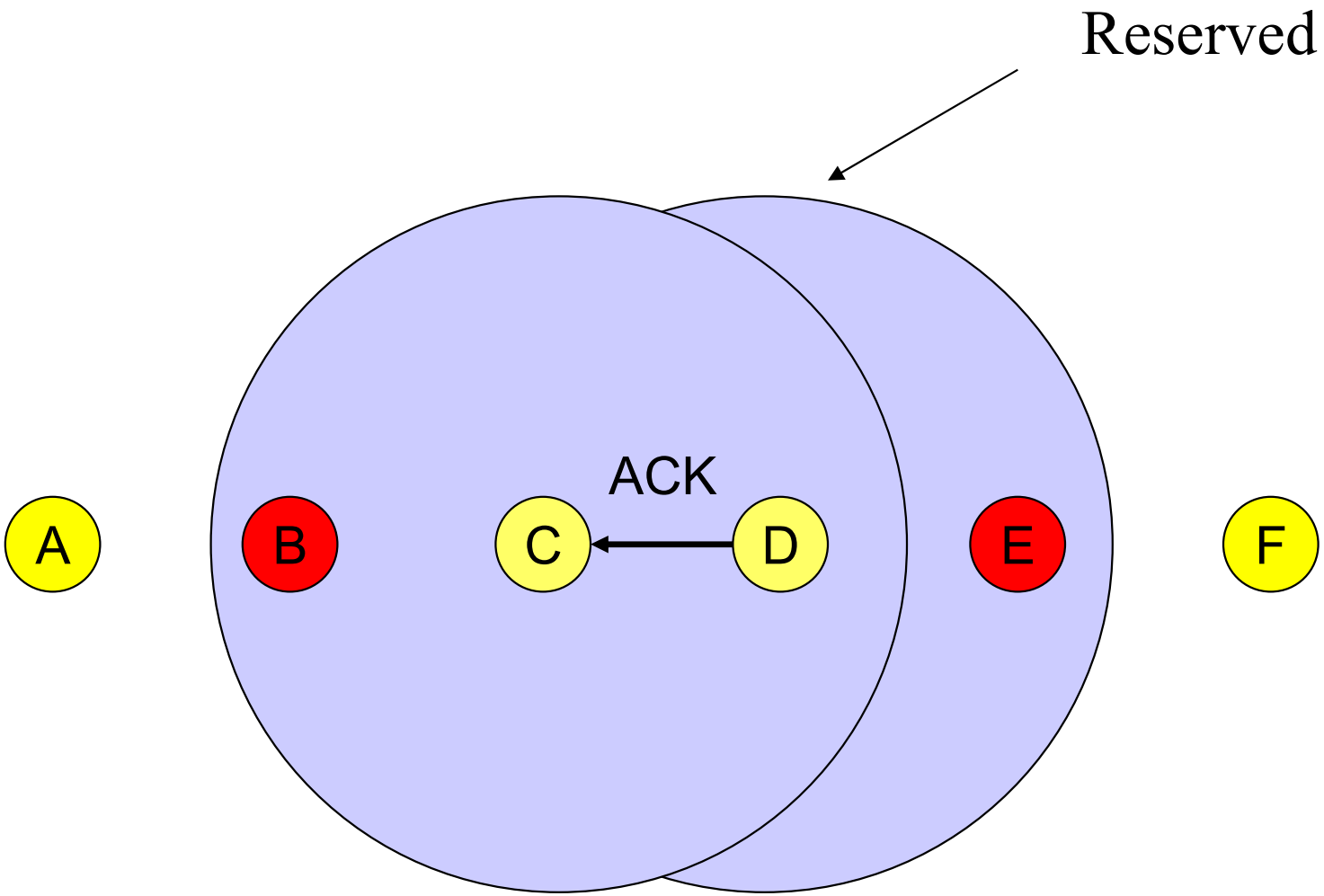
•DATA packet follows CTS. Successful data reception acknowledged using ACK.



IEEE 802.11

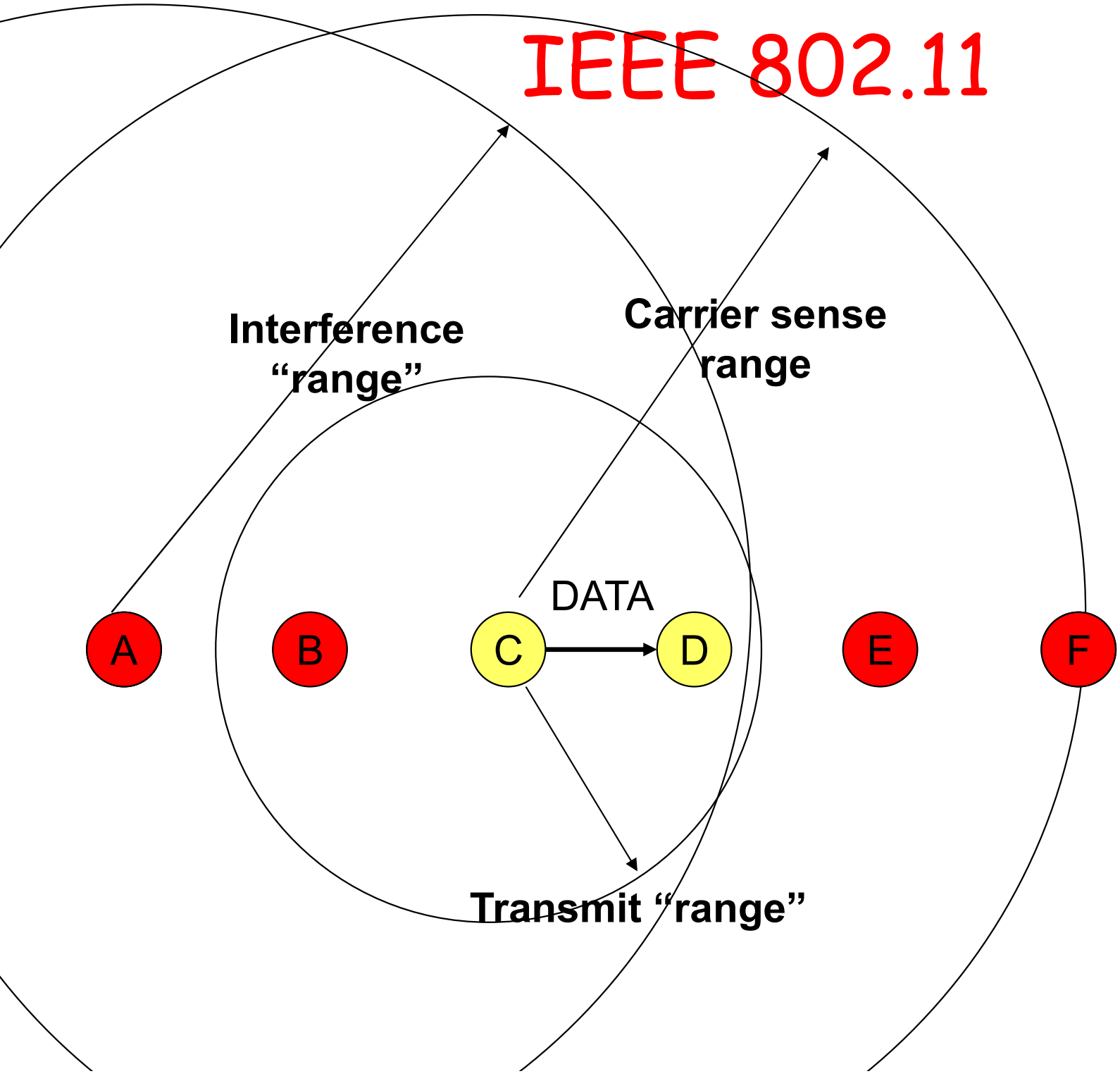


IEEE 802.11



Can RTS/CTS completely eliminate hidden terminals?

IEEE 802.11


Interference
“range”
Carrier sense
range
DATA
A
B
C
D
E
F
Transmit “range”

Review

- What is CSMA?
- What MAC protocol does Ethernet use?
- Is 802.11 a MAC protocol or PHY protocol?
- Why is collision detection hard in wireless networks?
- What MAC protocol does 802.11 use?
- How does carrier sense work in 802.11?
- What is a hidden terminal?
- How to address hidden terminal? What is the cost of this solution?

Can we send whenever carrier sense says the medium is idle?

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

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

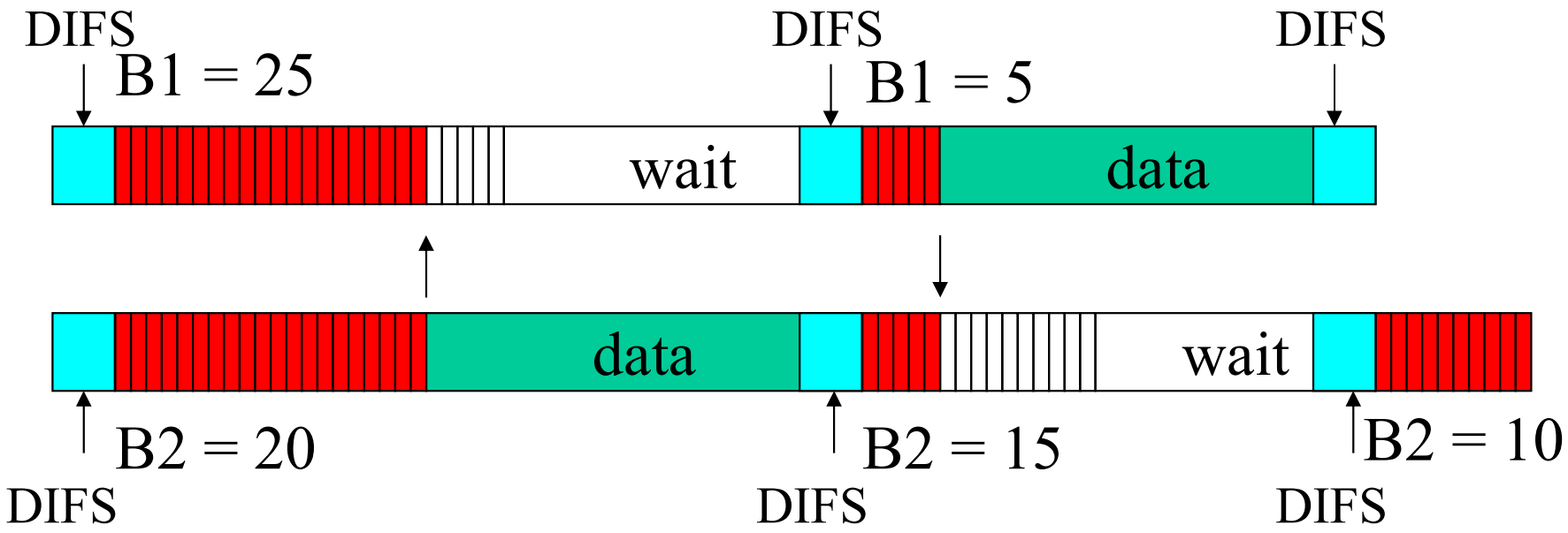
- IEEE 802.11 DCF: contention window *CW* is chosen dynamically depending on collision occurrence

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}

DCF Example



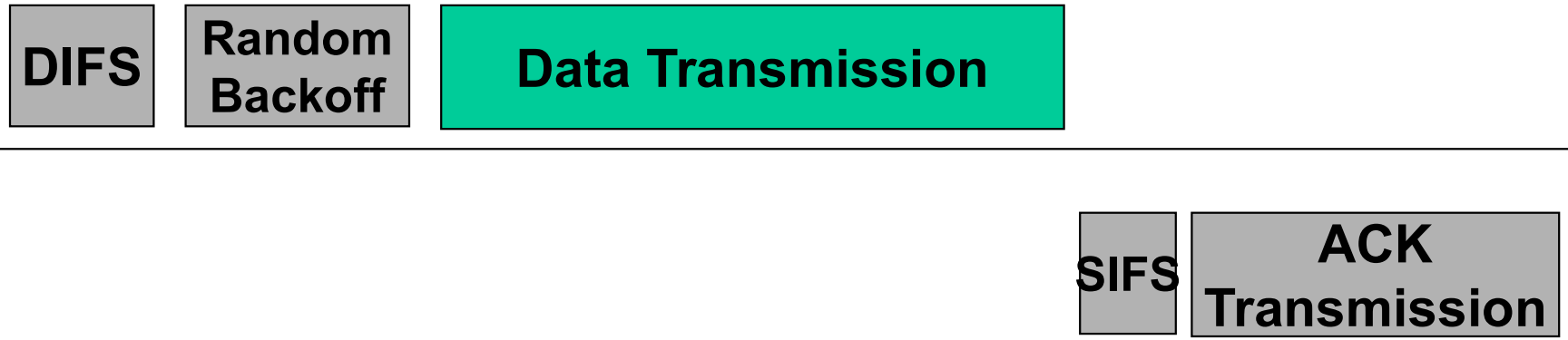
cw = 31

B1 and B2 are backoff intervals at nodes 1 and 2

MILD Algorithm in MACAW

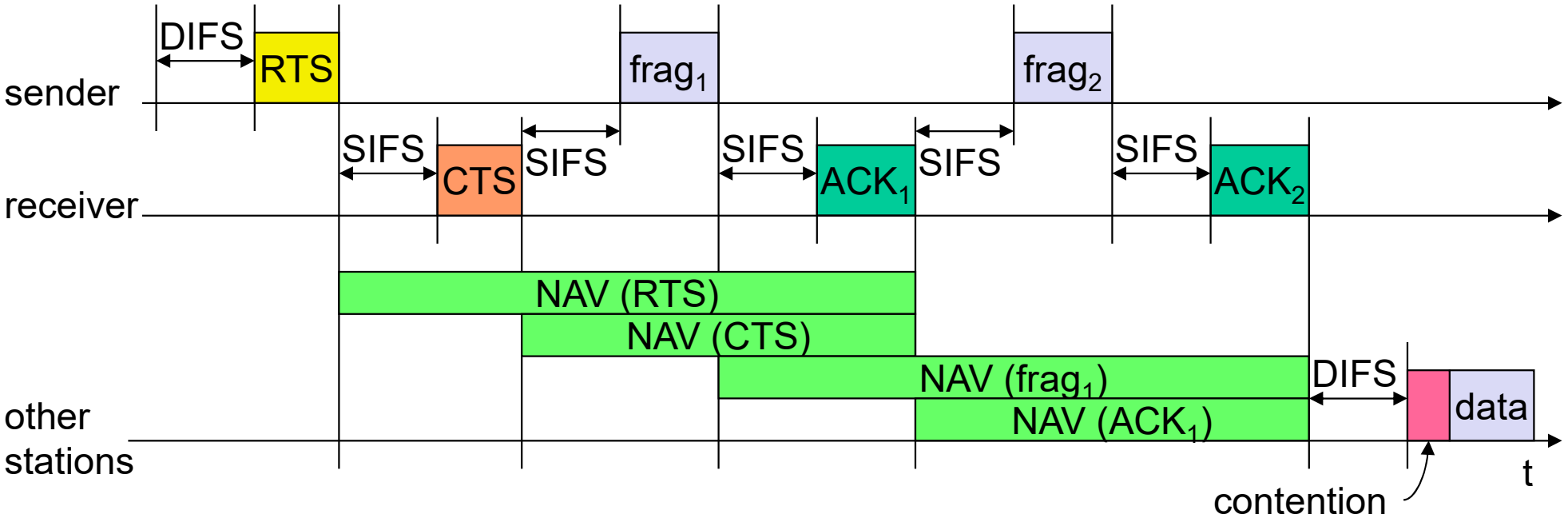
- MACAW uses exponential increase linear decrease to update CW
  - When a node successfully completes a transfer, reduces CW by 1
  - In 802.11, CW is restored to CW_{min}
  - In 802.11, CW reduces much faster than it increases
- MACAW can avoid wild oscillations of CW when many nodes contend for the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

802.11 Overhead

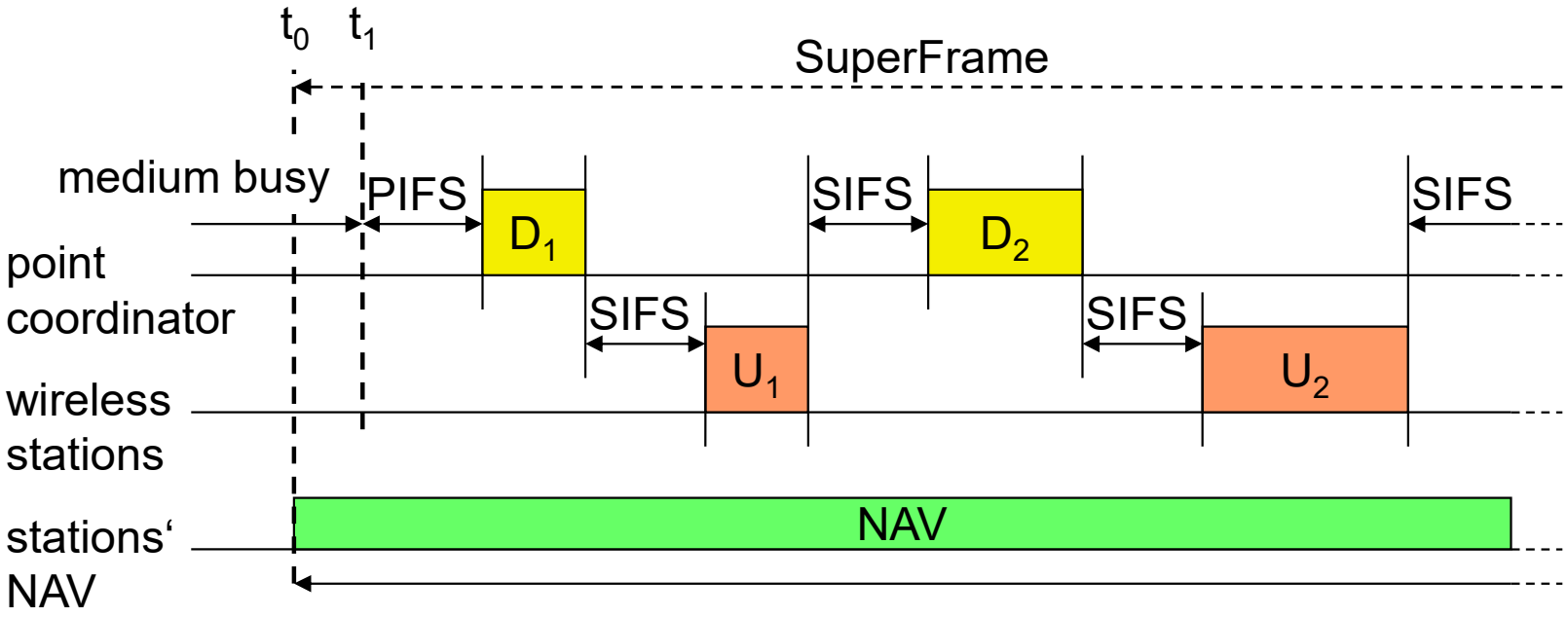


- Overhead:
  - DIFS
  - Random backoff
  - ACK/SIFS
  - Optional RTS/CTS handshake before transmission of data packet (often disabled due to its overhead)
  - Header overhead
- 802.11 has room for improvement. How?

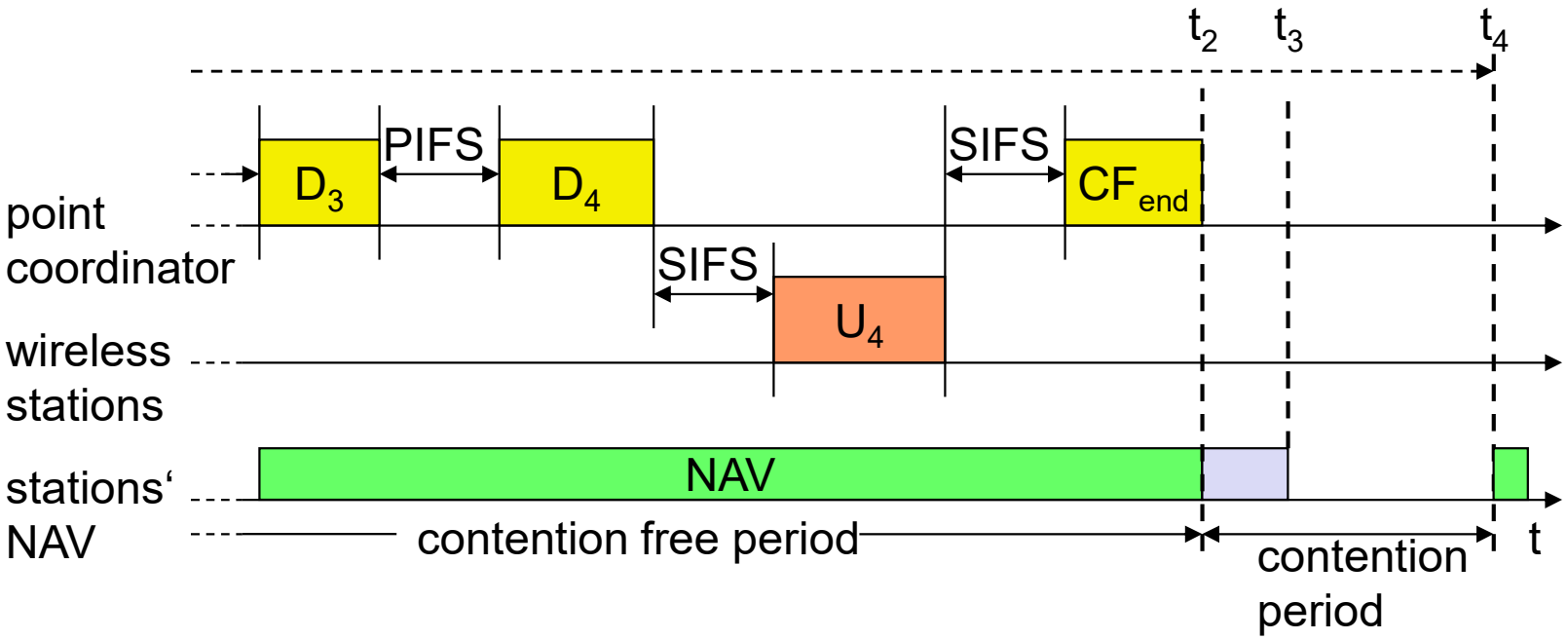
Fragmentation



DFWMAC-PCF I

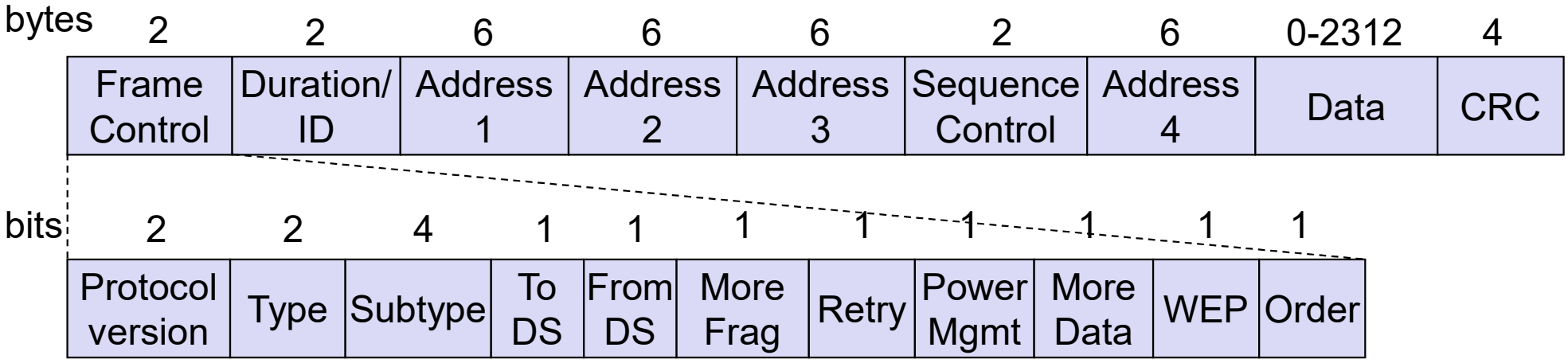

t0
t1
SuperFrame
medium busy
PIFS
D1
SIFS
D2
SIFS
point coordinator
SIFS
U1
SIFS
U2
wireless stations
NAV
stations' NAV

DFWMAC-PCF II



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



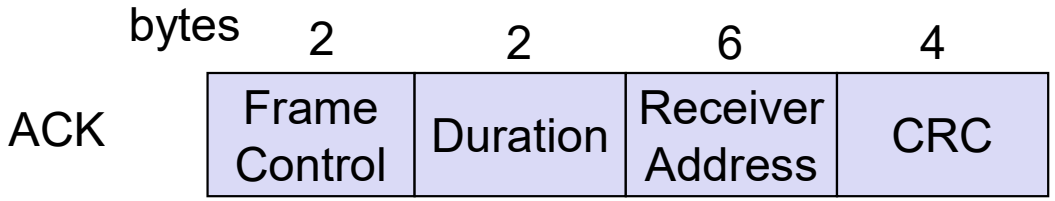
MAC address format

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

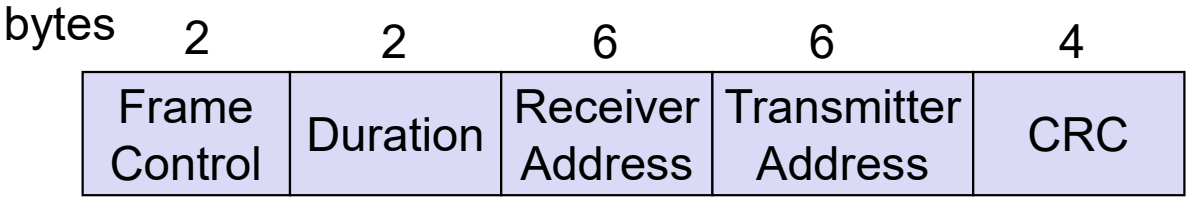
DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Basic Service Set Identifier
RA: Receiver Address
TA: Transmitter Address

Special Frames: ACK, RTS, CTS

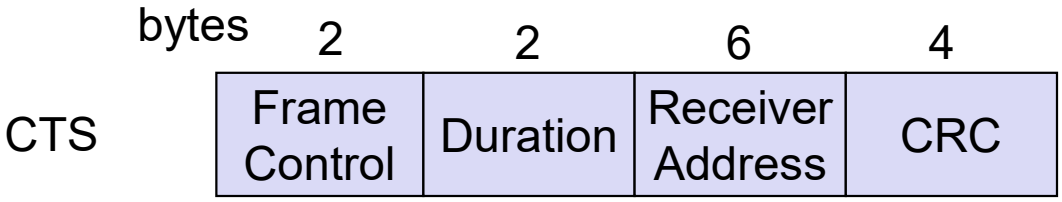
- Acknowledgement



- 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
  - scanning, i.e. active search for a network
  - integration into a LAN
  - roaming, i.e. change networks by changing access points
- Synchronization
  - timing
- Power management
  - sleep-mode without missing a message
  - periodic sleep, frame buffering, traffic measurements
- MIB - Management Information Base
  - managing, read, write

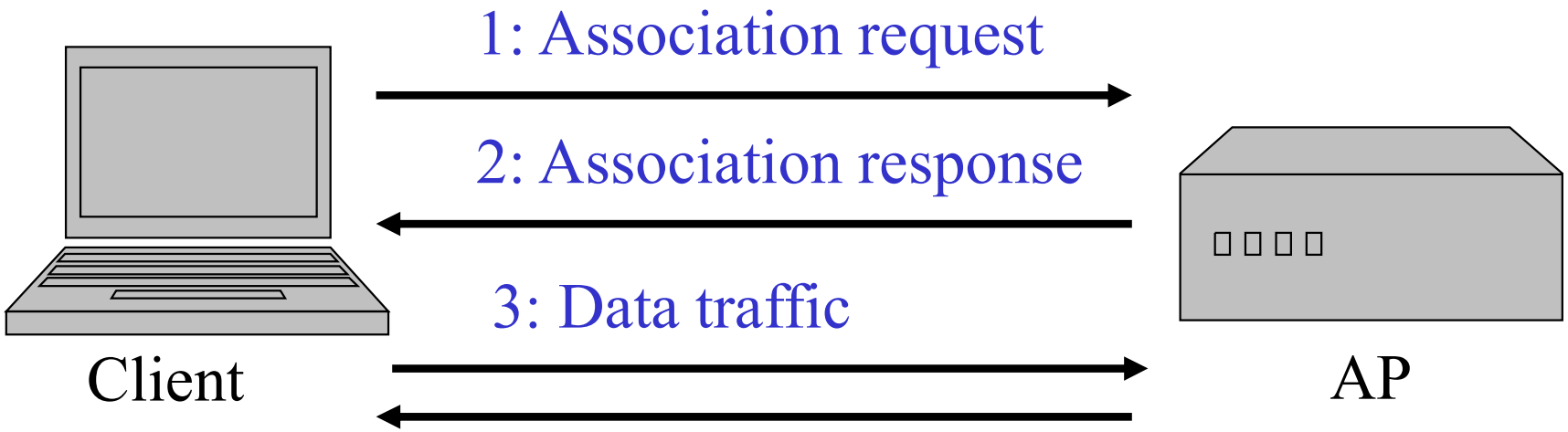
Association and Reassociation

- 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
  - Don't require transmissions
  - Move to each channel, and listen for Beacon frames
- Active scanning
  - Require transmissions
  - Move to each channel, and send Probe Request frames to solicit Probe Responses from a network

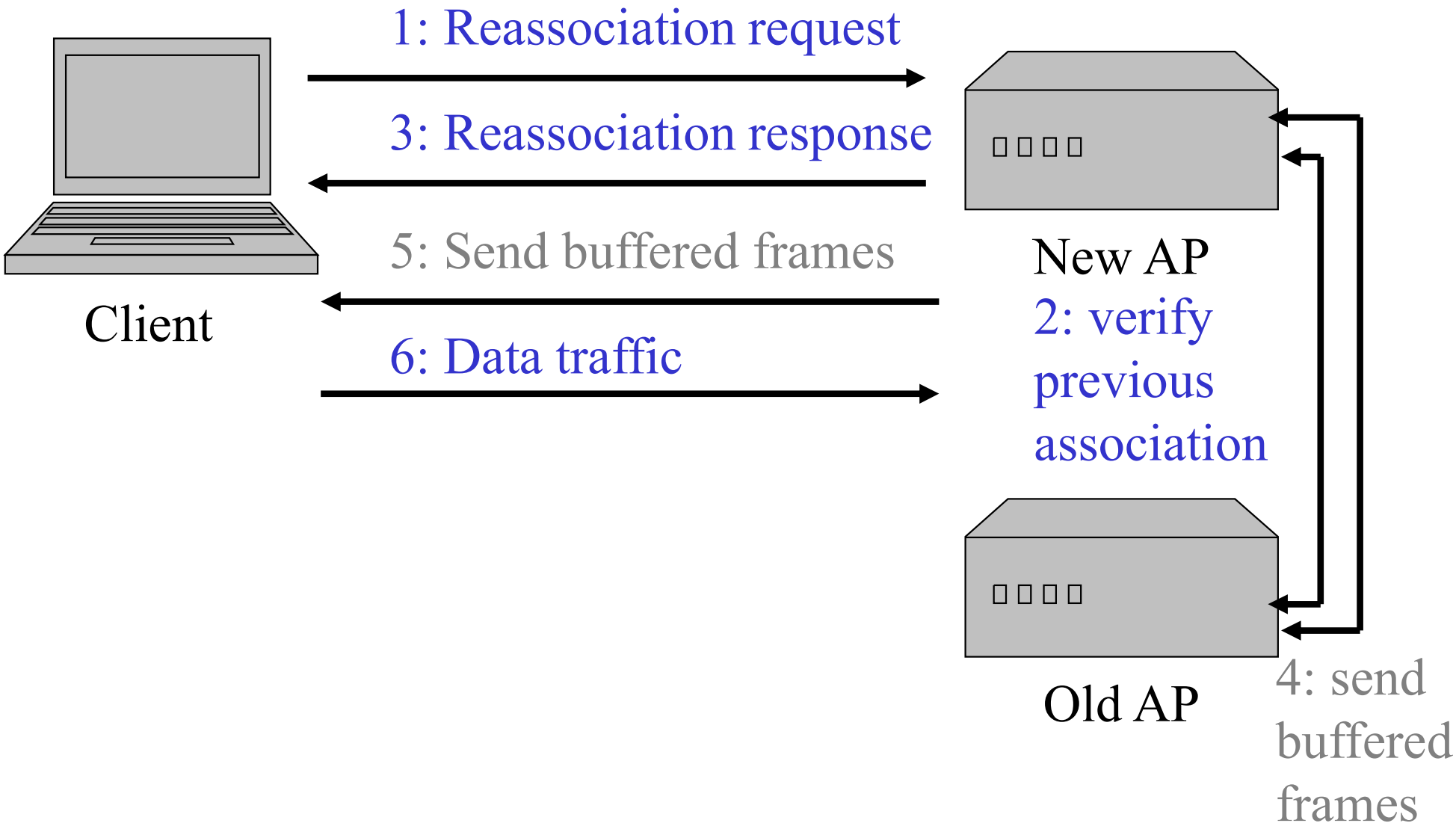
Association in 802.11



802.11 - Roaming

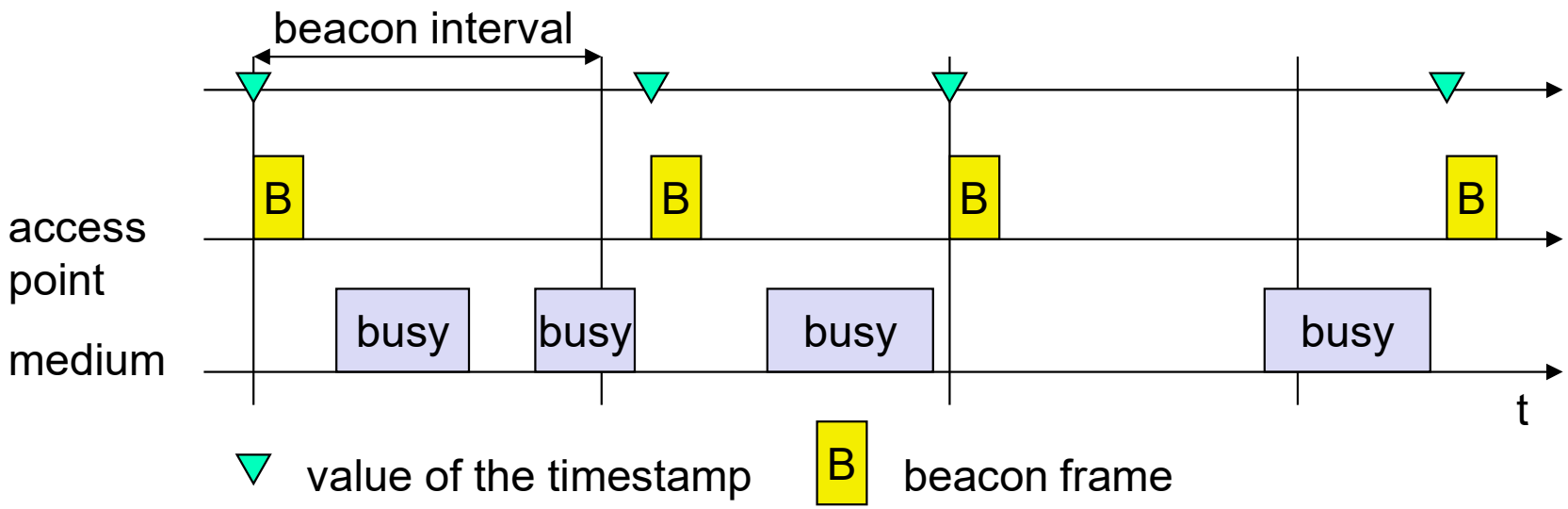
- No or bad connection? Then perform:
- Scanning
  - scan the environment, i.e., listen to the medium for beacon signals or send probes to the medium and wait for an answer
- Reassociation Request
  - station sends a request to one or several AP(s)
- Reassociation Response
  - success: AP has answered, station can now participate
  - failure: continue scanning
- AP accepts Reassociation Request
  - signal the new station to the distribution system
  - the distribution system updates its database (i.e., location information)
  - typically, the distribution system now informs the old AP so it can release resources

Reassociation in 802.11

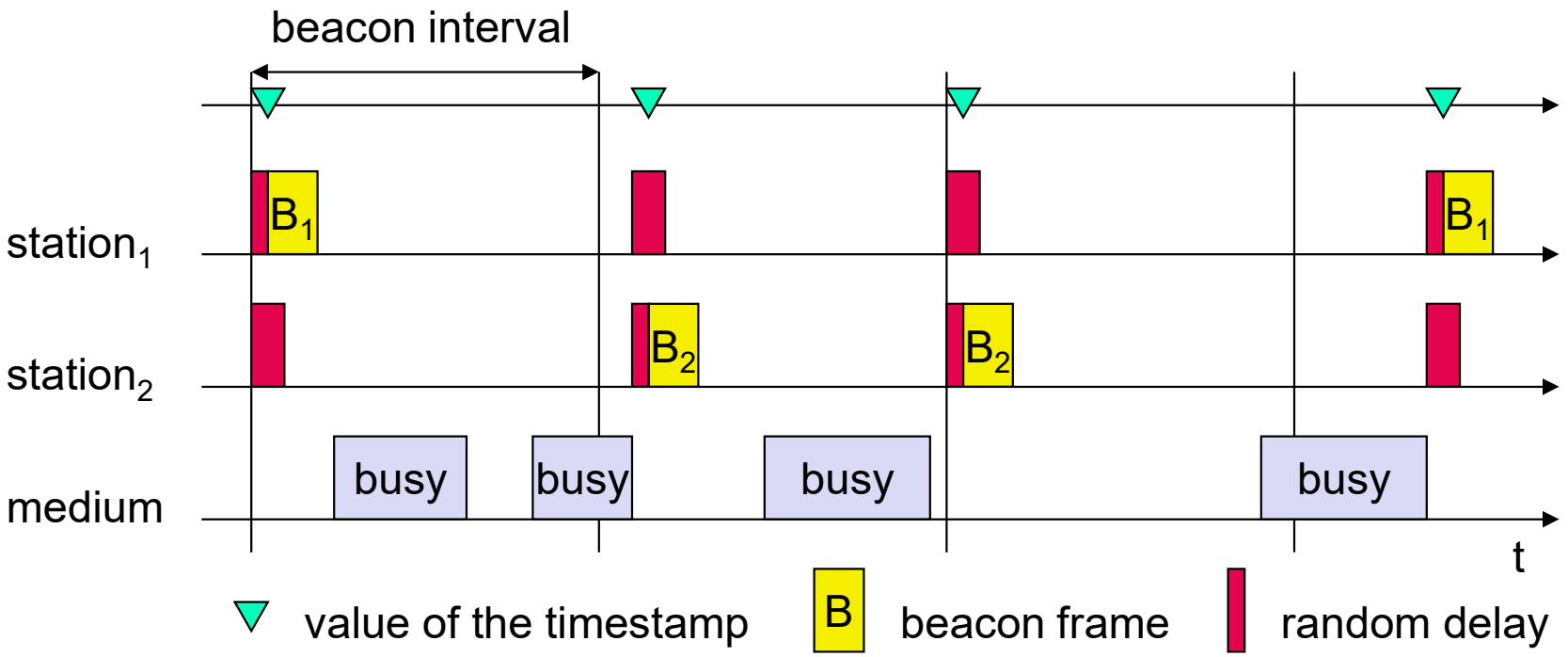


Synchronization using a Beacon (infrastructure)

Synchronization using a Beacon (infrastructure)



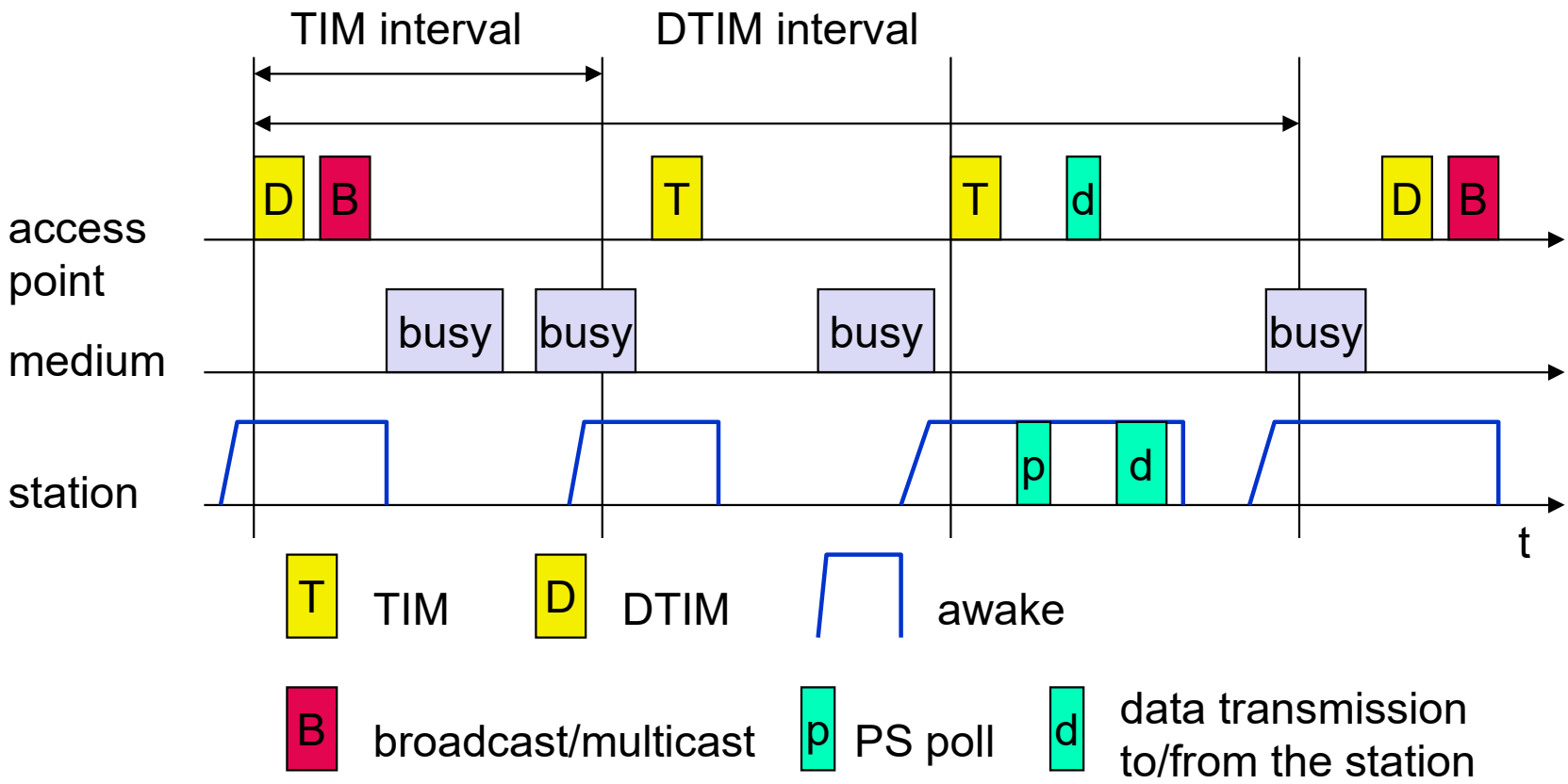
Synchronization using a Beacon (ad-hoc)



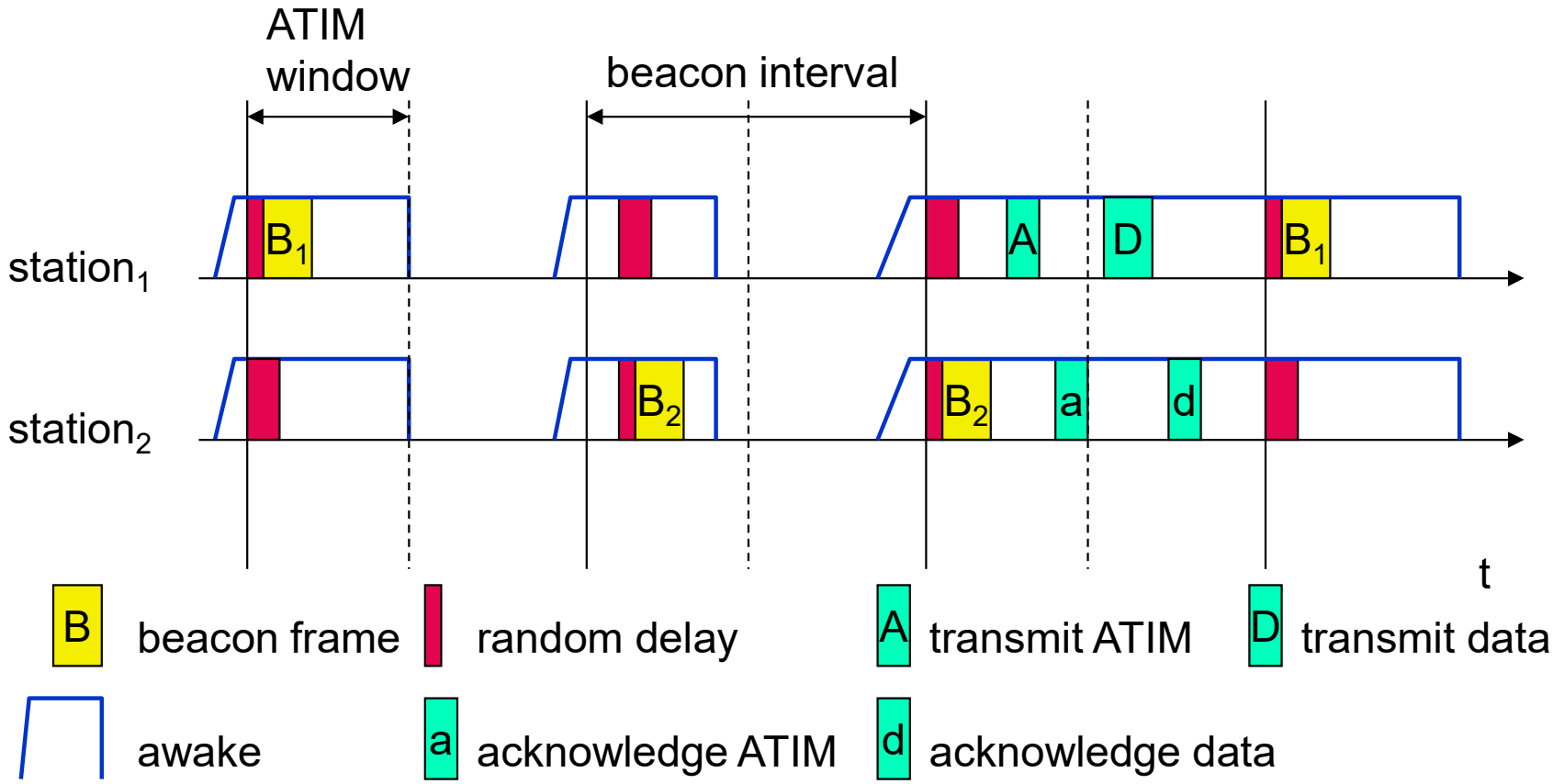
Power management

- 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
    - collision of ATIMs possible (scalability?)

Power saving with wake-up patterns (infrastructure)



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



IEEE 802.11 further 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

IEEE 802.11 further 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
- 802.11g: Data Rates > 20 Mbit/s at 2.4 GHz; 54 Mbit/s, OFDM
  - Successful successor of 802.11b, performance loss during mixed operation with 11b
- 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)

IEEE 802.11 further developments

- 802.11p: Vehicular networks
- 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/

Review

- How does a station associate with an AP?
- How does nodes synchronize?
- How do we prevent a sleeping node from losing its data?