Wireless LANs (IEEE802.1)

Guevara Noubir

Northeastern University

noubir@ccs.neu.edu

Slides partially from "Mobile Communications" by J. Schiller Chapter 7.

Outline

- Wireless LAN Technology
- Medium Access Control for Wireless
- IEEE802.11

Wireless LAN Applications

- LAN Extension
- Cross-building interconnect
- Nomadic Access
- Ad hoc networking

LAN Extension

- Wireless LAN linked into a wired LAN on same premises
  - Wired LAN
    - Backbone
    - Support servers and stationary workstations
  - Wireless LAN
    - Stations in large open areas
    - Manufacturing plants, stock exchange trading floors, and warehouses

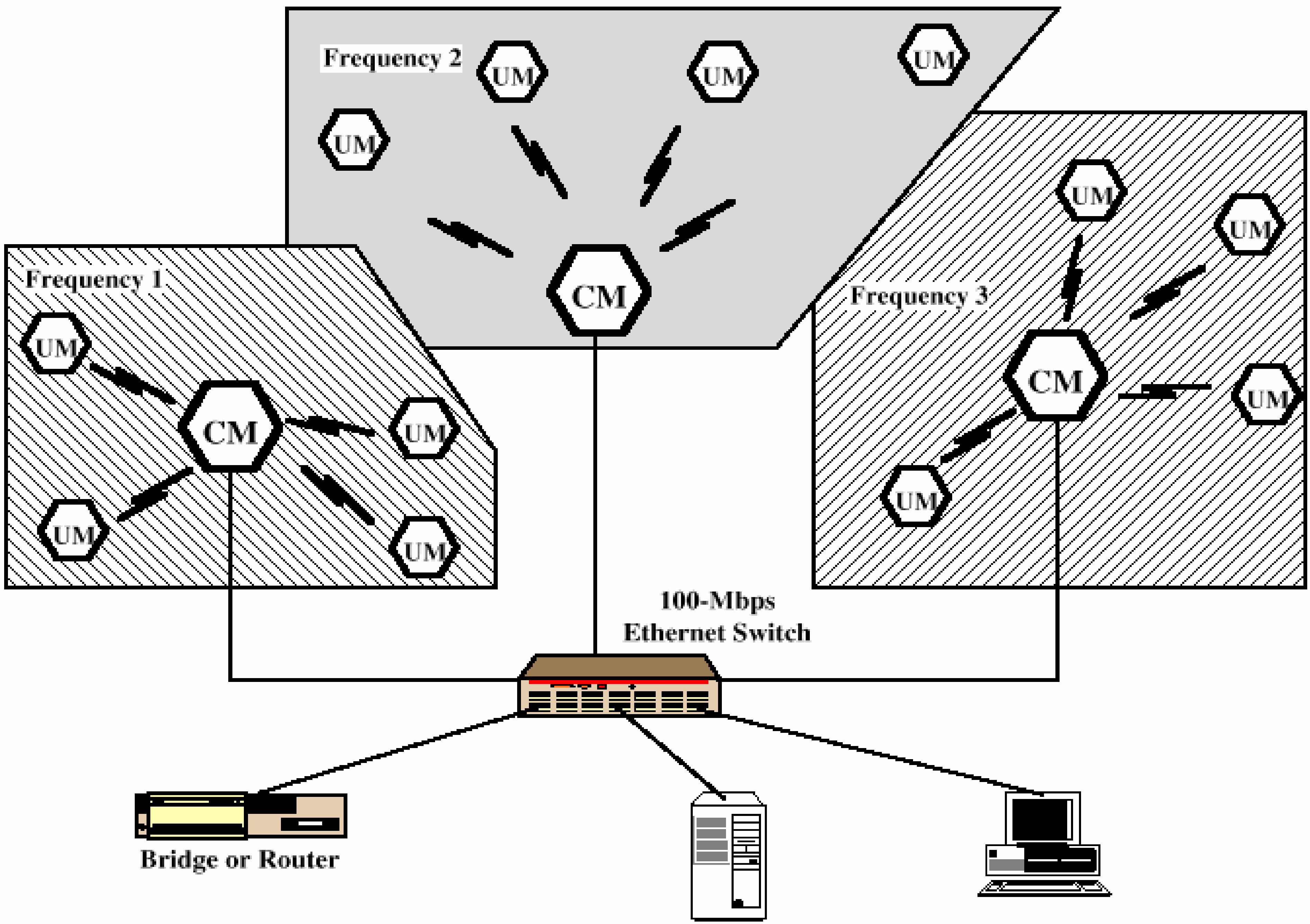


Figure 13.2 Example Multiple-Cell Wireless LAN Configuration

Cross-Building Interconnect

- Connect LANs in nearby buildings
  - Wired or wireless LANs
- Point-to-point wireless link is used
- Devices connected are typically bridges or routers

Nomadic Access

- Wireless link between LAN hub and mobile data terminal equipped with antenna
  - Laptop computer or notepad computer
- Uses:
  - Transfer data from portable computer to office server
  - Extended environment such as campus

Ad Hoc Networking

- Temporary peer-to-peer network set up to meet immediate need
- Example:
  - Group of employees with laptops convene for a meeting; employees link computers in a temporary network for duration of meeting

Wireless LAN Requirements

- Throughput
- Number of nodes
- Connection to backbone LAN
- Service area
- Battery power consumption
- Transmission robustness and security
- Collocated network operation
- License-free operation
- Handoff/roaming
- Dynamic configuration

Wireless LAN Categories

- Infrared (IR) LANs
- Spread spectrum LANs
- Narrowband microwave

Strengths of Infrared Over Microwave Radio

- Spectrum for infrared virtually unlimited
  - Possibility of high data rates
- Infrared spectrum unregulated
- Equipment inexpensive and simple
- Reflected by light-colored objects
  - Ceiling reflection for entire room coverage
- Doesn’t penetrate walls
  - More easily secured against eavesdropping
  - Less interference between different rooms

Drawbacks of Infrared Medium

- Indoor environments experience infrared background radiation
  - Sunlight and indoor lighting
  - Ambient radiation appears as noise in an infrared receiver
  - Transmitters of higher power required
    - Limited by concerns of eye safety and excessive power consumption
  - Limits range

IR Data Transmission Techniques

- Directed Beam Infrared
- Ominidirectional
- Diffused

Directed Beam Infrared

- Used to create point-to-point links
- Range depends on emitted power and degree of focusing
- Focused IR data link can have range of kilometers
  - Cross-building interconnect between bridges or routers

Ominidirectional

- Single base station within line of sight of all other stations on LAN
- Station typically mounted on ceiling
- Base station acts as a multiport repeater
  - Ceiling transmitter broadcasts signal received by IR transceivers
  - IR transceivers transmit with directional beam aimed at ceiling base unit

Diffused

- All IR transmitters focused and aimed at a point on diffusely reflecting ceiling
- IR radiation strikes ceiling
  - Reradiated omnidirectionally
  - Picked up by all receivers

Spread Spectrum LAN Configuration

- Multiple-cell arrangement
- Within a cell, either peer-to-peer or hub
- Peer-to-peer topology
  - No hub
  - Access controlled with MAC algorithm
    - CSMA
  - Appropriate for ad hoc LANs

Spread Spectrum LAN Configuration

- Hub topology
  - Mounted on the ceiling and connected to backbone
  - May control access
  - May act as multiport repeater
  - Automatic handoff of mobile stations
  - Stations in cell either:
    - Transmit to / receive from hub only
    - Broadcast using omnidirectional antenna

Narrowband Microwave LANs

- Use of a microwave radio frequency band for signal transmission
- Relatively narrow bandwidth
- Licensed
- Unlicensed

Licensed Narrowband RF

- Licensed within specific geographic areas to avoid potential interference
- Motorola - 600 licenses in 18-GHz range
  - Covers all metropolitan areas
  - Can assure that independent LANs in nearby locations don’t interfere
  - Encrypted transmissions prevent eavesdropping

Unlicensed Narrowband RF

- RadioLAN introduced narrowband wireless LAN in 1995
  - Uses unlicensed ISM spectrum
  - Used at low power (0.5 watts or less)
  - Operates at 10 Mbps in the 5.8-GHz band
  - Range = 50 m to 100 m

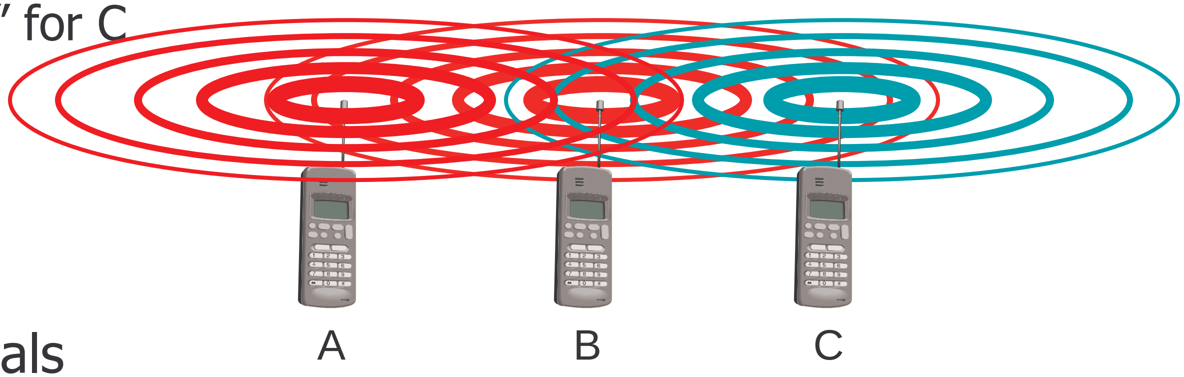
Motivation for Wireless MAC

- 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 as soon as the medium is free, listen into the medium if a collision occurs (original method in IEEE 802.3)
- Problems in wireless networks
  - signal strength decreases proportional to the square of the distance
  - the sender would apply CS and CD, but the collisions happen at the receiver
  - it might be the case that a sender cannot "hear" the collision, i.e., CD does not work
  - furthermore, CS might not work if, e.g., a terminal is "hidden"

Motivation - hidden and exposed terminals

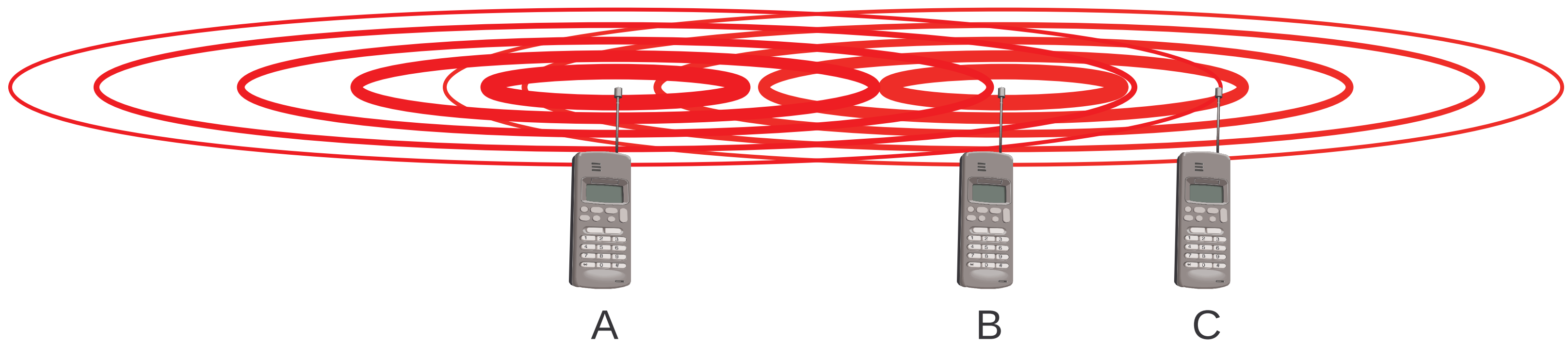
- Hidden terminals
  - A sends to B, C cannot receive A
  - C wants to send to B, C senses a "free" medium (CS fails)
  - collision at B, A cannot receive the collision (CD fails)
  - A is "hidden" for C



- Exposed terminals
  - B sends to A, C wants to send to another terminal (not A or B)
  - C has to wait, CS signals a medium in use
  - but A is outside the radio range of C, therefore waiting is not necessary
  - C is "exposed" to B

Motivation - near and far terminals

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



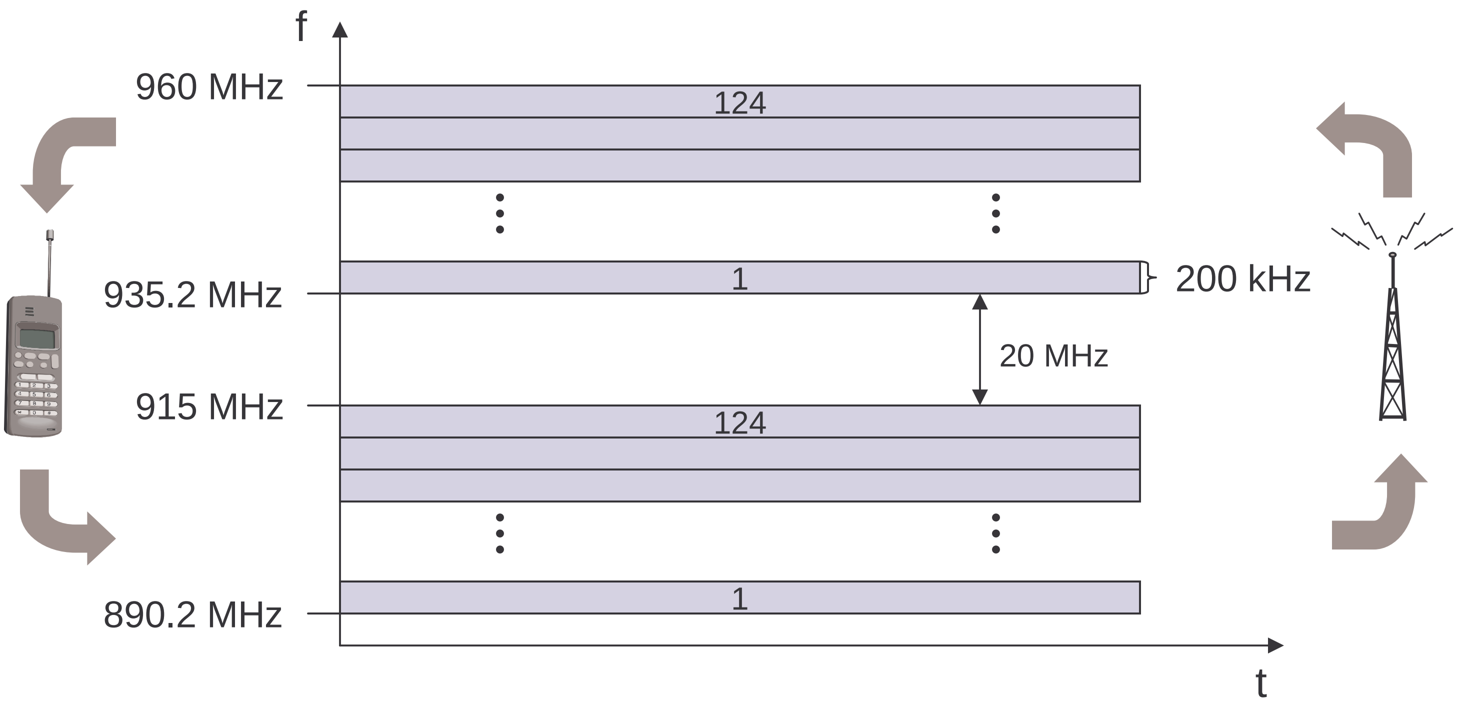
- If C for example was an arbiter for sending rights, terminal B would drown out terminal A already on the physical layer
- Also severe problem for CDMA-networks - precise power control needed!

Access methods SDMA/FDMA/TDMA

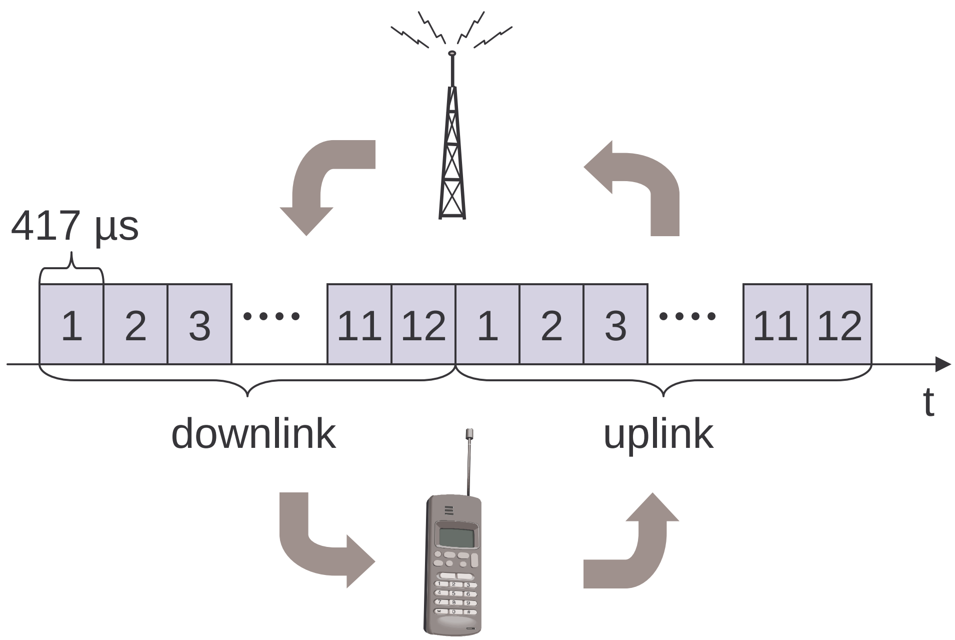
- SDMA (Space Division Multiple Access)
  - segment space into sectors, use directed antennas
  - cell structure
- FDMA (Frequency Division Multiple Access)
  - assign a certain frequency to a transmission channel between a sender and a receiver
  - permanent (e.g., radio broadcast), slow hopping (e.g., GSM), fast hopping (FHSS, Frequency Hopping Spread Spectrum)
- TDMA (Time Division Multiple Access)
  - assign the fixed sending frequency to a transmission channel between a sender and a receiver for a certain amount of time
- CDMA (Code Division Multiple Access)
  - assign a unique code to each station

- The multiplexing schemes are now used to control medium access!

FDD/FDMA - general scheme, example GSM



TDD/TDMA - general scheme, example DECT



Frequency Division Multiple Access

- Concept:
  - assign different frequency bands to different users
  - no sharing of a frequency band between two users
  - user separation using band-pass filters
  - continuous flow
  - two-way: two frequency bands or Time Division Duplex (TDD)
- Advantages: simple receivers
  - longer symbol duration: no-need for equalization
    - low inter-symbol interference
    - e.g., 50kb/s QPSK =>40 μs >> 1-10μs delay spread
- Drawbacks:
  - frequency guard bands, costly tight RF band-filters,
  - long fading duration: need slow frequency hopping
  - may need spatial diversity (multiple antennas/beam forming) Rx/Tx

Frequency Selection

- Frequency management:
  - Fixed (cellular phones-base stations): reuse factor
  - On demand (cellular phones-mobile terminals)
  - Dynamic (cordless/WLAN): based on sensing interference levels
  - Problems: congestion management, dynamic load, …

- Antenna implications:
  - High antennas (e.g., 50m): higher coverage but higher interference between base stations (need for synchronization)
  - Low antennas: higher attenuation, lower coverage, better reuse

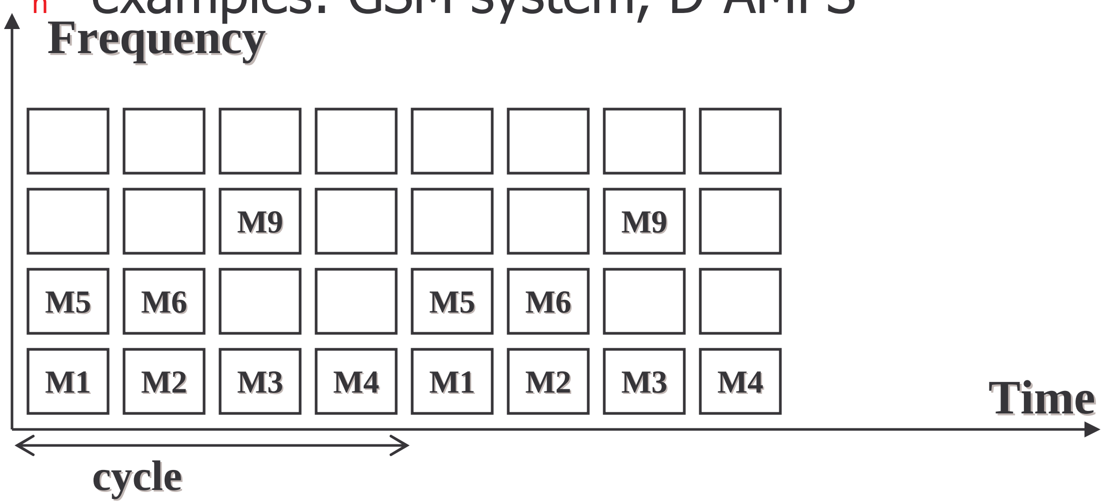
- Conclusion:
  - Pure FDMA is only interesting for simple cordless systems (CT-2)

Time Division Multiple Access

- Concept:
  - use the same frequency over non-overlapping periods of time
- Advantages:
  - simple filters (window)
  - transmit and receive over the same frequency channel
  - Half-rate capability
- Drawbacks:
  - users must be synchronized with BS (master clock over a BCH)
  - guard times: common 30-50µs, may be less in recent systems
  - short symbol duration: need for equalization, training sequences...
    - high inter-symbol interference
    - e.g., 50Kbps, QPSK, 8 users:
      - 5 µs symbol duration
      - delay spread: 1µs (cordless), upto 20µs for cellular

FDMA/TDMA

- First channel allocation:
  - random access channel (RACH) to send short requests
  - ALOHA type protocol over the RACH
- One can use both FDMA and TDMA
  - examples: GSM system, D-AMPS



Access method CDMA

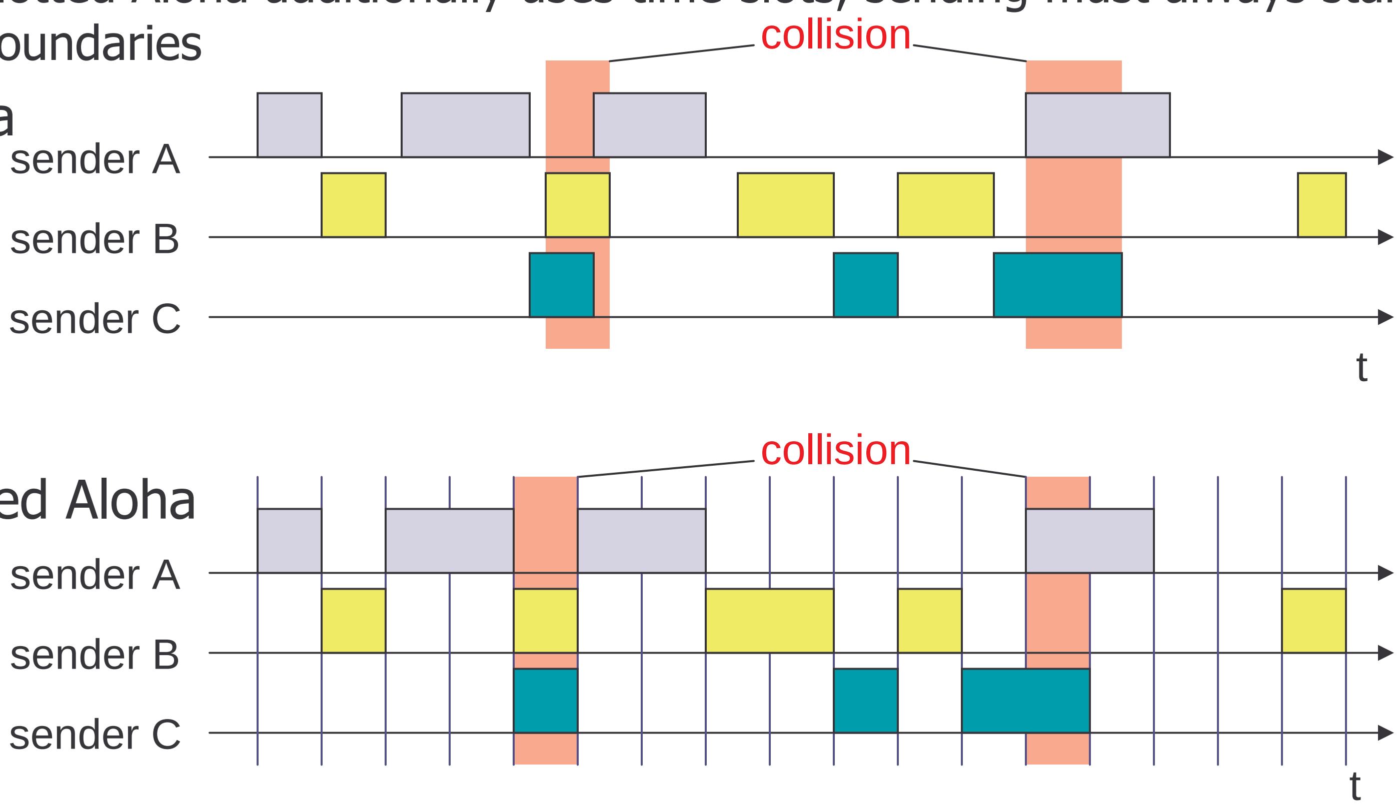
- CDMA (Code Division Multiple Access)
  - all terminals send on the same frequency probably at the same time and can use the whole bandwidth of the transmission channel
  - codes generate signals with “good-correlation” properties
  - signals from another user appear as “noise” (use spread spectrum technology)
  - signals are spread over a wideband using pseudo-noise sequences (e.g., each sender has a unique random number, the sender XORs the signal with this random number)
  - the receiver can “tune” into this signal if it knows the pseudo random number, tuning is done via a correlation function
- Disadvantages:
  - higher complexity of a receiver (receiver cannot just listen into the medium and start receiving if there is a signal)
  - all signals should have the same strength at a receiver (near-far effect)
- Advantages:
  - all terminals can use the same frequency => no planning needed; macrodiversity
  - huge code space (e.g. 2^{32}) compared to frequency space

Comparison SDMA/TDMA/FDMA/CDMA

Approach	SDMA	TDMA	FDMA	CDMA
Idea	segment space into cells/sectors	segment sending time into disjoint time-slots, demand driven or fixed patterns	segment the frequency band into disjoint sub-bands	spread the spectrum using orthogonal codes
Terminals	only one terminal can be active in one cell/one sector	all terminals are active for short periods of time on the same frequency	every terminal has its own frequency, uninterrupted	all terminals can be active at the same place at the same moment, uninterrupted
Signal separation	cell structure, directed antennas	synchronization in the time domain	filtering in the frequency domain	code plus special receivers
Advantages	very simple, increases capacity per km^2	established, fully digital, flexible	simple, established, robust	flexible, less frequency planning needed, soft handover
Dis-advantages	inflexible, antennas typically fixed	guard space needed (multipath propagation), synchronization difficult	inflexible, frequencies are a scarce resource	complex receivers, needs more complicated power control for senders
Comment	only in combination with TDMA, FDMA or CDMA useful	standard in fixed networks, together with FDMA/SDMA used in many mobile networks	typically combined with TDMA (frequency hopping patterns) and SDMA (frequency reuse)	Basis for 3rd generation

Aloha/slotted aloha

- Mechanism
  - random, distributed (no central arbiter), time-multiplex
  - Slotted Aloha additionally uses time-slots, sending must always start at slot boundaries
- Aloha
- Slotted Aloha



Carrier Sense Protocols

Use the fact that in some networks you can *sense* the medium to check whether it is currently free

- 1-persistent CSMA
- non-persistent CSMA
- p-persistent protocol
- CSMA with collision Detection (CSMA/CD): not applicable to wireless systems

- 1-persistent CSMA
  - when a station has a packet:
    - it waits until the medium is free to transmit the packet
    - if a collision occurs, the station waits a random amount of time
  - first transmission results in a collision if several stations are waiting for the channel

Carrier Sense Protocols (*Cont'd*)

- non-persistent CSMA
  - when a station has a packet:
    - if the medium is free, transmit the packet
    - otherwise wait for a random period of time and repeat the algorithm
  - higher delays, but better performance than pure ALOHA
- p-persistent protocol
  - when a station has a packet wait until the medium is free:
    - transmit the packet with probability p
    - wait for next slot with probability $1-p$
  - better throughput than other schemes but higher delay
- CSMA with collision Detection (CSMA/CD)
  - stations abort their transmission when they detect a collision
  - e.g., Ethernet, IEEE802.3 but not applicable to wireless systems

Throughputs of Some Random Access Protocols

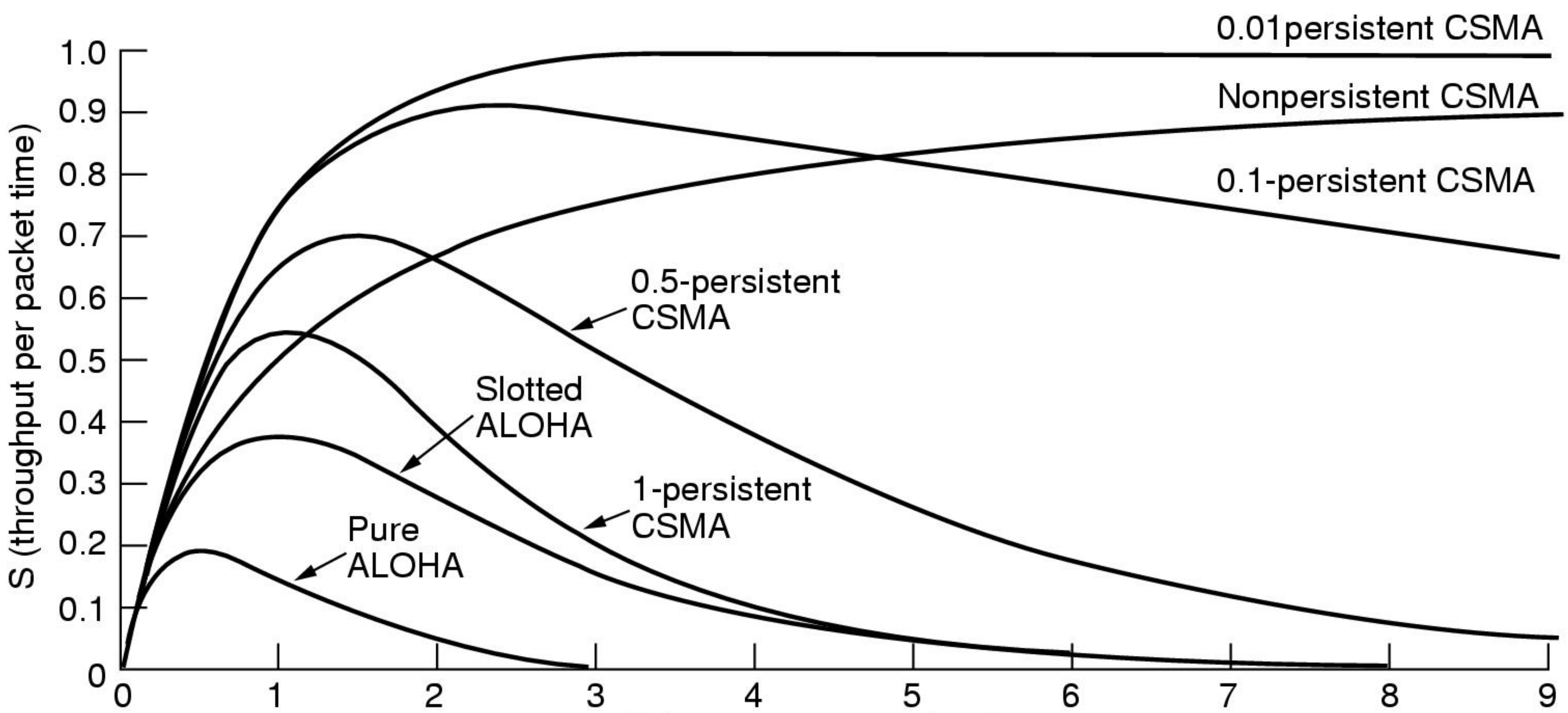
Protocol	Throughput
Pure-ALOHA	$S = Ge^{-2G}$
Slotted-ALOHA	$S = Ge^{-G}$
Non slotted 1-persistent	$S = \frac{G[1+G+aG(1+G+aG/2)]e^{-G(1+2a)}}{G(1+2a)-(1-e^{-aG})+(1+aG)e^{-G(1+a)}}$
Slotted 1-persistent CSMA	$S = \frac{G[1+G-e^{-aG}]e^{-G(1+a)}}{(1+a)-(1-e^{-aG})+ae^{-G(1+a)}}$
Nonpersistent non slotted CSMA	$S = \frac{Ge^{-aG}}{(1+2a)+e^{-aG}}$
Nonpersistent slotted CSMA	$S = \frac{aGe^{-aG}}{1-e^{-aG}+a}$

G: load (includes both successful transmissions and retransmissions)

S: successful transmission

a: ratio of propagation delay to the packet transmission delay

Comparison of MAC Algorithms



DAMA - Demand Assigned Multiple Access

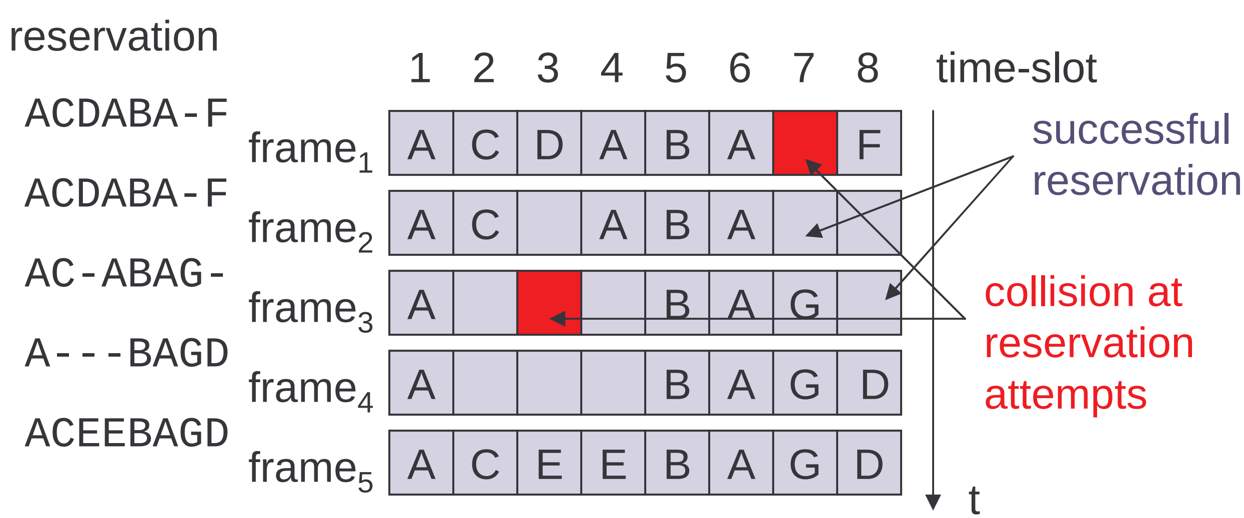
- Channel efficiency only 18% for Aloha, 36% for Slotted Aloha (assuming Poisson distribution for packet arrival and packet length)
- Reservation can increase efficiency to 80%
  - a sender *reserves* a future time-slot
  - sending within this reserved time-slot is possible without collision
  - reservation also causes higher delays
  - typical scheme for satellite links
- Examples for reservation algorithms:
  - *Explicit Reservation according to Roberts (Reservation-ALOHA)*
  - *Implicit Reservation (PRMA)*
  - *Reservation-TDMA*

Access method DAMA: Explicit Reservation

- Explicit Reservation (Reservation Aloha used for Sat. Com.):
  - two modes:
    - *ALOHA mode* for reservation:
      competition for small reservation slots, collisions possible
    - *reserved mode* for data transmission within successful reserved slots (no collisions possible)
  - it is important for all stations to keep the reservation list consistent at any point in time and, therefore, all stations have to synchronize from time to time

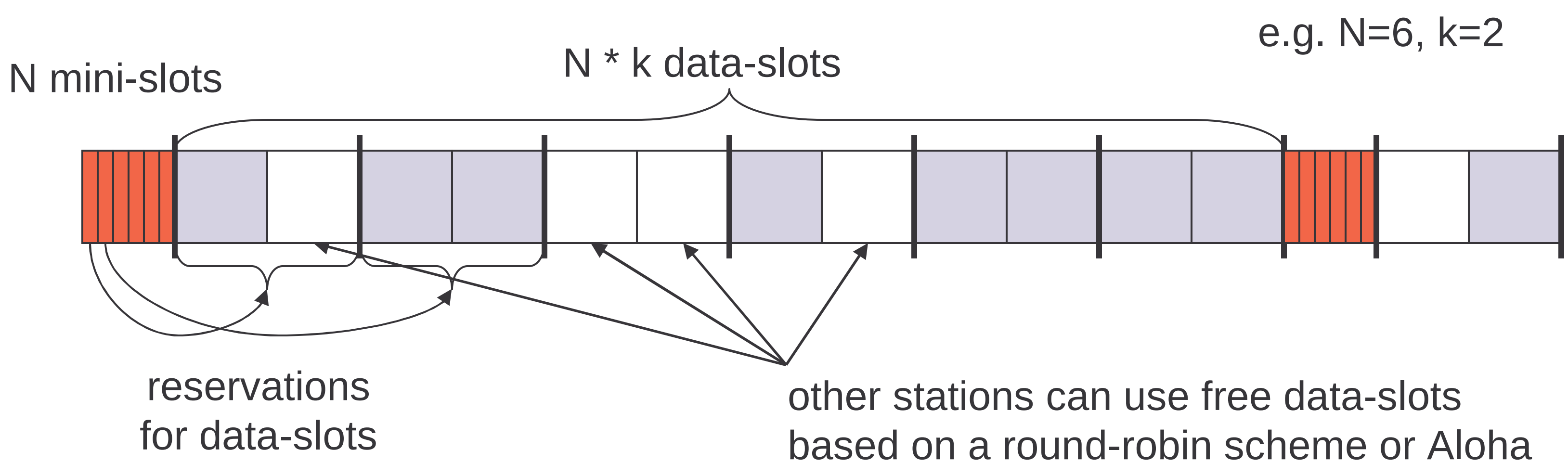
Access method DAMA: PRMA

- Implicit reservation (PRMA - Packet Reservation MA):
  - a certain number of slots form a frame, frames are repeated
  - stations compete for empty slots according to the slotted aloha principle
  - once a station reserves a slot successfully, this slot is automatically assigned to this station in all following frames as long as the station has data to send
  - competition for this slots starts again as soon as the slot was empty in the last frame



Access method DAMA: Reservation-TDMA

- Reservation Time Division Multiple Access
  - every frame consists of N mini-slots and x data-slots
  - every station has its own mini-slot and can reserve up to k data-slots using this mini-slot (i.e. x = N * k).
  - other stations can send data in unused data-slots according to a round-robin sending scheme (best-effort traffic)

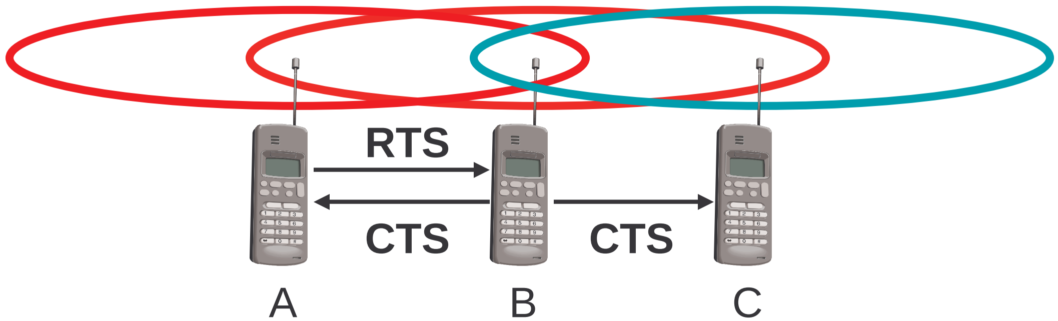


MACA - collision avoidance

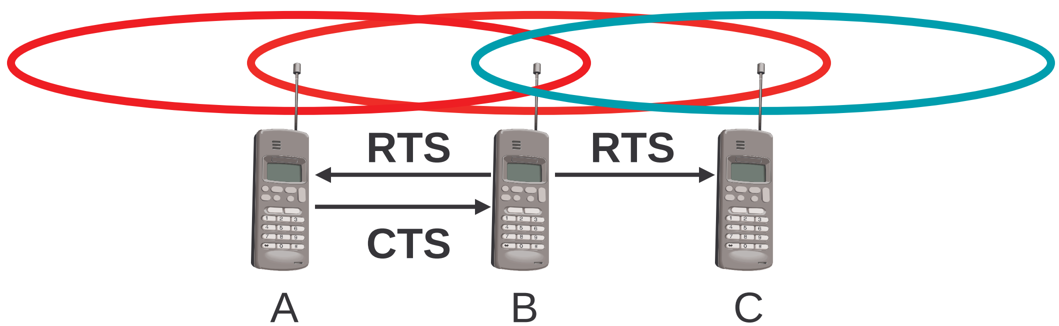
- MACA (Multiple Access with Collision Avoidance) uses short signaling packets for collision avoidance
  - RTS (request to send): a sender request the right to send from a receiver with a short RTS packet before it sends a data packet
  - CTS (clear to send): the receiver grants the right to send as 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 examples

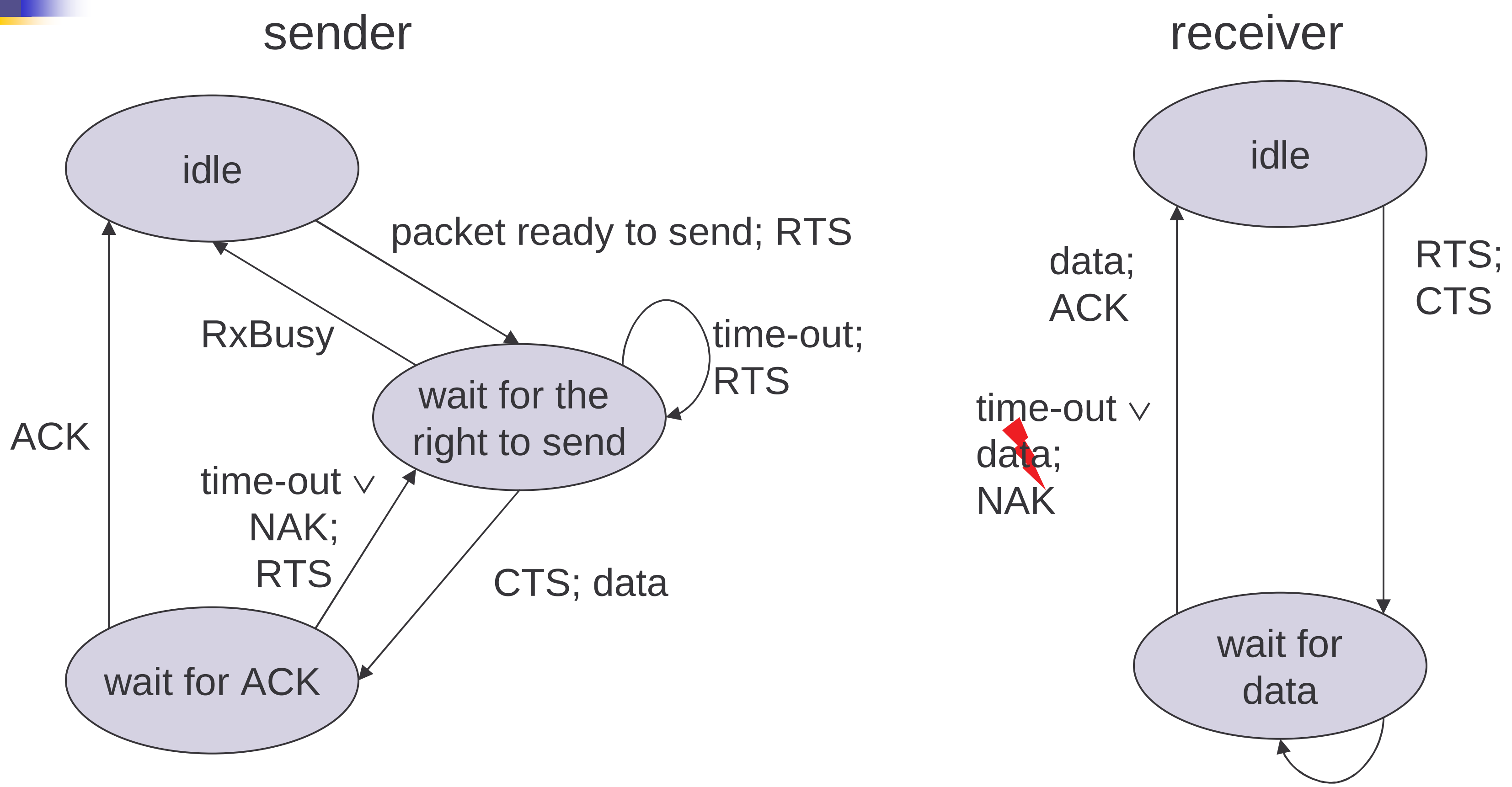
- MACA avoids the problem of hidden terminals
  - A and C want to send to B
  - A sends RTS first
  - C waits after receiving CTS from B



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



MACA variant: DFWMAC in IEEE802.11



ACK: positive acknowledgement
NAK: negative acknowledgement

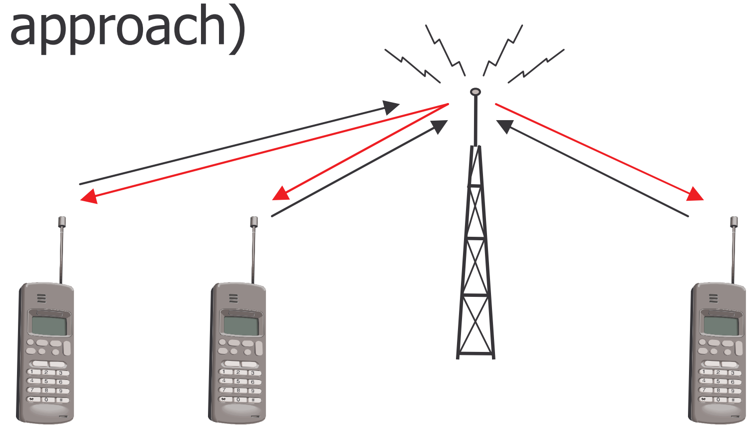
RxBusy: receiver busy

Polling mechanisms

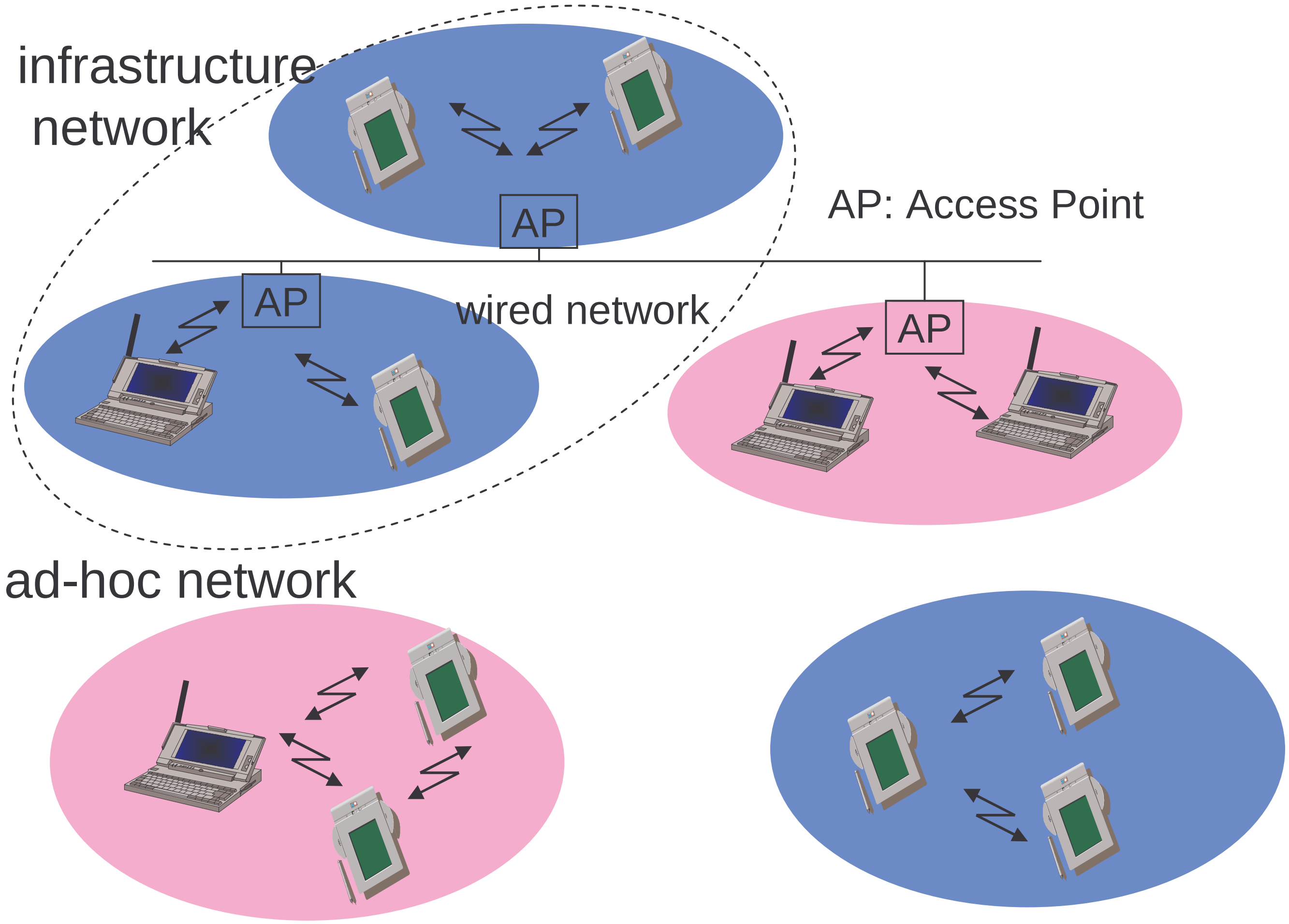
- If one terminal can be heard by all others, this “central” terminal (a.k.a. base station) can poll all other terminals according to a certain scheme
  - now all schemes known from fixed networks can be used (typical mainframe - terminal scenario)
- Example: Randomly Addressed Polling
  - base station signals readiness to all mobile terminals
  - terminals ready to send can now transmit a random number without collision with the help of CDMA or FDMA (the random number can be seen as dynamic address) or with collisions (over the Random Access CHannel)
  - the base station now chooses one address for polling from the list of all random numbers (collision if two terminals choose the same address)
  - the base station acknowledges correct packets and continues polling the next terminal
  - this cycle starts again after polling all terminals of the list

ISMA (Inhibit Sense Multiple Access)

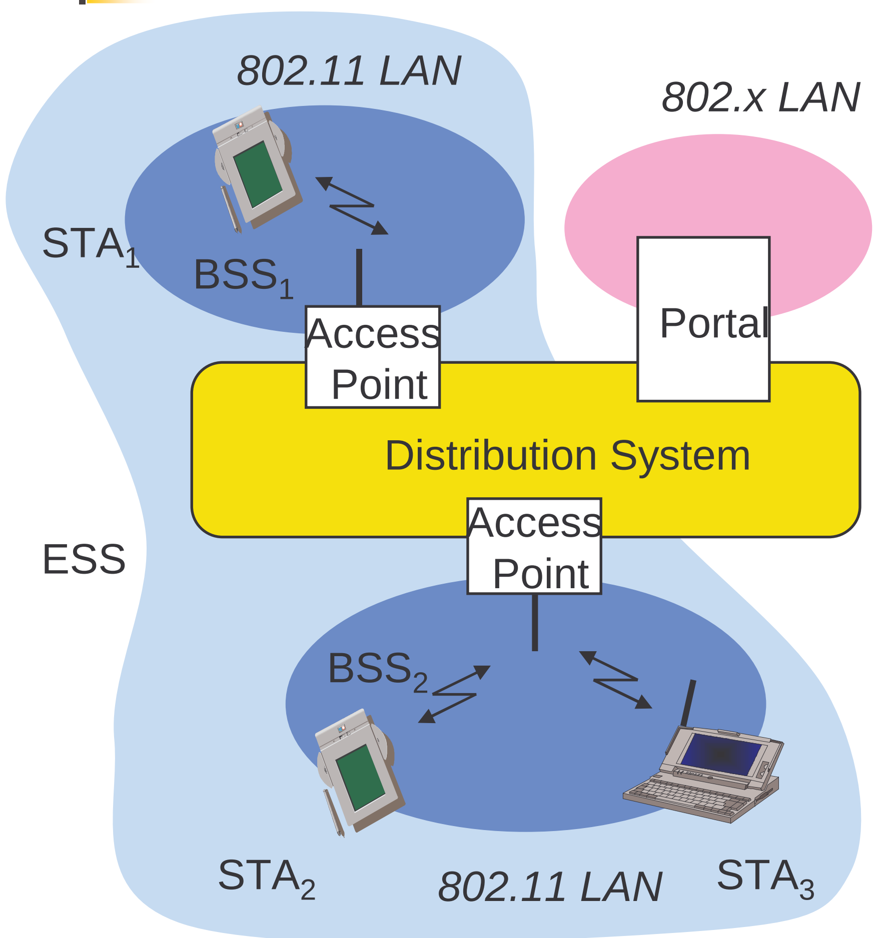
- Current state of the medium is signaled via a "busy tone"
  - the base station signals on the downlink (base station to terminals) if the medium is free or not
  - terminals must not send if the medium is busy
  - terminals can access the medium as soon as the busy tone stops
  - the base station signals collisions and successful transmissions via the busy tone and acknowledgements, respectively (media access is not coordinated within this approach)
  - mechanism used, e.g., for CDPD (USA, integrated into AMPS)



IEEE802.11

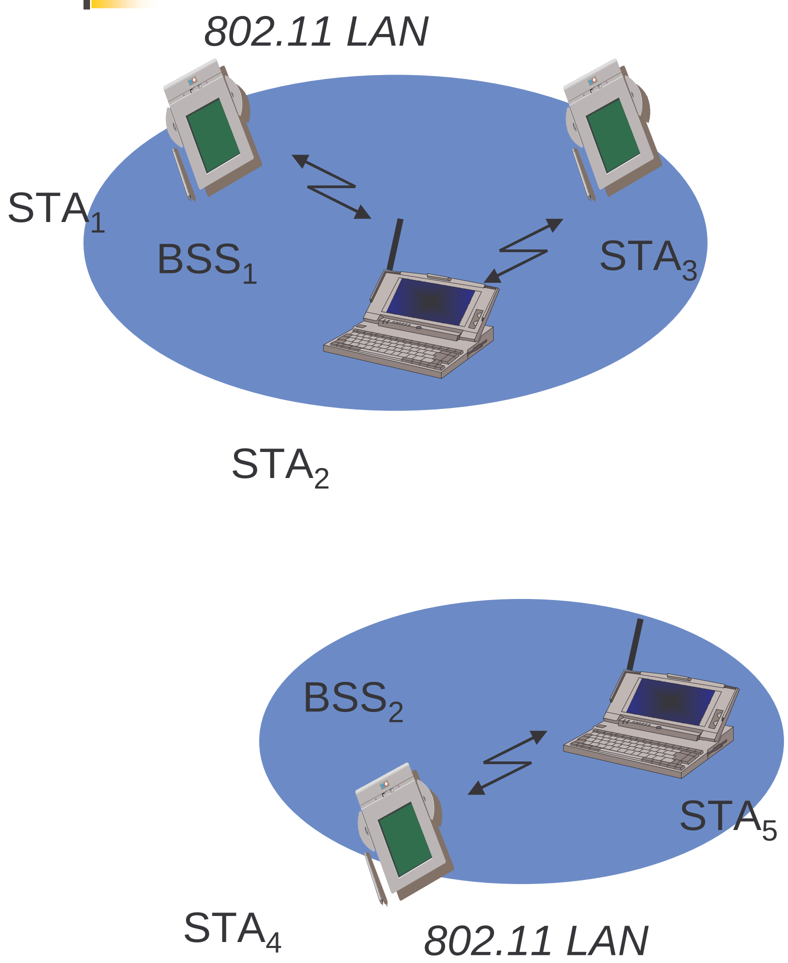

infrastructure
network
AP
AP: Access Point
AP
wired network
AP
ad-hoc network

802.11 - Architecture of an infrastructure network



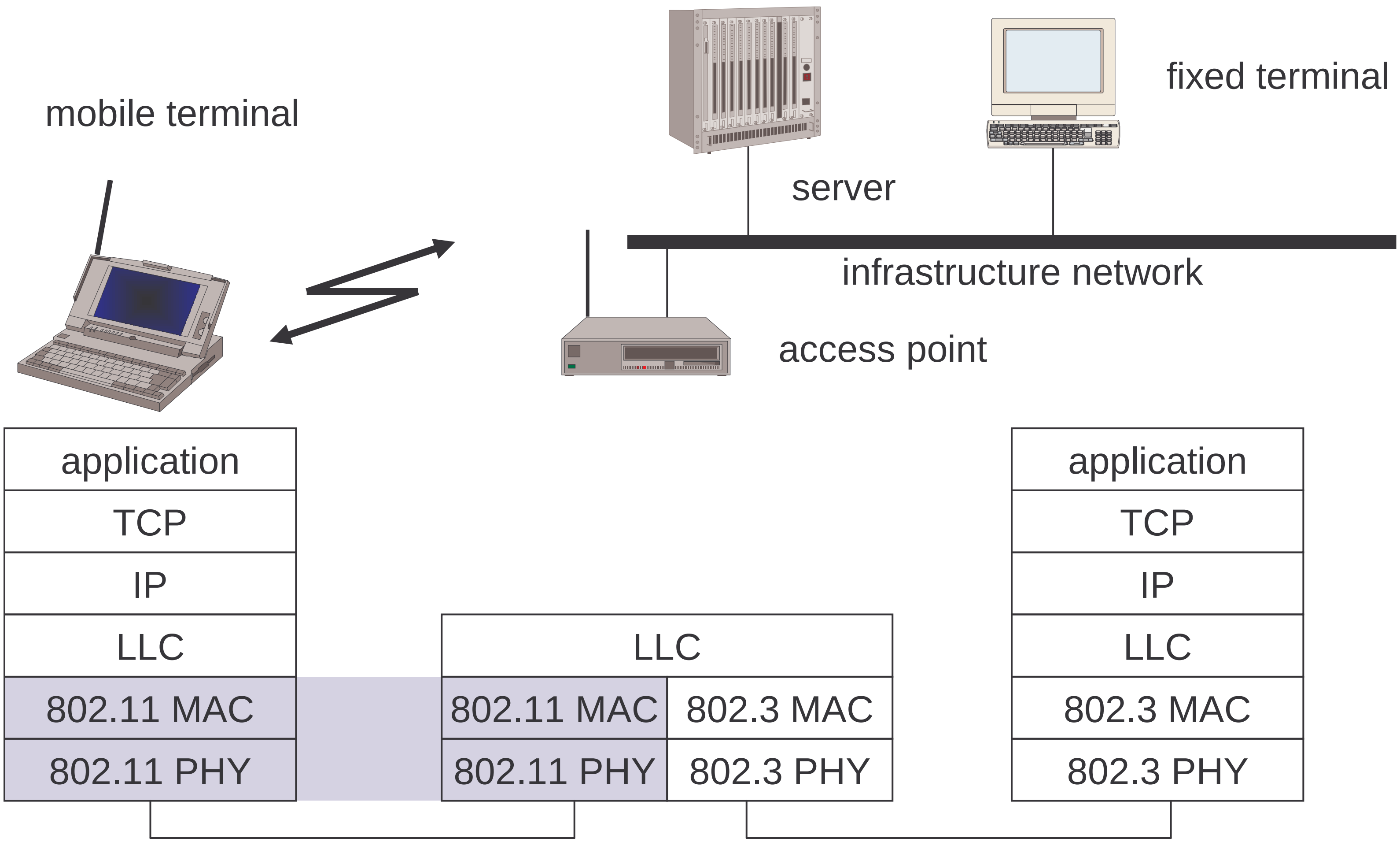
- Station (STA)
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- Basic Service Set (BSS)
  - group of stations using the same radio frequency
- Access Point
  - station integrated into the wireless LAN and the distribution system
- Portal
  - bridge to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

802.11 - Architecture of an ad-hoc network



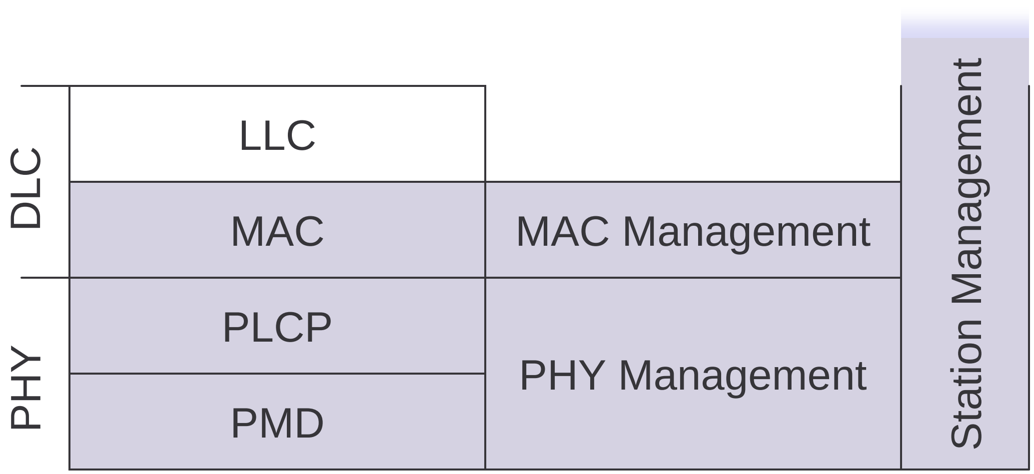
- Direct communication within a limited range
  - Station (STA): terminal with access mechanisms to the wireless medium
  - Basic Service Set (BSS): group of stations using the same radio frequency

IEEE standard 802.11



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



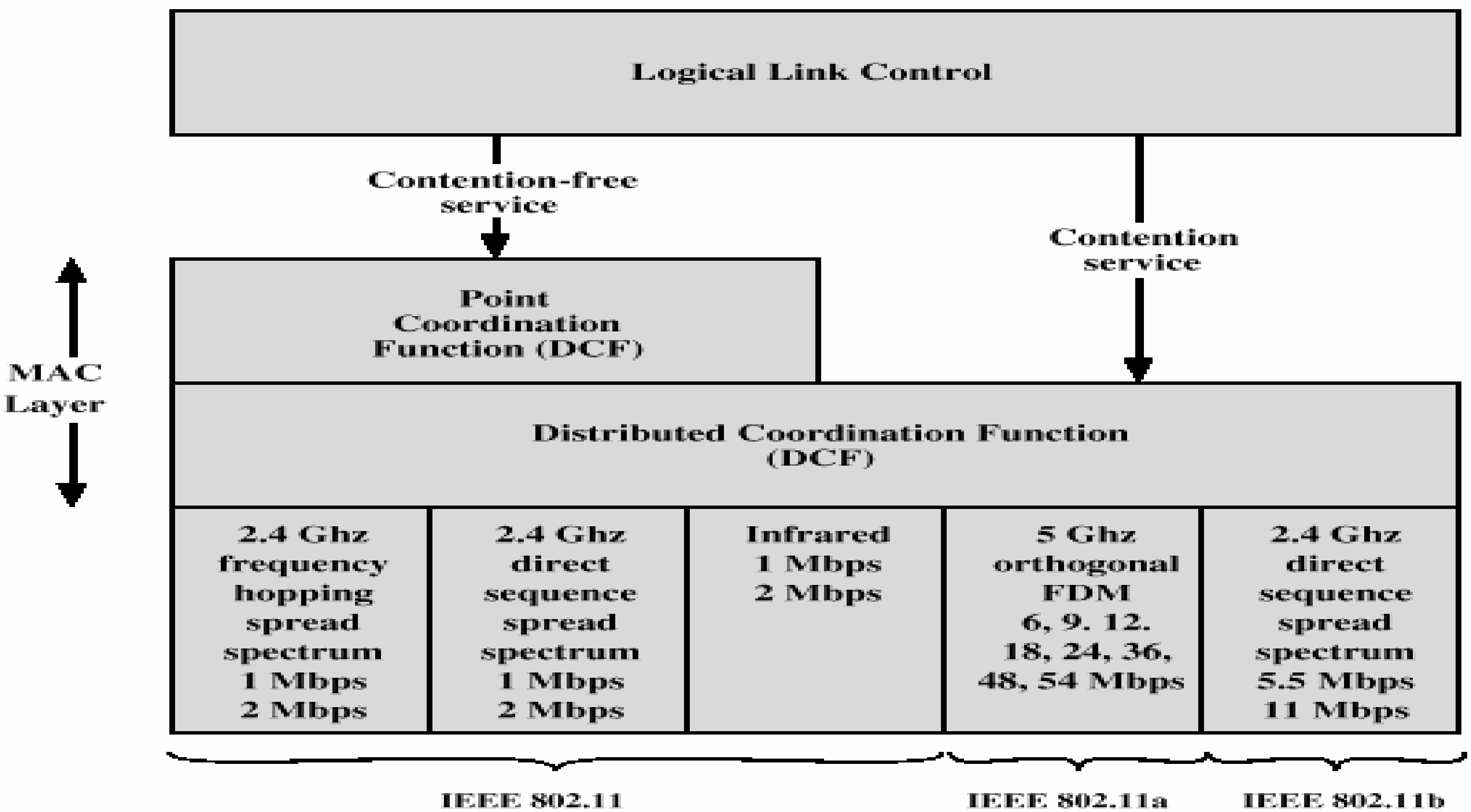


Figure 14.5 IEEE 802.11 Protocol Architecture

802.11 - Physical layer

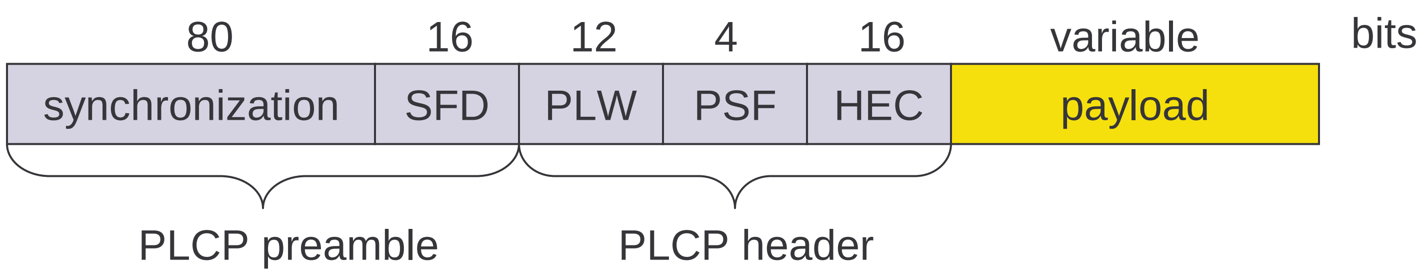
- 5 versions: 2 radio (typ. 2.4 GHz), 1 IR
  - data rates 1 or 2 Mbit/s
- FHSS (Frequency Hopping Spread Spectrum) 2.4 GHz
  - spreading, despreading, signal strength, typ. 1 Mbit/s
  - min. 2.5 frequency hops/s (USA), two-level GFSK modulation
- DSSS (Direct Sequence Spread Spectrum) 2.4GHz
  - DBPSK modulation for 1 Mbit/s (Differential Binary Phase Shift Keying), DQPSK for 2 Mbit/s (Differential Quadrature PSK)
  - preamble and header of a frame is always transmitted with 1 Mbit/s, rest of transmission 1 or 2 Mbit/s
  - chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
  - max. radiated power 1 W (USA), 100 mW (EU), min. 1mW
- Infrared
  - 850-950 nm, diffuse light, typ. 10 m range
  - carrier detection, energy detection, synchronization

IEEE 802.11a and IEEE 802.11b

- IEEE 802.11a
  - Makes use of 5-GHz band
  - Provides rates of 6, 9 , 12, 18, 24, 36, 48, 54 Mbps
  - Uses orthogonal frequency division multiplexing (OFDM)
  - Subcarrier modulated using BPSK, QPSK, 16-QAM or 64-QAM
- IEEE 802.11b
  - Provides data rates of 5.5 and 11 Mbps
  - Complementary code keying (CCK) modulation scheme

FHSS PHY packet format

- Synchronization
  - synch with 010101... pattern
- SFD (Start Frame Delimiter)
  - 0000110010111101 start pattern
- PLW (PLCP_PDU Length Word)
  - length of payload incl. 32 bit CRC of payload, PLW < 4096
- PSF (PLCP Signaling Field)
  - data rate of payload (1 or 2 Mbit/s)
- HEC (Header Error Check)
  - CRC with $x^{16}+x^{12}+x^5+1$



DSSS PHY packet format

- Synchronization
  - synch., gain setting, energy detection, frequency offset compensation
- SFD (Start Frame Delimiter)
  - 1111001110100000
- Signal
  - data rate of the payload (0A: 1 Mbit/s DBPSK; 14: 2 Mbit/s DQPSK)
- Service
  - future use, 00: 802.11 compliant
- Length
  - length of the payload
- HEC (Header Error Check)
  - protection of signal, service and length, $x^{16}+x^{12}+x^5+1$

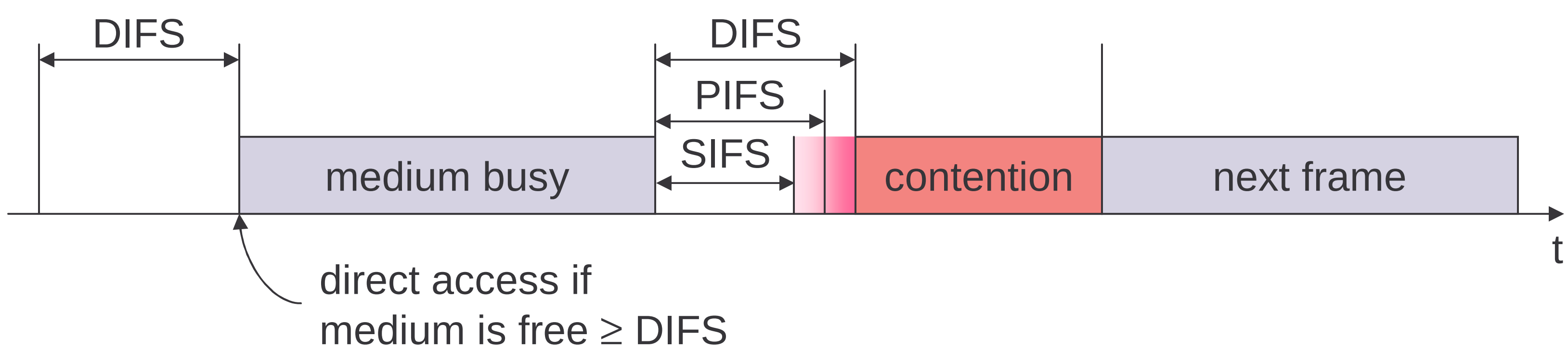
128	16	8	8	16	16	variable	bits
synchronization	SFD	signal	service	length	HEC	payload	
PLCP preamble		PLCP header					

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)
- 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 Foundation Wireless MAC
    - avoids hidden terminal problem
  - DFWMAC- PCF (optional)
    - access point polls terminals according to a list

802.11 - MAC layer II

- Priorities
  - defined through different inter frame spaces
  - 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

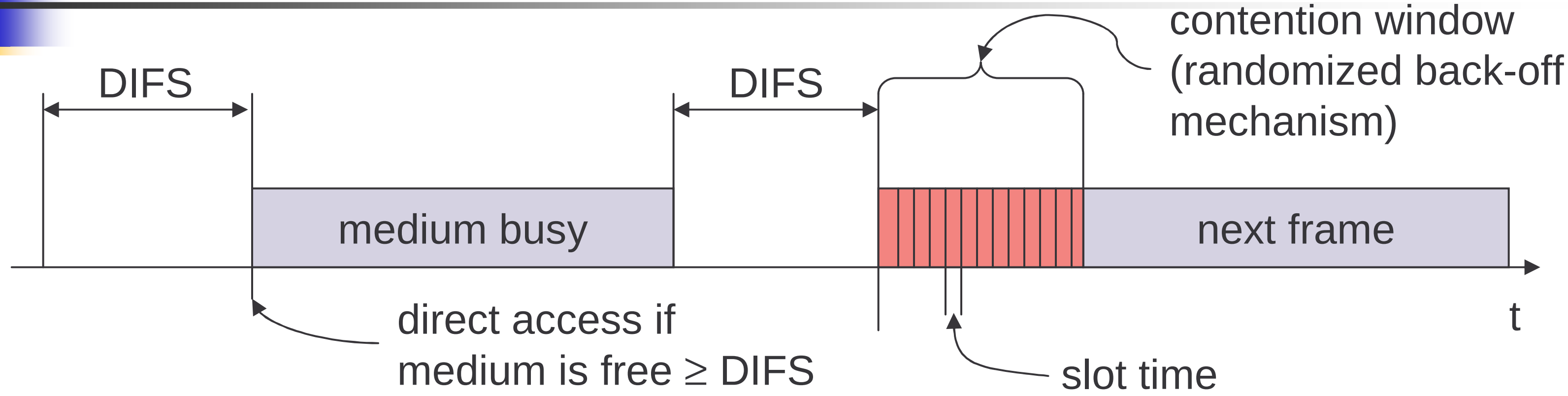


IFS Timing

- aSIFSTime = aRxRFDelay + aRxPLCPDelay + aMACProcessingDelay + aRxTxTurnaroundTime.
- aSlotTime = aCCATime + aRxTxTurnaroundTime + aAirPropagationTime + aMACProcessingDelay.

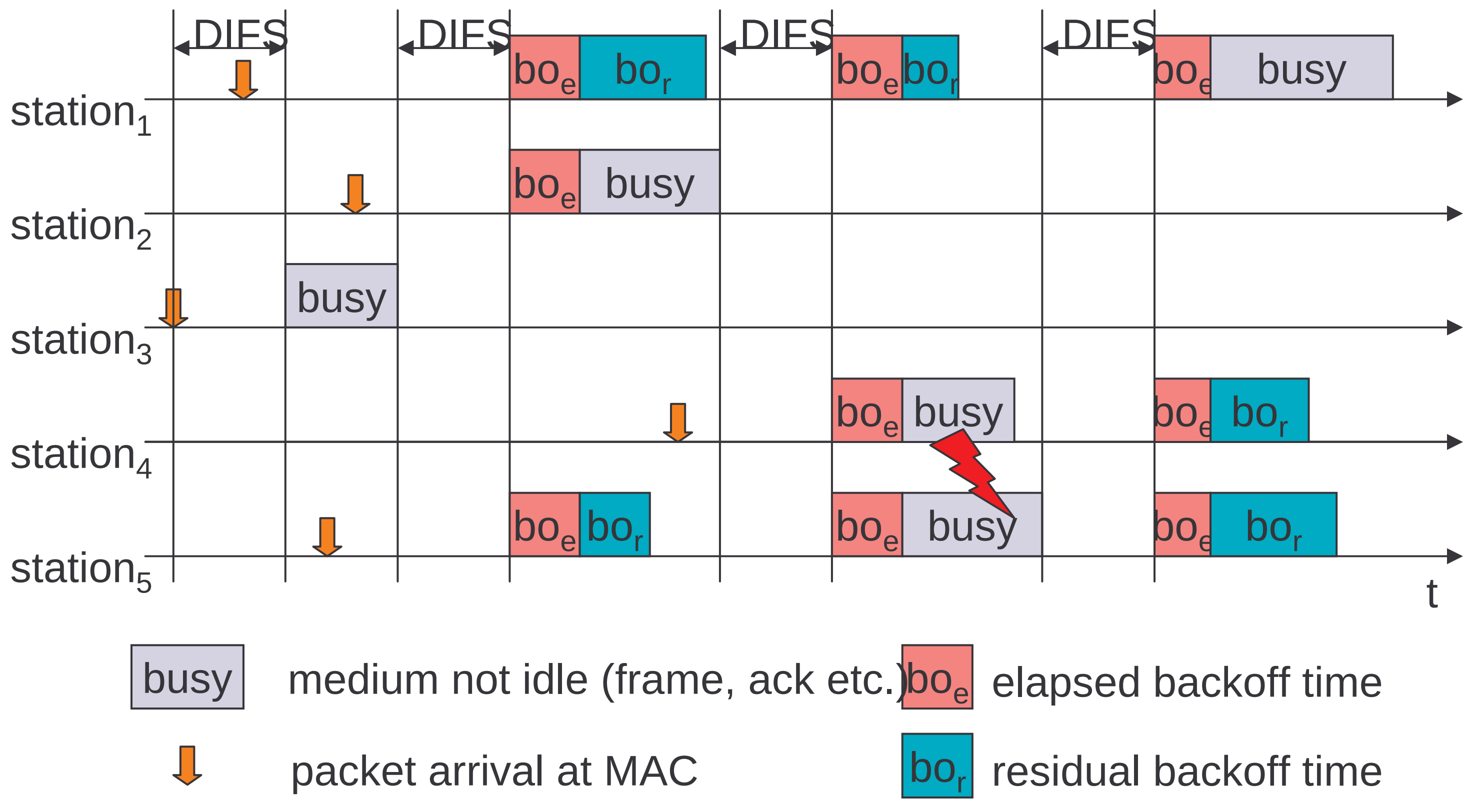
- PIFS = aSIFSTime + aSlotTime
- DIFS = aSIFSTime + 2∗aSlotTime
- EIFS = aSIFSTime + (8 × ACKSize) + aPreambleLength + aPLCPHeaderLngth+ DIFS
- For DSSS:
  - aSlotTime 20 µs
  - aSIFSTime 10 µs
  - aCCATime < 15 µs
  - aRxTxTurnaroundTime <5 µs

802.11 - CSMA/CA access method I



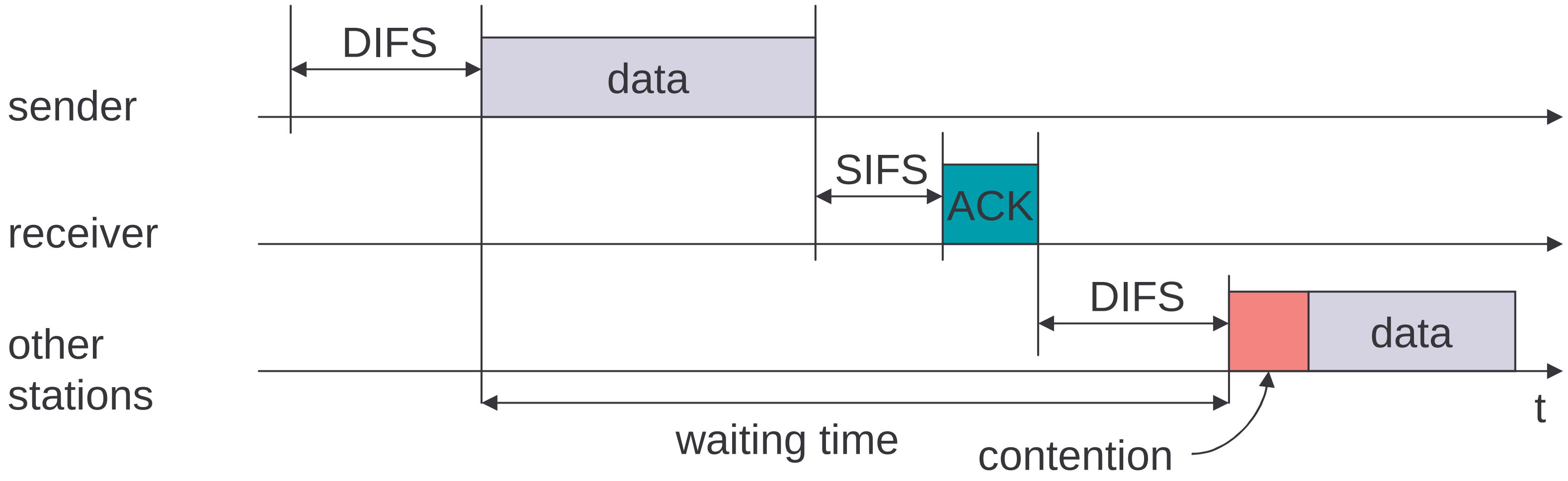
- station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, 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 - competing stations - simple version



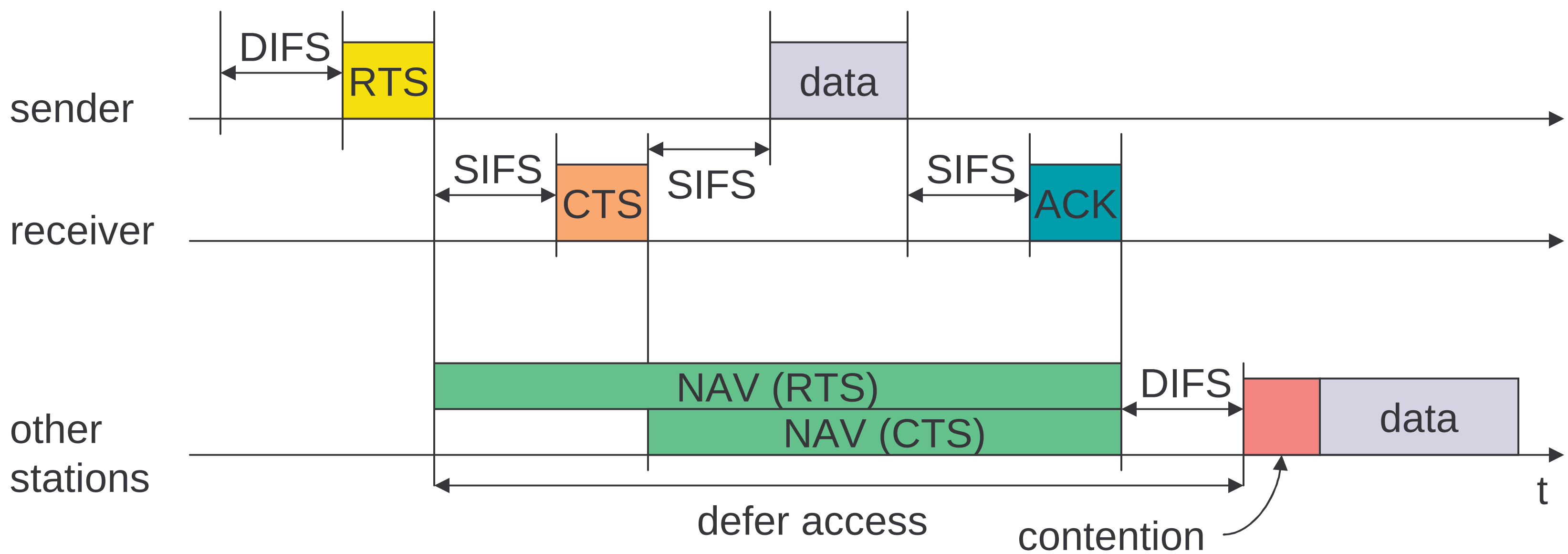
802.11 - CSMA/CA access method II

- Sending unicast packets
  - 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

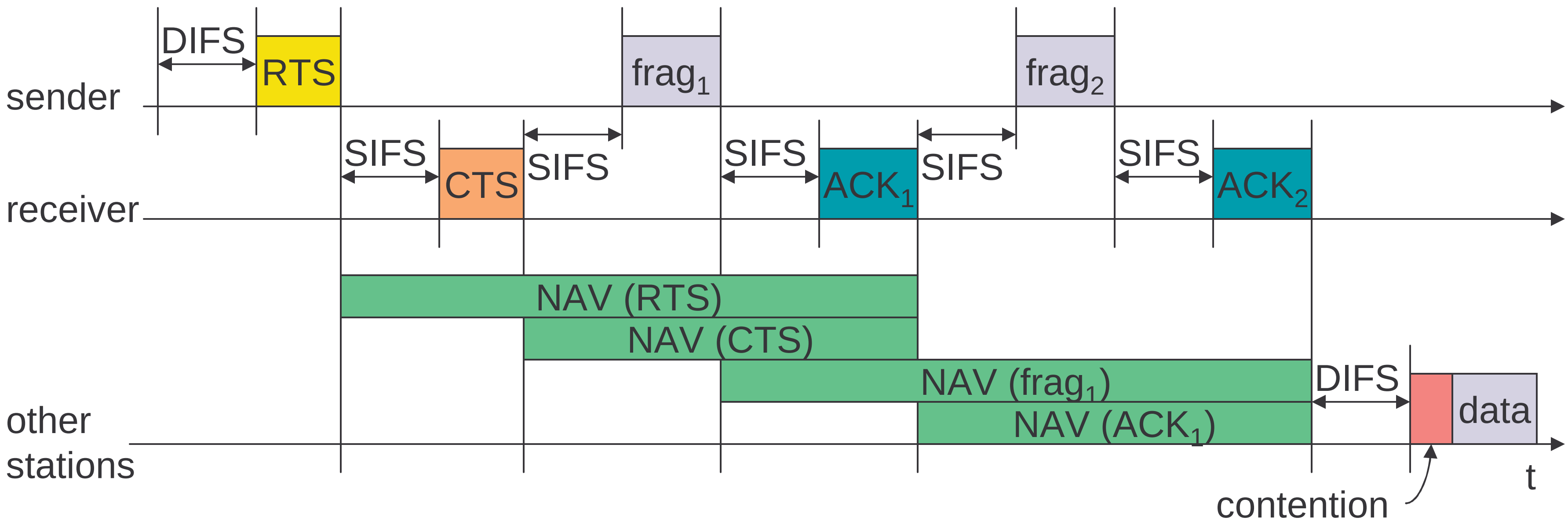


802.11 - DFWMAC

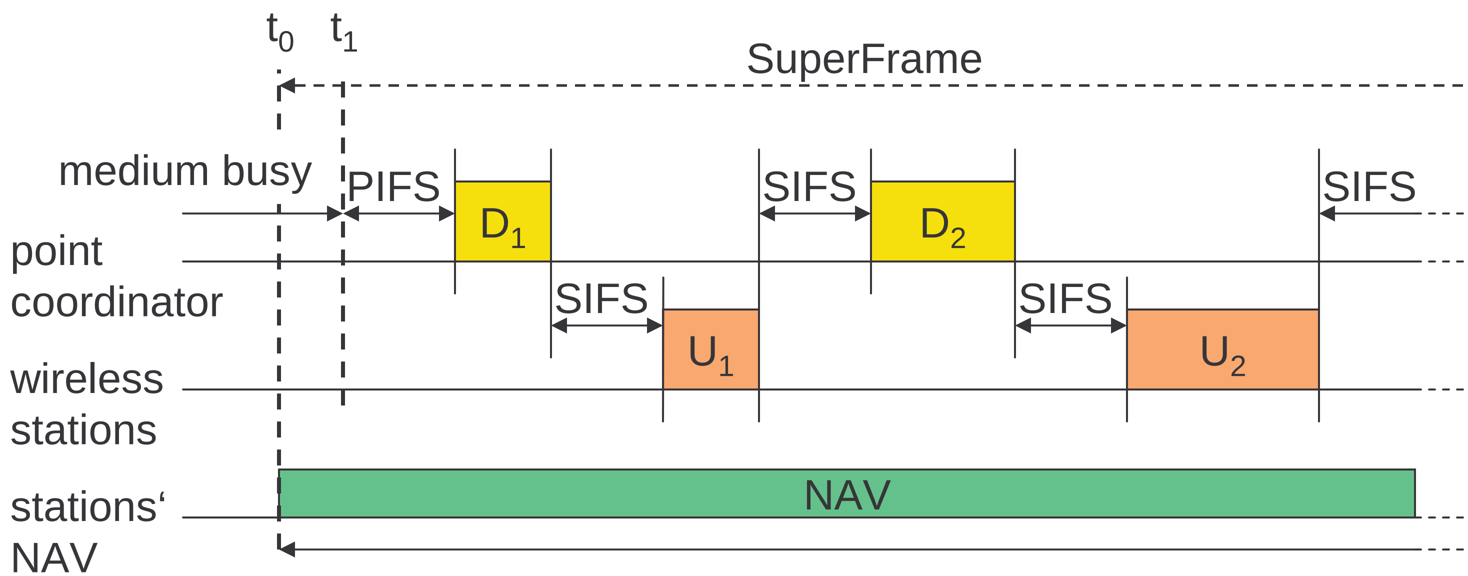
- Sending unicast packets
  - station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
  - acknowledgement via CTS after SIFS by receiver (if ready to receive)
  - sender can now send data at once, acknowledgement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



Fragmentation

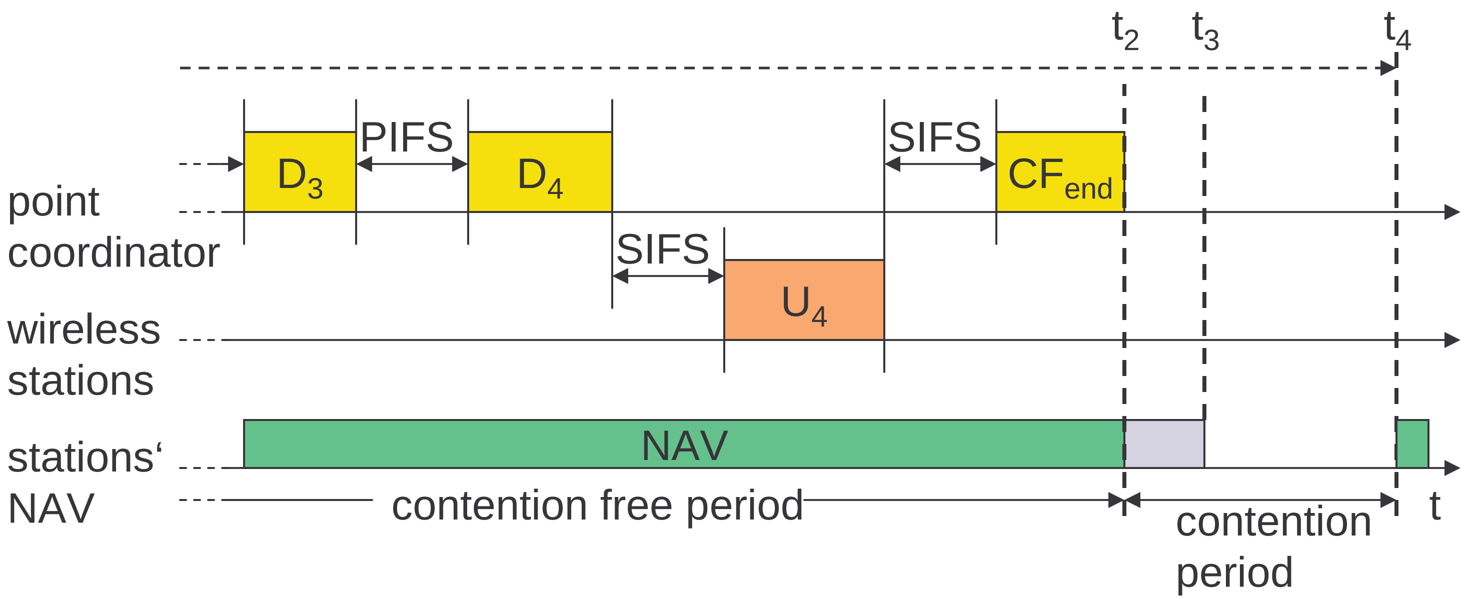


DFWMAC-PCF I



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

DFWMAC-PCF II



7.20.1

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

bytes	2	2	6	6	6	2	6	0-2312	4
	Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	CRC

Frame Control: Version, Type, Subtype, To DS, From DS, More Fragments, Retry, Power Management, More Data, Wired Equivalent Privacy (WEP), and Order

MAC address format

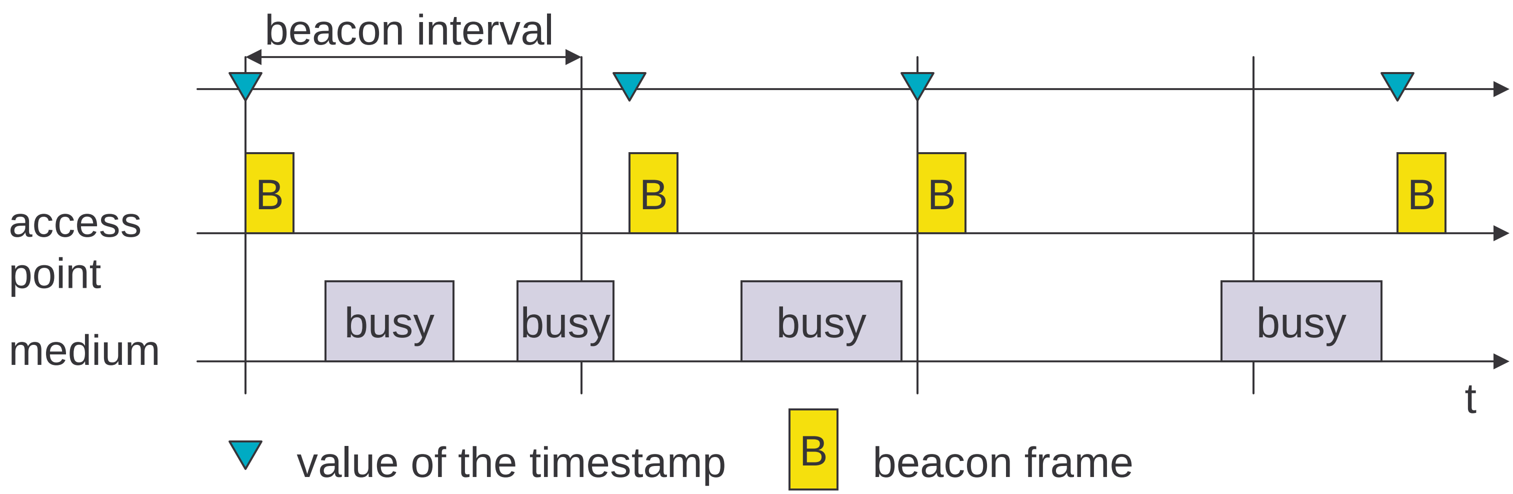
scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

DS: Distribution System
AP: Access Point
DA: Destination Address (final recipient)
SA: Source Address (initiator)
BSSID: Basic Service Set Identifier
RA: Receiver Address (immediate recipient)
TA: Transmitter Address (immediate sender)

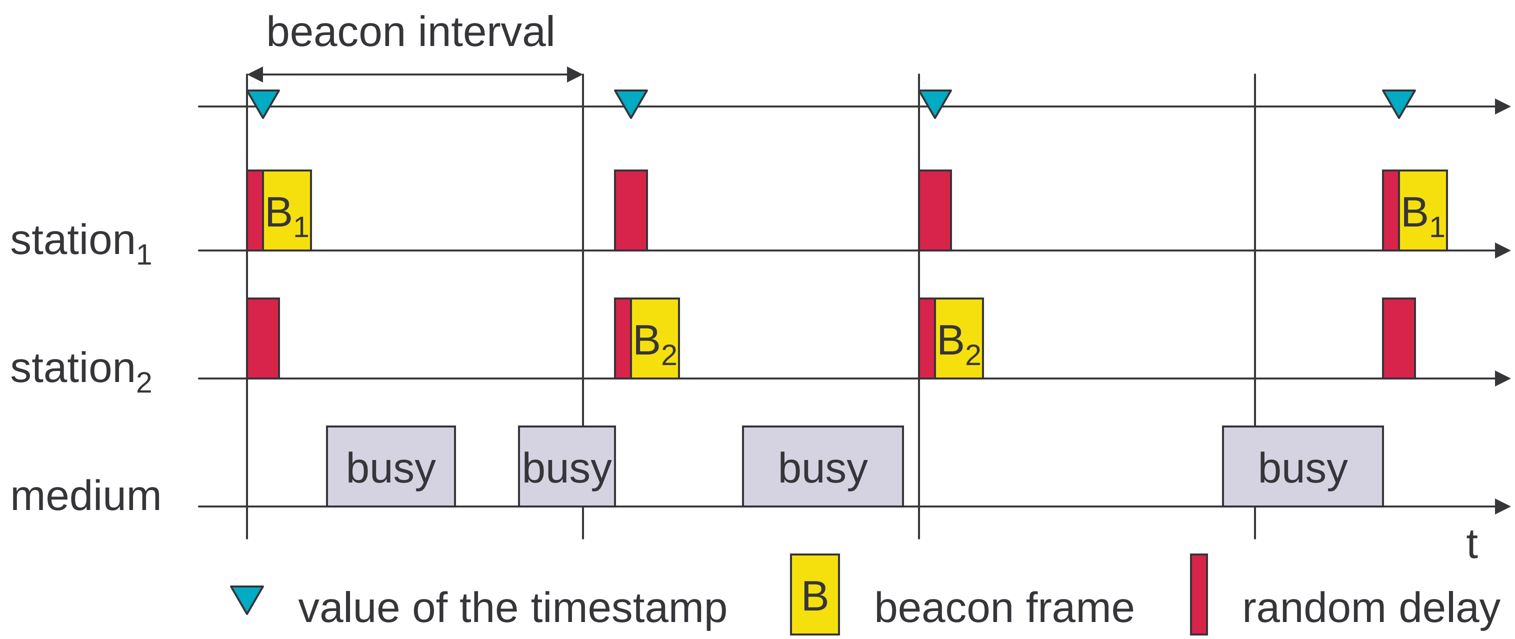
802.11 - MAC management

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

Synchronization using a Beacon (infrastructure)



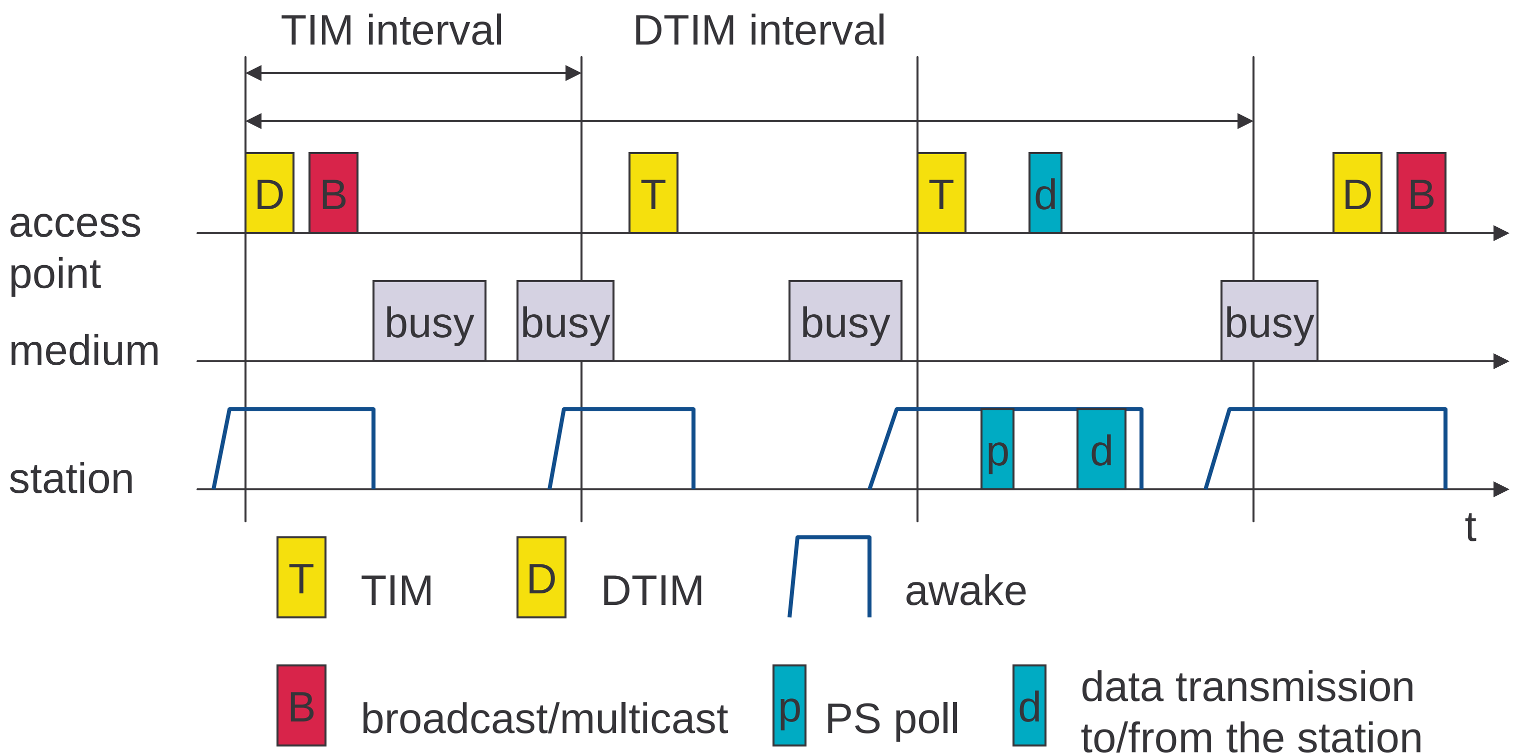
Synchronization using a Beacon (ad-hoc)



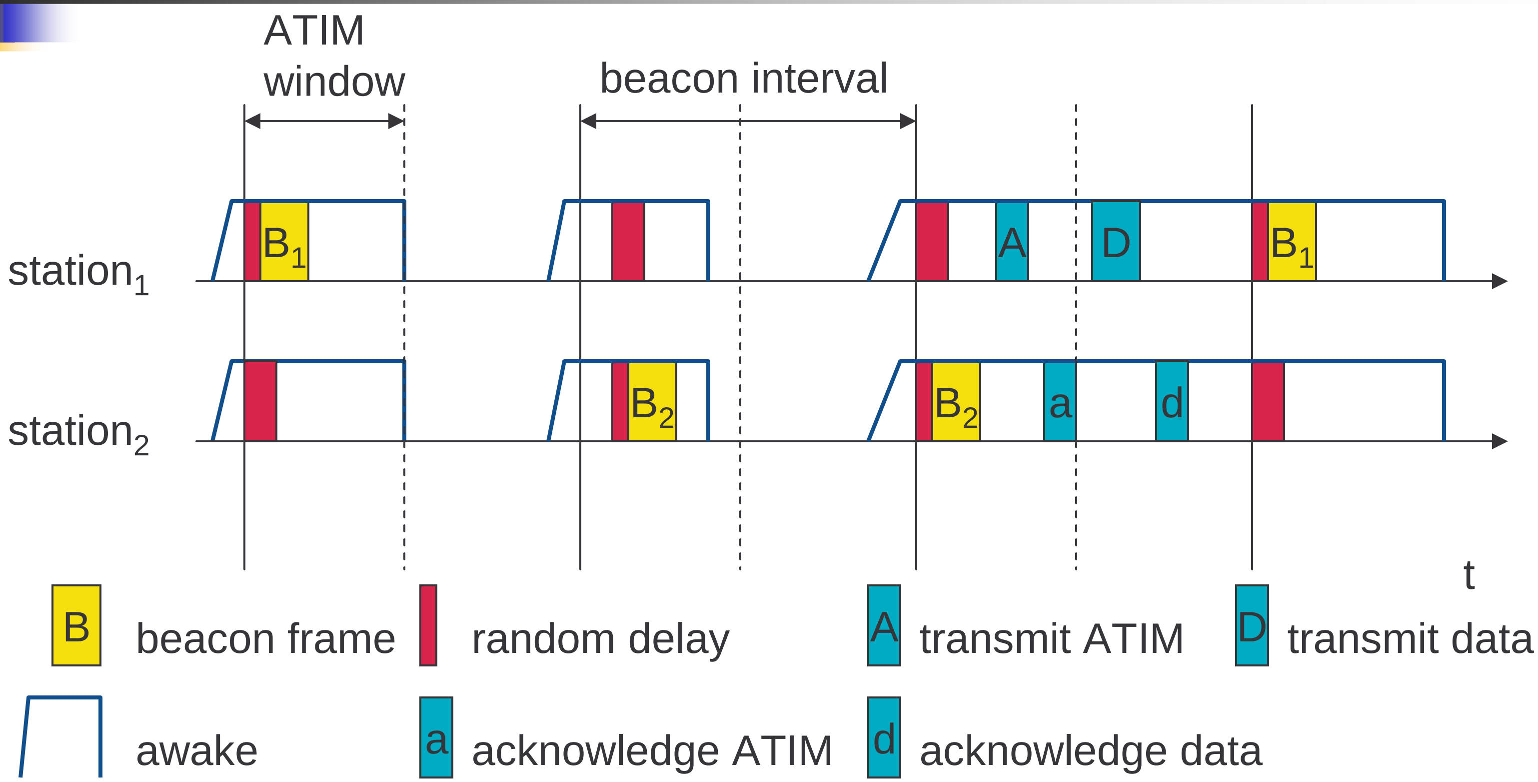
Power management

- 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)



802.11 - Roaming

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