IEEE 802.11a/g WLAN

outline

- background & overview
- mac & phy
- wlan management
- security

WLAN

- benefits
  - flexibility & mobility
  - installation
  - scalability
- disadvantages
  - distance
  - security
  - performance

IEEE 802.11a

- approved in 1999
- frequency range
  - 5.15 - 5.825 GHz
  - low operational distances (*LOS environment*)
- modulation
  - OFDM system with 52 subcarriers
  - BPSK, QPSK, 16-QAM, 64-QAM
- data rates
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s
- forward error correction with convolutional coding
  - coding rates 1/2, 2/3, 3/4

IEEE 802.11g

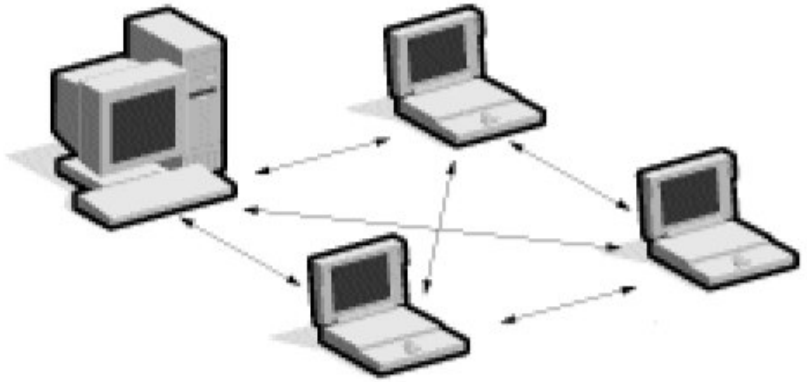
- approved in 2003
- higher operational distances
- frequency range
  - 2.4 – 2.4835 GHz
- physical layer same as in 802.11a
- compatible with 802.11b devices

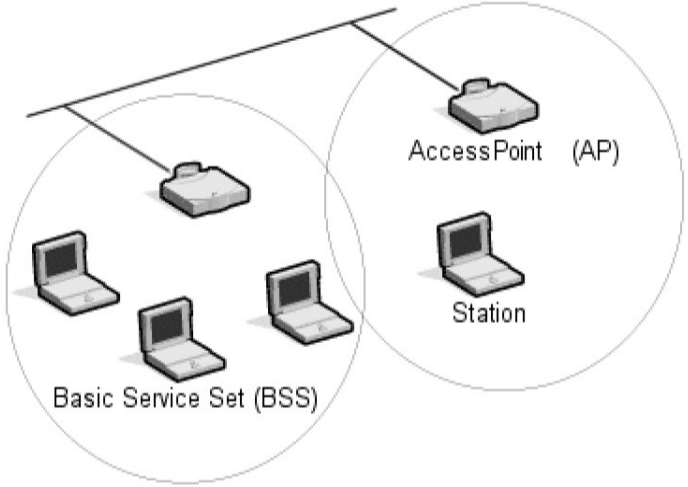
mac

- is a logical entity that coordinates medium access
- provides framing operation and interaction between stations and access points

mac

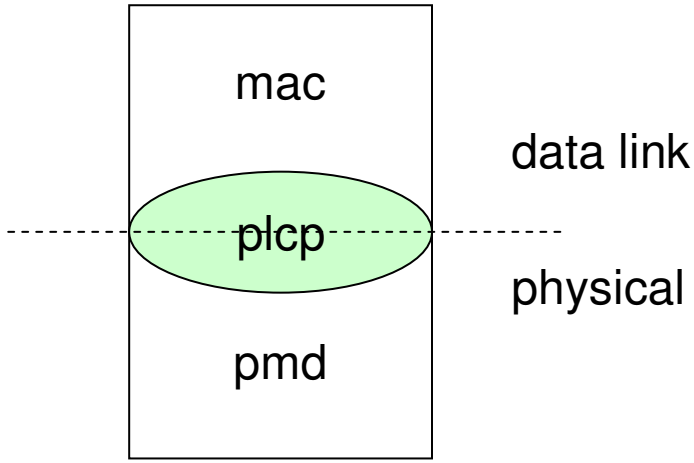
- different network topologies
  - IBSS, ESS
- provides two coordinated functions for medium access
  - Distributed Coordination Function
  - Point Coordination Function





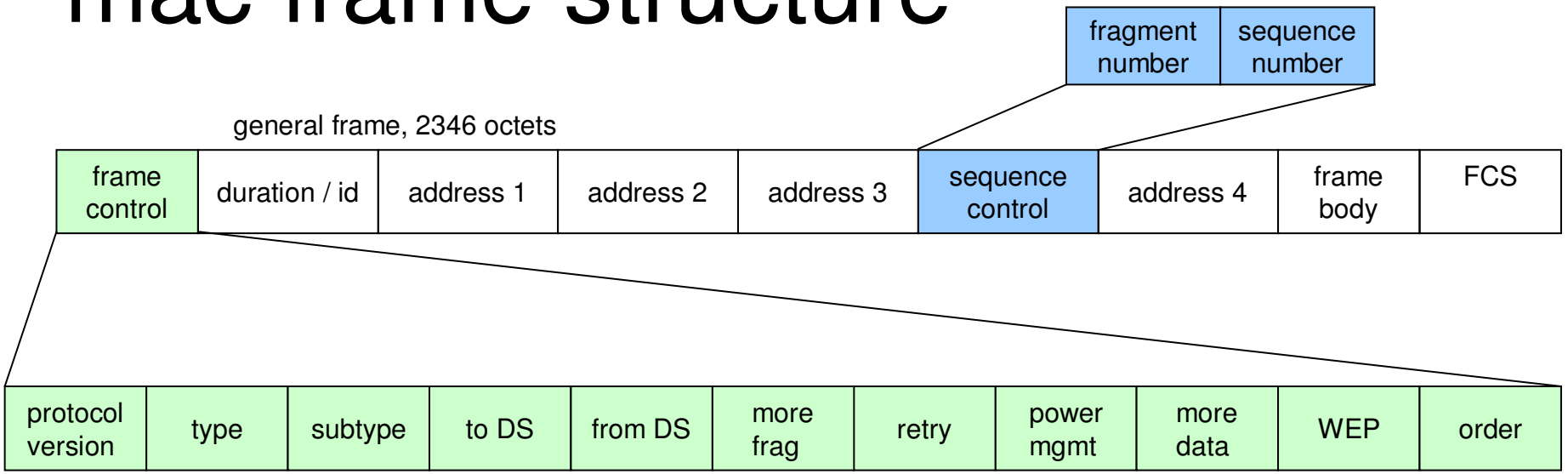
mac

- 802.11 divides phy into plcp and pmd layers
  - plcp maps the mac frames suitable for different mediums
- mac is the same for all versions



plpc = physical layer convergence procedure, pmd = physical medium dependent

mac frame structure



- **address**: from, to, fragment, bssid
- **type**: control, data, management
- **retry**: retransmission
- **FCS**: 32-bit CRC

RTS frame

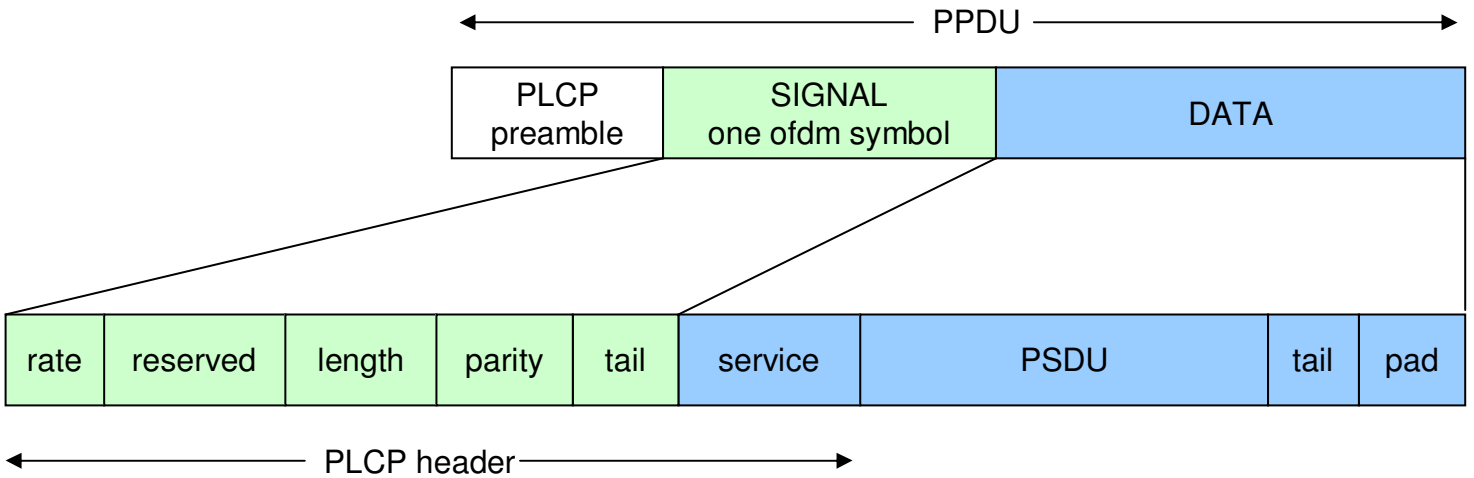
frame control	duration	RA	TA	FCS

management frame

frame control	duration	DA	SA	BSSID	sequence control	frame body	FCS

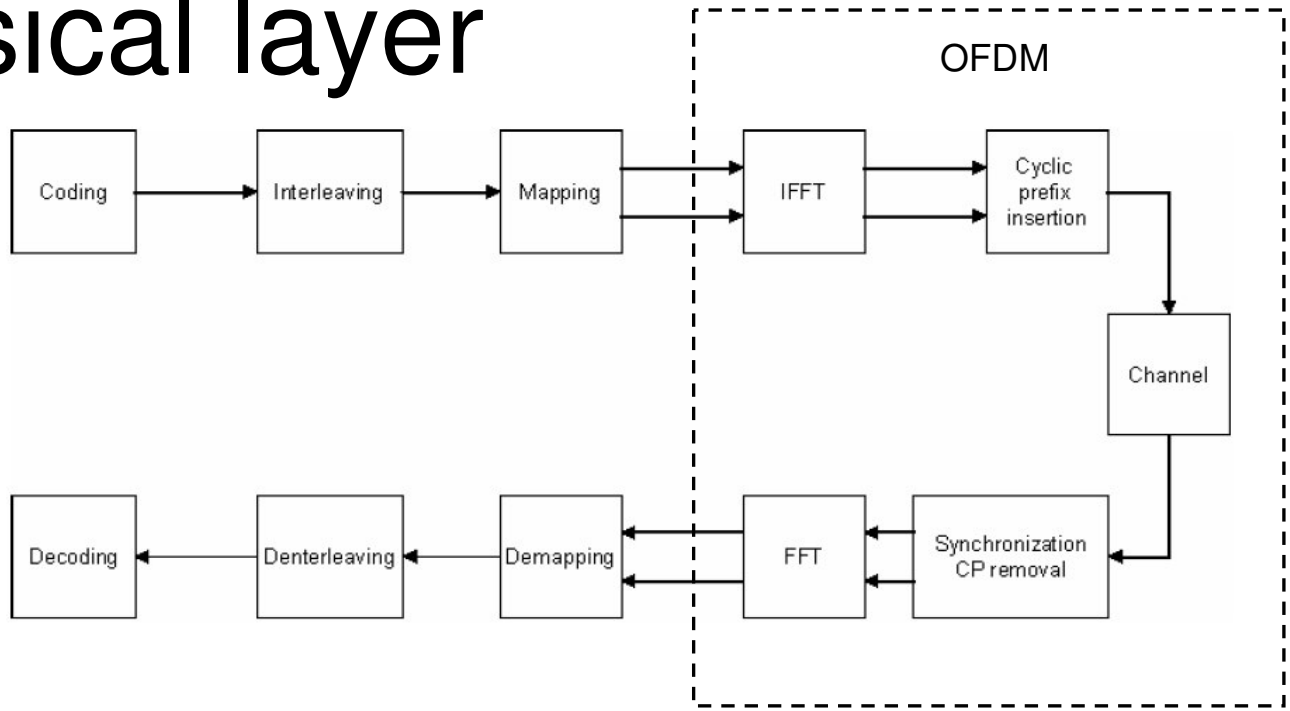
plcp

- Preamble and SIGNAL are DQPSK modulated in b/g – network (*cooperation*)
  - PLCP preamble: training sequence (agc, sync)
  - Tail: for convolutional coding



PPDU = PLCP protocol data unit

physical layer

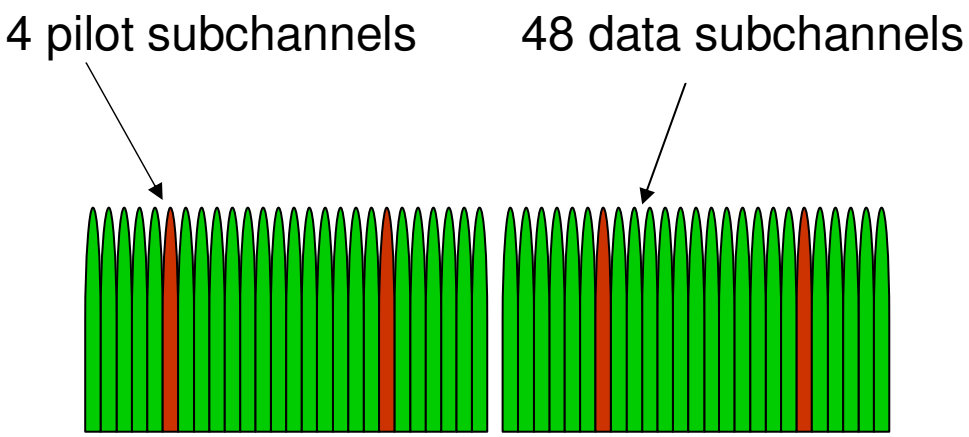


- convolutional coding
- interleaving, reduces the effect of error bursts
- mapping, bpsk, qpsk, 16-qam, 64-qam

physical layer

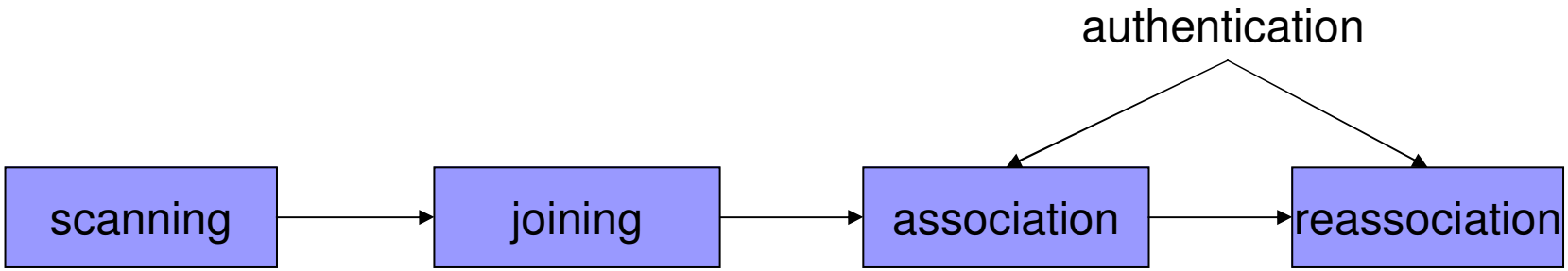
- 0,8 μs guard time allows ~240 m long multipath
- channel bw is ~16.7 MHz

Parameter	Value
Nr of data subcarriers	48
Nr of pilot subcarrier	4
Subcarrier spacing	312,5 kHz
FFT period	3,2 μs
guard interval	0,8 μs
symbol duration	4 μs

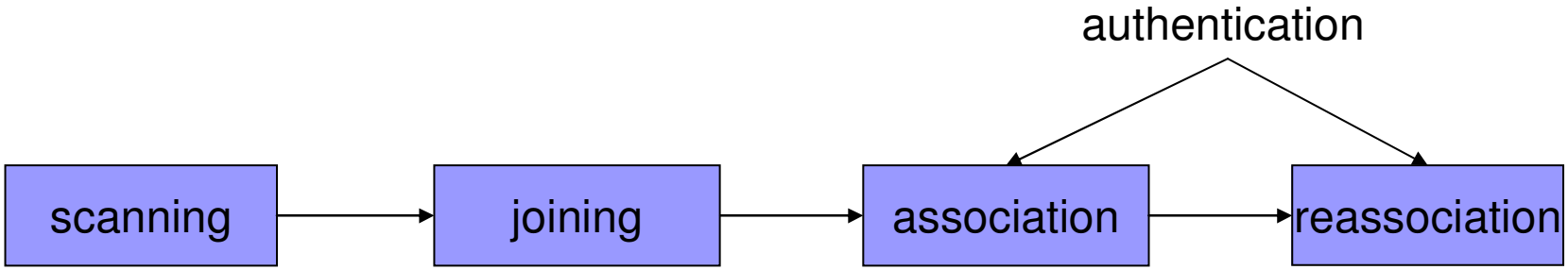


wlan management

- Because of the nature of wireless medium
  - unreliable
  - security
  - power limitation
- ➔ management operations



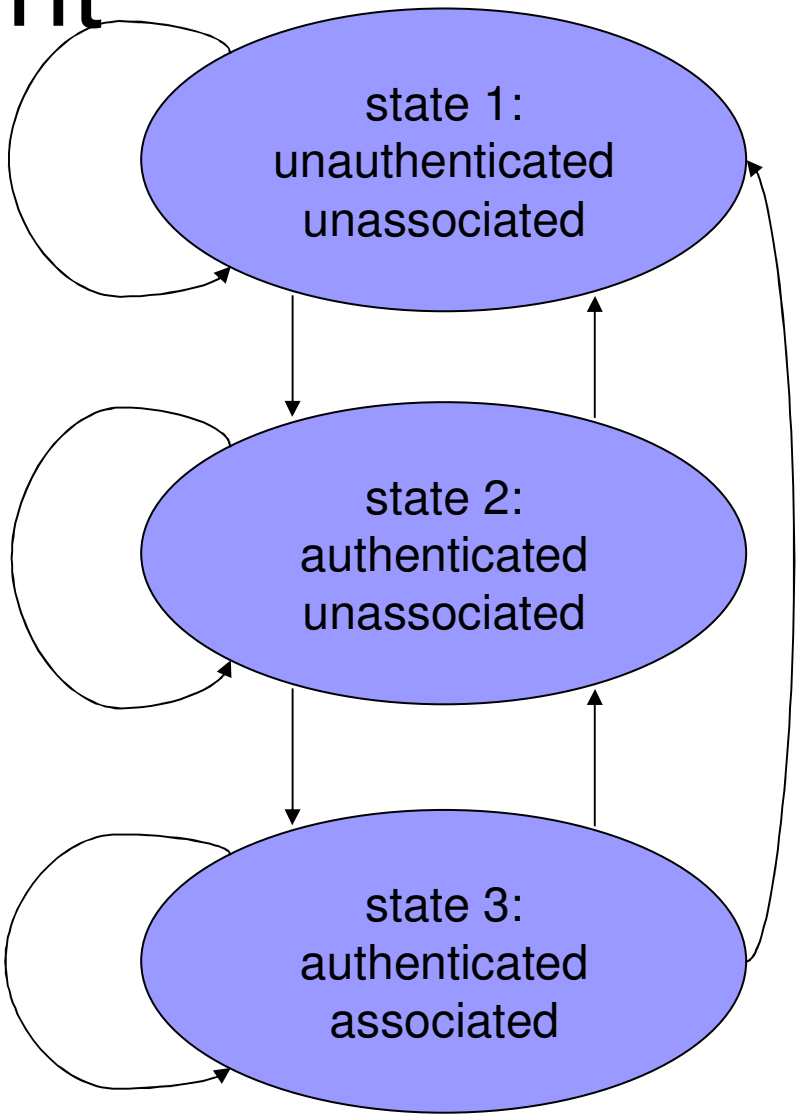
wlan management



- scanning
  - bssid, ssid, bsstype, scantype, channel list
- joining
  - matching local parameters, phy, synchronization, wep
- association
  - station is associated to a certain network
- reassociation
  - mobility management

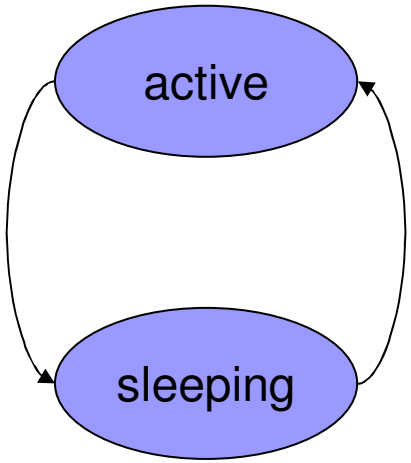
wlan management

- State 1, class 1 frames
  - RTS/CTS, ACK, beacons, …
- State 2, class 1& 2 frames
- State 3, class 1, 2 & 3 frames
  - data, power save, …



wlan management

- Power management
  - battery life
  - maximize the sleeping time
- Power save modes
  - sleeping (*off*)
  - active (*on*)



wlan management

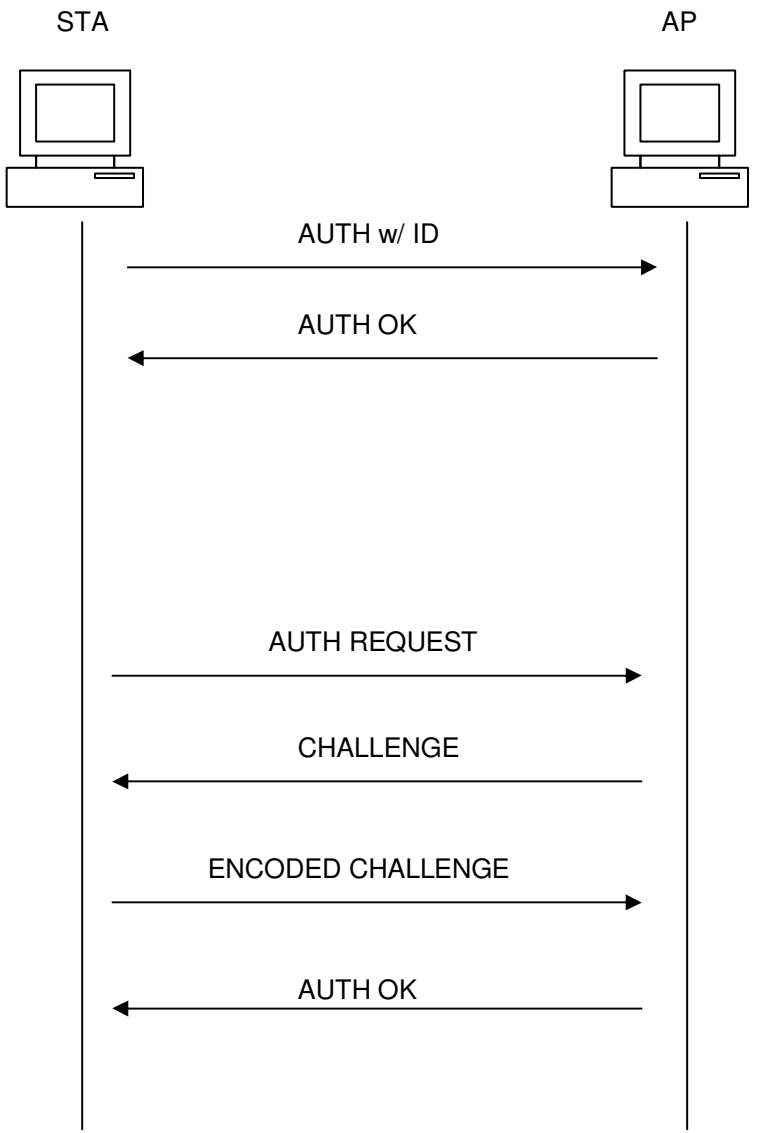
- Infrastructure *(w/ AP)*
  - AP buffers frames for sleeping (*off*) station
  - announces periodically buffer status
  - station powers up to listen buffer status
- Independent *(wo/ AP)*
  - sending station has to ensure that the receiver is active (*on*)
  - stations listen periodically for ATIM (*announcement traffic indication message*)

security

- Threats
  - Denial-of-Service (*DOS*)
  - Man-in-the-Middle (*MITM*)
  - Eavesdropping
    - Manipulating
  - Illicit Use
- Client and Access Point security
- Authentication, Authorization, Accounting

authentication

- open system
  - reply-response
  - address filtering
- shared key system
  - shared secret



security

- WEP
  - specified in 802.11
  - reasonably strong
    - length of the secret key
  - efficient
    - can be implemented in hardware or software
  - optional in 802.11
- problems
  - no access point authorization
  - poor key management *(static shared secret)*
  - considered as broken

security

- WPA
  - pre-shared keys
  - cipher and authetication negotiation
  - more secure key management
  - RADIUS
  - supports existing infrastructure
- problems
  - not a standard *(replaced with 802.11i)*

homework

- Show how the available data rates over the radio interface are derived
  - E.g. 6 Mbit/s uses BPSK (1 bit) and ½ coding rate (hint modulation * subchannels * coding = bits / symbol)

references

- OFDM Wireless LANs: A Theoretical and Practical Guide
  - Juha Heiskala
- 802.11 Security
  - Bruce Potter
- Wireless LANs: Implementing High Performance IEEE 802.11 Neworks
  - Jim Geier
- S-72.333 PG Course in Radiocommunications
  - 2004 presentations