# Chapter 5 (Part 3)
# LINK LAYER

Distributed Computing Group

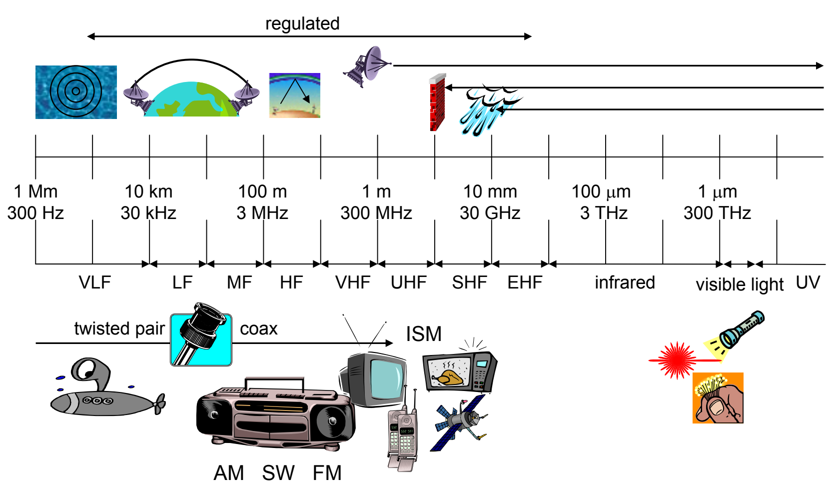
Computer Networks
Summer 2007

## Overview

- More Wireless Basics
- IEEE 802.11
  - Architecture, Protocol
  - PHY, MAC
  - Cyclic Redundancy codes
  - Roaming, Security
  - a, b, g, etc.
- Bluetooth
- RFID



## Physical Layer: Wireless Frequencies





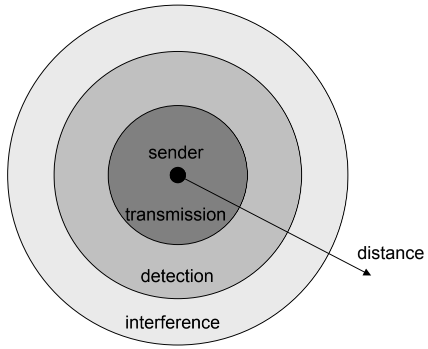

## Frequencies and regulations

- ITU-R holds auctions for new frequencies, manages frequency bands worldwide (WRC, World Radio Conferences)

| | Europe (CEPT/ETSI) | USA (FCC) | Japan |
|---|---|---|---|
| **Mobile phones** | **NMT** 453-457MHz, 463-467 MHz<br>**GSM** 890-915 MHz, 935-960 MHz, 1710-1785 MHz, 1805-1880 MHz | **AMPS**, **TDMA**, **CDMA** 824-849 MHz, 869-894 MHz<br>**TDMA**, **CDMA**, **GSM** 1850-1910 MHz, 1930-1990 MHz | **PDC** 810-826 MHz, 940-956 MHz, 1429-1465 MHz, 1477-1513 MHz |
| **Cordless telephones** | **CT1+** 885-887 MHz, 930-932 MHz<br>**CT2** 864-868 MHz<br>**DECT** 1880-1900 MHz | **PACS** 1850-1910 MHz, 1930-1990 MHz<br>**PACS-UB** 1910-1930 MHz | **PHS** 1895-1918 MHz<br>**JCT** 254-380 MHz |
| **Wireless LANs** | **IEEE 802.11** 2400-2483 MHz<br>**HIPERLAN 1** 5176-5270 MHz | **IEEE 802.11** 2400-2483 MHz | **IEEE 802.11** 2471-2497 MHz |

## Signal propagation ranges

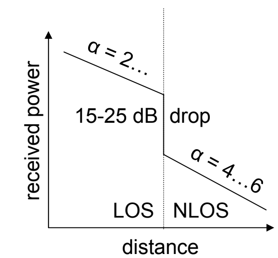
- Propagation in free space always like light (straight line)
- Transmission range
  - communication possible
  - low error rate
- Detection range
  - detection of the signal possible
  - no communication possible
- Interference range
  - signal may not be detected
  - signal adds to the background noise






## Attenuation by distance

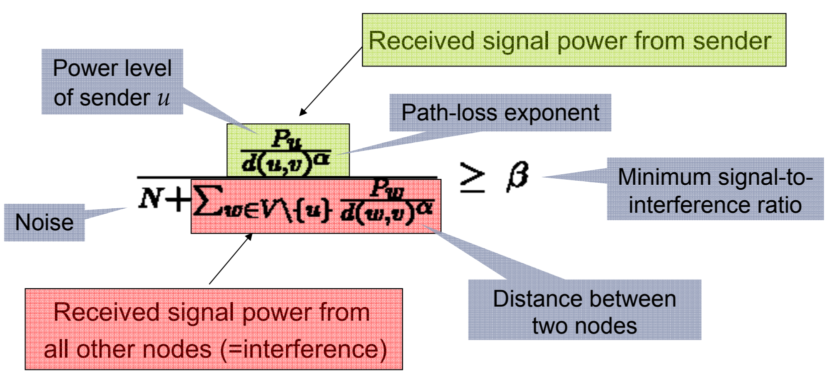
- Attenuation [dB] = 10 $\log_{10}$ (transmitted power / received power)
- Example: factor 2 loss = 10 $\log_{10} 2 \approx 3$ dB
- In theory/vacuum (and for short distances), receiving power is proportional to $1/d^2$, where d is the distance.
- In practice (for long distances), receiving power is proportional to $1/d^{\alpha}$, $\alpha$ = 4…6. We call $\alpha$ the path loss exponent.
- Example: Short distance, what is the attenuation between 10 and 100 meters distance?
  Factor 100 (=$100^2/10^2$) loss = 20 dB






## Signal-to-Interference-Plus-Noise Ratio

- Communication theorists study complex fading and signal-to-noise-plus-interference (SINR)-based models
- Simplest case:
  → packets can be decoded if SINR is larger than $\beta$ at receiver

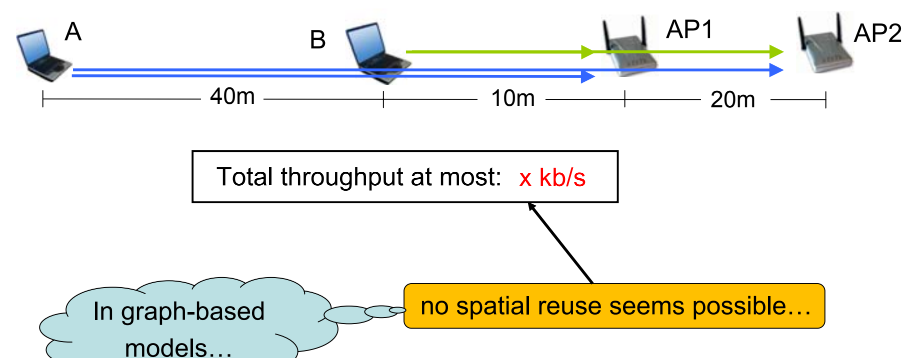



$$\frac{\frac{P_u}{d(u,v)^{\alpha}}}{N + \sum_{w \in V \setminus \{u\}} \frac{P_w}{d(w,v)^{\alpha}}} \geq \beta$$



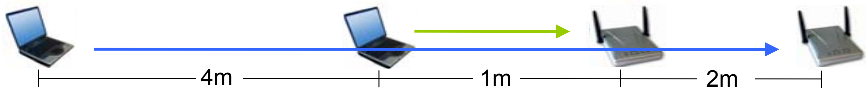
## Example

- Clients A and B want to send (max. rate x kb/s)
- Assume there is a single frequency
- What total throughput („spatial reuse“) can be achieved...?



## Example

A sends to AP2, B sends to AP1 → (max. rate x kb/s)




- Assume a single frequency (and no fancy decoding techniques!)
- Let $\alpha$=3, $\beta$=3, and N=10nW
- Set the transmission powers as follows $P_B$= -15 dBm and $P_A$= 1 dBm

SINR of A at AP2: $$\frac{1.26mW/(7m)^3}{0.01\mu W + 31.6\mu W/(3m)^3} \approx 3.11 \geq \beta$$

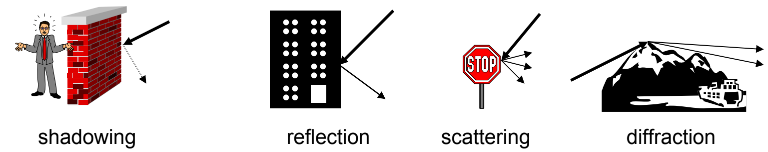
SINR of B at AP1: $$\frac{31.6\mu W/(1m)^3}{0.01\mu W + 1.26mW/(5m)^3} \approx 3.13 \geq \beta$$

**A total throughput of 2x kb/s is possible !**



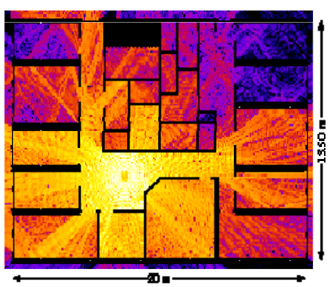
## Attenuation by objects

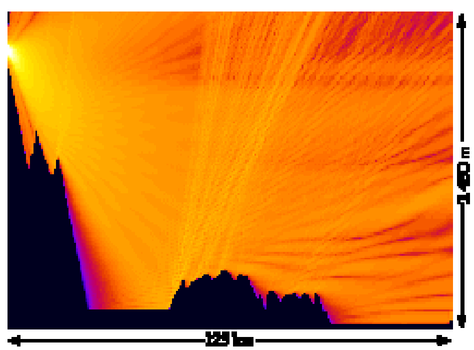
- Shadowing (3-30 dB):
  - textile (3 dB)
  - concrete walls (13-20 dB)
  - floors (20-30 dB)
- reflection at large obstacles
- scattering at small obstacles
- diffraction at edges
- fading (frequency dependent)






## Real World Examples

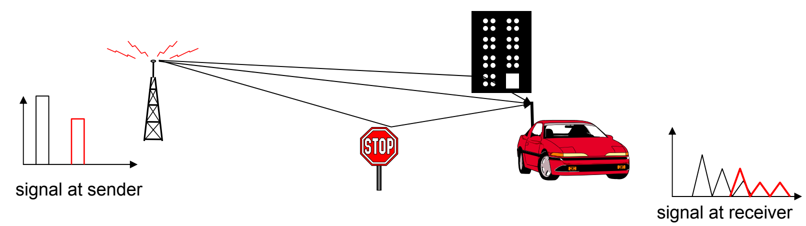






## Multipath propagation

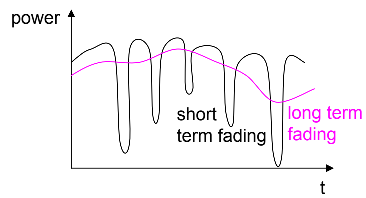
- Signal can take many different paths between sender and receiver due to reflection, scattering, diffraction




- Time dispersion: signal is dispersed over time
- Interference with "neighbor" symbols: Inter Symbol Interference (ISI)
- The signal reaches a receiver directly and phase shifted
- Distorted signal depending on the phases of the different parts

## Effects of mobility

- Channel characteristics change over time and location
  - signal paths change
  - different delay variations of different signal parts
  - different phases of signal parts
- quick changes in power received (short term fading)
- Additional changes in
  - distance to sender
  - obstacles further away
- slow changes in average power received (long term fading)




- Doppler shift: Random frequency modulation



## Wireless LAN 802.11: Design goals

- Global, seamless operation
- Low power consumption for battery use
- No special permissions or licenses required
- Robust transmission technology
- Simplified spontaneous cooperation at meetings
- Easy to use for everyone, simple management
- Interoperable with wired networks
- Security (no one should be able to read my data), privacy (no one should be able to collect user profiles), safety (low radiation)
- Transparency concerning applications and higher layer protocols, but also location awareness if necessary



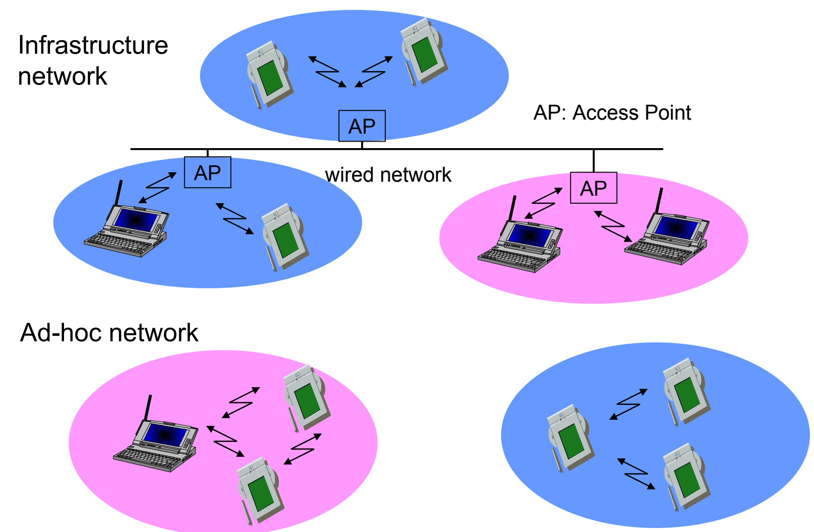
## Wireless LAN 802.11: Characteristics

+ Very flexible (economical to scale)
+ Ad-hoc networks without planning possible
+ (Almost) no wiring difficulties (e.g. historic buildings, firewalls)
+ More robust against disasters or users pulling a plug

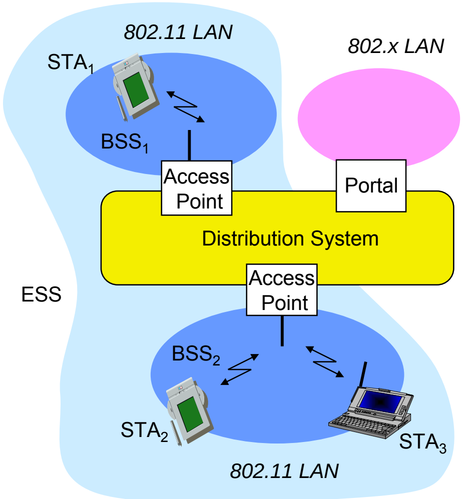
– Low bandwidth compared to wired networks (10 vs. 100[0] Mbit/s)
– Many proprietary solutions, especially for higher bit-rates, standards take their time
– Products have to follow many national restrictions if working wireless, it takes a long time to establish global solutions (IMT-2000)
– Security
– Economy



## Infrastructure vs. ad-hoc networks



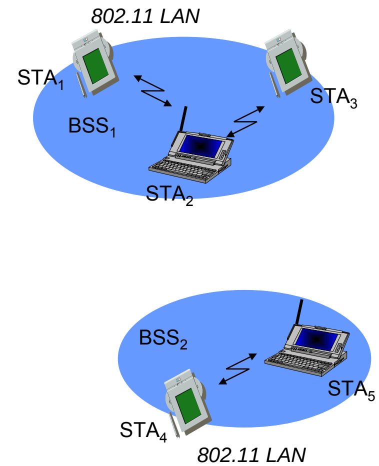
## 802.11 – Architecture of an infrastructure network




- 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 (ESS: Extended Service Set) based on several BSS



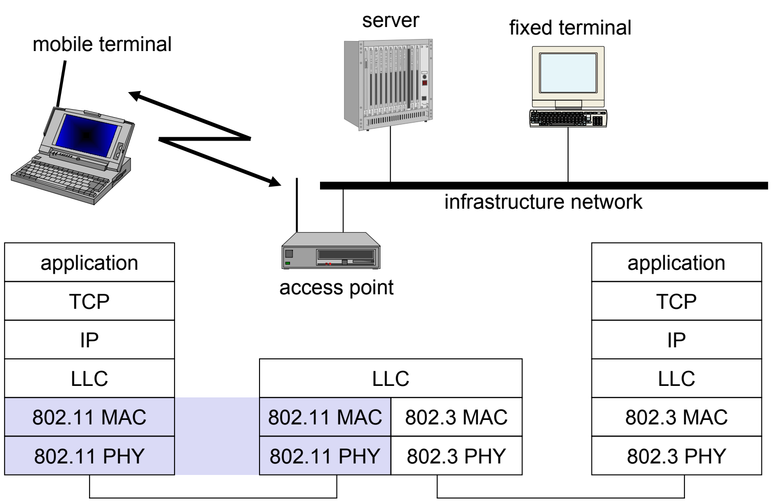
## 802.11 – Architecture of an ad-hoc network




- Direct communication within a limited range
  - Station (STA): terminal with access mechanisms to the wireless medium
  - [Independent] Basic Service Set ([I]BSS): group of stations using the same radio frequency
- You may use SDM or FDM to establish several BSS.



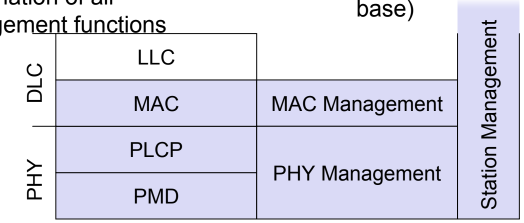
## 802.11 – Protocol architecture






## 802.11 – The lower layers in detail

- PMD (Physical Medium Dependent)
  - modulation, coding
- PLCP (Physical Layer Convergence Protocol)
  - clear channel assessment signal (carrier sense)
- PHY Management
  - channel selection, PHY-MIB
- Station Management
  - coordination of all management functions
- MAC
  - access mechanisms
  - fragmentation
  - encryption
- MAC Management
  - Synchronization
  - roaming
  - power management
  - MIB (management information base)



# Infrared vs. Radio transmission

Infrared
- uses IR diodes, diffuse light, multiple reflections (walls, furniture etc.)
- \+ simple, cheap, available in many mobile devices
- \+ no licenses needed
- \+ simple shielding possible
- – interference by sunlight, heat sources etc.
- – many things shield or absorb IR light
- – low bandwidth
- Example: IrDA (Infrared Data Association) interface available everywhere

Radio
- typically using the license free ISM band at 2.4 GHz
- \+ experience from wireless WAN and mobile phones can be used
- \+ coverage of larger areas possible (radio can penetrate walls, furniture etc.)
- – very limited license free frequency bands
- – shielding more difficult, interference with other electrical devices
- Examples: HIPERLAN, Bluetooth



# 802.11 - Physical layer (802.11legacy)

- 3 versions: 2 radio (2.4 GHz), 1 IR (outdated):
- FHSS (Frequency Hopping Spread Spectrum)
  - spreading, despreading, signal strength, 1 Mbit/s
  - at least 2.5 frequency hops/s, two-level GFSK modulation
- DSSS (Direct Sequence Spread Spectrum)
  - 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 2 (or optionally 1) Mbit/s
  - chipping sequence: Barker code (+ – + + – + + + – – –)
  - max. radiated power 1 W (USA), 100 mW (EU), min. 1mW
- Infrared
  - 850-950 nm, diffuse light,10 m range
  - carrier detection, energy detection, synchronization



# DSSS PHY packet format

- Synchronization
  - synch., gain setting, energy detection, frequency offset compensation
- SFD (Start Frame Delimiter)
  - 1111001110100000
- Signal
  - data rate of the payload (0x0A: 1 Mbit/s DBPSK; 0x14: 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 | | | | | |

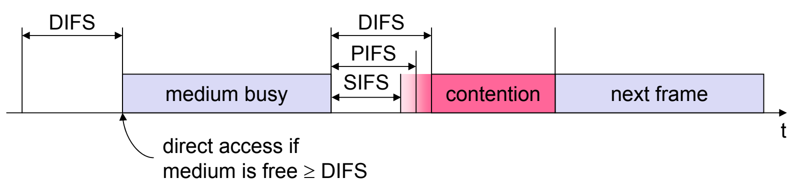


# MAC layer: DFWMAC

- 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 binary exponential back-off mechanism
    - minimum distance between consecutive packets
    - ACK packet for acknowledgements (not used for broadcasts)
  - DFWMAC-DCF w/ RTS/CTS (optional)
    - avoids hidden terminal problem
  - DFWMAC-PCF (optional)
    - access point polls terminals according to a list

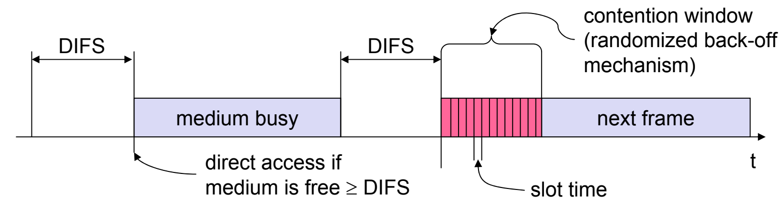
# MAC layer

- defined through different inter frame spaces
- no guaranteed, 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





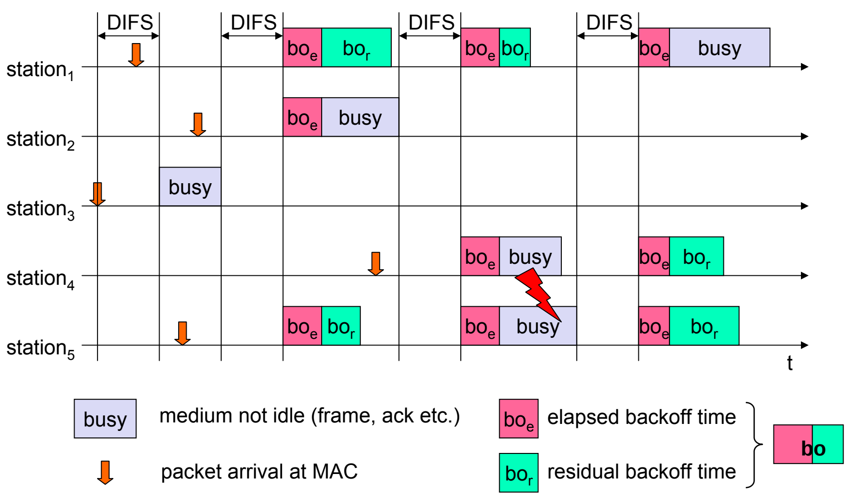

# CSMA/CA




- 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)



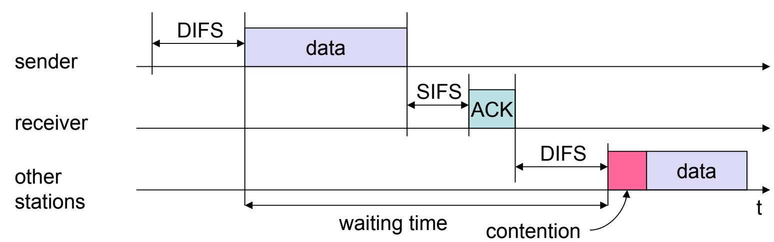
# Competing stations - simple example





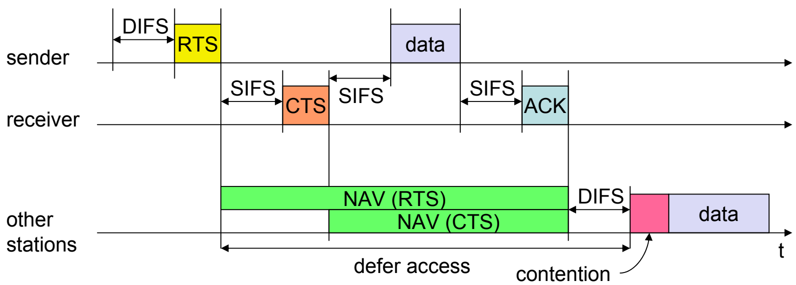

# CSMA/CA 2

- 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



# DFWMAC

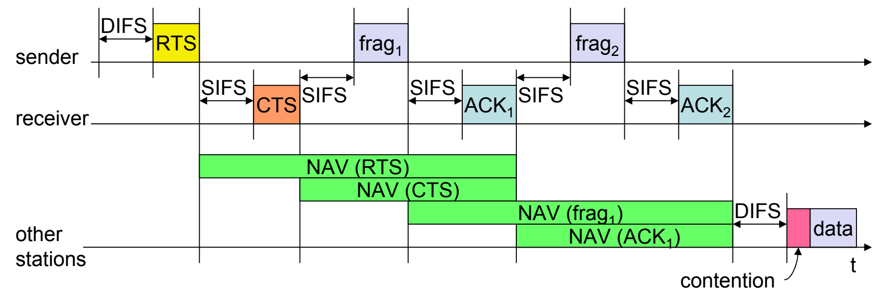
- station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
- acknowledgement via CTS after SIFS by receiver (if ready to receive)
- sender can now send data at once, acknowledgement via ACK
- other stations store medium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






# Fragmentation

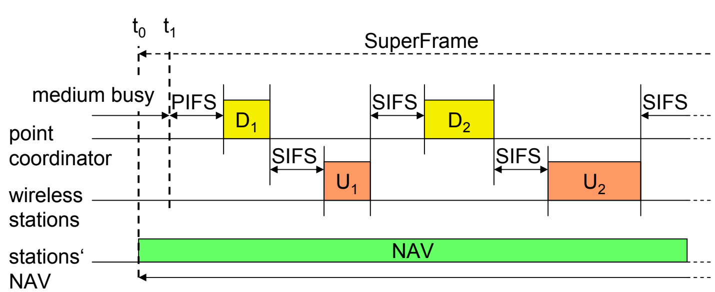
- If packet gets too long transmission error probability grows
- A simple back of the envelope calculation determines the optimal fragment size





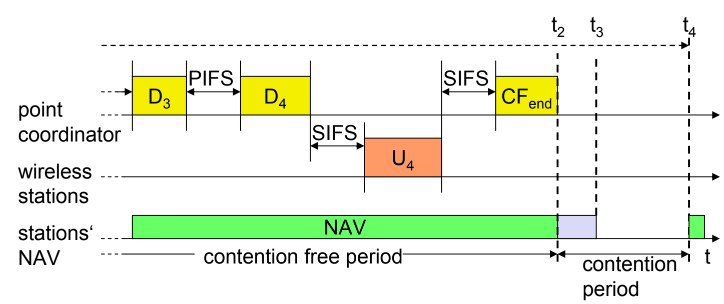

# DFWMAC-PCF

- An access point can poll stations






# DFWMAC-PCF 2



## Frame format

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

Byte 1: version, type, subtype
Byte 2: two DS-bits, fragm., retry, power man., more data, WEP, order

- Type
  - control frame, management frame, data frame
- Sequence control
  - important against duplicated frames due to lost ACKs
- Addresses
  - receiver, transmitter (physical), BSS identifier, sender (logical)
- 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

ACK

| bytes | 2 | 2 | 6 | 4 |
|---|---|---|---|---|
| | Frame Control | Duration | Receiver Address | CRC |

- Request To Send

RTS

| bytes | 2 | 2 | 6 | 6 | 4 |
|---|---|---|---|---|---|
| | Frame Control | Duration | Receiver Address | Transmitter Address | CRC |

- Clear To Send

CTS

| bytes | 2 | 2 | 6 | 4 |
|---|---|---|---|---|
| | Frame Control | Duration | Receiver Address | CRC |

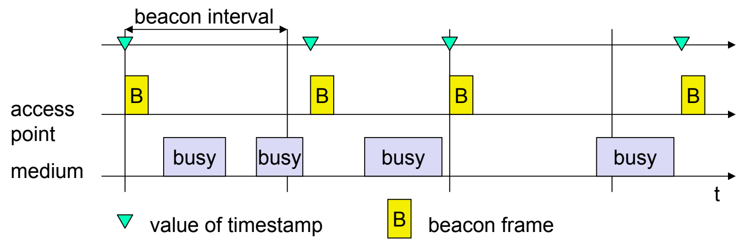


## MAC management

- 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

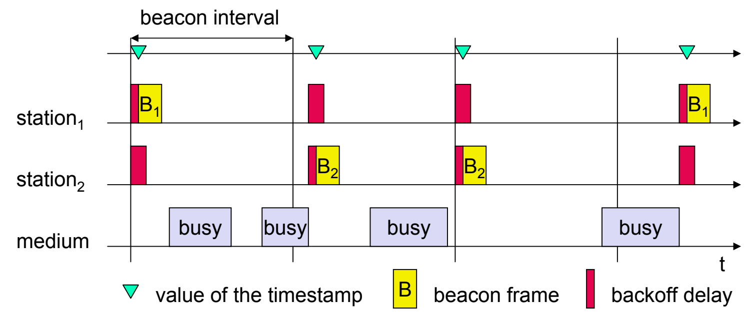
- In an infrastructure network, the access point can send a beacon






## Synchronization

- In an ad-hoc network, the beacon has to be sent by any station



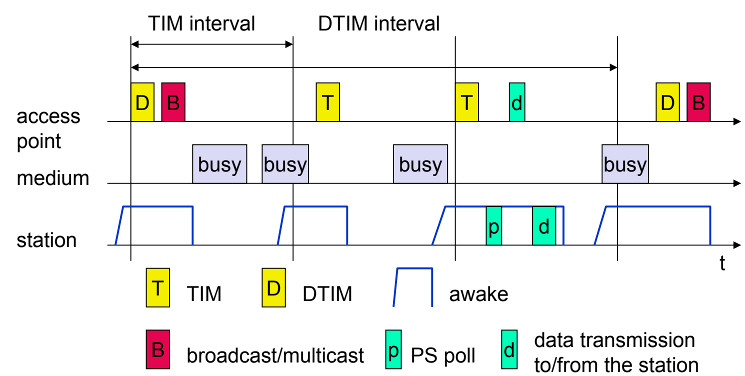



## Power management

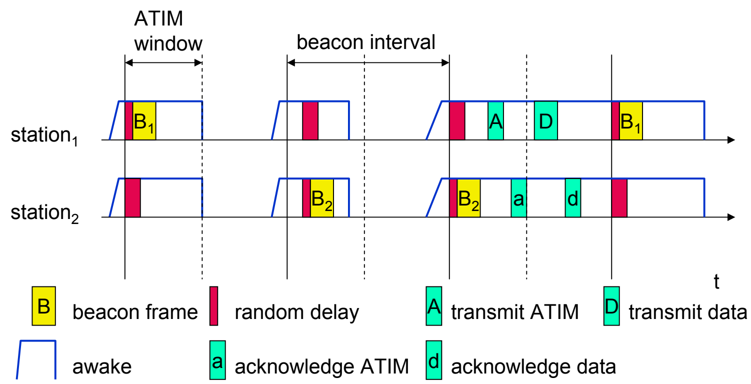
- Idea: if not needed turn off the transceiver
- States of a station: sleep and awake
- Timing Synchronization Function (TSF)
  - stations wake up at the same time
- Infrastructure
  - Traffic Indication Map (TIM)
    - list of unicast receivers transmitted by AP
  - Delivery Traffic Indication Map (DTIM)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






## Roaming

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



## Mobile Communication Technology according to IEEE

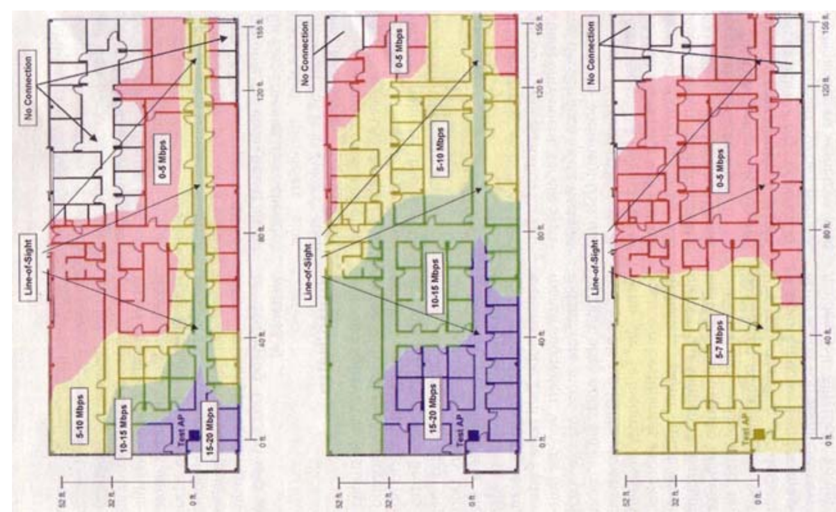
Local wireless networks
**WLAN** 802.11 — **WiFi**
- 802.11a → 802.11h
- 802.11i/e/…/w
- 802.11b → 802.11g

Personal wireless nw
**WPAN** 802.15
- **ZigBee** 802.15.4 → 802.15.4a/b
- 802.15.5
- 802.15.3 → 802.15.3a/b
- 802.15.2
- 802.15.1 **Bluetooth**

Wireless distribution networks
**WMAN** 802.16 (Broadband Wireless Access) **WiMAX**
- **+ Mobility** → 802.20 (Mobile Broadband Wireless Access)



## Quiz: Which 802.11 standard?



## WLAN: IEEE 802.11 – future developments (03/2005)

- 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)



## WLAN: IEEE 802.11– future developments (03/2005)

- 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 above 100Mbit/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



## WLAN: IEEE 802.11– future developments (03/2005)

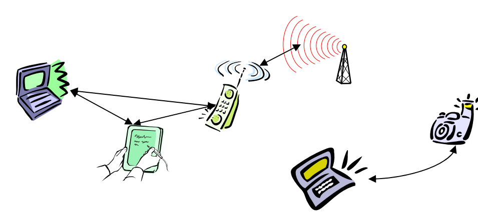
- 802.11r: Faster Handover between BSS
  - Secure, fast handover of a station from one AP to another within an ESS
  - Current mechanisms (even newer standards like 802.11i) plus incompatible devices from different vendors are massive problems for the use of, e.g., VoIP in WLANs
  - Handover should be 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.



## Bluetooth

- Idea
  - Universal radio interface for ad-hoc wireless connectivity
  - Interconnecting computer and peripherals, handheld devices, PDAs, cell phones – replacement of IrDA
  - Embedded in other devices, goal: 5€/device (2005: 40€/USB bluetooth)
  - Short range (10 m), low power consumption, license-free 2.45 GHz ISM
  - Voice and data transmission, approx. 1 Mbit/s gross data rate

One of the first modules (Ericsson).



## Bluetooth

- History
  - 1994: Ericsson (Mattison/Haartsen), “MC-link” project
  - Renaming of the project: Bluetooth according to Harald “Blåtand” Gormsen [son of Gorm], King of Denmark in the 10th century
  - 1998: foundation of Bluetooth SIG, www.bluetooth.org
  - 1999: erection of a rune stone at Ercisson/Lund ;-)
  - 2001: first consumer products for mass market, spec. version 1.1 released
- Special Interest Group
  - Original founding members: Ericsson, Intel, IBM, Nokia, Toshiba
  - Added promoters: 3Com, Agere (was: Lucent), Microsoft, Motorola
  - > 2500 members
  - Common specification and certification of products



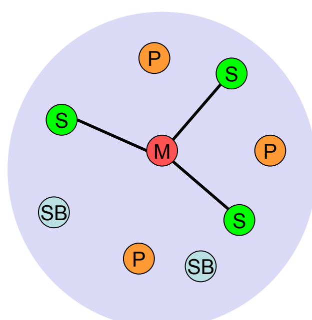
## Characteristics

- 2.4 GHz ISM band, 79 RF channels, 1 MHz carrier spacing
  - Channel 0: 2402 MHz … channel 78: 2480 MHz
  - G-FSK modulation, 1-100 mW transmit power
- FHSS and TDD
  - Frequency hopping with 1600 hops/s
  - Hopping sequence in a pseudo random fashion, determined by a master
  - Time division duplex for send/receive separation
- Voice link – SCO (Synchronous Connection Oriented)
  - FEC (forward error correction), no retransmission, 64 kbit/s duplex, point-to-point, circuit switched
- Data link – ACL (Asynchronous ConnectionLess)
  - Asynchronous, fast acknowledge, point-to-multipoint, up to 433.9 kbit/s symmetric or 723.2/57.6 kbit/s asymmetric, packet switched
- Topology
  - Overlapping piconets (stars) forming a scatternet



## Piconet

- Collection of devices connected in an ad hoc fashion
- One unit acts as master and the others as slaves for the lifetime of the piconet
- Master determines hopping pattern, slaves have to synchronize
- Each piconet has a unique hopping pattern
- Participation in a piconet = synchronization to hopping sequence
- Each piconet has one master and up to 7 simultaneous slaves (> 200 could be parked)

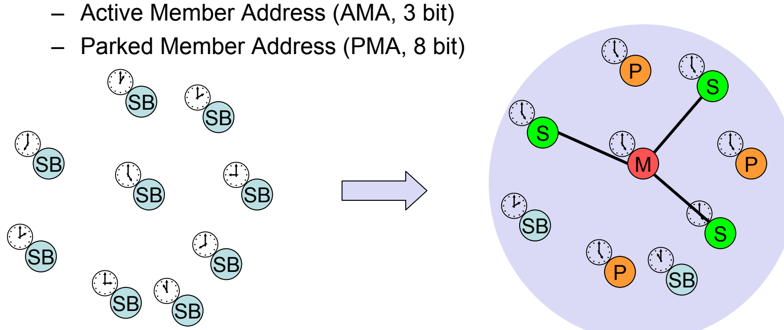



M=Master  
S=Slave  
P=Parked  
SB=Standby



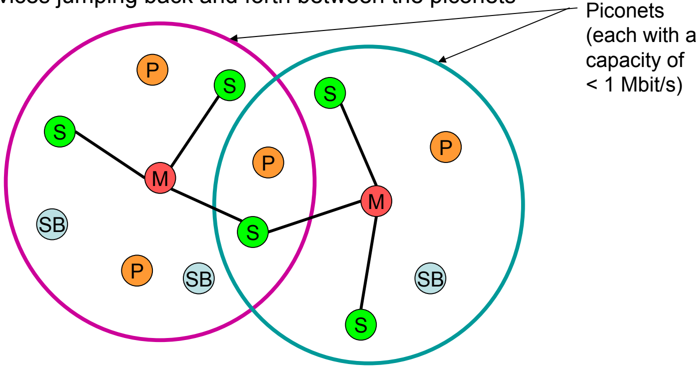
## Forming a piconet

- All devices in a piconet hop together
  - Master gives slaves its clock and device ID
    - Hopping pattern: determined by device ID (48 bit, unique worldwide)
    - Phase in hopping pattern determined by clock
- Addressing
  - Active Member Address (AMA, 3 bit)
  - Parked Member Address (PMA, 8 bit)



## Scatternet

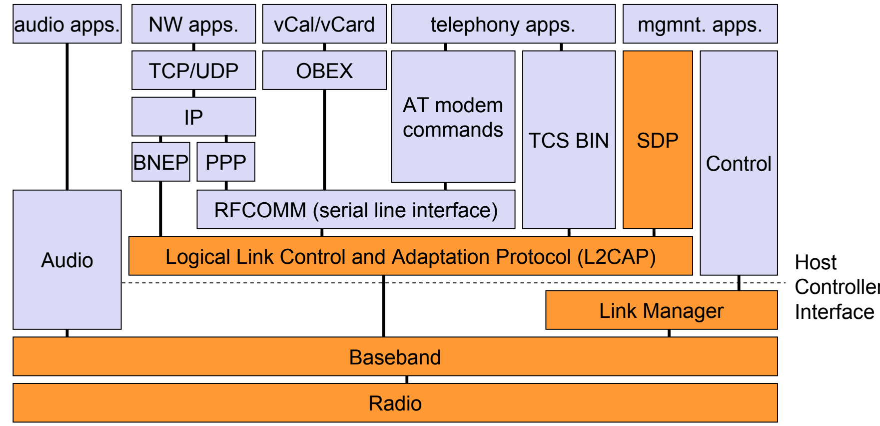
- Linking of multiple co-located piconets through the sharing of common master or slave devices
  - Devices can be slave in one piconet and master of another
- Communication between piconets
  - Devices jumping back and forth between the piconets




M=Master
S=Slave
P=Parked
SB=Standby



## Bluetooth protocol stack

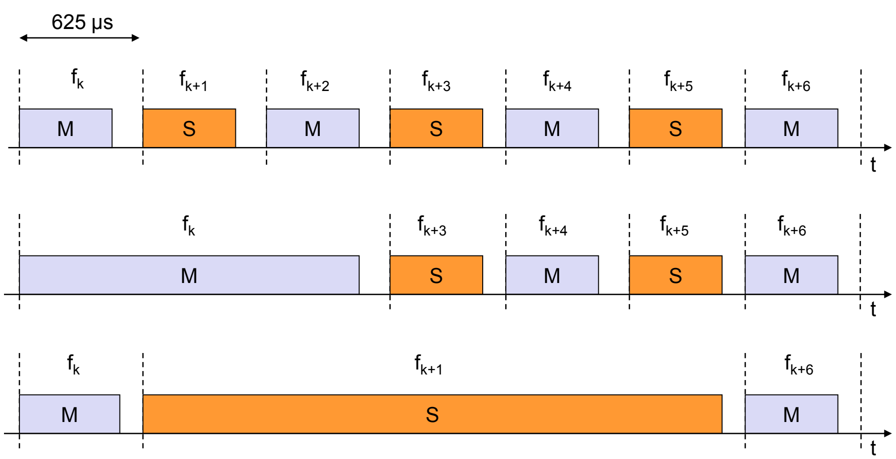



AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol

SDP: service discovery protocol
RFCOMM: radio frequency comm.



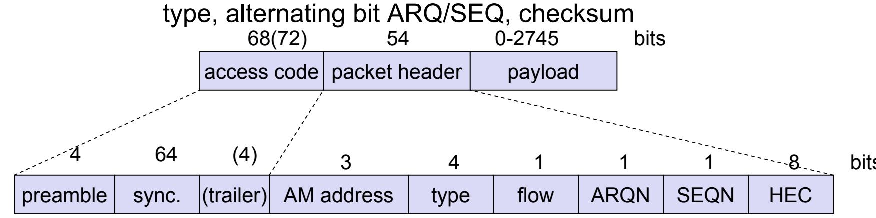
## Frequency selection during data transmission



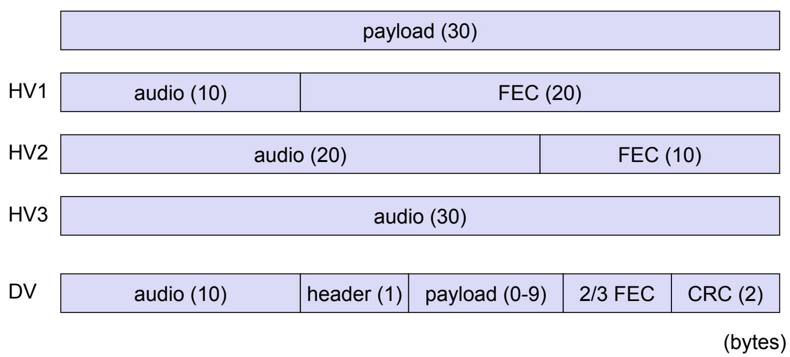



## Baseband

- Piconet/channel definition
- Low-level packet definition
  - Access code
    - Channel, device access, e.g., derived from master
  - Packet header
    - 1/3-FEC, active member address (broadcast + 7 slaves), link type, alternating bit ARQ/SEQ, checksum

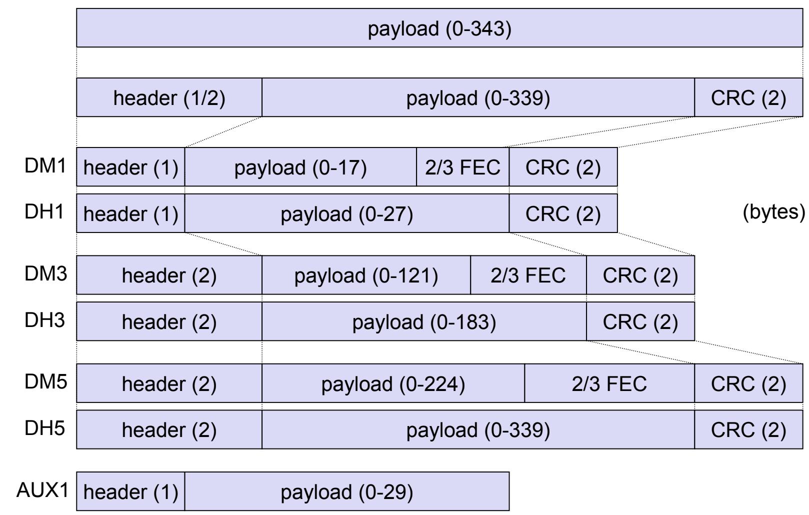


## SCO payload types






## ACL Payload types






## Baseband data rates

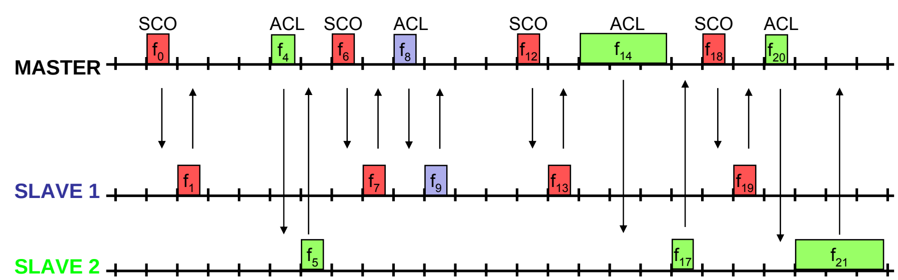
| ACL | Type | Payload Header [byte] | User Payload [byte] | FEC | CRC | Symmetric max. Rate [kbit/s] | Asymmetric max. Rate [kbit/s] Forward | Reverse |
|---|---|---|---|---|---|---|---|---|
| 1 slot | DM1 | 1 | 0-17 | 2/3 | yes | 108.8 | 108.8 | 108.8 |
| | DH1 | 1 | 0-27 | no | yes | 172.8 | 172.8 | 172.8 |
| 3 slot | DM3 | 2 | 0-121 | 2/3 | yes | 258.1 | 387.2 | 54.4 |
| | DH3 | 2 | 0-183 | no | yes | 390.4 | 585.6 | 86.4 |
| 5 slot | DM5 | 2 | 0-224 | 2/3 | yes | 286.7 | 477.8 | 36.3 |
| | DH5 | 2 | 0-339 | no | yes | **433.9** | **723.2** | 57.6 |
| | AUX1 | 1 | 0-29 | no | no | 185.6 | 185.6 | 185.6 |
| SCO | HV1 | na | 10 | 1/3 | no | 64.0 | | |
| | HV2 | na | 20 | 2/3 | no | 64.0 | | |
| | HV3 | na | 30 | no | no | 64.0 | | |
| | DV | 1 D | 10+(0-9) D | 2/3 D | yes D | 64.0+57.6 D | | |

*Data Medium/High rate, High-quality Voice, Data and Voice*



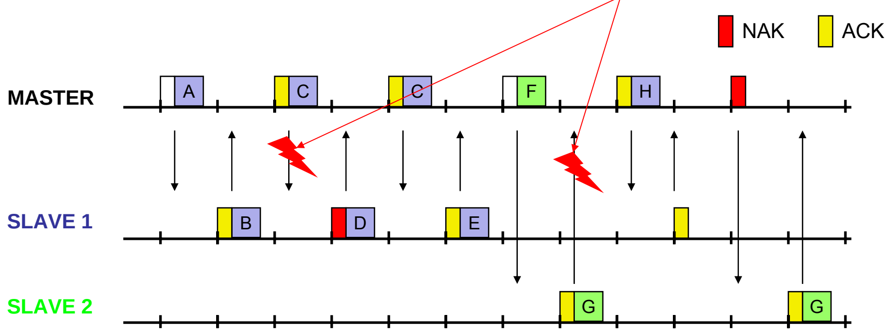
## Baseband link types

- Polling-based TDD packet transmission
  - 625µs slots, master polls slaves
- SCO (Synchronous Connection Oriented) – Voice
  - Periodic single slot packet assignment, 64 kbit/s full-duplex, point-to-point
- ACL (Asynchronous ConnectionLess) – Data
  - Variable packet size (1,3,5 slots), asymmetric bandwidth, point-to-multipoint



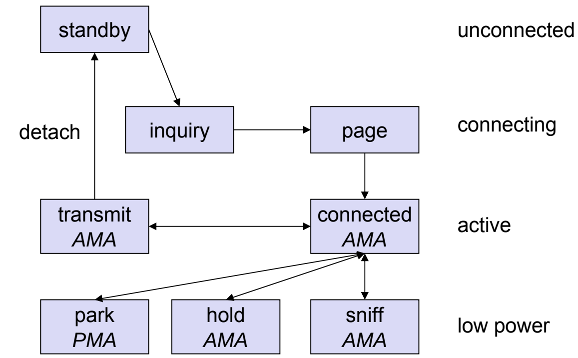
## Robustness

- Slow frequency hopping with hopping patterns determined by a master
  - Protection from interference on certain frequencies
  - Separation from other piconets (FH-CDMA)
- Retransmission
  - ACL only, very fast
- Forward Error Correction: SCO and ACL






## Baseband States of a Bluetooth Device




Standby: do nothing
Inquire: search for other devices
Page: connect to a specific device
Connected: participate in a piconet

Park: release AMA, get PMA
Sniff: listen periodically, not each slot
Hold: stop ACL, SCO still possible, possibly participate in another piconet



## Example: Power consumption/CSR BlueCore2

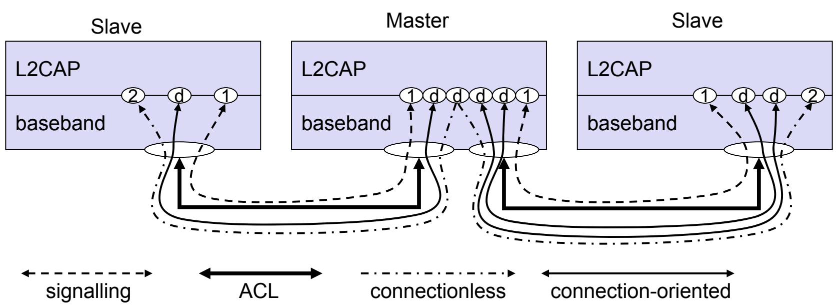
- **Typical Average Current Consumption (1)**
- VDD=1.8V Temperature = 20°C
- **Mode**
- SCO connection HV3 (1s interval Sniff Mode) (Slave) 26.0 mA
- SCO connection HV3 (1s interval Sniff Mode) (Master) 26.0 mA
- SCO connection HV1 (Slave) 53.0 mA
- SCO connection HV1 (Master) 53.0 mA
- ACL data transfer 115.2kbps UART (Master) 15.5 mA
- ACL data transfer 720kbps USB (Slave) 53.0 mA
- ACL data transfer 720kbps USB (Master) 53.0 mA
- ACL connection, Sniff Mode 40ms interval, 38.4kbps UART 4.0 mA
- ACL connection, Sniff Mode 1.28s interval, 38.4kbps UART 0.5 mA
- Parked Slave, 1.28s beacon interval, 38.4kbps UART 0.6 mA
- Standby Mode (Connected to host, no RF activity) 47.0 µA
- Deep Sleep Mode(2) 20.0 µA
- **Notes:**
- (1) Current consumption is the sum of both BC212015A and the flash.
- (2) Current consumption is for the BC212015A device only.
- (More: www.csr.com )



## L2CAP - Logical Link Control and Adaptation Protocol

- Simple data link protocol on top of baseband
- Connection oriented, connectionless, and signaling channels
- Protocol multiplexing
  - RFCOMM, SDP, telephony control
- Segmentation & reassembly
  - Up to 64kbyte user data, 16 bit CRC used from baseband
- QoS flow specification per channel
  - Follows RFC 1363, specifies delay, jitter, bursts, bandwidth
- Group abstraction
  - Create/close group, add/remove member

## L2CAP logical channels






## L2CAP packet formats

Connectionless PDU

| 2 | 2 | ≥2 | 0-65533 | bytes |
|---|---|---|---|---|
| length | CID=2 | PSM | payload | |

Connection-oriented PDU

| 2 | 2 | 0-65535 | bytes |
|---|---|---|---|
| length | CID | payload | |

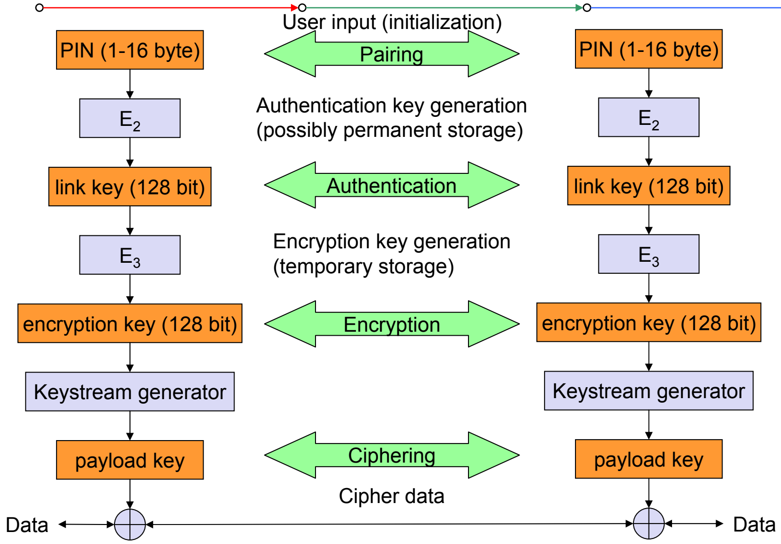
Signaling command PDU

| 2 | 2 | | bytes |
|---|---|---|---|
| length | CID=1 | One or more commands | |

| 1 | 1 | 2 | ≥0 |
|---|---|---|---|
| code | ID | length | data |



## Security






## SDP – Service Discovery Protocol

- Inquiry/response protocol for discovering services
  - Searching for and browsing services in radio proximity
  - Adapted to the highly dynamic environment
  - Can be complemented by others like SLP, Jini, Salutation, …
  - Defines discovery only, not the usage of services
  - Caching of discovered services
  - Gradual discovery
- Service record format
  - Information about services provided by attributes
  - Attributes are composed of an 16 bit ID (name) and a value
  - values may be derived from 128 bit Universally Unique Identifiers (UUID)

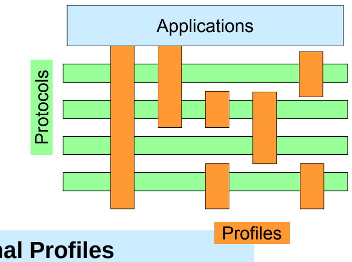
## Additional protocols to support legacy protocols/apps

- RFCOMM
  - Emulation of a serial port (supports a large base of legacy applications)
  - Allows multiple ports over a single physical channel
- Telephony Control Protocol Specification (TCS)
  - Call control (setup, release)
  - Group management
- OBEX
  - Exchange of objects, IrDA replacement
- WAP
  - Interacting with applications on cellular phones



## Profiles

- Represent default solutions for usage models
  - Vertical slice through the protocol stack
  - Basis for interoperability
- Generic Access Profile
- Service Discovery Application Profile
- Cordless Telephony Profile
- Intercom Profile
- Serial Port Profile
- Headset Profile
- Dial-up Networking Profile
- Fax Profile
- LAN Access Profile
- Generic Object Exchange Profile
- Object Push Profile
- File Transfer Profile
- Synchronization Profile




**Additional Profiles**
Advanced Audio Distribution
PAN
Audio Video Remote Control
Basic Printing
Basic Imaging
Extended Service Discovery
Generic Audio Video Distribution
Hands Free
Hardcopy Cable Replacement



## WPAN: IEEE 802.15-1 – Bluetooth

- Data rate
  - Synchronous, connection-oriented: 64 kbit/s
  - Asynchronous, connectionless
    - 433.9 kbit/s symmetric
    - 723.2 / 57.6 kbit/s asymmetric
- Transmission range
  - POS (Personal Operating Space) up to 10 m
  - with special transceivers up to 100 m
- Frequency
  - Free 2.4 GHz ISM-band
- Security
  - Challenge/response (SAFER+), hopping sequence
- Cost
  - 50€ adapter, drop to 5€ if integrated
- Availability
  - Integrated into some products, several vendors



## WPAN: IEEE 802.15-1 – Bluetooth

- Connection set-up time
  - Depends on power-mode
  - Max. 2.56s, avg. 0.64s
- Quality of Service
  - Guarantees, ARQ/FEC
- Manageability
  - Public/private keys needed, key management not specified, simple system integration

\+ Advantages: already integrated into several products, available worldwide, free ISM-band, several vendors, simple system, simple ad-hoc networking, peer to peer, scatternets

– Disadvantages: interference on ISM-band, limited range, max. 8 devices/network&master, high set-up latency

## WPAN: IEEE 802.15 – future developments

- 802.15-2: Coexistence
  - Coexistence of Wireless Personal Area Networks (802.15) and Wireless Local Area Networks (802.11), quantify the mutual interference
- 802.15-3: High-Rate
  - Standard for high-rate (20Mbit/s or greater) WPANs, while still low-power/low-cost
  - Data Rates: 11, 22, 33, 44, 55 Mbit/s
  - Quality of Service isochronous protocol
  - Ad-hoc peer-to-peer networking
  - Security
  - Low power consumption
  - Low cost
  - Designed to meet the demanding requirements of portable consumer imaging and multimedia applications



## WPAN: IEEE 802.15 – future developments

- 802.15-4: Low-Rate, Very Low-Power
  - Low data rate solution with multi-month to multi-year battery life and very low complexity
  - Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation
  - Data rates of 20-250 kbit/s, latency down to 15 ms
  - Master-Slave or Peer-to-Peer operation
  - Support for critical latency devices, such as joysticks
  - CSMA/CA channel access (data centric), slotted (beacon) or unslotted
  - Automatic network establishment by the PAN coordinator
  - Dynamic device addressing, flexible addressing format
  - Fully handshaked protocol for transfer reliability
  - Power management to ensure low power consumption
  - 16 channels in the 2.4 GHz ISM band, 10 channels in the 915 MHz US ISM band and one channel in the European 868 MHz band



## RFID – Radio Frequency Identification

- Function
  - Standard: In response to a radio interrogation signal from a reader (base station) the RFID tags transmit their ID
  - Enhanced: additionally data can be sent to the tags, different media access schemes (collision avoidance)
- Features
  - No line-of sight required (compared to, e.g., laser scanners)
  - RFID tags withstand difficult environmental conditions (sunlight, cold, frost, dirt etc.)
  - Products available with read/write memory, smart-card capabilities
- Categories
  - Passive RFID: operating power comes from the reader over the air which is feasible up to distances of 3 m, low price (1€)
  - Active RFID: battery powered, distances up to 100 m



## RFID – Radio Frequency Identification

- Data rate
  - Transmission of ID only (e.g., 48 bit, 64kbit, 1 Mbit)
  - 9.6 – 115 kbit/s
- Transmission range
  - Passive: up to 3 m
  - Active: up to 30-100 m
  - Simultaneous detection of up to, e.g., 256 tags, scanning of, e.g., 40 tags/s
- Frequency
  - 125 kHz, 13.56 MHz, 433 MHz, 2.4 GHz, 5.8 GHz and many others
- Security
  - Application dependent, typ. no crypt. on RFID device
- Cost
  - Very cheap tags, down to $1 (passive)
- Availability
  - Many products, many vendors
- Connection set-up time
  - Depends on product/medium access scheme (typ. 2 ms per device)
- Quality of Service
  - none
- Manageability
  - Very simple, same as serial interface

\+ Advantages: extremely low cost, large experience, high volume available, no power for passive RFIDs needed, large variety of products, relative speeds up to 300 km/h, broad temp. range

– Disadvantages: no QoS, simple denial of service, crowded ISM bands, typ. one-way (activation/ transmission of ID)

## RFID – Radio Frequency Identification

- Applications
  - Total asset visibility: tracking of goods during manufacturing, localization of pallets, goods etc.
  - Loyalty cards: customers use RFID tags for payment at, e.g., gas stations, collection of buying patterns
  - Automated toll collection: RFIDs mounted in windshields allow commuters to drive through toll plazas without stopping
  - Others: access control, animal identification, tracking of hazardous material, inventory control, warehouse management, ...
- Local Positioning Systems
  - GPS useless indoors or underground, problematic in cities with high buildings
  - RFID tags transmit signals, receivers estimate the tag location by measuring the signal‘s time of flight



## RFID – Radio Frequency Identification

- Example Product: Intermec RFID UHF OEM Reader
  - Read range up to 7m
  - Anticollision algorithm allows for scanning of 40 tags per second regardless of the number of tags within the reading zone
  - US: unlicensed 915 MHz, Frequency Hopping
  - Read: 8 byte < 32 ms
  - Write: 1 byte < 100ms

- Example Product: Wireless Mountain Spider
  - Proprietary sparse code anti-collision algorithm
  - Detection range 15 m indoor, 100 m line-of-sight
  - > 1 billion distinct codes
  - Read rate > 75 tags/s
  - Operates at 308 MHz



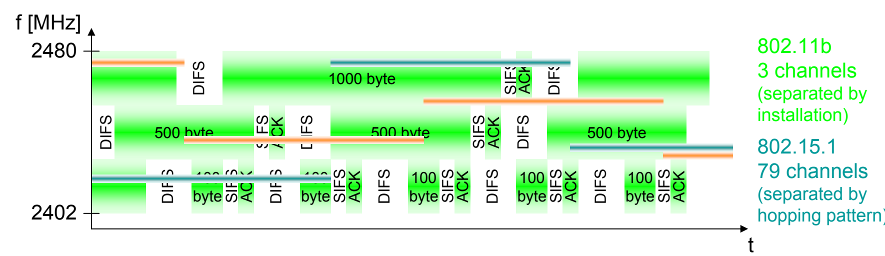
## ISM band interference

- Many sources of interference
  - Microwave ovens, microwave lightning
  - 802.11, 802.11b, 802.11g, 802.15, Home RF
  - Even analog TV transmission, surveillance
  - Unlicensed metropolitan area networks
  - …
- Levels of interference
  - Physical layer: interference acts like noise
    - Spread spectrum tries to minimize this
    - FEC/interleaving tries to correct
  - MAC layer: algorithms not harmonized
    - E.g., Bluetooth might confuse 802.11



## 802.11 vs. Bluetooth

- Bluetooth may act like a rogue member of the 802.11 network
  - Does not know anything about gaps, inter frame spacing etc.




- IEEE 802.15-2 discusses these problems
  - Proposal: Adaptive Frequency Hopping
    - a non-collaborative Coexistence Mechanism
- Real effects? Many different opinions, publications, tests, formulae:
  - Results from complete breakdown to almost no effect
  - Bluetooth (FHSS) seems more robust than 802.11b (DSSS)