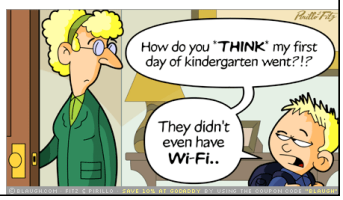
Wireless LANs

- Characteristics
- IEEE 802.11 (PHY, MAC, Roaming, .11a, b, g, h, i, n … z)
- Bluetooth / IEEE 802.15.x
- IEEE 802.16/.20/.21/.22
- RFID
- Comparison



Mobile Communication Technology according to IEEE (examples)

WiFi
Local wireless networks
WLAN 802.11
802.11a → 802.11h
802.11i/e/…/n/…/z
802.11b → 802.11g

ZigBee
Personal wireless nets
WPAN 802.15
802.15.4 → 802.15.4a/b/c/d/e
802.15.5, .6 (WBAN)
802.15.2
802.15.3 → 802.15.3b/c
802.15.1
Bluetooth

Wireless distribution networks
WMAN 802.16 (Broadband Wireless Access)
WiMAX
+ Mobility
[802.20 (Mobile Broadband Wireless Access)]
802.16e (addition to .16 for mobile devices)

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)
  - more robust against disasters like, e.g., earthquakes, fire - or users pulling a plug...
  - cheap (additional users don't increase cost)
- Disadvantages
  - typically very low bandwidth compared to wired networks (1-10 Mbit/s) due to shared medium, more interferences
  - many proprietary solutions, especially for higher bit-rates, standards take their time (e.g., IEEE 802.11n)
  - products have to follow many national regulations, takes time for global solutions (IMT-2000).
  - safety/security

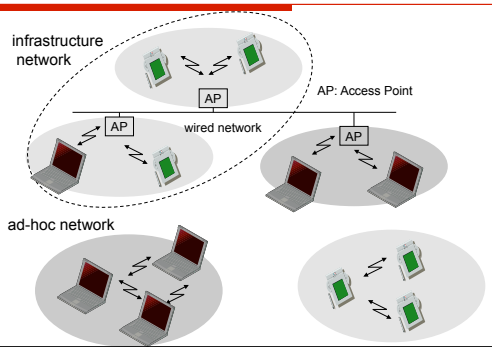
Design goals for wireless LANs

- global, seamless operation
- low power for battery use
- no special permissions or 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 (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
- …

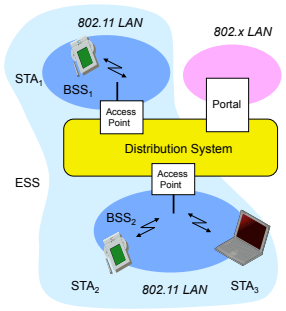
Comparison: infrared vs. radio transmission

- Infrared
  - uses IR diodes, diffuse light, multiple reflections (walls, furniture, etc.)
- Advantages
  - simple, cheap, available in many mobile devices
  - no licenses needed
  - simple shielding possible
- Disadvantages
  - 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
- Advantages
  - experience from wireless WAN and mobile phones can be used
  - coverage of larger areas possible (radio can penetrate walls, furniture etc.)
  - higher transmission rates
- Disadvantages
  - very limited license free frequency bands
  - shielding more difficult, interference with other electrical devices
- Example
  - many different products

Comparison: infrastructure vs. ad-hoc networks

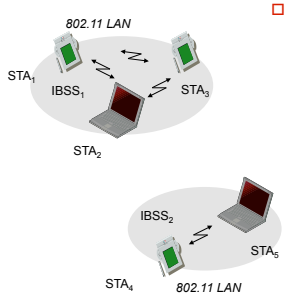


802.11 - Architecture of an infrastructure network



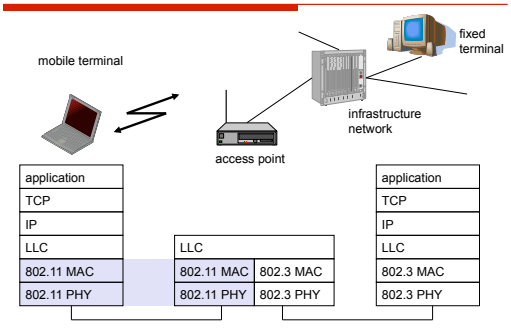
- Station (STA)
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- Basic Service Set (BSS)
  - group of stations using the same radio frequency
- Access Point
  - station integrated into the wireless LAN and the distribution system
- Portal
  - bridge to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

IEEE standard 802.11

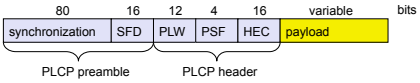


802.11 - Physical layer

- 3 versions: 2 radio (typ. 2.4 GHz), 1 IR
  - data rates 1 or 2 Mbit/s
- FHSS (Frequency Hopping Spread Spectrum)
  - spreading, despreading, signal strength, typ. 1 Mbit/s
  - min. 2.5 frequency hops/s (USA), 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 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

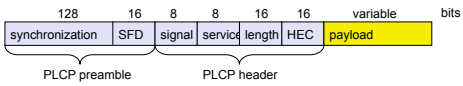
FHSS PHY packet format

- 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 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., 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, $x^{16}+x^{12}+x^5+1$

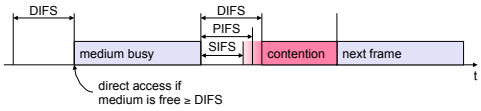


802.11 - MAC layer I - DFWMAC

- 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

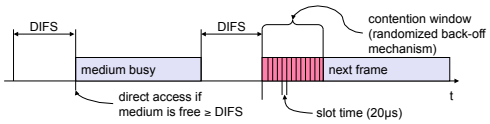
802.11 - MAC layer II

- Priorities
  - defined through different inter frame spaces
  - 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

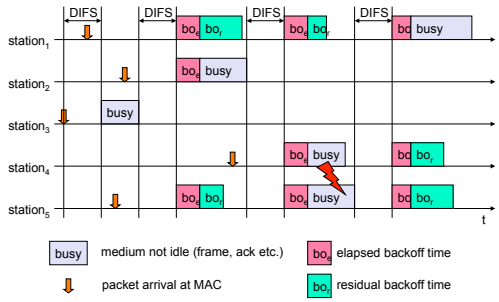


802.11 - CSMA/CA access method I

- 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)

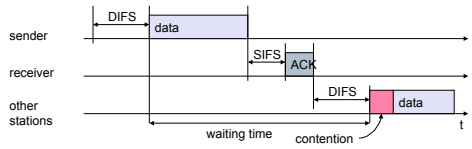


802.11 - competing stations - simple version



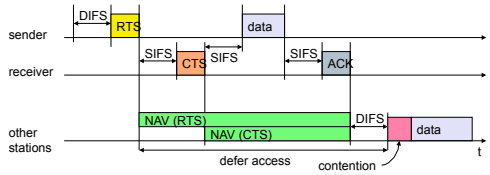
802.11 - CSMA/CA access method II

- 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

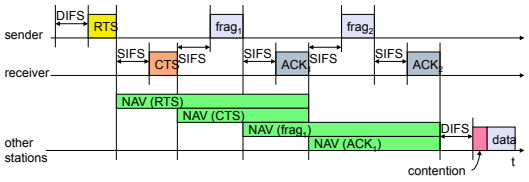


802.11 - DFWMAC

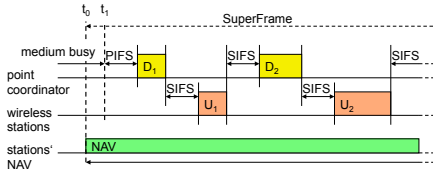
- Sending unicast packets
  - station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
  - acknowledgement via CTS after SIFS by receiver (if ready to receive)
  - sender can now send data at once, acknowledgement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



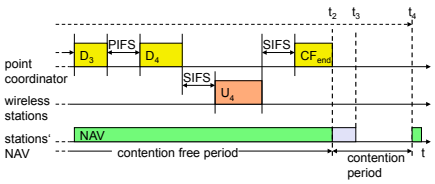
Fragmentation



DFWMAC-PCF I (almost never used)

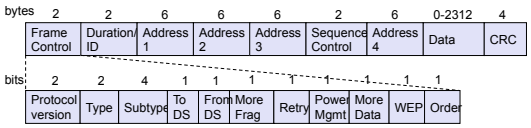


DFWMAC-PCF II



802.11 - Frame format

- Types
  - control frames, management frames, data frames
- Sequence numbers
  - important against duplicated frames due to lost ACKs
- Addresses
  - receiver, transmitter (physical), BSS identifier, sender (logical)
- Miscellaneous
  - sending time, checksum, frame control, data



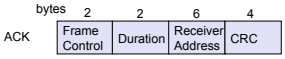
MAC address format

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

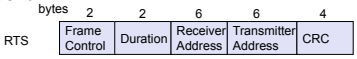
DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Basic Service Set Identifier
RA: Receiver Address
TA: Transmitter Address

Special Frames: ACK, RTS, CTS

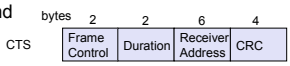
- Acknowledgement



- Request To Send



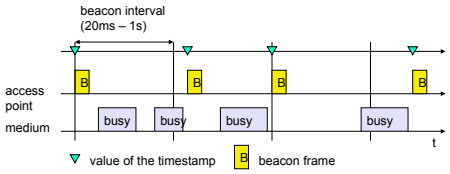
- Clear To Send



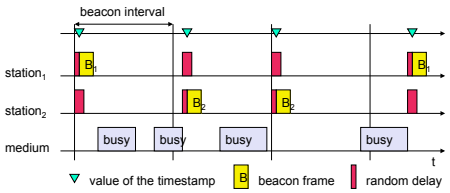
802.11 - MAC management

- Synchronization
  - try to find a LAN, try to stay within a LAN
  - synchronization of internal clocks, generation of beacons
- 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)



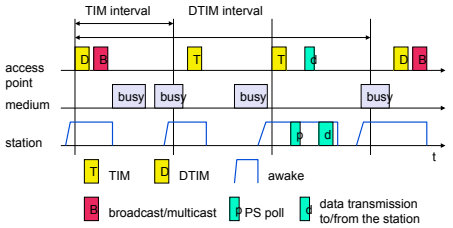
Synchronization using a Beacon (ad-hoc)



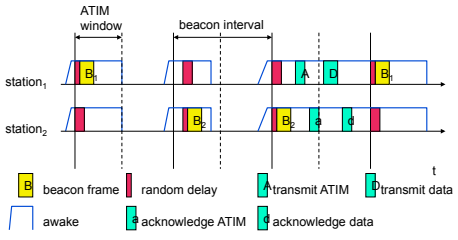
Power management

- 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?)
- APSD (Automatic Power Save Delivery)
  - new method in 802.11e replacing above schemes

Power saving with wake-up patterns (infrastructure)



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



802.11 - Roaming

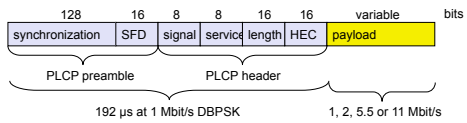
- No or bad connection? Then perform:
- Scanning
  - scan the environment, i.e., listen into the medium for beacon signals or send probes into the medium and wait for an answer
- Reassociation Request
  - station sends a request to one or several AP(s)
- Reassociation Response
  - success: AP has answered, 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
- Fast roaming – 802.11r
  - e.g., for vehicle-to-roadside networks

WLAN: IEEE 802.11b

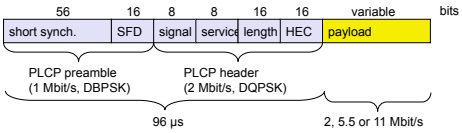
- Data rate
  - 1, 2, 5.5, 11 Mbit/s, depending on SNR
  - User data rate max. approx. 6 Mbit/s
- Transmission range
  - 300m outdoor, 30m indoor
  - Max. data rate ~10m indoor
- Frequency
  - DSSS, 2.4 GHz ISM-band
- Security
  - Limited, WEP insecure, SSID
- Availability
  - Many products, many vendors
- Connection set-up time
  - connectionless/always on
- Quality of Service
  - typ. best effort, no guarantees (unless polling is used, limited support in products)
- Manageability
  - limited (no automated key distribution, sym. encryption)
- Special Advantages/Disadvantages
  - advantage: many installed systems, lot of experience, available worldwide, free ISM-band, many vendors, integrated in laptops, simple system
  - disadvantage: heavy interference on ISM-band, no service guarantees, slow relative speed only

IEEE 802.11b – PHY frame formats

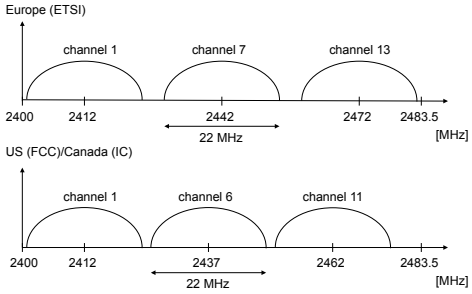
Long PLCP PPDU format



Short PLCP PPDU format (optional)



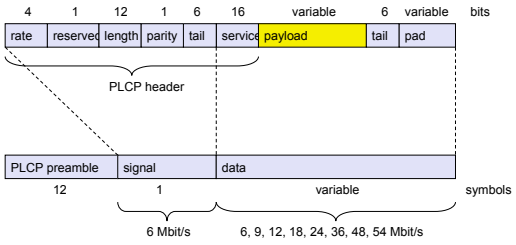
Channel selection (non-overlapping)



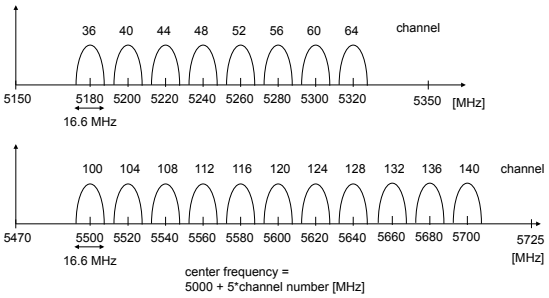
WLAN: IEEE 802.11a

- Data rate
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, depending on SNR
  - User throughput (1500 byte packets): 5.3 (6), 18 (24), 24 (36), 32 (54)
  - 6, 12, 24 Mbit/s mandatory
- Transmission range
  - 100m outdoor, 10m indoor
    - E.g., 54 Mbit/s up to 5 m, 48 up to 12 m, 36 up to 25 m, 24 up to 30m, 18 up to 40 m, 12 up to 60 m
- Frequency
  - Free 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz ISM-band
- Security
  - Limited, WEP insecure, SSID
- Availability
  - Some products, some vendors
- Connection set-up time
  - Connectionless/always on
- Quality of Service
  - Typ. best effort, no guarantees (same as all 802.11 products)
- Manageability
  - Limited (no automated key distribution, sym. Encryption)
- Special Advantages/Disadvantages
  - Advantage: fits into 802.x standards, free ISM-band, available, simple system, uses less crowded 5 GHz band
  - Disadvantage: stronger shading due to higher frequency, no QoS

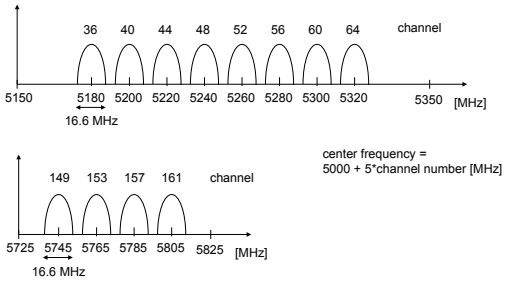
IEEE 802.11a – PHY frame format



Operating channels of 802.11a in Europe

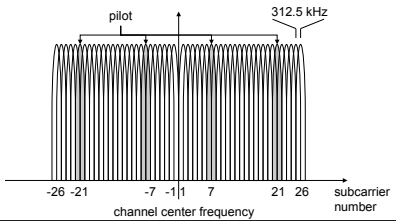


Operating channels for 802.11a / US U-NII



OFDM in IEEE 802.11a

- OFDM with 52 used subcarriers (64 in total)
  - 48 data + 4 pilot
    - (plus 12 virtual subcarriers)
  - 312.5 kHz spacing



WLAN: IEEE 802.11 – current developments (05/2008)

- 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… supported by HCCA (HCF (Hybrid Coordinator Function) Controlled Channel Access, optional)
  - Additional energy saving mechanisms and more efficient retransmission
  - EDCA (Enhanced Distributed Channel Access): high priority traffic waits less for channel access
- 802.11f: Inter-Access Point Protocol (withdrawn)
  - Establish an Inter-Access Point Protocol for data exchange via the distribution system
- **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)
- 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

WLAN: IEEE 802.11– current developments (05/2008)

- 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
- **802.11-2007**: Current "complete" standard
  - Comprises amendments a, b, d, e, g, h, i, j
- 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 802.11-2007 standard
- **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
- 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

WLAN: IEEE 802.11– current developments (05/2008)

- 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.
- 802.11y: Extensions for the 3650-3700 MHz band in the USA
- 802.11z: Extension to direct link setup

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

Bluetooth

Bluetooth

- Basic 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, very cheap
  - Short range (10 m), low power consumption, license-free 2.45 GHz ISM
  - Voice and data transmission, approx. 1 Mbit/s data rate

One of the first modules (Ericsson).

Bluetooth

(was: 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
  - 2005: 5 million chips/week

Bluetooth™

- Special Interest Group
  - Original founding members: Ericsson, Intel, IBM, Nokia, Toshiba
  - Added promoters: 3Com, Agere (was: Lucent), Microsoft, Motorola
  - > 10000 members
  - Common specification and certification of products

History and hi-tech…

…and the real rune stone

Located in Jelling, Denmark, erected by King Harald "Blåtand" in memory of his parents.
The stone has three sides – one side showing a picture of Christ.

This could be the "original" colors of the stone.

Inscription:
"Harald king executes these sepulchral monuments after Gorm, his father and Thyra, his mother. The Harald who won the whole of Denmark and Norway and turned the Danes to Christianity."

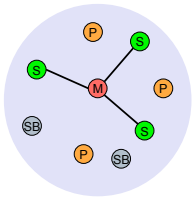
Btw: Blåtand means "of dark complexion" (not having a blue tooth…)

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, acknowledgments, 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)

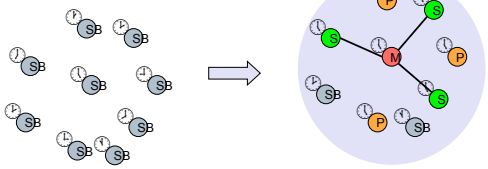


M=Master
S=Slave

P=Parked
SB=Standby

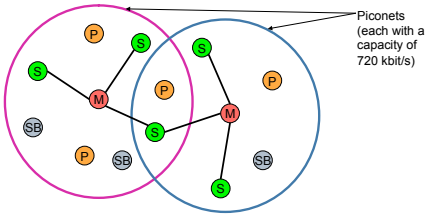
Forming a piconet

- 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

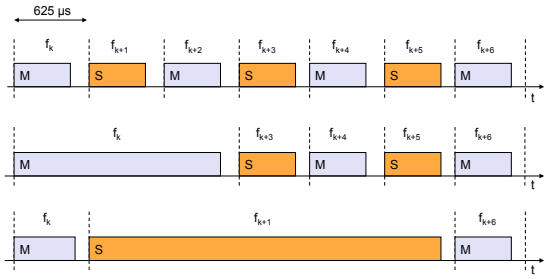
- Linking of multiple co-located piconets through the sharing of common master or slave devices
  - Devices can be slave in one piconet and master of another
- Communication between piconets
  - Devices jumping back and forth between the piconets



Piconets (each with a capacity of 720 kbit/s)

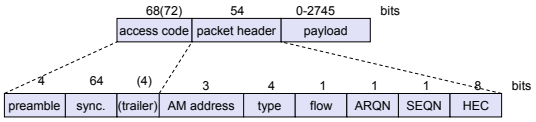
M=Master
S=Slave
P=Parked
SB=Standby

Frequency selection during data transmission

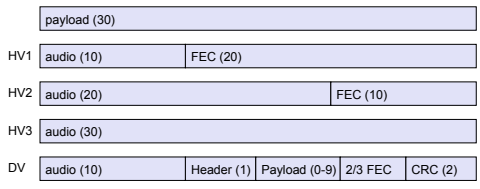


Baseband

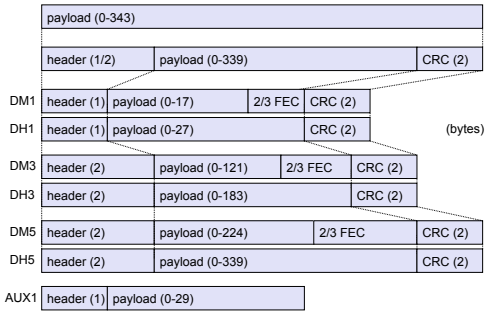
- Piconet/channel definition
- Low-level packet definition
  - Access code
    - Channel, device access, e.g., derived from master
  - Packet header
    - active member address (broadcast + 7 slaves), link type, alternating bit ARQ/SEQ, checksum



SCO payload types

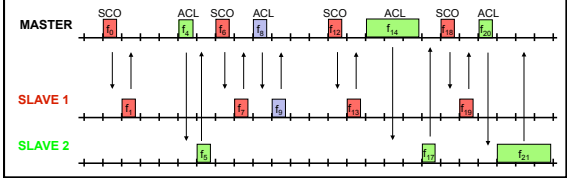


ACL Payload types



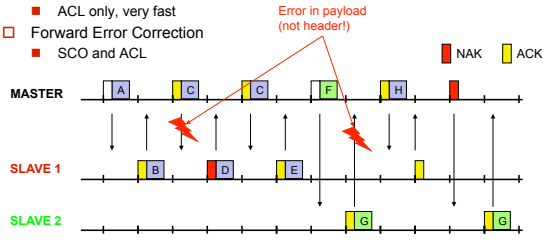
Baseband link types

- 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

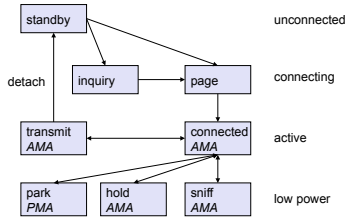


Robustness

- 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

Bluetooth versions

- Bluetooth 1.1
  - also IEEE Standard 802.15.1-2002
  - initial stable commercial standard
- Bluetooth 1.2
  - also IEEE Standard 802.15.1-2005
  - eSCO (extended SCO): higher, variable bitrates, retransmission for SCO
  - AFH (adaptive frequency hopping) to avoid interference
- Bluetooth 2.0 + EDR (2004, no more IEEE)
  - EDR (enhanced date rate) of 3.0 Mbit/s for ACL and eSCO
  - lower power consumption due to shorter duty cycle
- Bluetooth 2.1 + EDR (2007)
  - better pairing support, e.g., using NFC
  - improved security

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, hopping sequence
- Availability
  - Integrated into many products, several vendors
- 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
- Special Advantages/ Disadvantages
  - Advantage: already integrated into several products, available worldwide, free ISM-band, several vendors, simple system, simple ad-hoc networking, peer to peer, scatternets
  - Disadvantage: interference on ISM-band, limited range, max. 8 active devices/network, high set-up latency

WPAN: IEEE 802.15 – future developments 1

- 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
  - Ad hoc peer-to-peer networking
  - Security
  - Low power and low cost
  - Designed to meet the demanding requirements of portable consumer imaging and multimedia applications

WPAN: IEEE 802.15 – future developments 2

- Several working groups extend the 802.15.3 standard
- 802.15.3a: - withdrawn -
  - Alternative PHY with higher data rate as extension to 802.15.3
  - Applications: multimedia, picture transmission
- 802.15.3b:
  - Enhanced interoperability of MAC
  - Correction of errors and ambiguities in the standard
- 802.15.3c:
  - Alternative PHY at 57-64 GHz
  - Goal: data rates above 2 Gbit/s
- Not all these working groups really create a standard, not all standards will be found in products later …

WPAN: IEEE 802.15 – future developments 3

- 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
  - Up to 254 devices or 64516 simpler nodes
  - Support for critical latency devices, such as joysticks
  - CSMA/CA channel access (data centric), slotted (beacon), 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
- Basis of the ZigBee technology – www.zigbee.org

ZigBee

- Relation to 802.15.4 similar to Bluetooth / 802.15.1
- Pushed by Chipcon (now TI), Ember, Freescale (Motorola), Honeywell, Mitsubishi, Motorola, Philips, Samsung…
- More than 260 members
  - about 15 promoters, 133 participants, 111 adopters
  - must be member to commercially use ZigBee spec
- ZigBee platforms comprise
  - IEEE 802.15.4 for layers 1 and 2
  - ZigBee protocol stack up to the applications

WPAN: IEEE 802.15 – future developments 4

- 802.15.4a:
  - Alternative PHY with lower data rate as extension to 802.15.4
  - Properties: precise localization (< 1m precision), extremely low power consumption, longer range
- 802.15.4b, c, d:
  - Extensions, corrections, and clarifications regarding 802.15.4
  - Usage of new bands, more flexible security mechanisms
- 802.15.5: Mesh Networking
  - Partial meshes, full meshes
  - Range extension, more robustness, longer battery live
- 802.15.6: Body Area Networks
  - Low power networks e.g. for medical or entertainment use
- Not all these working groups really create a standard, not all standards will be found in products later …

Some more IEEE standards for mobile communications

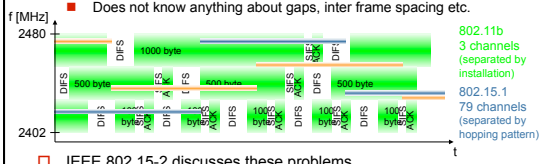
- IEEE 802.16: Broadband Wireless Access / WirelessMAN / WiMax
  - Wireless distribution system, e.g., for the last mile, alternative to DSL
  - 75 Mbit/s up to 50 km LOS, up to 10 km NLOS; 2-66 GHz band
  - Initial standards without roaming or mobility support
  - 802.16e adds mobility support, allows for roaming at 150 km/h
- IEEE 802.20: Mobile Broadband Wireless Access (MBWA)
  - Licensed bands < 3.5 GHz, optimized for IP traffic
  - Peak rate > 1 Mbit/s per user
  - Different mobility classes up to 250 km/h and ranges up to 15 km
  - Relation to 802.16e unclear
- IEEE 802.21: Media Independent Handover Interoperability
  - Standardize handover between different 802.x and/or non 802 networks
- IEEE 802.22: Wireless Regional Area Networks (WRAN)
  - Radio-based PHY/MAC for use by license-exempt devices on a non-interfering basis in spectrum that is allocated to the TV Broadcast Service

ISM band interference

- Many sources of interference
  - Microwave ovens, microwave lighting
  - 802.11, 802.11b, 802.11g, 802.15, …
  - 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. 802.15/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)