Mobile Communications
Chapter 7: Wireless LANs

- Characteristics
- IEEE 802.11
  - PHY
  - MAC
  - Roaming
- HIPERLAN
  - Standards
  - PHY
  - MAC
  - Ad-hoc networks
- Bluetooth

Characteristics of wireless LANs

Advantages
- very flexible within the reception area
- Ad-hoc networks without previous planning possible
- (almost) no wiring difficulties (e.g. historic buildings, firewalls)
- more robust against disasters like, e.g., earthquakes, fire - or users pulling a plug...

Disadvantages
- typically very low bandwidth compared to wired networks (1-10 Mbit/s)
- many proprietary solutions, especially for higher bit-rates, standards take their time (e.g. IEEE 802.11)
- products have to follow many national restrictions if working wireless, it takes a vary long time to establish global solutions like, e.g., IMT-2000

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

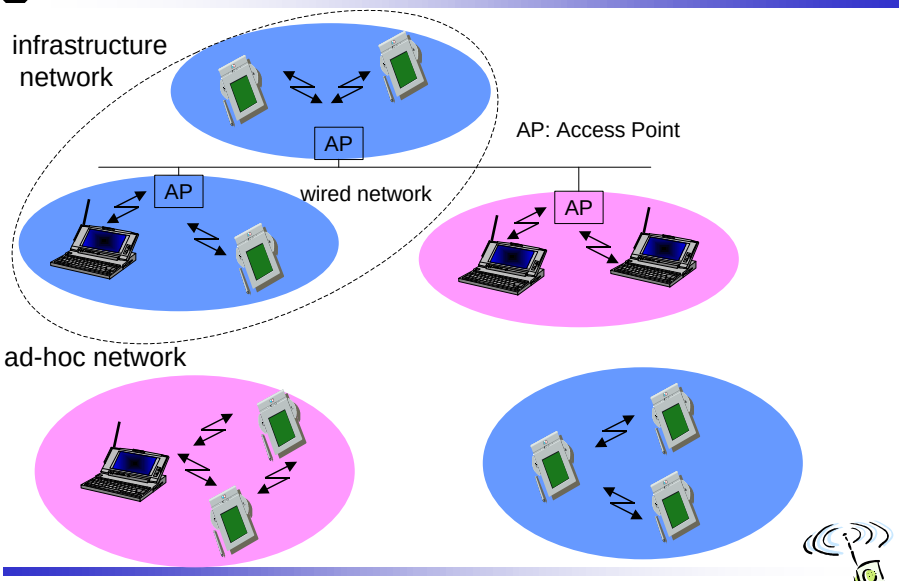
Radio
- typically using the license free ISM band at 2.4 GHz

Advantages
- experience from wireless WAN and mobile phones can be used
- coverage of larger areas possible (radio can penetrate walls, furniture etc.)

Disadvantages
- very limited license free frequency bands
- shielding more difficult, interference with other electrical devices

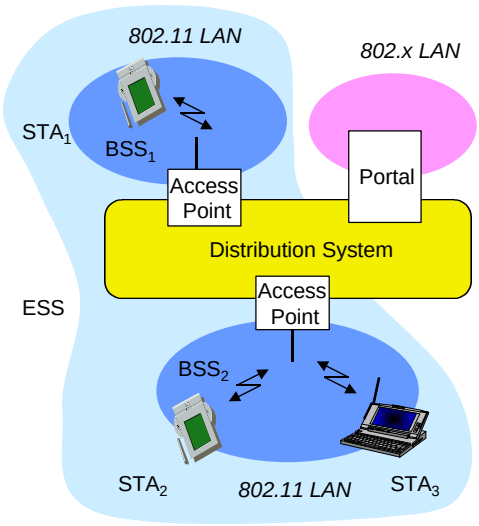
Example
- WaveLAN, HIPERLAN, Bluetooth

Comparison: infrastructure vs. ad-hoc networks



Mobile Communications: Wireless LANs 7.4.1

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

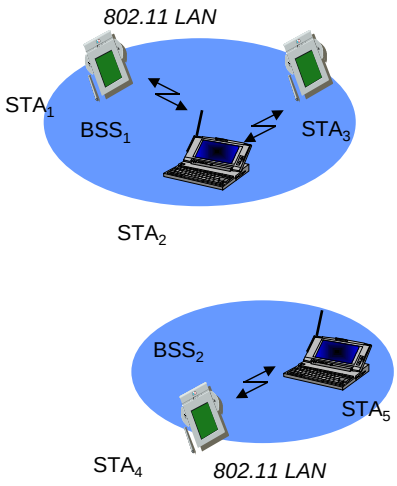
Access Point
- station integrated into the wireless LAN and the distribution system

Portal
- bridge to other (wired) networks

Distribution System
- interconnection network to form one logical network (EES: Extended Service Set) based on several BSS

Mobile Communications: Wireless LANs 7.5.1

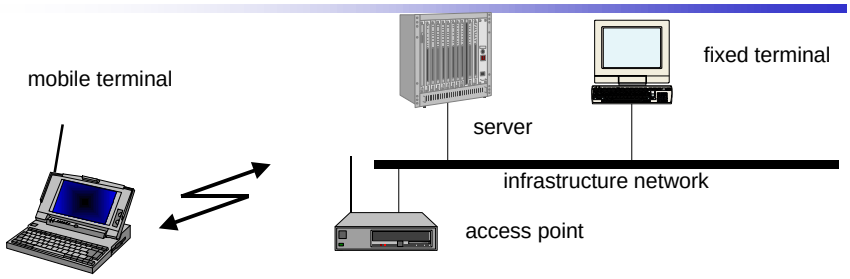
802.11 - Architecture of an ad-hoc network



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



application		application
TCP		TCP
IP		IP
LLC	LLC	LLC
802.11 MAC	802.11 MAC / 802.3 MAC	802.3 MAC
802.11 PHY	802.11 PHY / 802.3 PHY	802.3 PHY

802.11 - Layers and functions

MAC
- access mechanisms, fragmentation, encryption

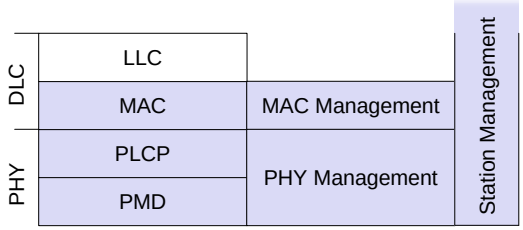
MAC Management
- synchronization, roaming, MIB, power management

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



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), 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 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, synchonization

FHSS PHY packet format

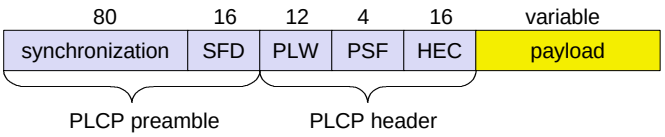
Synchronization
- synch with 010101... pattern

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 $x^{16}+x^{12}+x^5+1$



Mobile Communications: Wireless LANs 7.10.1

DSSS PHY packet format

Synchronization
- synch., gain setting, energy detection, frequency offset compensation

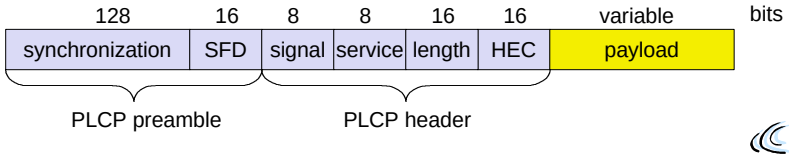
SFD (Start Frame Delimiter)
- 1111001110100000

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



Mobile Communications: Wireless LANs 7.11.1

802.11 - MAC layer I - DFWMAC

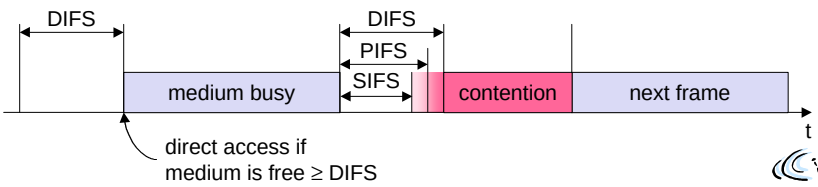
Traffic services
- Asynchronous Data Service (mandatory)
  - exchange of data packets based on “best-effort”
  - support of broadcast and multicast
- Time-Bounded Service (optional)
  - implemented using PCF (Point Coordination Function)

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

Mobile Communications: Wireless LANs 7.12.1

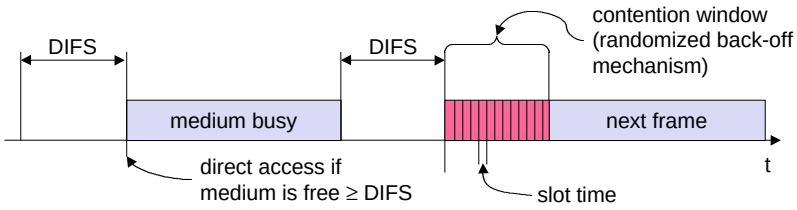
802.11 - MAC layer II

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



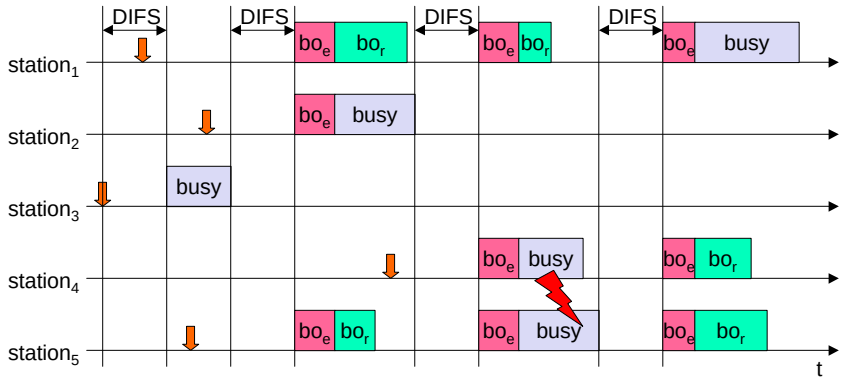
Mobile Communications: Wireless LANs 7.13.1

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



busy — medium not idle (frame, ack etc.)

packet arrival at MAC

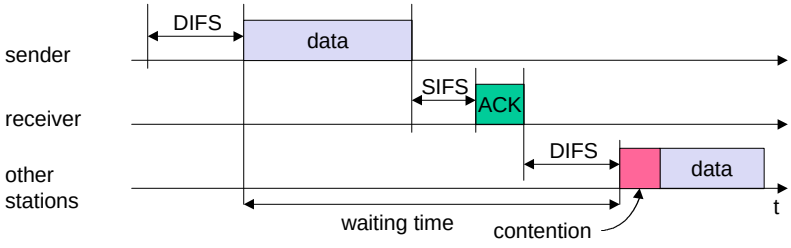
bo_e — elapsed backoff time

bo_r — residual backoff time

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

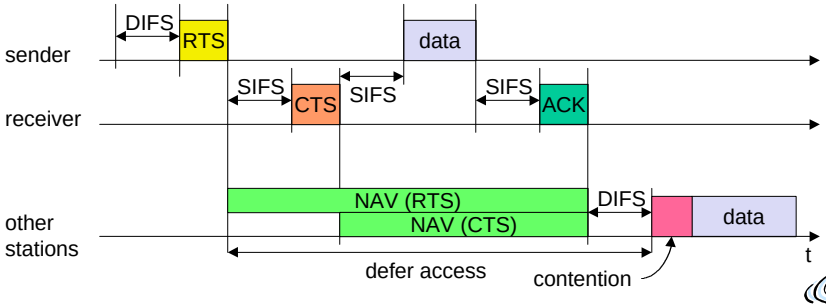


Mobile Communications: Wireless LANs 7.16.1

802.11 - DFWMAC

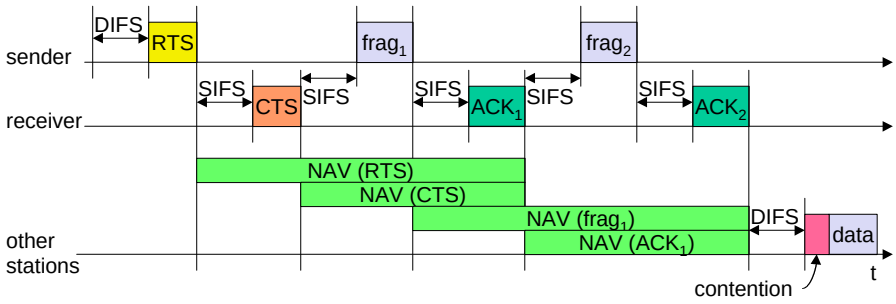
Sending unicast packets

- 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



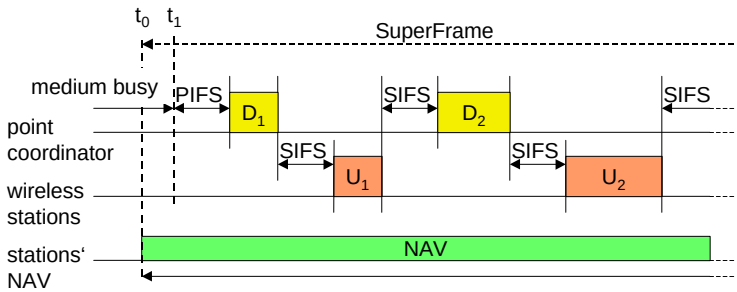
Mobile Communications: Wireless LANs 7.17.1

Fragmentation



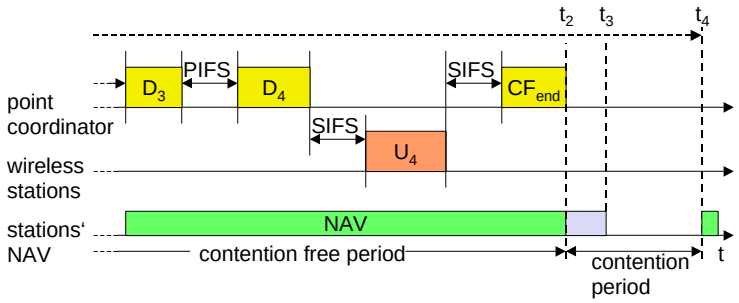
Mobile Communications: Wireless LANs 7.18.1

DFWMAC-PCF I



Mobile Communications: Wireless LANs 7.19.1

DFWMAC-PCF II



Mobile Communications: Wireless LANs 7.20.1

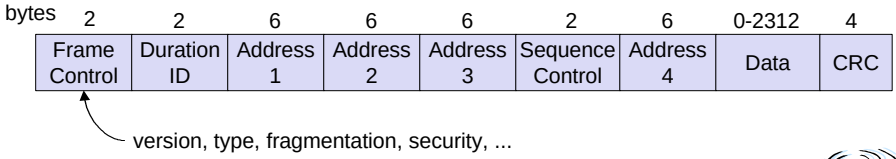
802.11 - Frame format

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



Mobile Communications: Wireless LANs 7.21.1

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

802.11 - MAC management

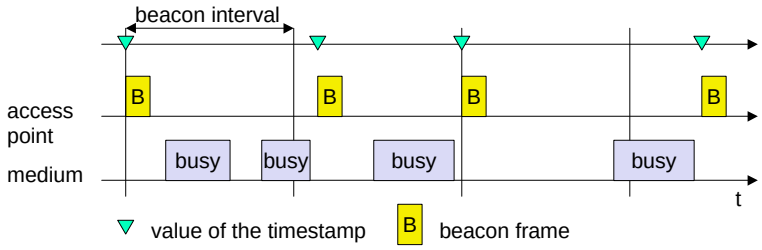
Synchronization
- try to find a LAN, try to stay within a LAN
- timer etc.

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

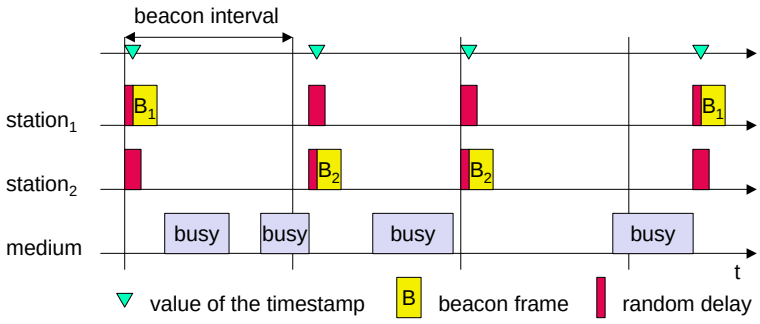
MIB - Management Information Base
- managing, read, write

Synchronization using a Beacon (infrastructure)



Mobile Communications: Wireless LANs 7.24.1

Synchronization using a Beacon (ad-hoc)



Mobile Communications: Wireless LANs 7.25.1

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

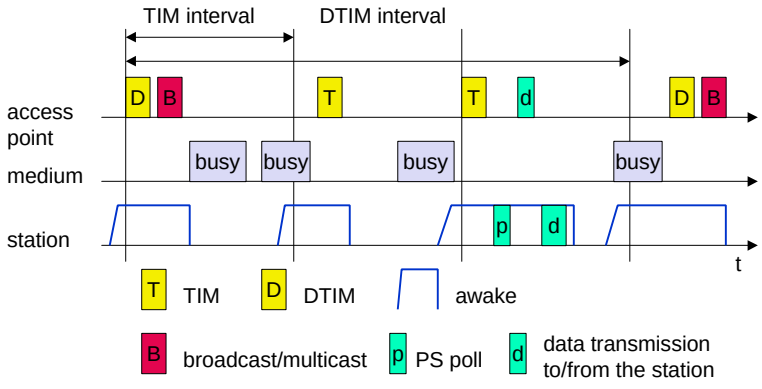
- Traffic Indication Map (TIM)
  - list of unicast receivers transmitted by AP
- Delivery Traffic Indication Map (DTIM)
  - list of broadcast/multicast receivers transmitted by AP

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?)

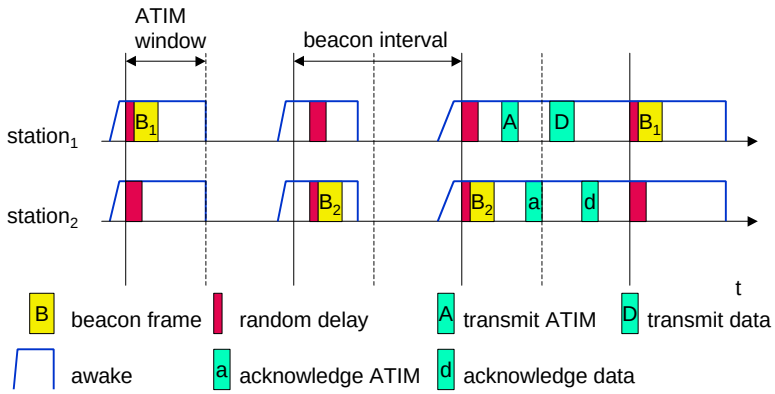
Mobile Communications: Wireless LANs 7.26.1

Power saving with wake-up patterns (infrastructure)



Mobile Communications: Wireless LANs 7.27.1

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

Future developments

IEEE 802.11a
- compatible MAC, but now 5 GHz band
- transmission rates up to 20 Mbit/s
- close cooperation with BRAN (ETSI Broadband Radio Access Network)

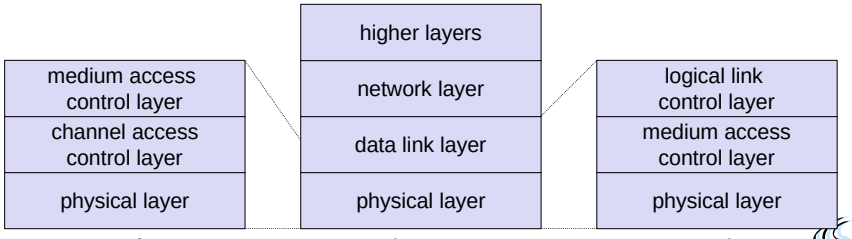
IEEE 802.11b
- higher data rates at 2.4 GHz
- proprietary solutions already offer 10 Mbit/s

IEEE WPAN (Wireless Personal Area Networks)
- market potential
- compatibility
- low cost/power, small form factor
- technical/economic feasibility
  ➔ Bluetooth

ETSI - HIPERLAN

ETSI standard
- European standard, cf. GSM, DECT, ...
- Enhancement of local Networks and interworking with fixed networks
- integration of time-sensitive services from the early beginning

HIPERLAN family
- one standard cannot satisfy all requirements
  - range, bandwidth, QoS support
  - commercial constraints
- HIPERLAN 1 standardized since 1996



Overview: original HIPERLAN protocol family

	HIPERLAN 1	HIPERLAN 2	HIPERLAN 3	HIPERLAN 4
Application	wireless LAN	access to ATM fixed networks	wireless local loop	point-to-point wireless ATM connections
Frequency	5.1-5.3GHz			17.2-17.3GHz
Topology	decentralized ad-hoc/infrastructure	cellular, centralized	point-to-multipoint	point-to-point
Antenna	omni-directional		directional	
Range	50 m	50-100 m	5000 m	150 m
QoS	statistical	ATM traffic classes (VBR, CBR, ABR, UBR)		
Mobility	<10m/s		stationary	
Interface	conventional LAN	ATM networks		
Data rate	23.5 Mbit/s	>20 Mbit/s		155 Mbit/s
Power conservation	yes		not necessary	

Check out Wireless ATM for new names!

Mobile Communications: Wireless LANs 7.32.1

HIPERLAN 1 - Characteristics

Data transmission
- point-to-point, point-to-multipoint, connectionless
- 23.5 Mbit/s, 1 W power, 2383 byte max. packet size

Services
- asynchronous and time-bounded services with hierarchical priorities
- compatible with ISO MAC

Topology
- infrastructure or ad-hoc networks
- transmission range can be larger then coverage of a single node („forwarding“ integrated in mobile terminals)

Further mechanisms
- power saving, encryption, checksums

Mobile Communications: Wireless LANs 7.33.1

HIPERLAN 1 - Services and protocols

CAC service
- definition of communication services over a shared medium
- specification of access priorities
- abstraction of media characteristics

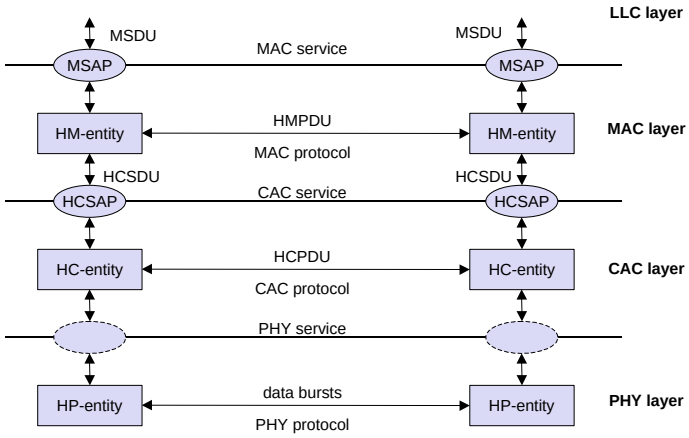
MAC protocol
- MAC service, compatible with ISO MAC and ISO MAC bridges
- uses HIPERLAN CAC

CAC protocol
- provides a CAC service, uses the PHY layer, specifies hierarchical access mechanisms for one or several channels

Physical protocol
- send and receive mechanisms, synchronization, FEC, modulation, signal strength

Mobile Communications: Wireless LANs 7.34.1

HIPERLAN layers, services, and protocols



Mobile Communications: Wireless LANs 7.35.1

HIPERLAN 1 - Physical layer

Scope
- modulation, demodulation, bit and frame synchronization
- forward error correction mechanisms
- measurements of signal strength
- channel sensing

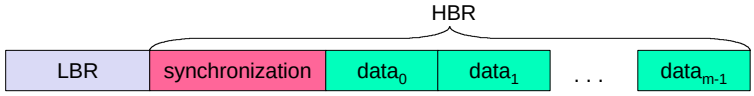
Channels
- 3 mandatory and 2 optional channels (with their carrier frequencies)
- mandatory
  - channel 0: 5.1764680 GHz
  - channel 1: 5.1999974 GHz
  - channel 2: 5.2235268 GHz
- optional (not allowed in all countries)
  - channel 3: 5.2470562 GHz
  - channel 4: 5.2705856 GHz

Mobile Communications: Wireless LANs 7.36.1

HIPERLAN 1 - Physical layer frames

Maintaining a high data-rate (23.5 Mbit/s) is power consuming - problematic for mobile terminals
- packet header with low bit-rate comprising receiver information
- only receiver(s) address by a packet continue receiving

Frame structure
- LBR (Low Bit-Rate) header with 1.4 Mbit/s
- 450 bit synchronization
- minimum 1, maximum 47 frames with 496 bit each
- for higher velocities of the mobile terminal (> 1.4 m/s) the maximum number of frames has to be reduced



Modulation
- GMSK for high bit-rate, FSK for LBR header

Mobile Communications: Wireless LANs 7.37.1

HIPERLAN 1 - CAC sublayer

Channel Access Control (CAC)

- assure that terminal does not access forbidden channels
- priority scheme, access with EY-NPMA

Priorities

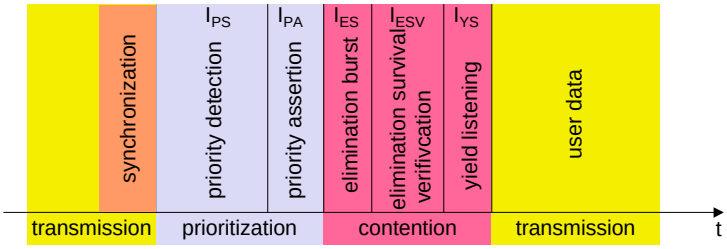
- 5 priority levels for QoS support
- QoS is mapped onto a priority level with the help of the packet lifetime (set by an application)
  - if packet lifetime = 0 it makes no sense to forward the packet to the receiver any longer
  - standard start value 500ms, maximum 16000ms
  - if a terminal cannot send the packet due to its current priority, waiting time is permanently subtracted from lifetime
  - based on packet lifetime, waiting time in a sender and number of hops to the receiver, the packet is assigned to one out of five priorities
  - the priority of waiting packets, therefore, rises automatically

Mobile Communications: Wireless LANs 7.38.1

HIPERLAN 1 - EY-NPMA I

EY-NPMA (Elimination Yield Non-preemptive Priority Multiple Access)

- 3 phases: priority resolution, contention resolution, transmission
- finding the highest priority
  - every priority corresponds to a time-slot to send in the first phase, the higher the priority the earlier the time-slot to send
  - higher priorities can not be preempted
  - if an earlier time-slot for a higher priority remains empty, stations with the next lower priority might send
  - after this first phase the highest current priority has been determined



Mobile Communications: Wireless LANs 7.39.1

HIPERLAN 1 - EY-NPMA II

Several terminals can now have the same priority and wish to send

- contention phase
  - Elimination Burst: all remaining terminals send a burst to eliminate contenders (11111010100010011100000110010110, high bit- rate)
  - Elimination Survival Verification: contenders now sense the channel, if the channel is free they can continue, otherwise they have been eliminated
  - Yield Listening: contenders again listen in slots with a nonzero probability, if the terminal senses its slot idle it is free to transmit at the end of the contention phase
  - the important part is now to set the parameters for burst duration and channel sensing (slot-based, exponentially distributed)
- data transmission
  - the winner can now send its data (however, a small chance of collision remains)
  - if the channel was idle for a longer time (min. for a duration of 1700 bit) a terminal can send at once without using EY-NPMA
- synchronization using the last data transmission

HIPERLAN 1 - DT-HCPDU/AK-HCPDU

LBR

0	1	2	3	4	5	6	7	bit
1	0	1	0	1	0	1	0	
0	1	HI	HDA					
HDA					HDACS			
BLIR = n							BL-	
IRCS	1							

HBR

0	1	2	3	4	5	6	7	bit / byte
TI	BLI = n							1
PLI = m								2
HID								3 - 6
DA								7 - 12
SA								13 - 18
UD								19 - (52n-m-4)
PAD								(52n-m-3) - (52n-4)
CS								(52n-3) - 52n

Data HCPDU

LBR

0	1	2	3	4	5	6	7	bit
1	0	1	0	1	0	1	0	
0	1	HI	AID					
AID					AIDCS			

Acknowledgement HCPDU

HI: HBR-part Indicator
HDA: Hashed Destination HCSAP Address
HDACS: HDA CheckSum
BLIR: Block Length Indicator
BLIRCS: BLIR CheckSum
TI: Type Indicator
BLI: Block Length Indicator
HID: HIPERLAN IDentifier
DA: Destination Address
SA: Source Address
UD: User Data (1-2422 byte)
PAD: PADding
CS: CheckSum
AID: Acknowledgement IDentifier
AIDS: AID CheckSum

HIPERLAN 1 - MAC layer

Compatible to ISO MAC

Supports time-bounded services via a priority scheme

Packet forwarding

- support of directed (point-to-point) forwarding and broadcast forwarding (if no path information is available)
- support of QoS while forwarding

Encryption mechanisms

- mechanisms integrated, but without key management

Power conservation mechanisms

- mobile terminals can agree upon awake patterns (e.g., periodic wake-ups to receive data)
- additionally, some nodes in the networks must be able to buffer data for sleeping terminals and to forward them at the right time (so called stores)

HIPERLAN 1 - DT-HMPDU

0 1 2 3 4 5 6 7 (bit)	byte
LI = n	1 - 2
TI = 1	3
RL	4 - 5
PSN	6 - 7
DA	8 - 13
SA	14 - 19
ADA	20 - 25
ASA	26 - 31
UP | ML	32
ML	33
KID | IV	34
IV	35 - 37
UD	38 - (n-2)
SC	(n-1) - n

Data HMPDU n= 40–2422

LI: Length Indicator
TI: Type Indicator
RL: Residual Lifetime
PSN: Sequence Number
DA: Destination Address
SA: Source Address
ADA: Alias Destination Address
ASA: Alias Source Address
UP: User Priority
ML: MSDU Lifetime
KID: Key Identifier
IV: Initialization Vector
UD: User Data, 1–2383 byte
SC: Sanity Check (for the unencrypted PDU)

Information bases

Route Information Base (RIB) - how to reach a destination
- [destination, next hop, distance]

Neighbor Information Base (NIB) - status of direct neighbors
- [neighbor, status]

Hello Information Base (HIB) - status of destination (via next hop)
- [destination, status, next hop]

Alias Information Base (AIB) - address of nodes outside the net
- [original MSAP address, alias MSAP address]

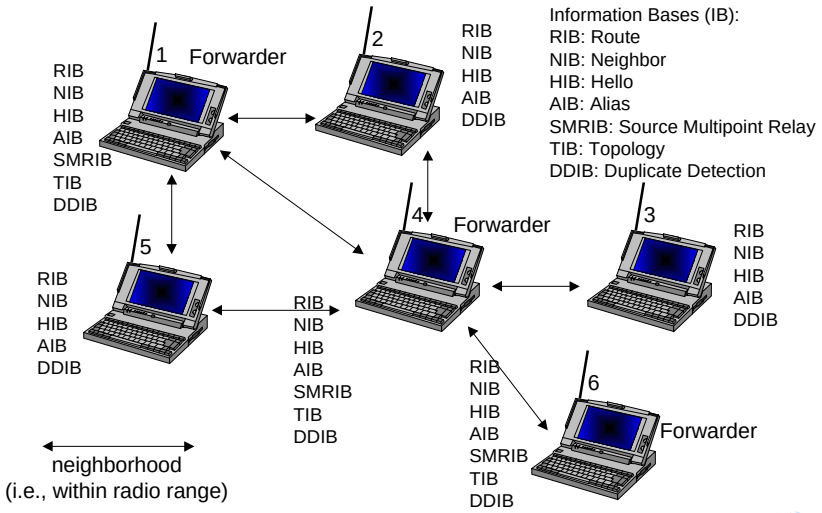
Source Multipoint Relay Information Base (SMRIB) - current MP status
- [local multipoint forwarder, multipoint relay set]

Topology Information Base (TIB) - current HIPERLAN topology
- [destination, forwarder, sequence]

Duplicate Detection Information Base (DDIB) - remove duplicates
- [source, sequence]

Mobile Communications: Wireless LANs 7.44.1

Ad-hoc networks using HIPERLAN 1



Mobile Communications: Wireless LANs 7.45.1

Bluetooth

Consortium: Ericsson, Intel, IBM, Nokia, Toshiba - many members

Scenarios

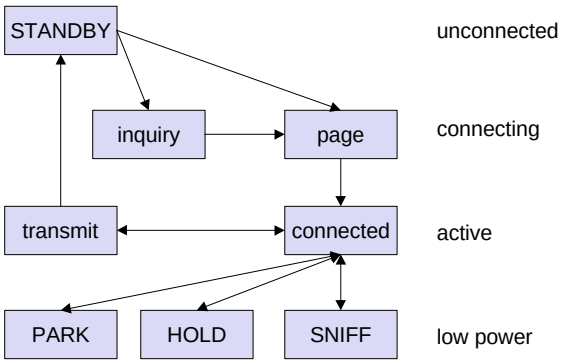
- connection of peripheral devices
  - loudspeaker, joystick, headset
- support of ad-hoc networking
  - small devices, low-cost
- bridging of networks
  - e.g., GSM via mobile phone - Bluetooth - laptop

Simple, cheap, replacement of IrDA, low range, lower data rates

- 2.4 GHz, FHSS, TDD, CDMA

Mobile Communications: Wireless LANs 7.46.1

States of a Bluetooth device (PHY layer)



Mobile Communications: Wireless LANs 7.47.1

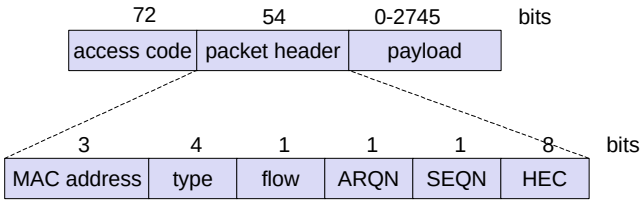
Bluetooth MAC layer

Synchronous Connection-Oriented link (SCO)
- symmetrical, circuit switched, point-to-point

Asynchronous Connectionless Link (ACL)
- packet switched, point-to-multipoint, master polls

Access code
- synchronization, derived from master, unique per channel

Packet header
- 1/3-FEC, MAC address (1 master, 7 slaves), link type, alternating bit ARQ/SEQ, checksum



Mobile Communications: Wireless LANs 7.48.1

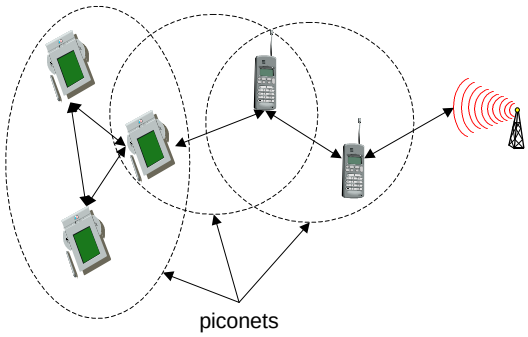
Scatternets

Each piconet has one master and up to 7 slaves

Master determines hopping sequence, slaves have to synchronize

Participation in a piconet = synchronization to hopping sequence

Communication between piconets = devices jumping back and forth between the piconets



Mobile Communications: Wireless LANs 7.49.1