Mobile Communications
Chapter 7: Wireless LANs

Slides by Jochen Schiller
with modifications by Emmanuel Agu

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

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)

Characteristics of wireless LANs

Advantages

- very flexible within reception area
- Ad-hoc networks do not need planning
- (almost) no wiring difficulties (e.g. historic buildings, firewalls)
- more robust against disasters like, e.g., earthquakes, fire

Disadvantages

- 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)
- many national restrictions for wireless, 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.)

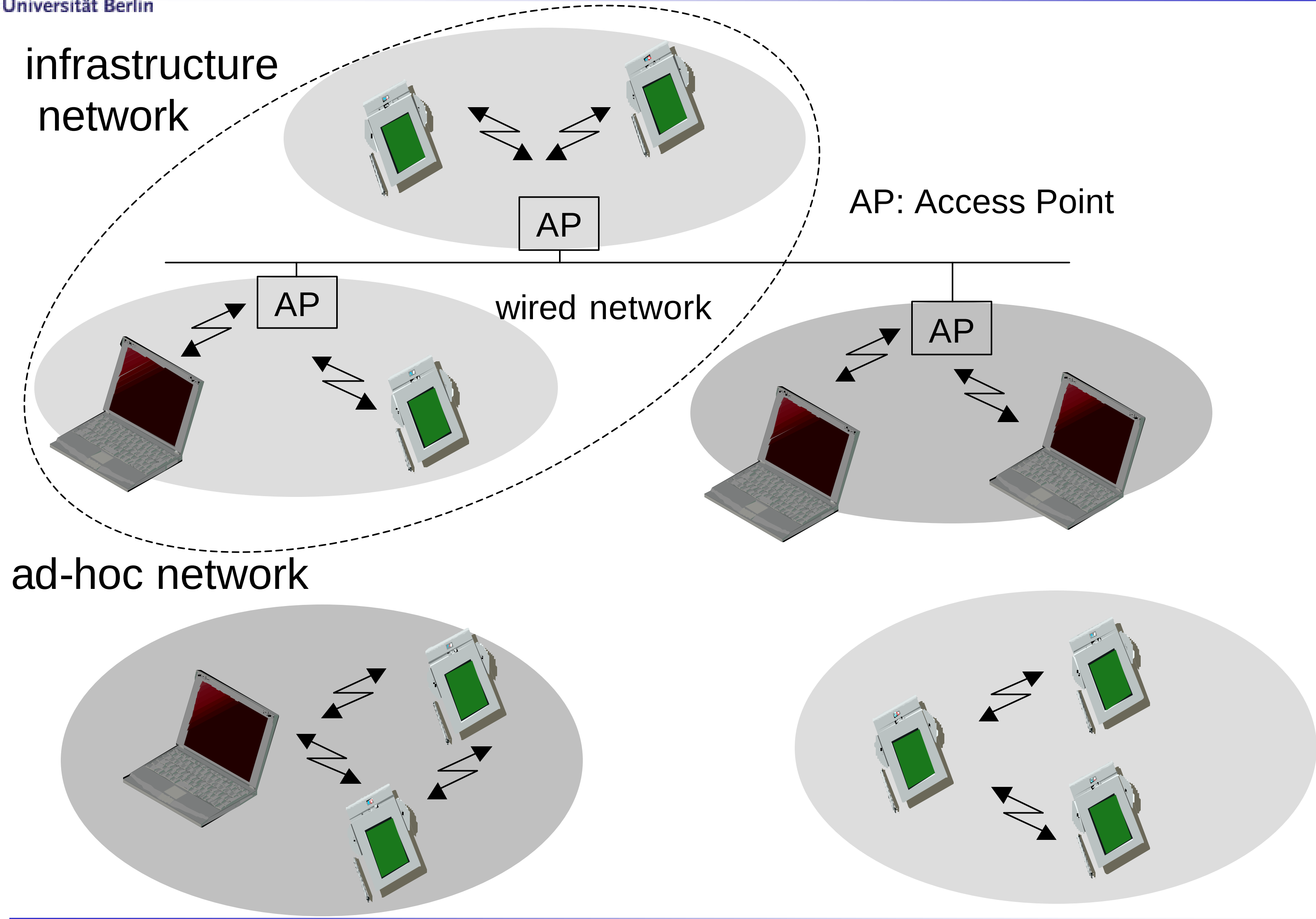
Disadvantages

- limited license free frequency bands
- shielding more difficult, electrical interference

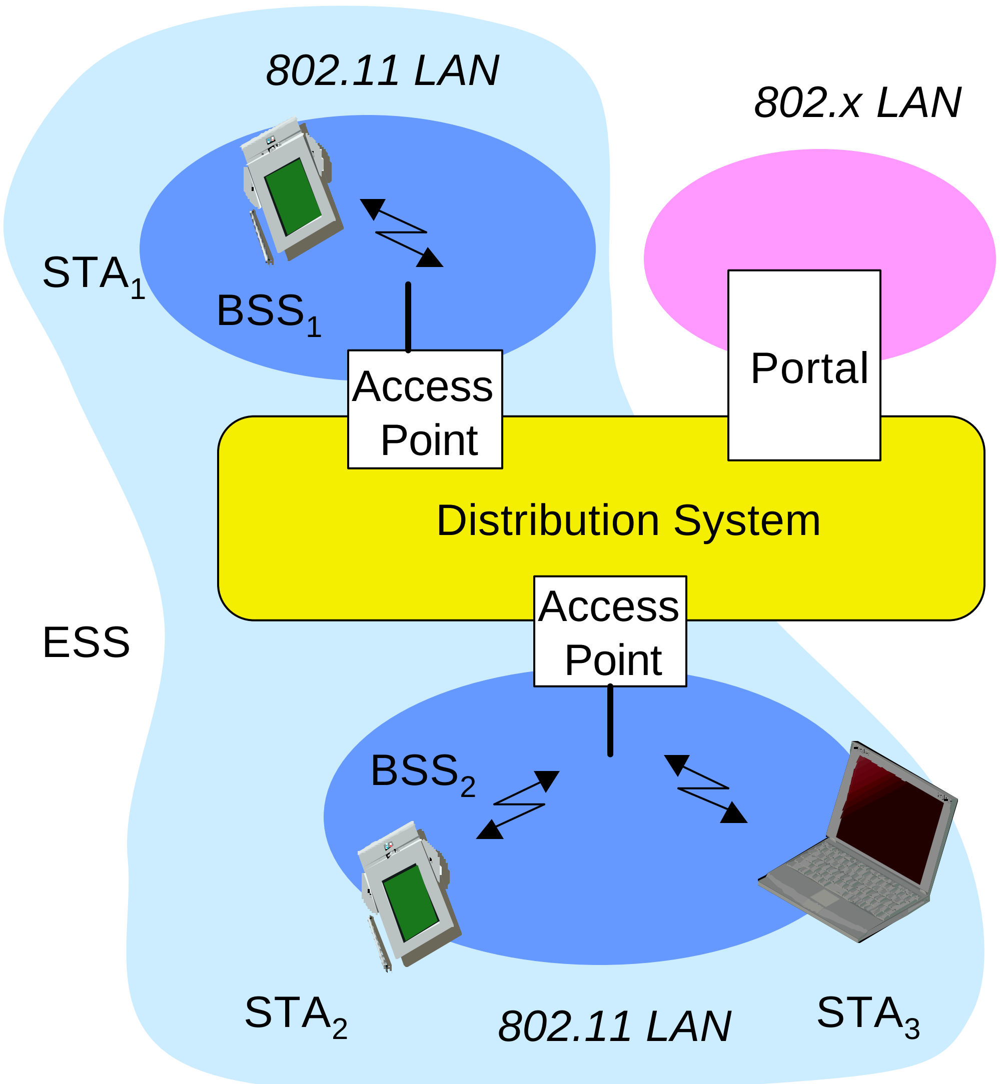
Example

- 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

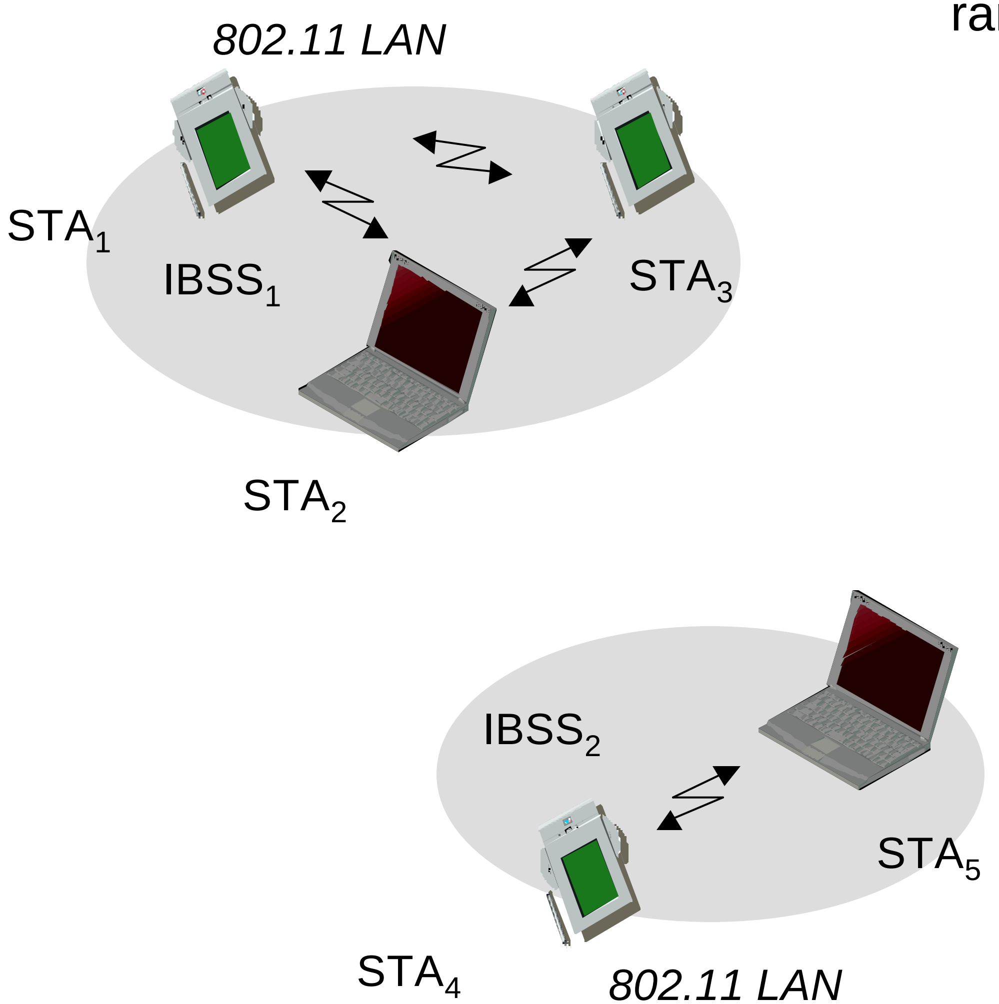
Portal

- bridge to other (wired) networks

Distribution System

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

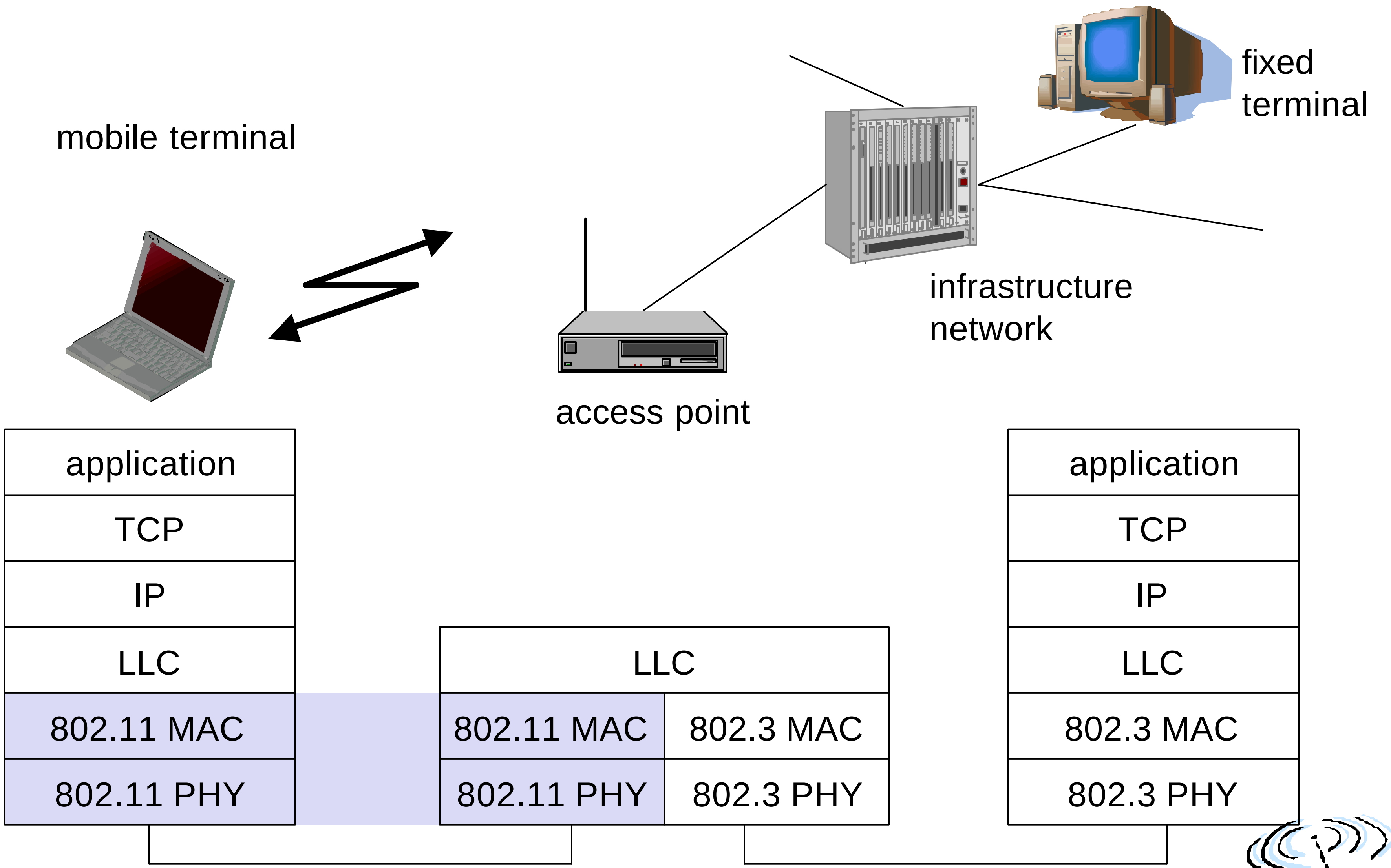
802.11 - Architecture of an ad-hoc network



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 - Layers and functions

MAC
- access mechanisms, fragmentation, encryption

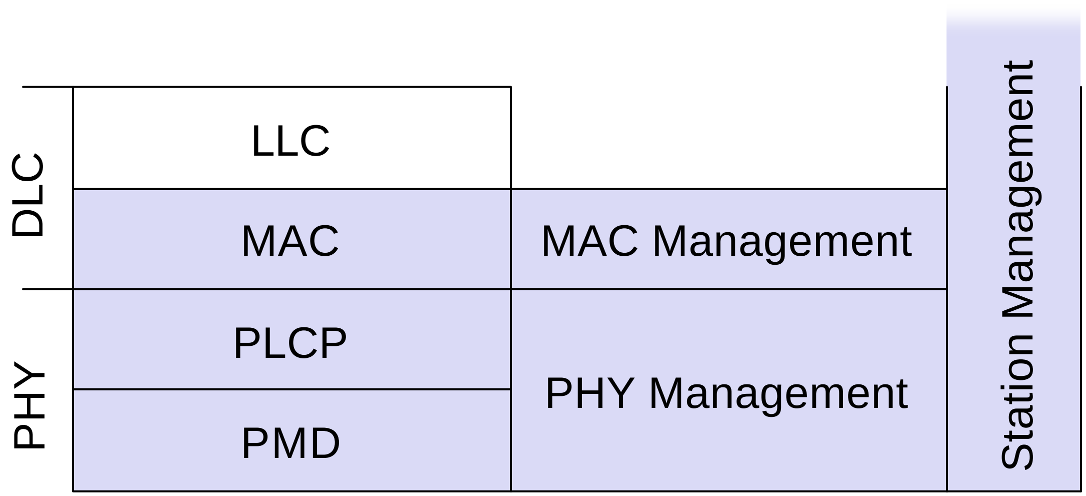
MAC Management
- synchronization, roaming, MIB, power management

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 (classical)

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, synchronization

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)

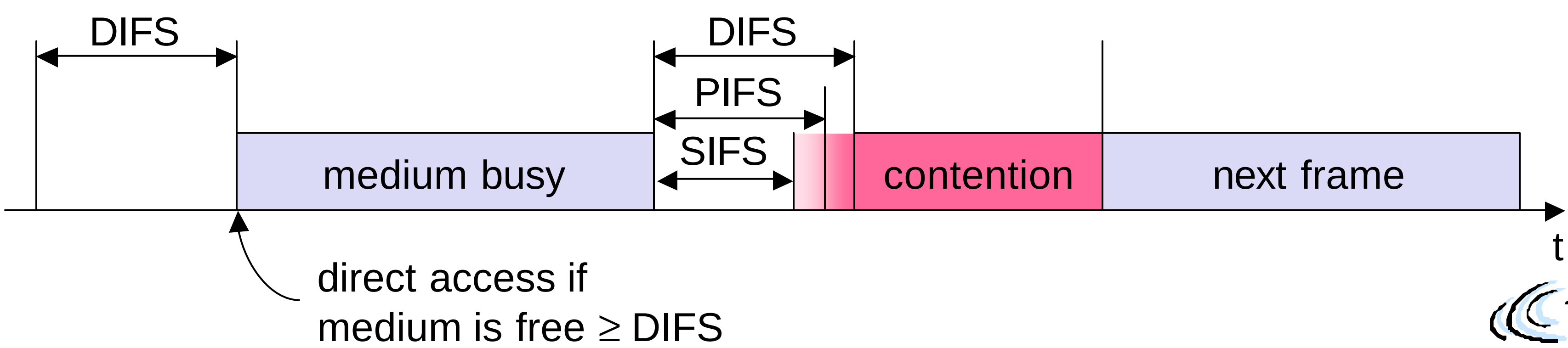
Access methods

- 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

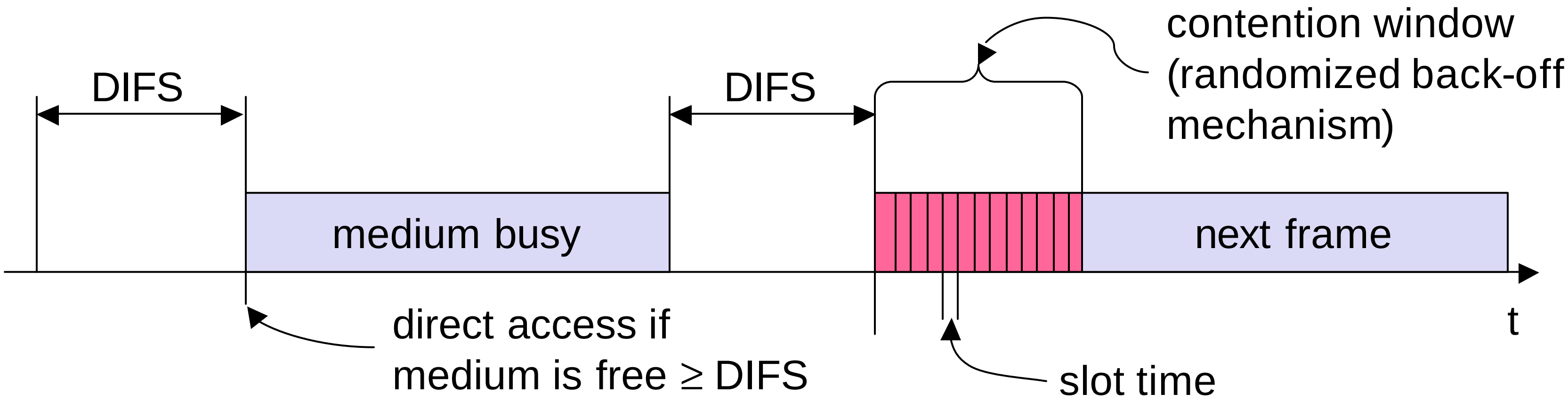
802.11 - MAC layer II

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

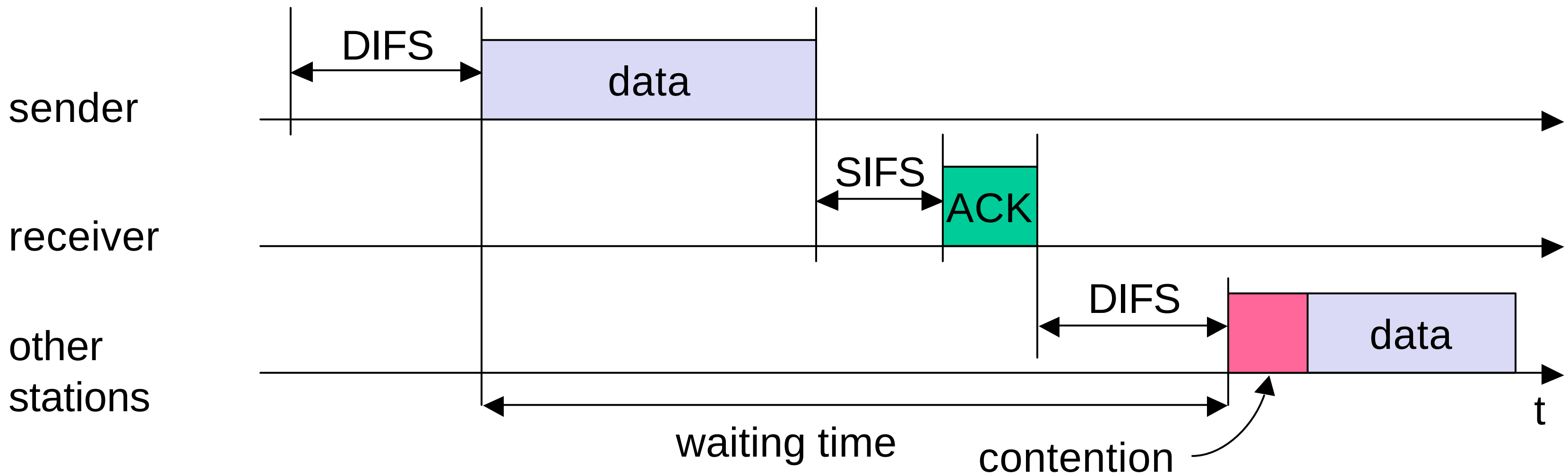


- station ready to send senses medium (based on PHY layer CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, then the station 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)
- If multiple stations have backed off, when 1 timer expires, other timers frozen

802.11 - CSMA/CA access method II

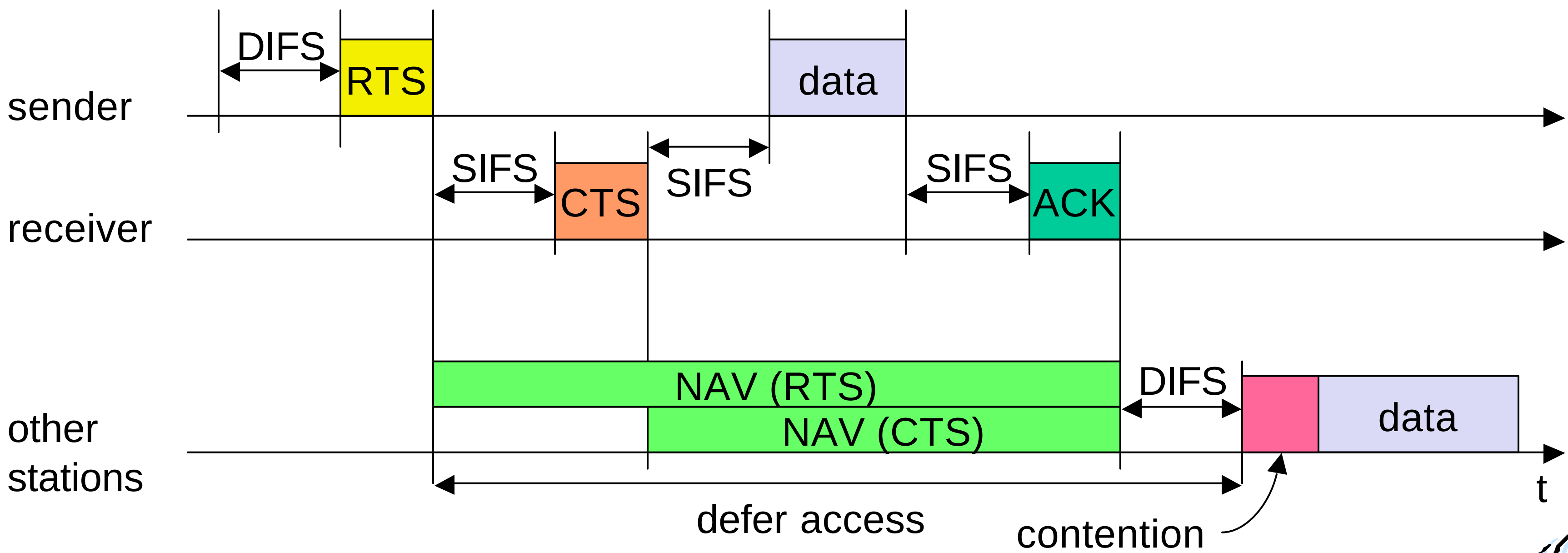
Sending unicast packets

- 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

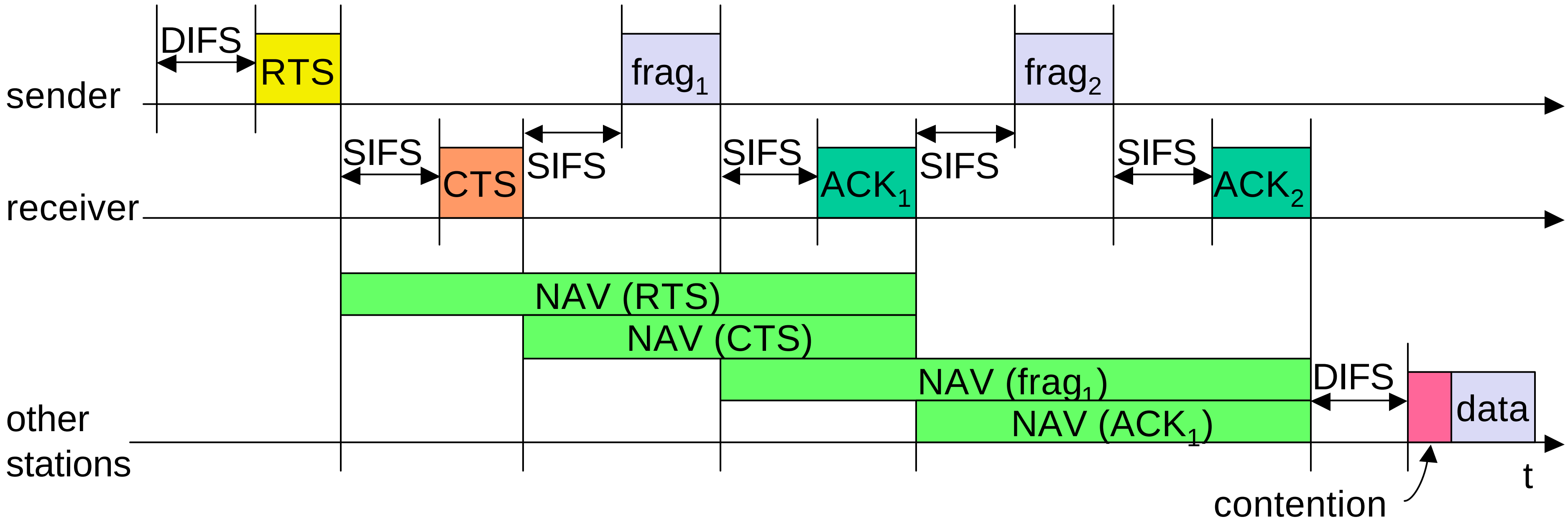


Sending unicast packets

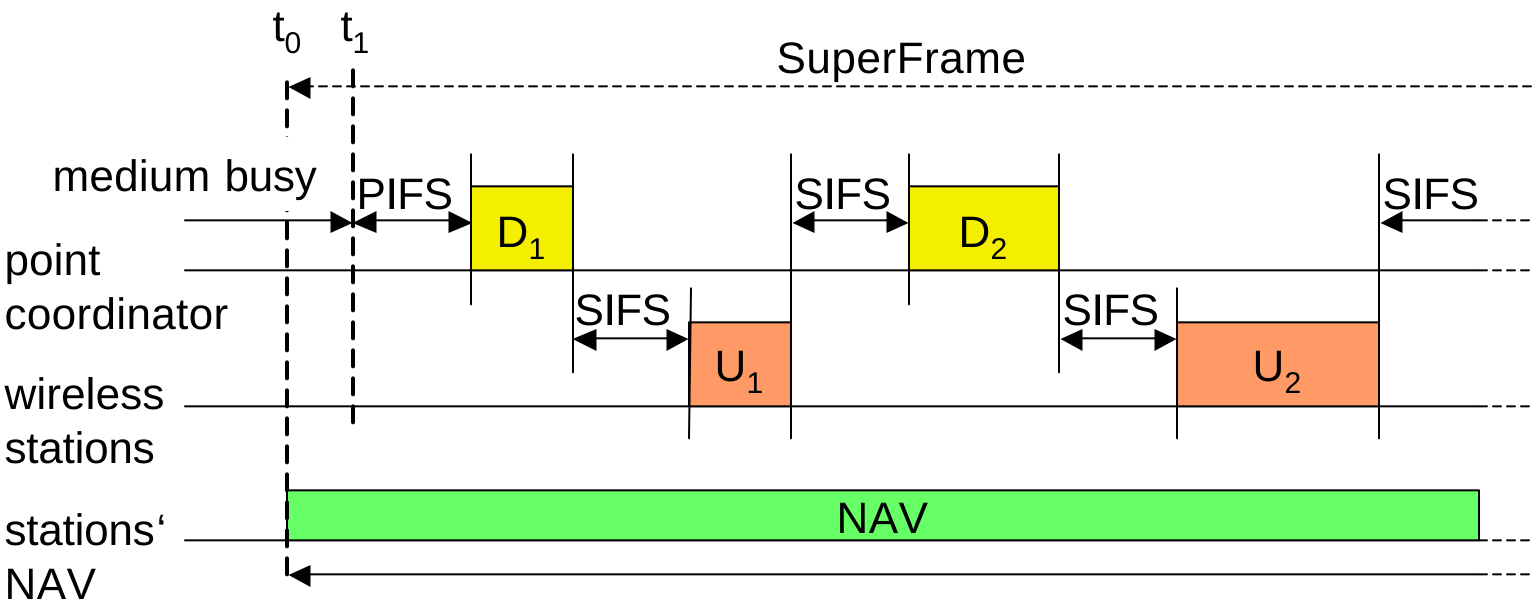
- station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
- acknowledgement via CTS after SIFS by receiver (if ready to receive)
- sender can now send data at once, acknowledgement via ACK
- other stations store medium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



Fragmentation



DFWMAC-PCF I



t_0
t_1
SuperFrame
medium busy
PIFS
D_1
SIFS
D_2
SIFS
point coordinator
SIFS
U_1
SIFS
U_2
wireless stations
NAV
stations' NAV

802.11 - Frame format

Types
- control frames, management frames, data frames

Sequence numbers
- important against duplicated frames due to lost ACKs

Addresses
- receiver, transmitter (physical), BSS identifier, sender (logical)

Miscellaneous
- sending time, checksum, frame control, data

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

bits	2	2	4	1	1	1	1	1	1	1	1
	Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Mgmt	More Data	WEP	Order

802.11 - MAC management

Synchronization

- Clock skew may happen
- *Infrastructure:* AP broadcasts beacons, other nodes correct skew
- *Ad hoc:* All nodes broadcast beacons

Power management

- Save battery, nodes can go to sleep, wake up periodically to receive
- *Infrastructure:* AP buffers packets for sleeping nodes
- *Ad hoc:* sender buffers packets for sleeping destinations

Association/Reassociation

- Roaming: Move from access point to access point as user moves
- scanning, i.e. active search for a network
- Node sends message to new AP, says goodbye to old AP

MIB - Management Information Base

- All information for managing network, node stored in SNMP MIB
- MIB can be read (access) or written to (update)

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
- Free 2.4 GHz ISM-band

Security
- Limited, WEP insecure, SSID

Availability
- Many products, many vendors

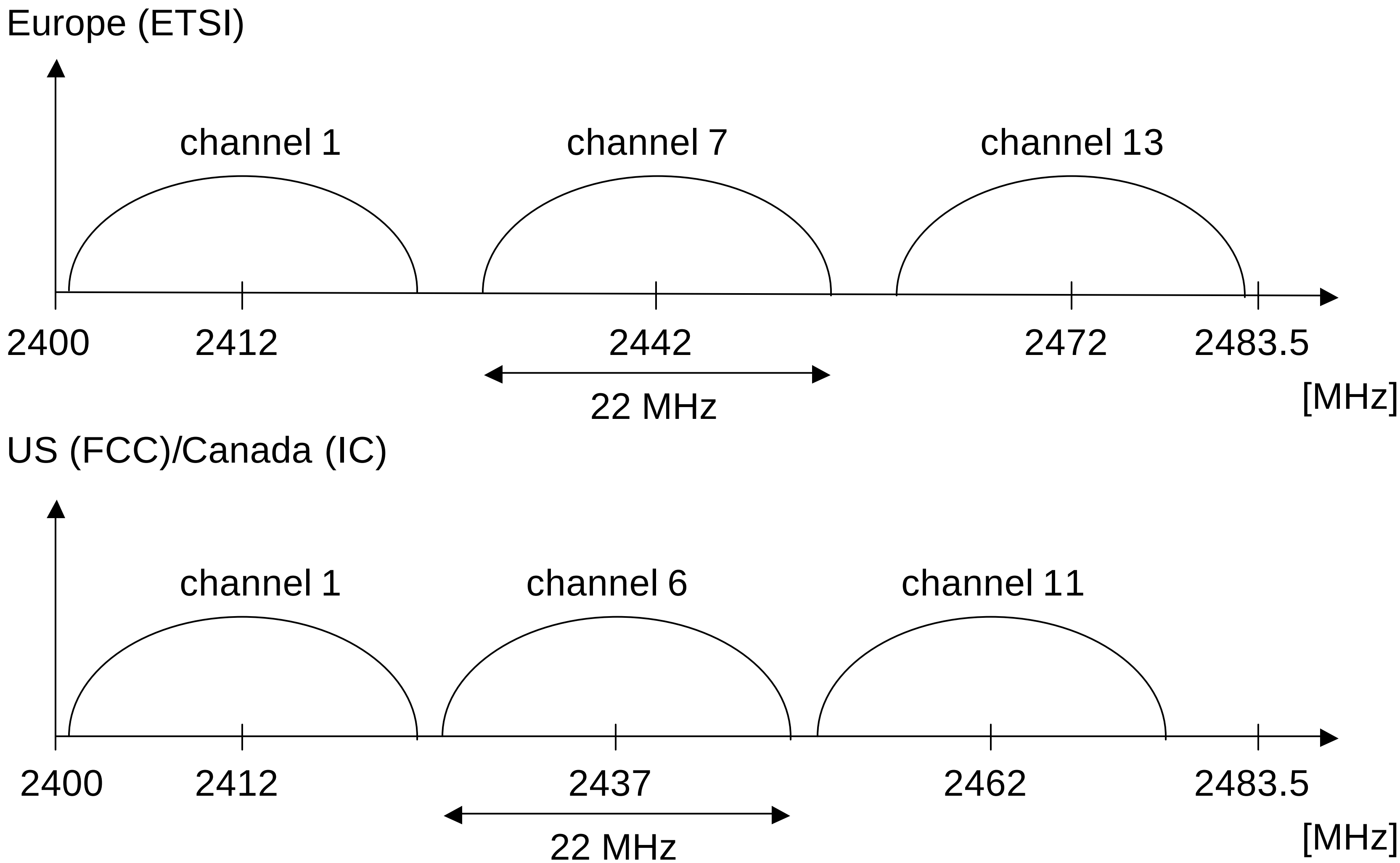
Connection set-up time
- Connectionless/always on

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

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

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.

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/

ETSI – HIPERLAN (historical)

Freie Universität Berlin

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 – no products!

HIPERLAN layers	OSI layers	IEEE 802.x layers
	higher layers	
medium access control layer	network layer	logical link control layer
channel access control layer	data link layer	medium access control layer
physical layer	physical layer	physical layer

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	

HIPERLAN 1 never reached product status,
the other standards have been renamed/modfied !

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

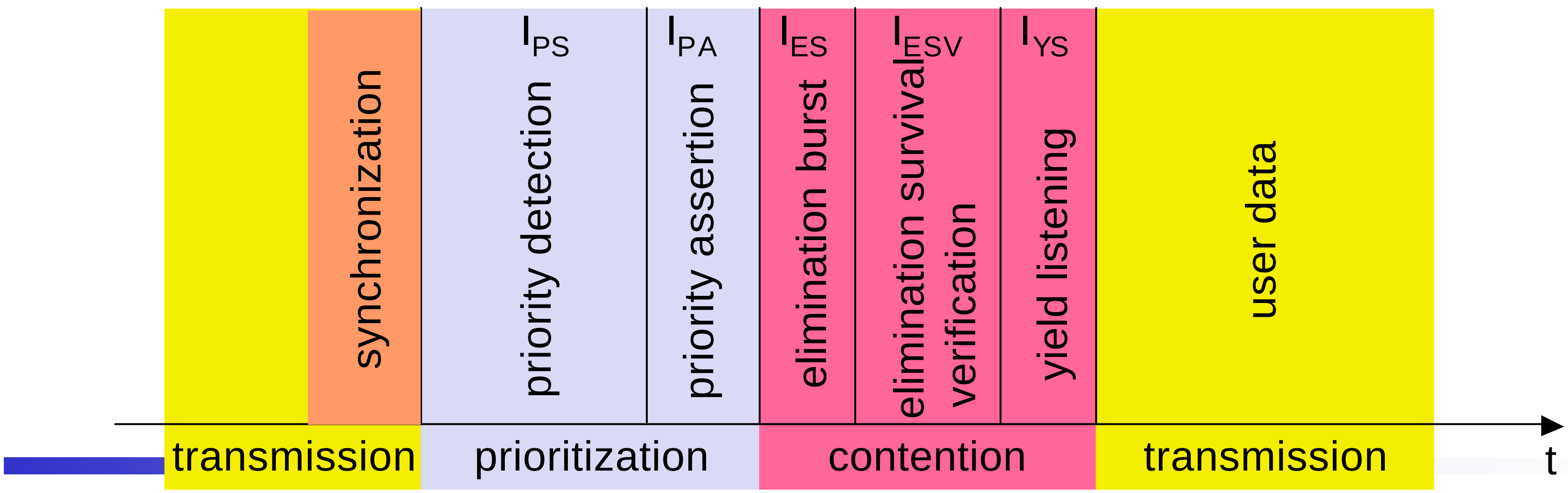
HIPERLAN 1 - CAC sublayer

Channel Access Control (CAC)

- assure that terminal does not access forbidden channels
- priority scheme, access with EY-NPMA
- 3 EY-NPMA phases: priority resolution, contention resolution, transmission

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)



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 - 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)

Some history: Why wireless ATM?

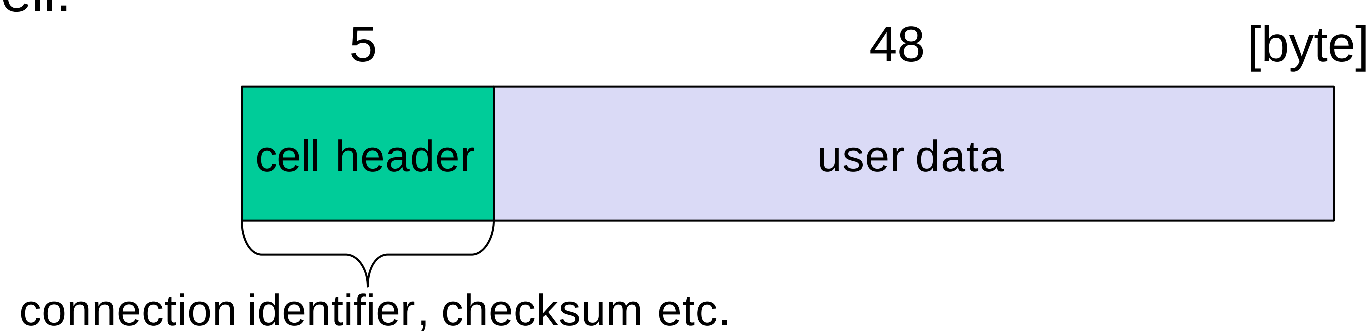
- seamless connection to wired ATM, a integrated services high-performance network supporting different types a traffic streams
- ATM networks scale well: private and corporate LANs, WAN
- B-ISDN uses ATM as backbone infrastructure and integrates several different services in one universal system
- mobile phones and mobile communications have increasing importance in everyday life
- current wireless LANs do not offer adequate support for multimedia data streams
- merging mobile communication and ATM leads to wireless ATM from a telecommunication provider point of view
- goal: seamless integration of mobility into B-ISDN

Problem: very high complexity of the system – never reached products

ATM - basic principle

- favored by the telecommunication industry for advanced high-performance networks, e.g., B-ISDN, as transport mechanism
- statistical (asynchronous, on demand) TDM (ATDM, STDM)
- cell header determines the connection the user data belongs to
- mixing of different cell-rates is possible
  - different bit-rates, constant or variable, feasible
- interesting for data sources with varying bit-rate:
  - e.g., guaranteed minimum bit-rate
  - additionally bursty traffic if allowed by the network

ATM cell:



Cell-based transmission

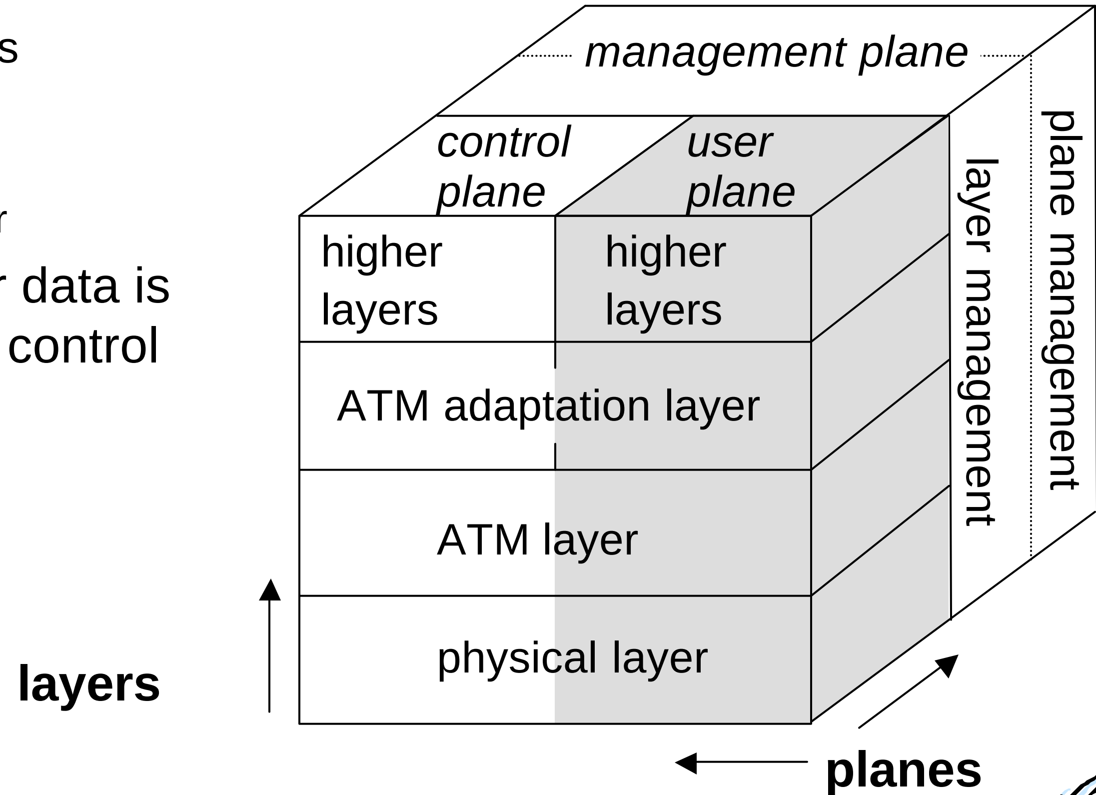
- asynchronous, cell-based transmission as basis for ATM
- continuous cell-stream
- additional cells necessary for operation and maintenance of the network (OAM cells; Operation and Maintenance)
- OAM cells can be inserted after fixed intervals to create a logical frame structure
- if a station has no data to send it automatically inserts idle cells that can be discarded at every intermediate system without further notice

B-ISDN protocol reference model

3 dimensional reference model

- three vertical planes (columns)
  - user plane
  - control plane
  - management plane
- three hierarchical layers
  - physical layer
  - ATM layer
  - ATM adaptation layer

Out-of-Band-Signaling: user data is transmitted separately from control information



ATM Forum Wireless ATM Working Group

- ATM Forum founded the *Wireless ATM Working Group* June 1996
- Task: development of specifications to enable the use of ATM technology also for wireless networks with a large coverage of current network scenarios (private and public, local and global)
- compatibility to existing ATM Forum standards important
- it should be possible to easily upgrade existing ATM networks with mobility functions and radio access
- two sub-groups of work items

Radio Access Layer (RAL) Protocols

- radio access layer
- wireless media access control
- wireless data link control
- radio resource control
- handover issues

Mobile ATM Protocol Extensions

- handover signaling
- location management
- mobile routing
- traffic and QoS Control
- network management

WATM services

Office environment

- multimedia conferencing, online multimedia database access

Universities, schools, training centers

- distance learning, teaching

Industry

- database connection, surveillance, real-time factory management

Hospitals

- reliable, high-bandwidth network, medical images, remote monitoring

Home

- high-bandwidth interconnect of devices (TV, CD, PC, ...)

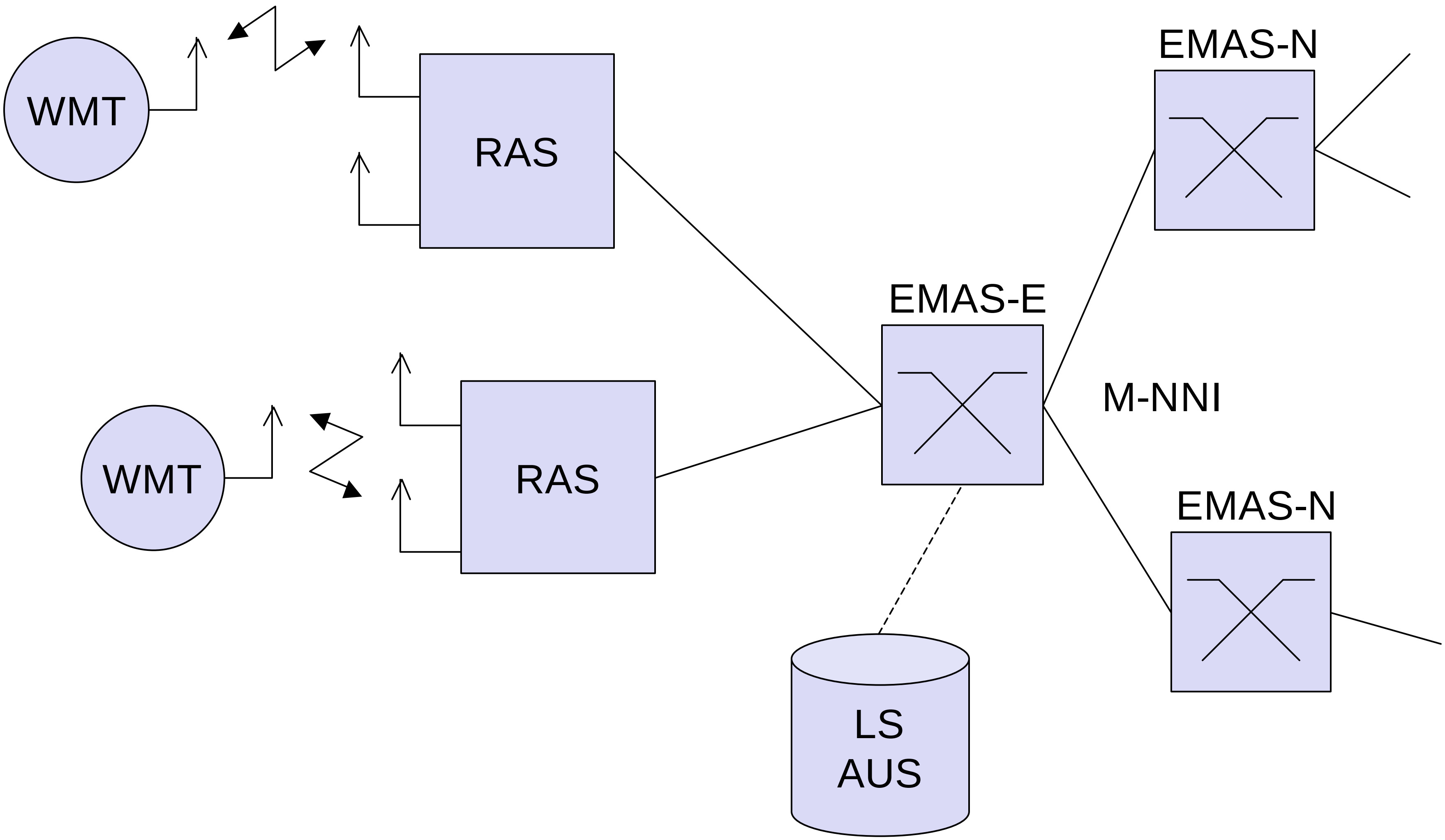
Networked vehicles

- trucks, aircraft etc. interconnect, platooning, intelligent roads

WATM components

- WMT (Wireless Mobile ATM Terminal)
- RAS (Radio Access System)
- EMAS-E (End-user Mobility-supporting ATM Switch - Edge)
- EMAS-N (End-user Mobility-supporting ATM Switch - Network)
- M-NNI (Network-to-Network Interface with Mobility support)
- LS (Location Server)
- AUS (Authentication Server)

Reference model



BRAN – Broadband Radio Access Networks

Motivation

- deregulation, privatization, new companies, new services
- How to reach the customer?
  - alternatives: xDSL, cable, satellite, radio

Radio access

- flexible (supports traffic mix, multiplexing for higher efficiency, can be asymmetrical)
- quick installation
- economic (incremental growth possible)

Market

- private customers (Internet access, tele-xy...)
- small and medium sized business (Internet, MM conferencing, VPN)

Scope of standardization

- access networks, indoor/campus mobility, 25-155 Mbit/s, 50 m-5 km
- coordination with ATM Forum, IETF, ETSI, IEEE, ...

Broadband network types

Common characteristics

- ATM QoS (CBR, VBR, UBR, ABR)

HIPERLAN/2

- short range (< 200 m), indoor/campus, 25 Mbit/s user data rate
- access to telecommunication systems, multimedia applications, mobility (<10 m/s)

HIPERACCESS

- wider range (< 5 km), outdoor, 25 Mbit/s user data rate
- fixed radio links to customers (“last mile”), alternative to xDSL or cable modem, quick installation
- Several (proprietary) products exist with 155 Mbit/s plus QoS

HIPERLINK – currently no activities

- intermediate link, 155 Mbit/s
- connection of HIPERLAN access points or connection between HIPERACCESS nodes

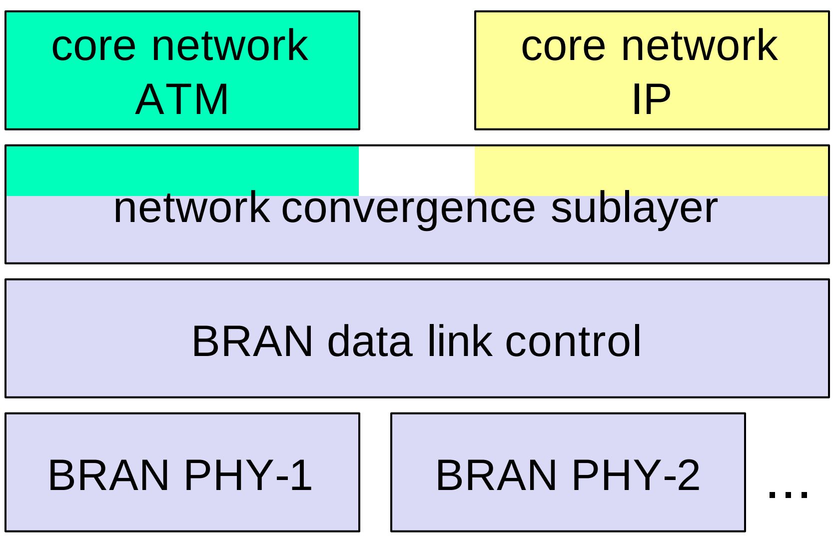
BRAN and legacy networks

Independence

- BRAN as access network independent from the fixed network
- Interworking of TCP/IP and ATM under study

Layered model

- Network Convergence Sub-layer as superset of all requirements for IP and ATM



Coordination

- IETF (TCP/IP)
- ATM forum (ATM)
- ETSI (UMTS)
- CEPT, ITU-R, ...
  (radio frequencies)

HiperLAN2 (historical)

Official name: BRAN HIPERLAN Type 2

- H/2, HIPERLAN/2 also used

High data rates for users

- More efficient than 802.11a

Connection oriented

QoS support

Dynamic frequency selection

Security support

- Strong encryption/authentication

Mobility support

Network and application independent

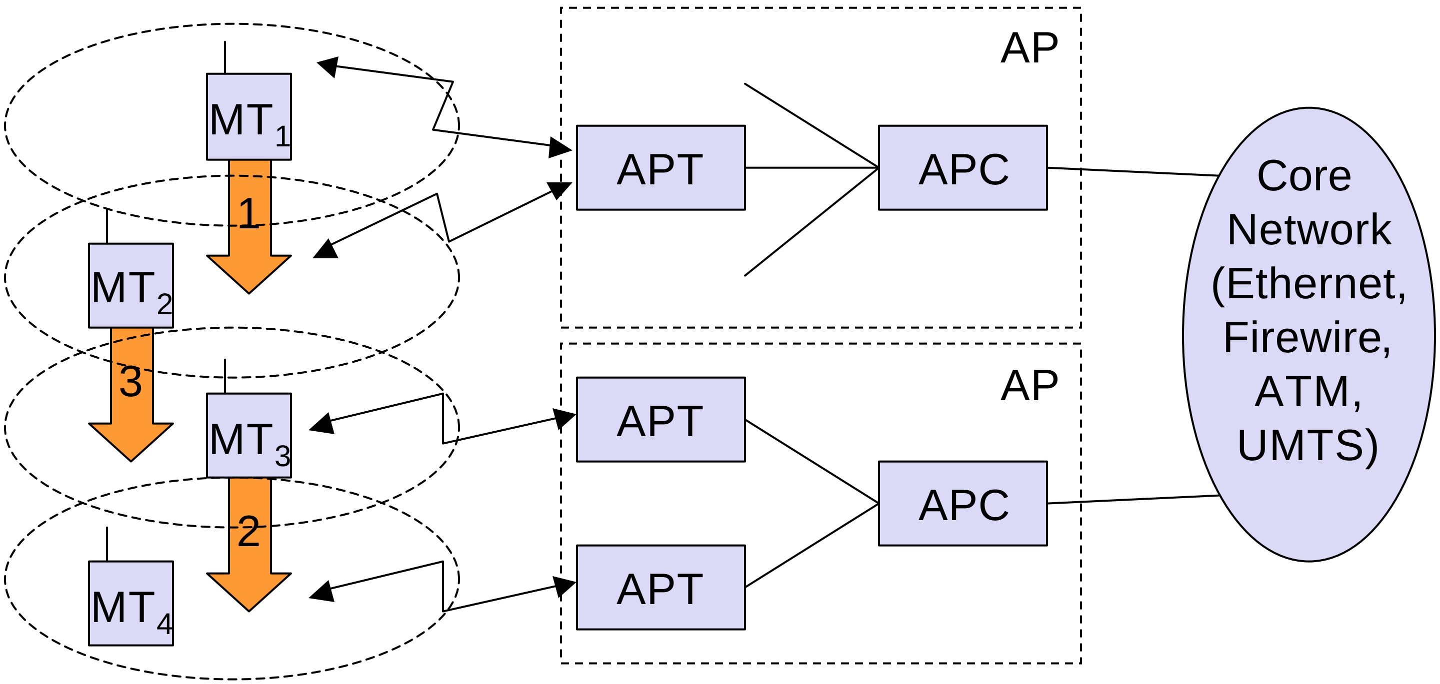
- convergence layers for Ethernet, IEEE 1394, ATM, 3G

Power save modes

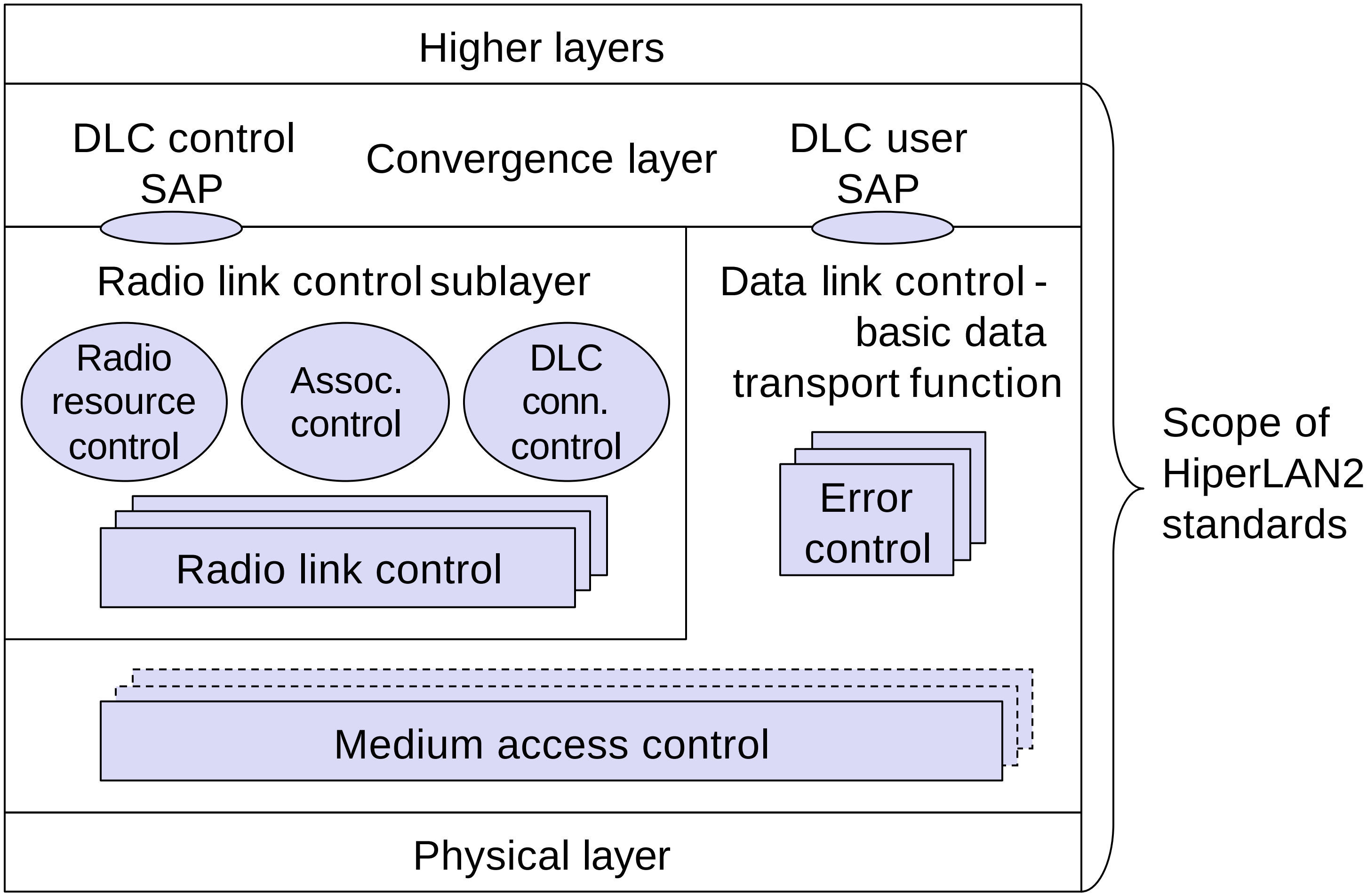
Plug and Play

No products – but several mechanisms have been
Adopted by other standards (e.g. 802.11a)

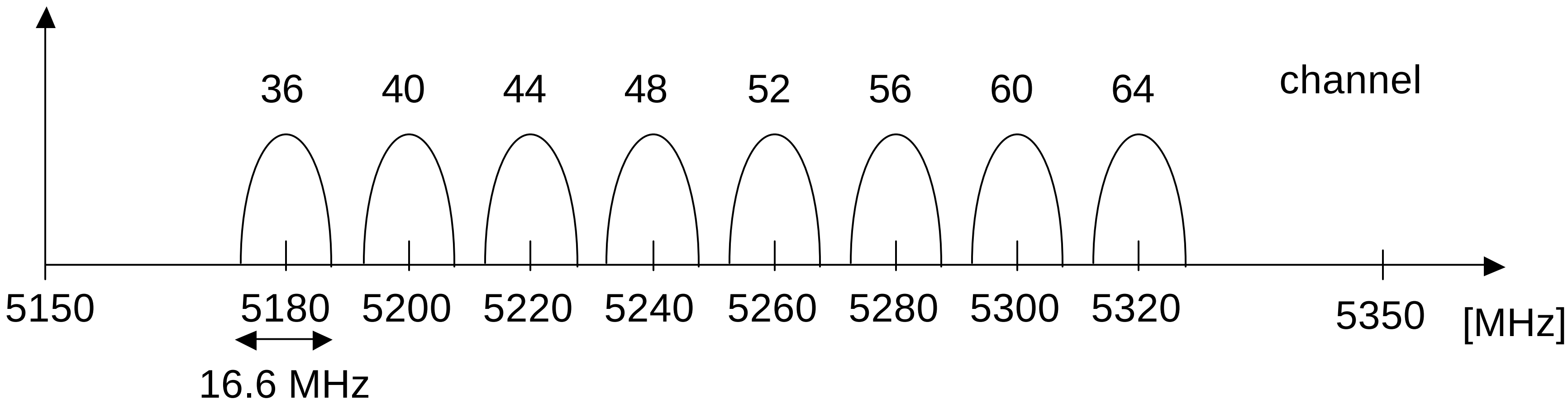
HiperLAN2 architecture and handover scenarios

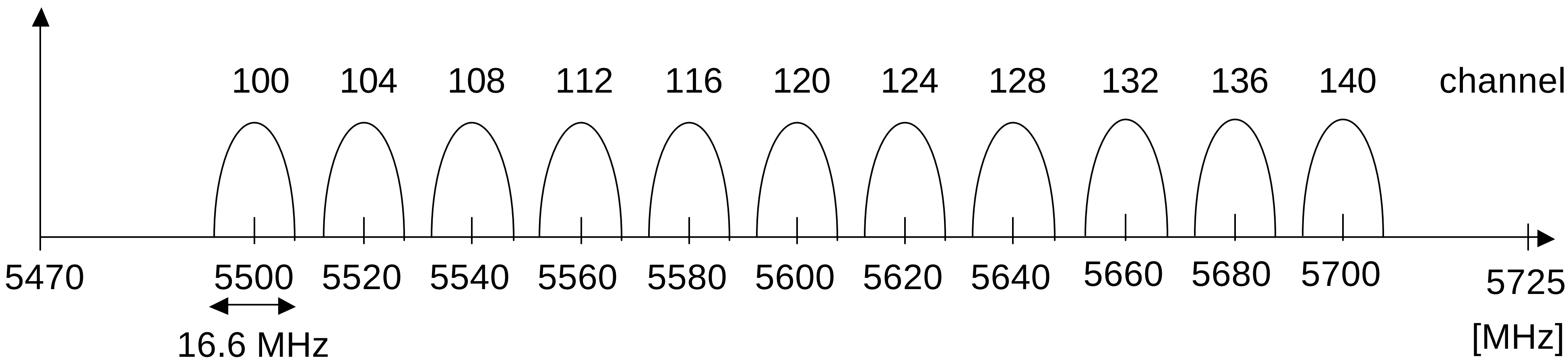


HiperLAN2 protocol stack



Operating channels of HiperLAN2 in Europe



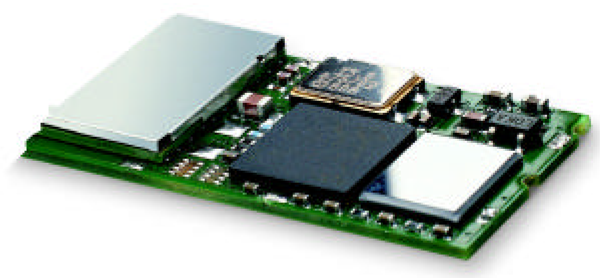


center frequency =
5000 + 5*channel number [MHz]

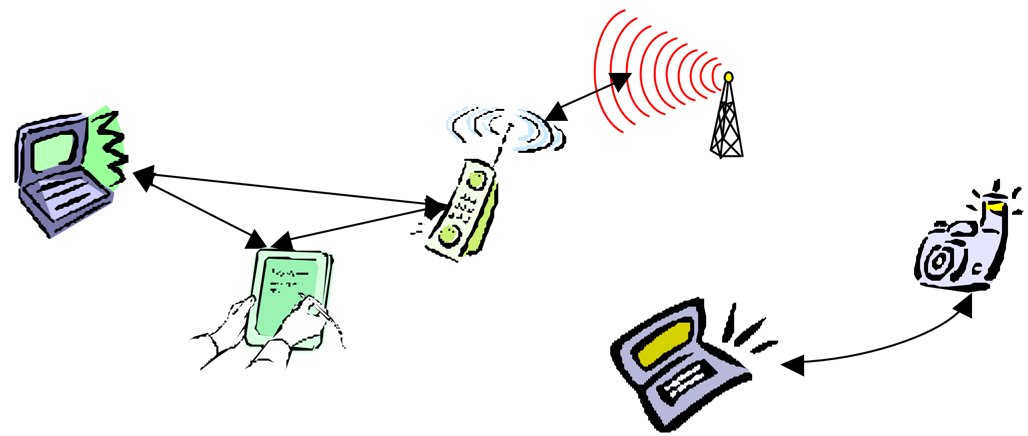
Bluetooth

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

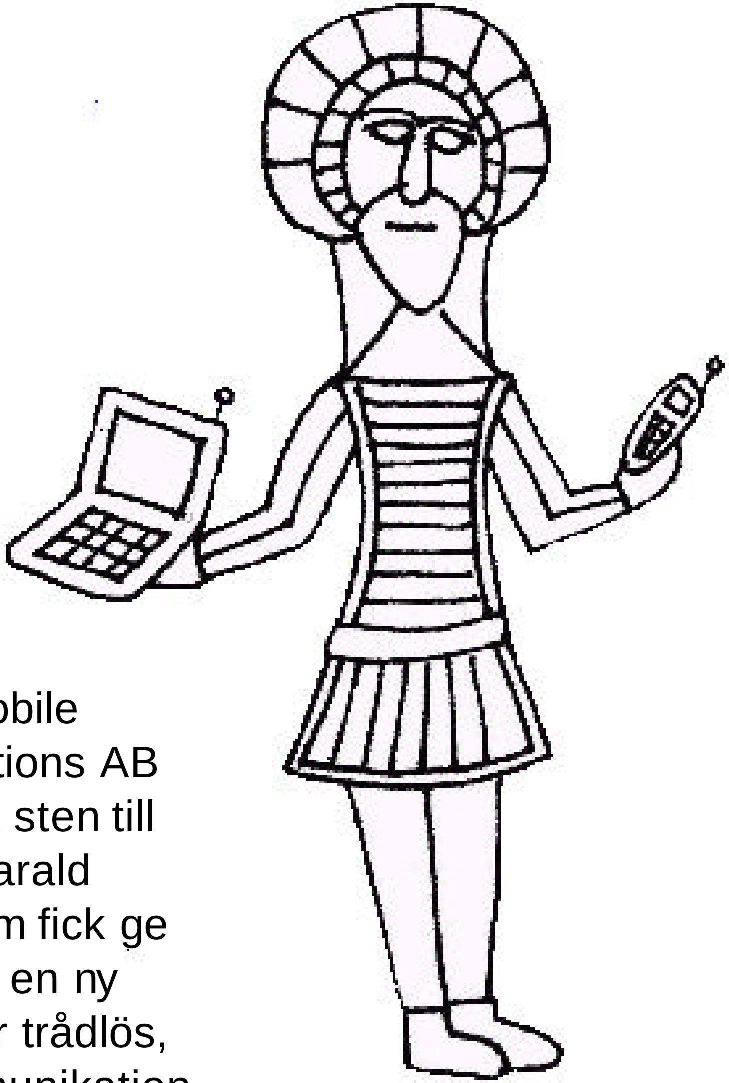
- 1994: Ericsson (Mattison/Haartsen), “MC-link” project
- Renaming of the project: Bluetooth according to Harald “Blåtand” Gormsen [son of Gorm], King of Denmark in the 10th century
- 1998: foundation of Bluetooth SIG, www.bluetooth.org (was: Bluetooth)
- 1999: erection of a rune stone at Ercisson/Lund ;-)
- 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
- > 2500 members
- Common specification and certification of products

History and hi-tech…



1999:
Ericsson mobile communications AB reste denna sten till minne av Harald Blåtand, som fick ge sitt namn åt en ny teknologi för trådlös, mobil kommunikation.

Characteristics

2.4 GHz ISM band, 79 (23) 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

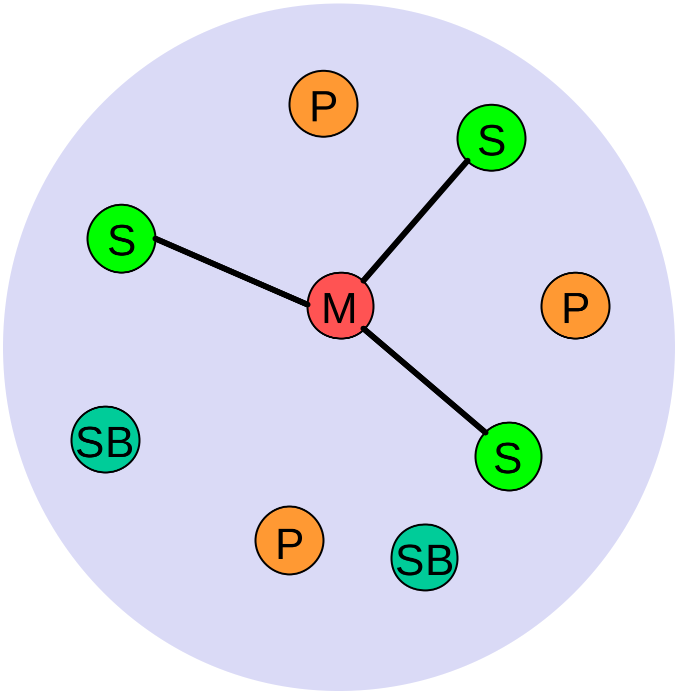
Topology

- Overlapping piconets (stars) forming a scatternet

Freie Universität Berlin

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

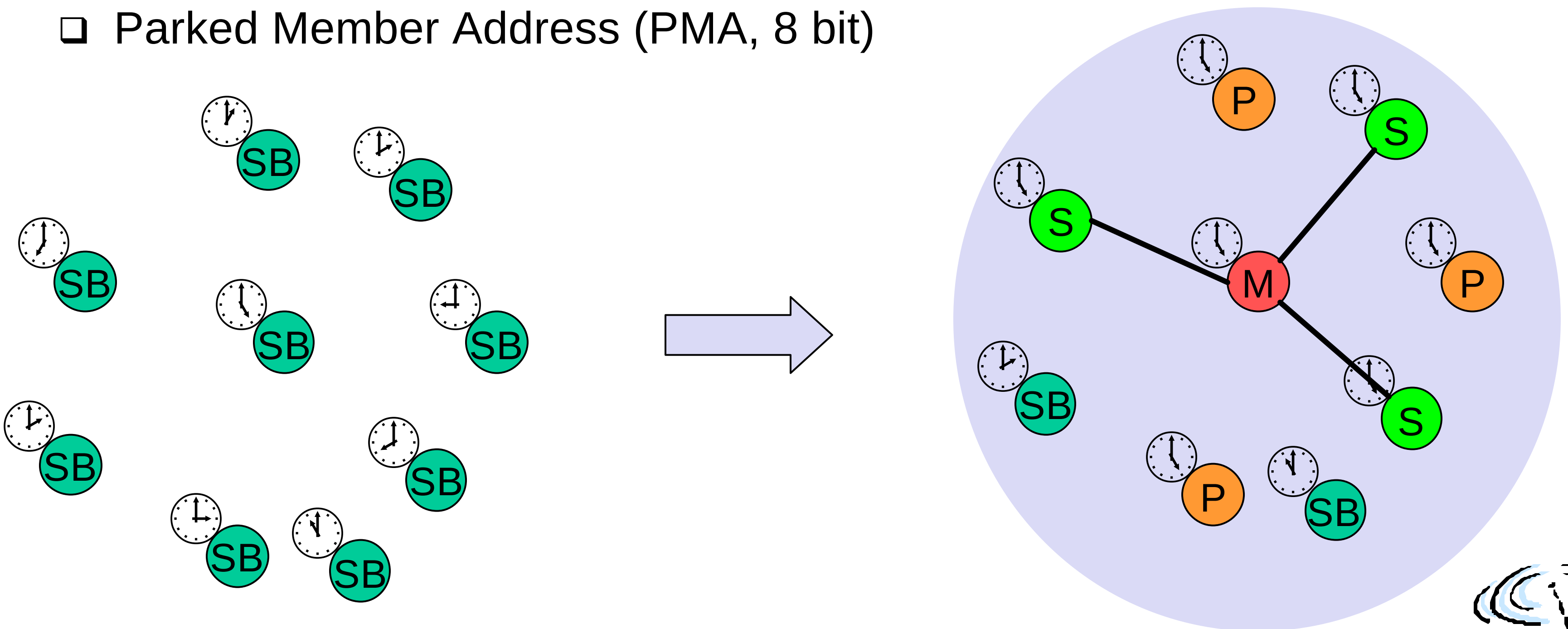
Forming a piconet

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)



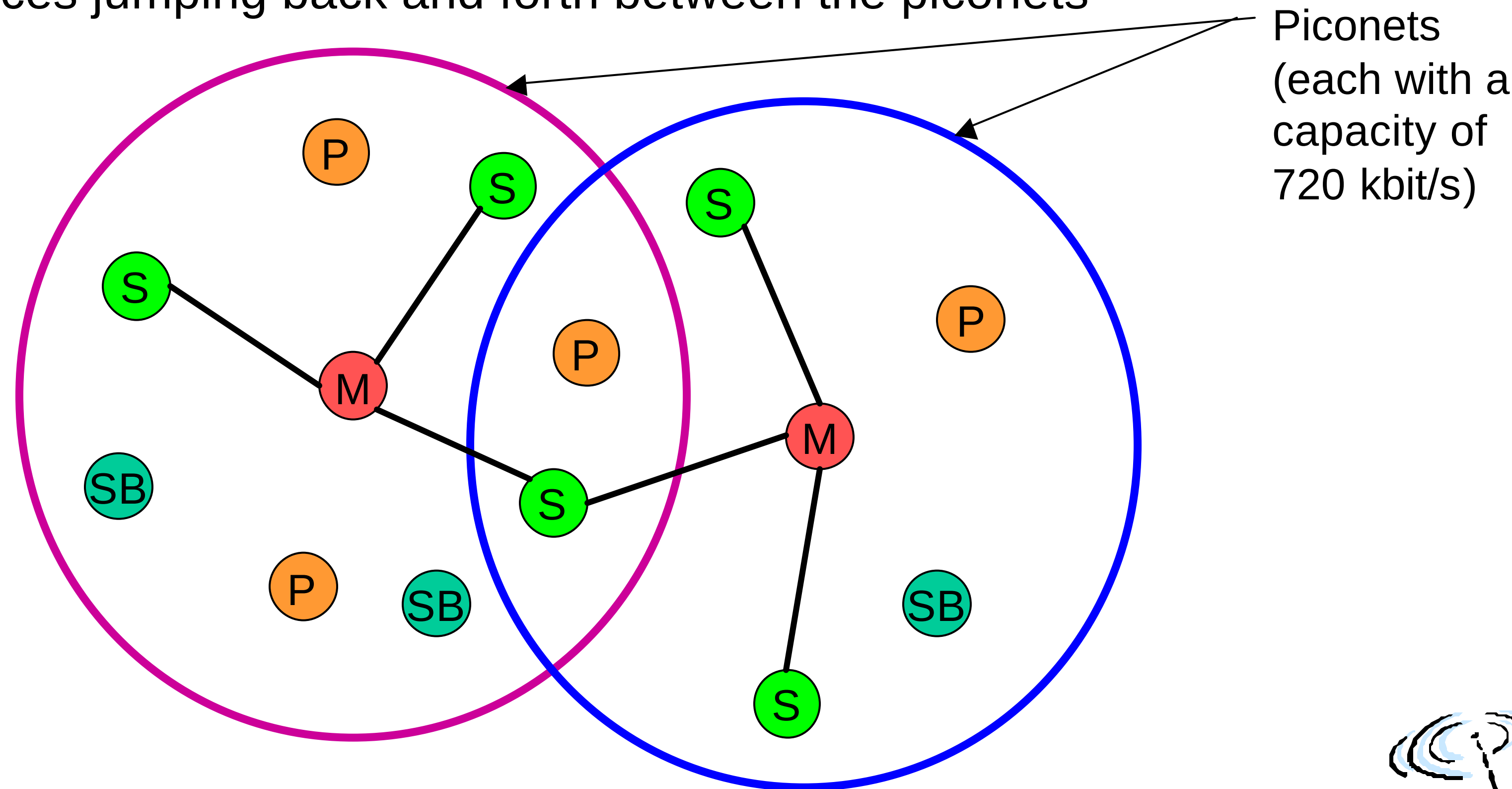
Scatternet

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

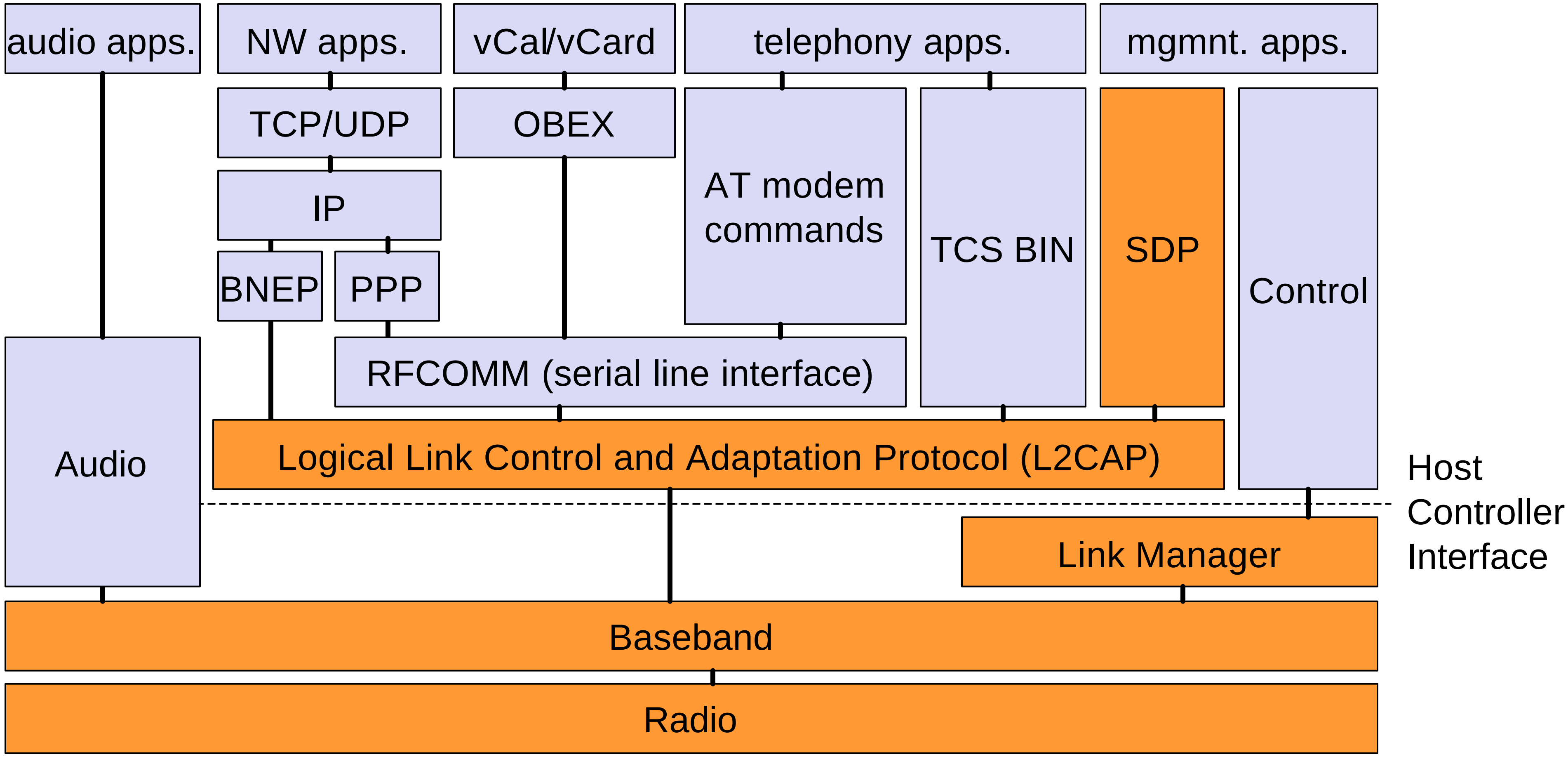
Communication between piconets

- Devices jumping back and forth between the piconets



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

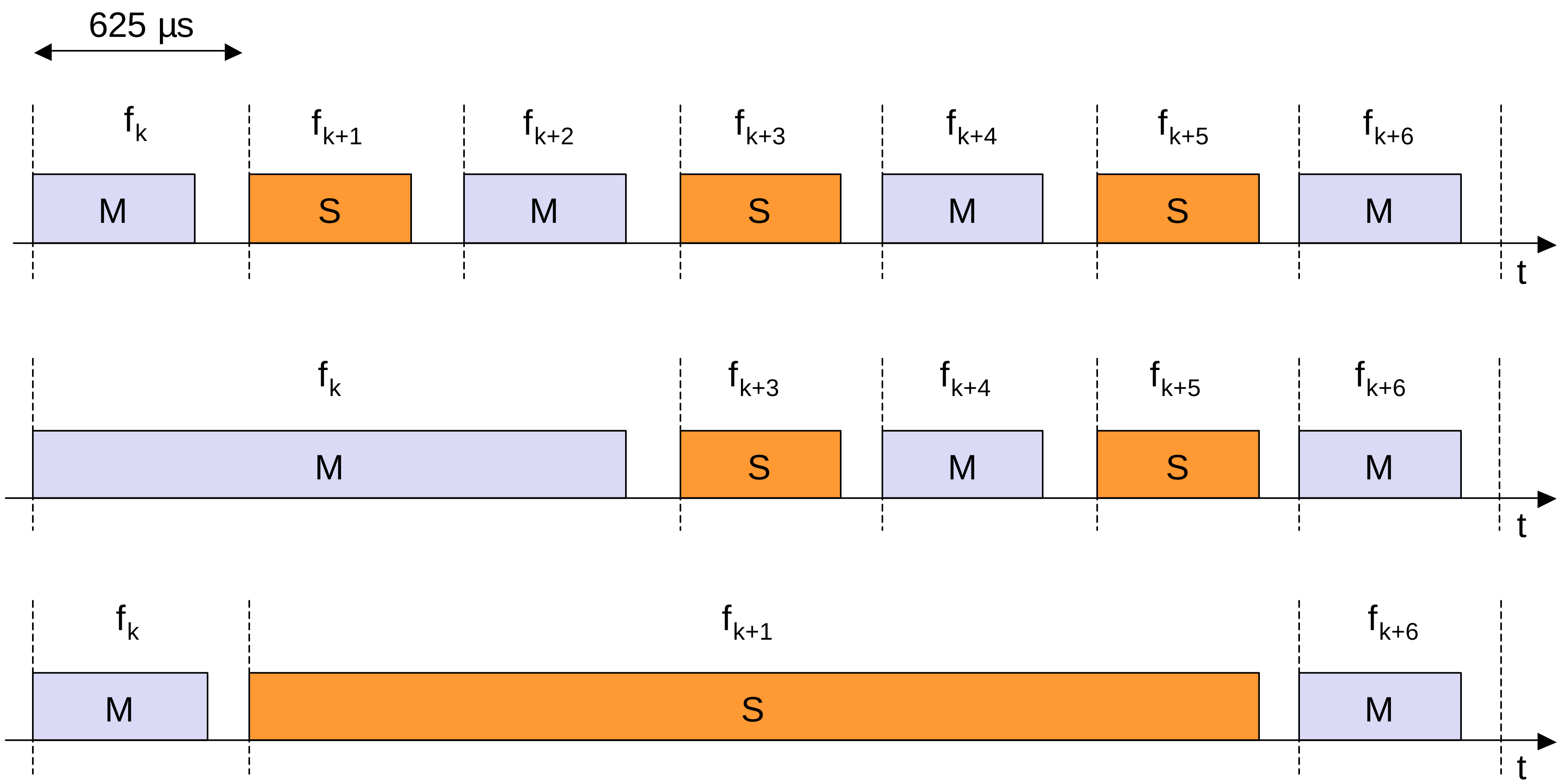
Bluetooth protocol stack



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



SCO payload types

	payload (30)
HV1	audio (10) | FEC (20)
HV2	audio (20) | FEC (10)
HV3	audio (30)
DV	audio (10) | header (1) | payload (0-9) | 2/3 FEC | CRC (2)

(bytes)

Baseband link types

Polling-based TDD packet transmission

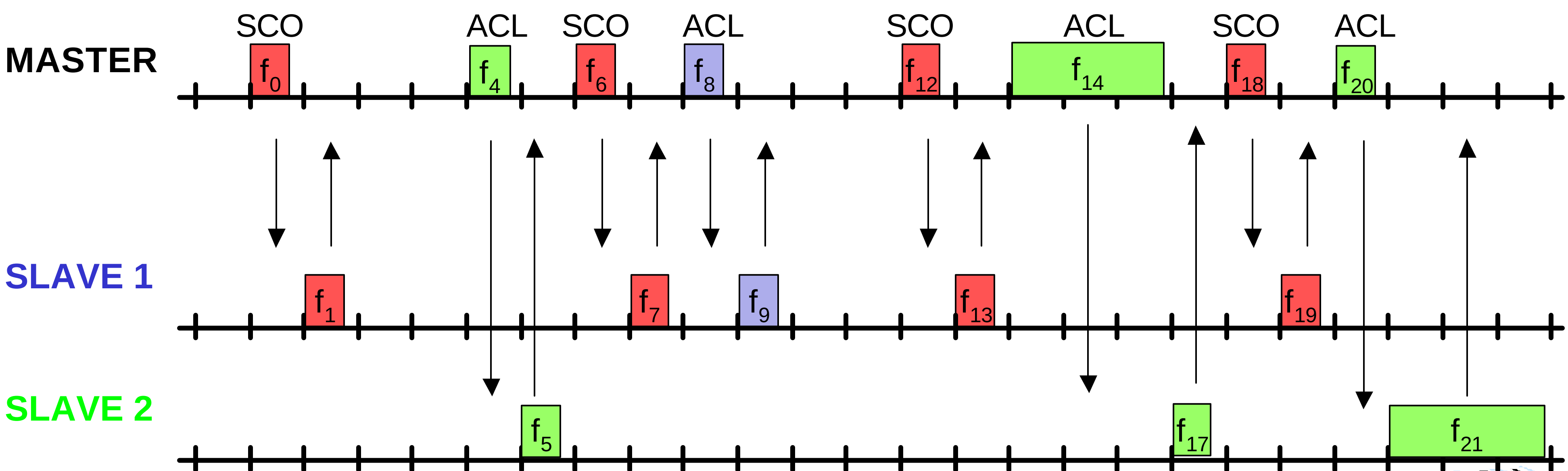
- 625µs slots, master polls slaves

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

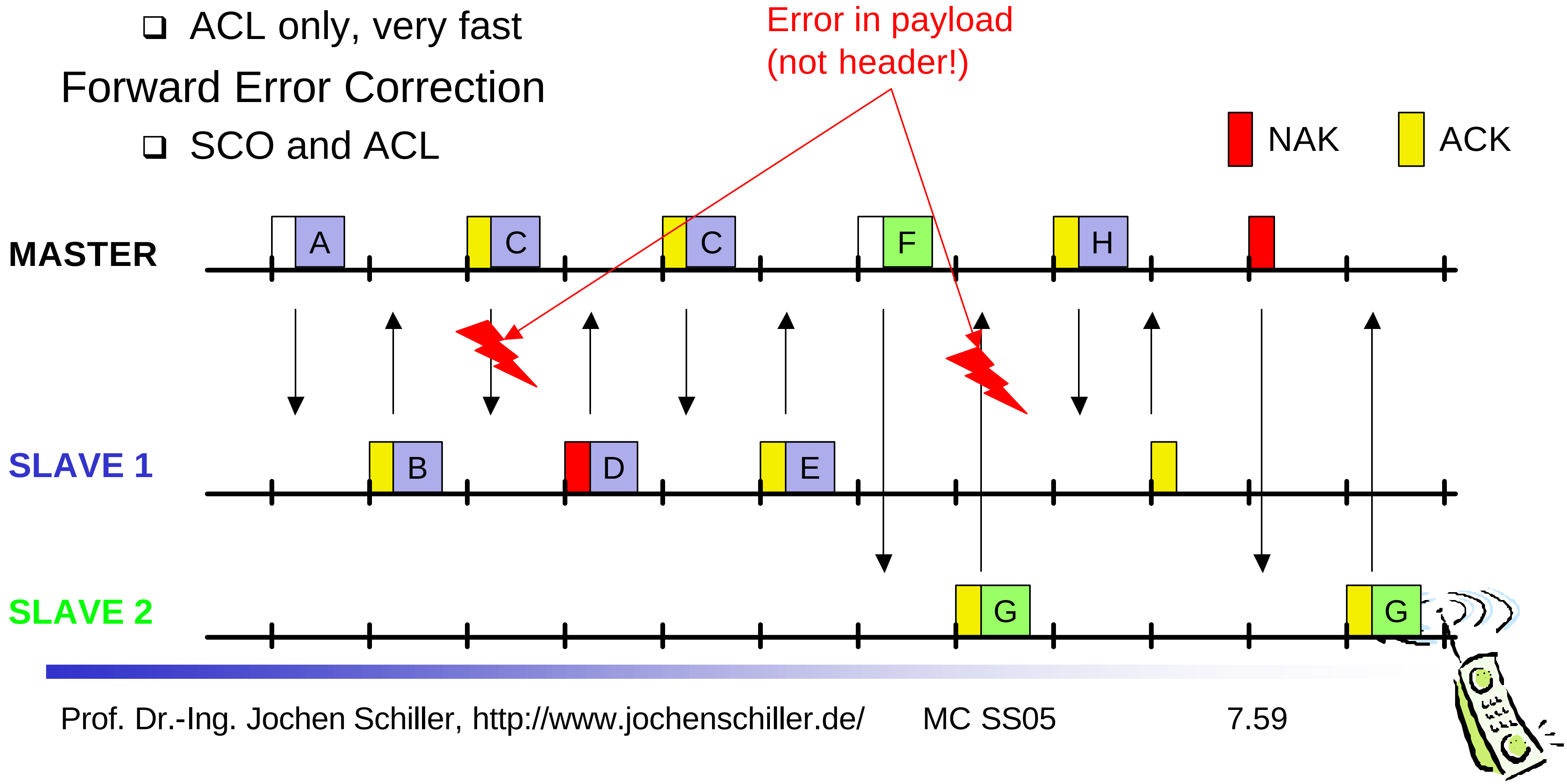
- Protection from interference on certain frequencies
- Separation from other piconets (FH-CDMA)

Retransmission

- ACL only, very fast

Forward Error Correction

- SCO and ACL



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

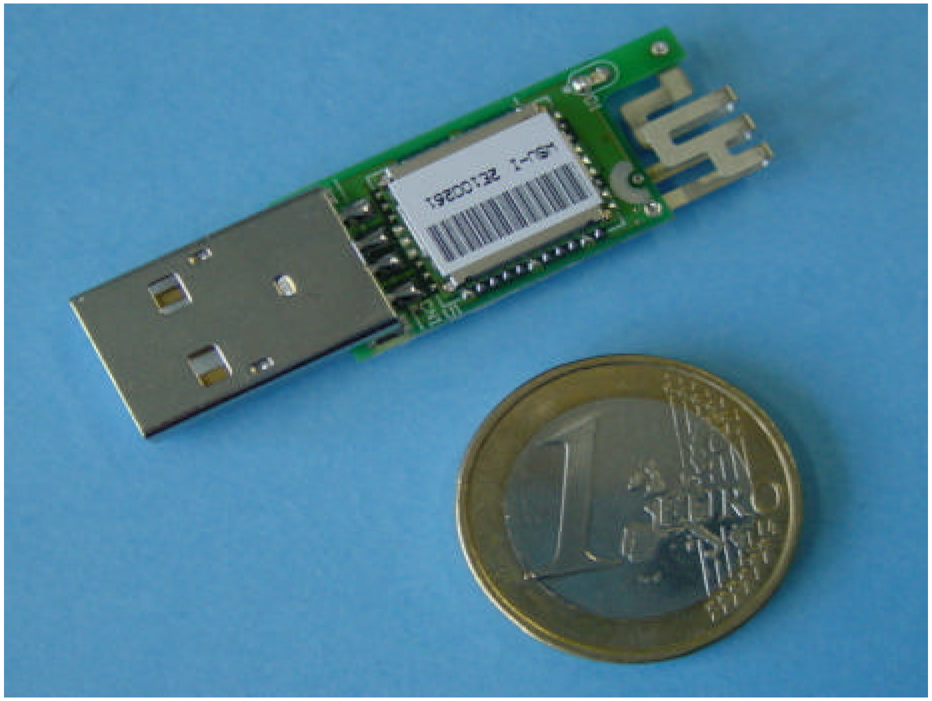
Notes:

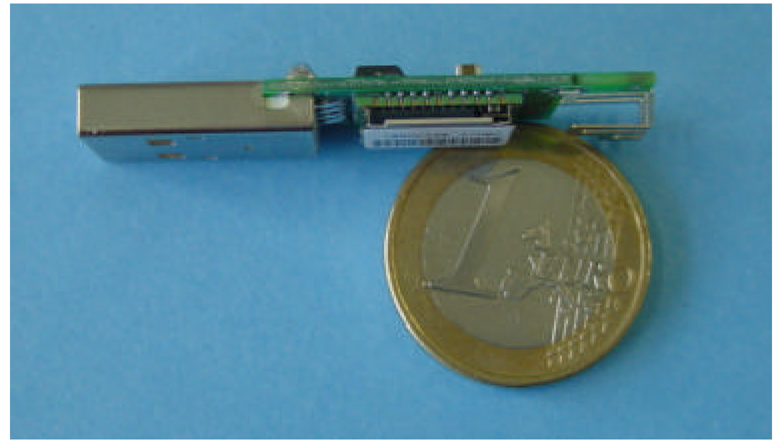
(1) Current consumption is the sum of both BC212015A and the flash.

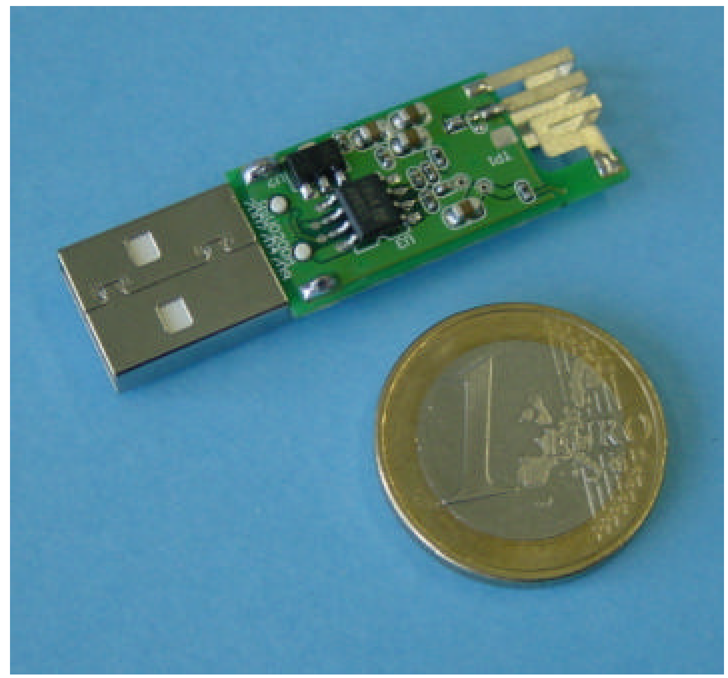
(2) Current consumption is for the BC212015A device only.

(More: www.csr.com)

Example: Bluetooth/USB adapter (2002: 50€)







L2CAP - Logical Link Control and Adaptation Protocol

Simple data link protocol on top of baseband

Connection oriented, connectionless, and signalling channels

Protocol multiplexing

- RFCOMM, SDP, telephony control

Segmentation & reassembly

- Up to 64kbyte user data, 16 bit CRC used from baseband

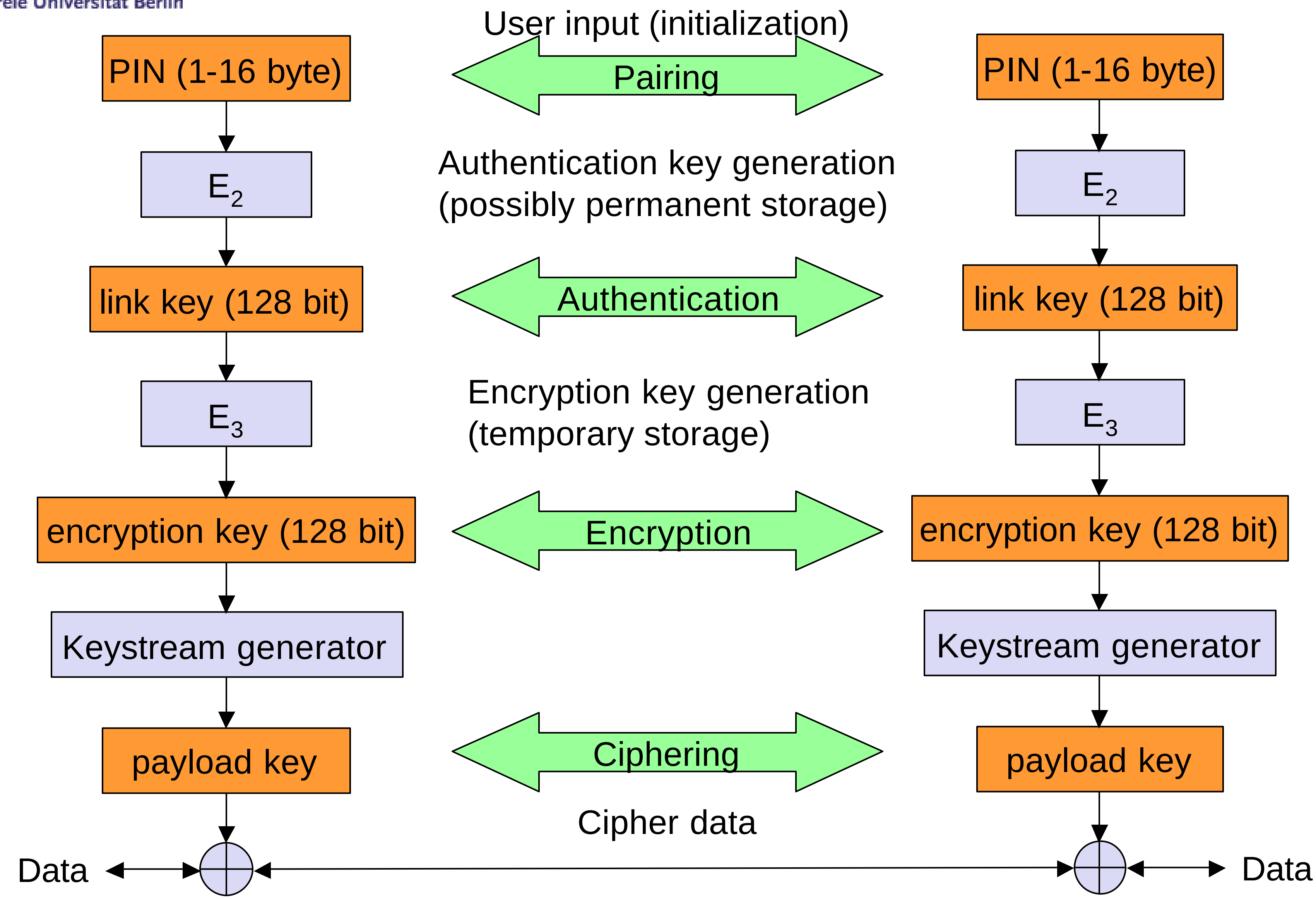
QoS flow specification per channel

- Follows RFC 1363, specifies delay, jitter, bursts, bandwidth

Group abstraction

- Create/close group, add/remove member

Security


User input (initialization)
PIN (1-16 byte)
Pairing
PIN (1-16 byte)
E2
Authentication key generation
(possibly permanent storage)
E2
link key (128 bit)
Authentication
link key (128 bit)
E3
Encryption key generation
(temporary storage)
E3
encryption key (128 bit)
Encryption
encryption key (128 bit)
Keystream generator
Keystream generator
payload key
Ciphering
payload key
Cipher data
Data
Data

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

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

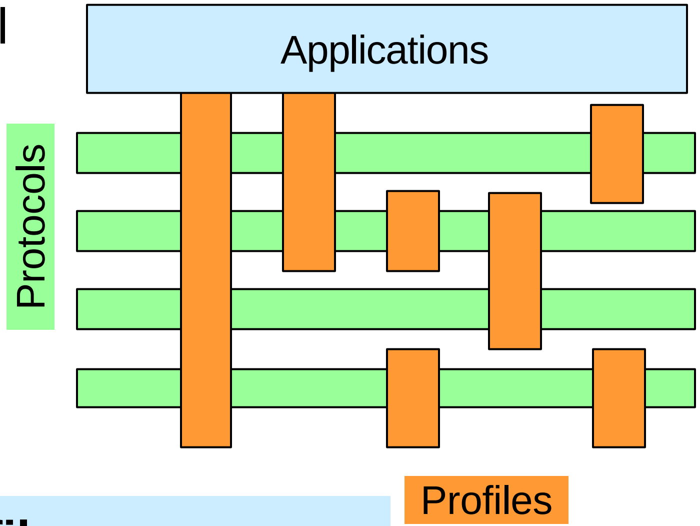
WAP

- Interacting with applications on cellular phones

Profiles

Represent default solutions for a certain usage model

- 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

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 devices/network&master, 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 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 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) 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

Basis of the ZigBee technology – www.zigbee.org

ZigBee

Relation to 802.15.4 similar to Bluetooth / 802.15.1

Pushed by Chipcon, ember, freescale (Motorola), Honeywell, Mitsubishi, Motorola, Philips, Samsung

More than 150 members

- Promoter (40000$/Jahr), Participant (9500$/Jahr), Adopter (3500$/Jahr)

No free access to the specifications (only promoters and participants)

ZigBee platforms comprise

- IEEE 802.15.4 for layers 1 and 2
- ZigBee protocol stack up to the applications

802.15.5: Mesh Networking

- Partial meshes, full meshes
- Range extension, more robustness, longer battery live

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
  - Unclear relation to 802.20, 802.16 started as fixed system…

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

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

WLAN: Home RF – yet another standard, no success

Data rate
- 0.8, 1.6, 5, 10 Mbit/s

Transmission range
- 300m outdoor, 30m indoor

Frequency
- 2.4 GHz ISM

Security
- Strong encryption, no open access

Cost
- Adapter 130€, base station 230€

Availability
- Several products from different vendors, no more support

Connection set-up time
- 10 ms bounded latency

Quality of Service
- Up to 8 streams A/V, up to 8 voice streams, priorities, best-effort

Manageability
- Like DECT & 802-LANs

Special Advantages/Disadvantages
- Advantage: extended QoS support, host/client and peer/peer, power saving, security
- Disadvantage: future uncertain due to DECT-only devices plus 802.11a/b for data

RFID – Radio Frequency Identification (1)

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

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

RFID – Radio Frequency Identification (2)

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 (3)

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 (4)

Security

- Denial-of-Service attacks are always possible
  - Interference of the wireless transmission, shielding of transceivers
- IDs via manufacturing or one time programming
- Key exchange via, e.g., RSA possible, encryption via, e.g., AES

Future Trends

- RTLS: Real-Time Locating System – big efforts to make total asset visibility come true
- Integration of RFID technology into the manufacturing, distribution and logistics chain
- Creation of „electronic manifests“ at item or package level (embedded inexpensive passive RFID tags)
- 3D tracking of children, patients

RFID – Radio Frequency Identification (5)

Devices and Companies

- AXCESS Inc., www.axcessinc.com
- Checkpoint Systems Group, www.checkpointsystems.com
- GEMPLUS, www.gemplus.com/app/smart_tracking
- Intermec/Intellitag, www.intermec.com
- I-Ray Technologies, www.i-ray.com
- RF Code, www.rfcode.com
- Texas Instruments, www.ti-rfid.com/id
- WhereNet, www.wherenet.com
- Wireless Mountain, www.wirelessmountain.com
- XCI, www.xci-inc.com

Only a very small selection…

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
- …

© Fusion Lighting, Inc.

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

Bluetooth may act like a rogue member of the 802.11 network

IEEE 802.15-2 discusses these problems

- Proposal: Adaptive Frequency Hopping