Structure of the Lecture

Chapter 2

- Technical Basics: Layer 1
- Methods for Medium Access: Layer 2

Chapter 3

- Wireless Networks: Bluetooth, WLAN, WirelessMAN, WirelessWAN
- Mobile Telecommunication Networks: GSM, GPRS, UMTS
- Satellites and Broadcast Networks

Large variety of standards for different purposes:

- *Bluetooth* for wireless ad-hoc connections in personal space
- *WLAN* for installing wireless local networks (focus on mobility)
- *WirelessMAN* for wireless broadband access in whole buildings (focus on capacity)
- *WirelessWAN* for wireless access in larger regions, also with high speeds

Chapter 4

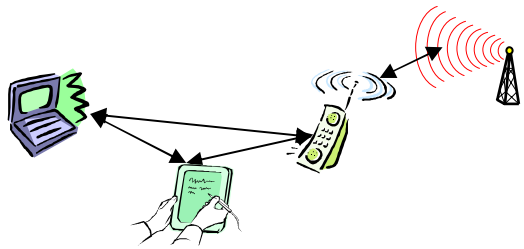
- Mobility on the network layer: Mobile IP, Routing, Ad-Hoc Networks
- Mobility on the transport layer: reliable transmission, flow control, QoS
- Mobility support on the application layer

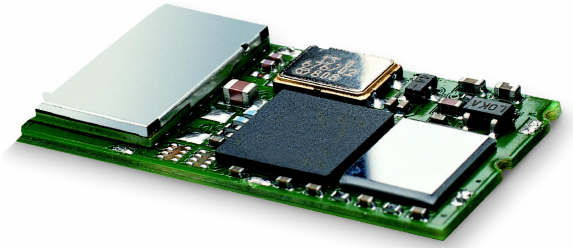
WPAN

- Smallest radio network: *Wireless Personal Area Network (WPAN)*
- Prominent example: *Bluetooth*
  - 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 the Bluetooth Special Interest Group (Ericsson, Intel, IBM, Nokia, Toshiba), www.bluetooth.org
  - Later joined: 3Com, Agere, Microsoft, Motorola
  - More than 2500 members
  - 2001: first consumer products for mass market, specification v1.1 released
  - Adopted from IEEE WPAN Working Group for integration into the 802.15 standard. Several variants:
    - Higher transmission rates
    - Low transmission rates with very low power consumption
    - More stations per network

WPAN - Bluetooth

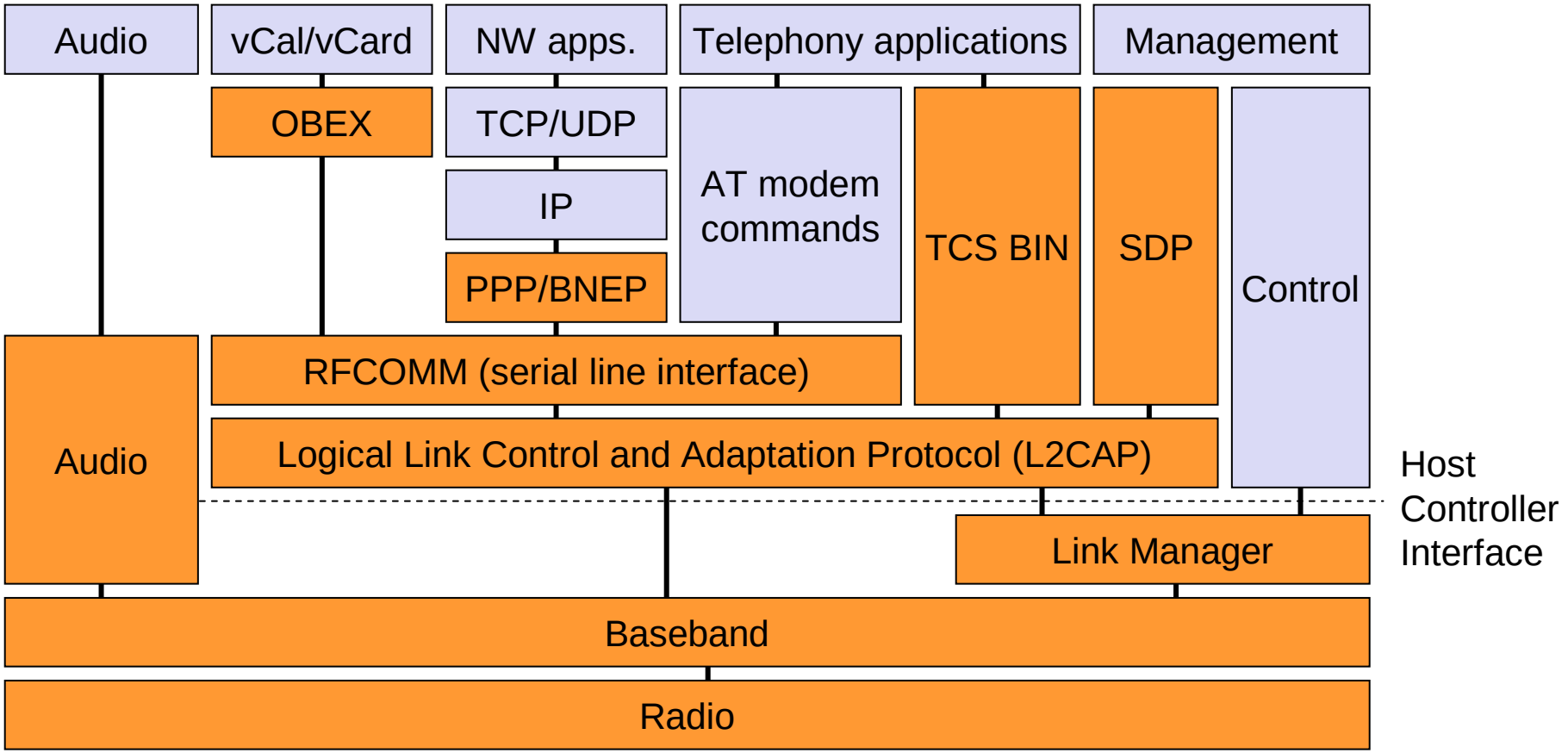
- Universal radio interface for ad-hoc wireless connectivity of heterogeneous devices
- Interconnection of computers with peripherals, handheld devices, PDAs, cellular phones – i.e. target group: small devices with low capabilities
- Embedded in other devices, goal: 5€/device (2002: 50€/USB Bluetooth)
- Often for devices already supporting GSM/GPRS or UMTS
- Short range (10 m, to achieve a low power consumption)
- Uses license-free 2,4 GHz ISM (Industrial-Scientific-Medical) band
- Voice and data transmission, ca. 2 Mbit/s gross data rate
- Automatic connection with devices in range
- Searching for services installed on other devices
- Possible: bandwidth reservation, QoS parameters
- Authentication and ciphering





One of the first modules (Ericsson)

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.

Bluetooth Protocols

Baseband/Radio

- Provide radio access for higher layer protocols

Link Manager Protocol (LMP)

- Connection management

L2CAP

- Provides several logical channels
- Segmentation of large messages for data transfer

Host Controller Interface (HCI)

- Command interface for access to baseband functions

Service Discovery Protocol (SDP)

- Searching for services on other devices

RFCOMM

- Emulation of serial interfaces (by this support of a variety of existing applications)

Telephony Control Protocol Specification - Binary (TCS BIN)

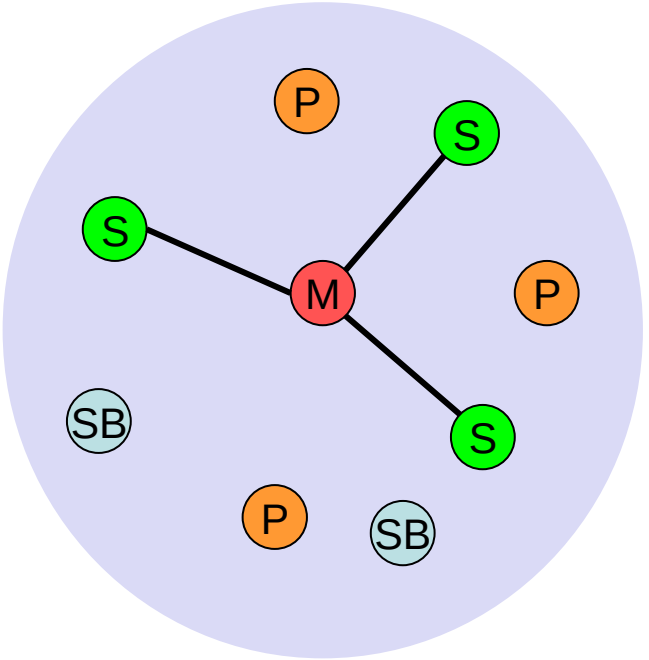
- Function for phone call control

Radio/Baseband

- Usage of 2,4 GHz ISM band
  - 79 channels (some countries: only 23) with a bandwidth of 1 MHz each
  - Channel 0: 2402 MHz … Channel 78: 2480 MHz
  - *GMSK* for Modulation
- Medium access: *TDD* and *FHSS*
  - Election of a master for transmission coordination
  - Frequency hopping with 1600 hops/sec (resulting slot duration: 625µs)
  - Hopping sequence in a pseudo random fashion, determined by the master
  - Time Division Duplex for separation of send/receive operation of the master
- Topology
  - Basic unit: *Piconet*
  - Overlapping piconets (stars) form a scatternet
- Devices
  - Three classes of devices, depending on transmission power
  - Class 1 (100 mW), class 2 (2.5 mW), class 3 (1 mW)

Piconet

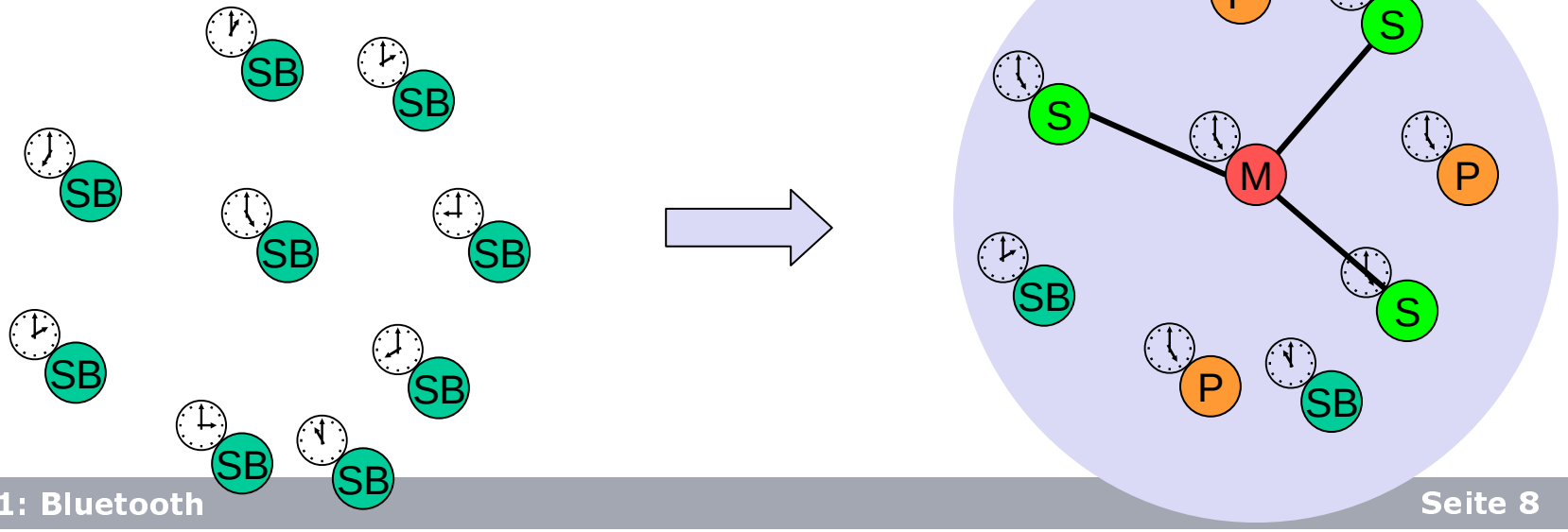
- Basic unit of a Bluetooth network
- Connection of devices in an ad-hoc fashion
- Consists of one master (M) and up to 7 slaves (S)
- The master coordinates medium access (hopping sequence)
- Slaves only communicate with the master
- Possible: independent overlapping piconets. Devices which exchange data belong to the same piconet
- Each piconet has a unique hopping pattern, participation of a slave in the piconet means synchronization to that sequence



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

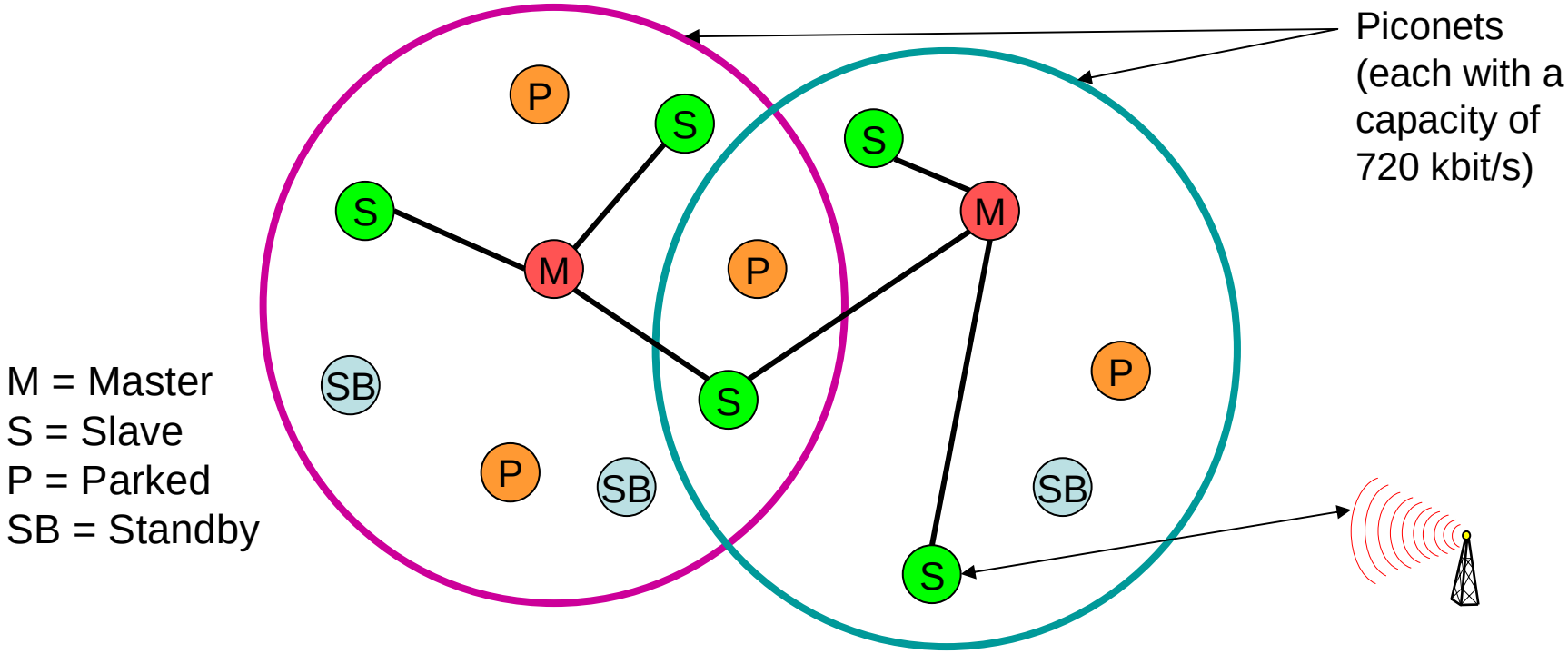
Forming a Piconet

- All devices in a piconet hop together
  - The master sends out 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)
  - And: unique Bluetooth address (B_ADDR) for each device

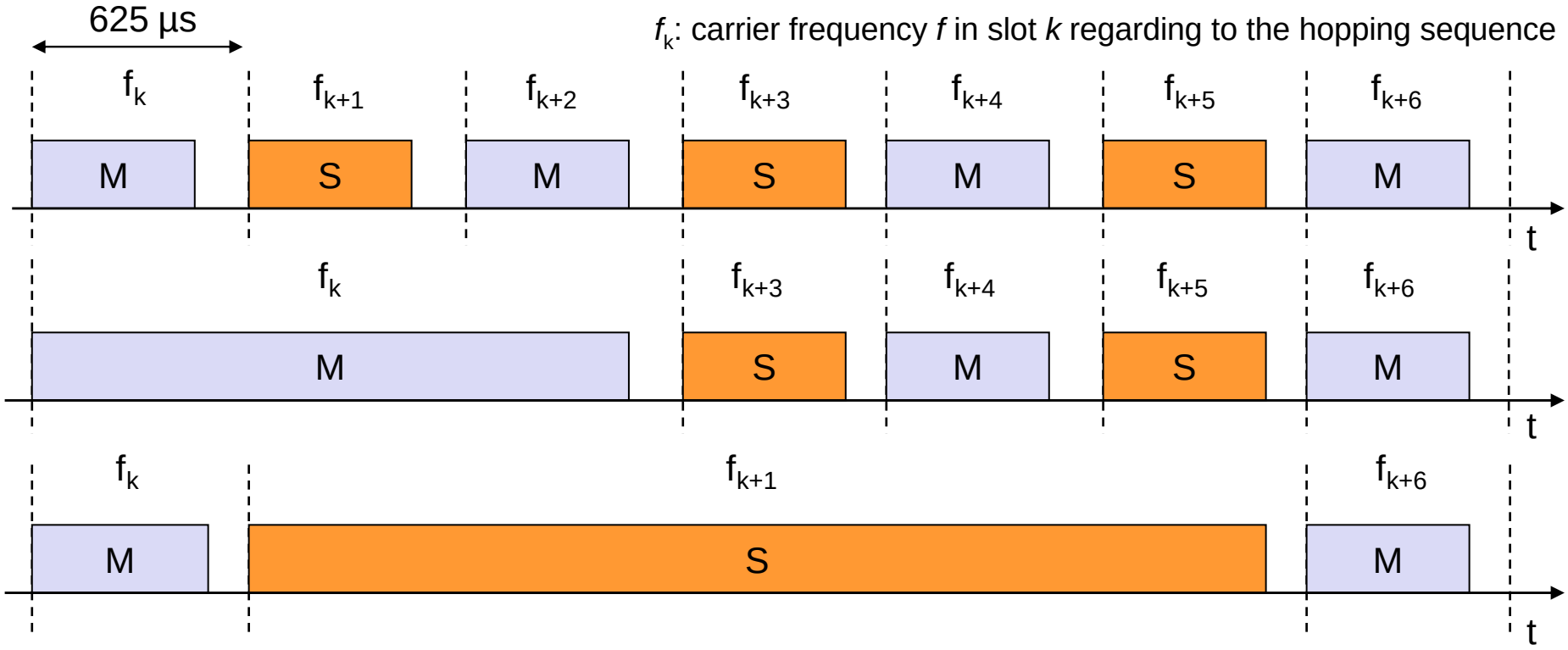


Scatternet

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



Frequency Selection during Data Transmission



- TDMA for coordinating the medium access
- TDD for duplex transmission: the master send in odd, the slave in even slots
- If several slaves are in the piconet: capacity is divided, the master cyclically polls all slaves (Master all odd slots, slaves share the even slots)
- 3 or 5 slots hops can be combined to one frame. No hoping during the frame, the hops are simply skipped

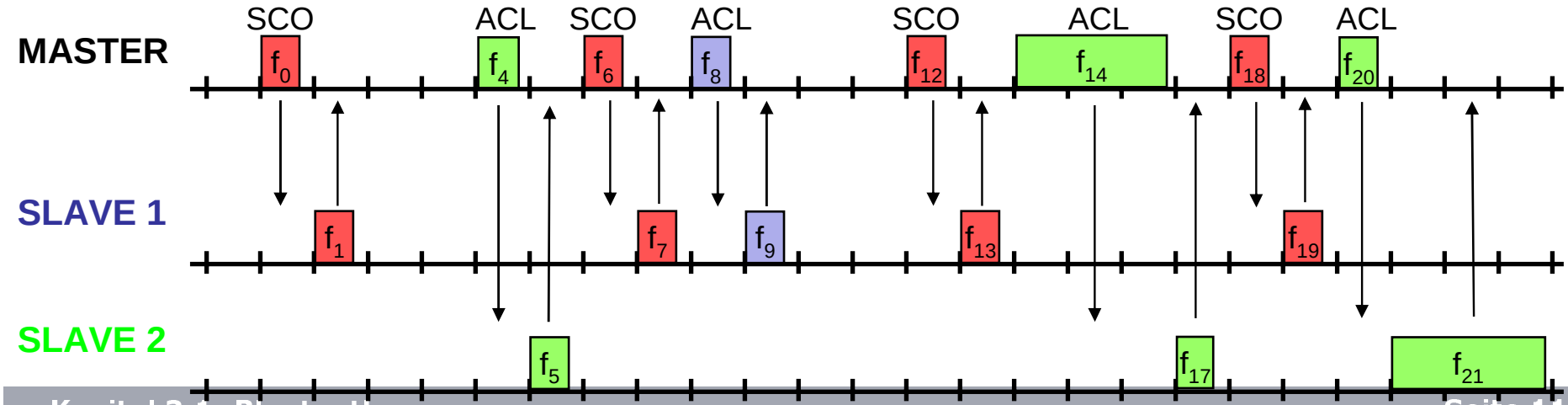
Link Types

SCO (Synchronous Connection-Oriented) – Voice

- Reservation of slots in firm intervals
- 64 kbit/s data rate
- Point-to-point links, connection-oriented
- Only FEC (Forward Error Correction), no retransmissions

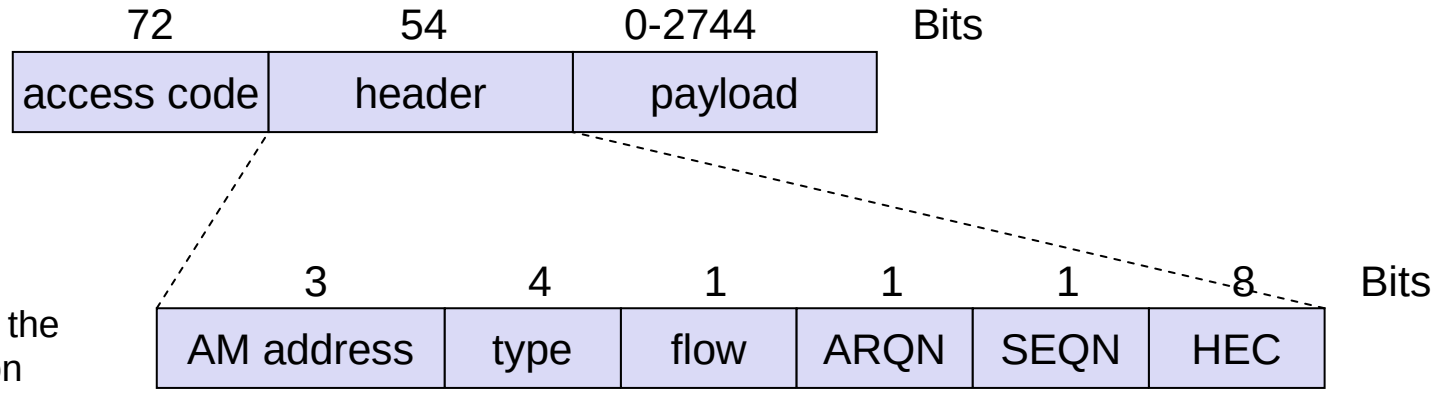
ACL (Asynchronous Connectionless) – Data

- Variable frame size (1,3,5 slots)
- Asymmetric (723,2:57,6 kbit/s) or symmetric (433,9 kbit/s) bandwidth
- Point-to-multipoint connections, connectionless with flow control



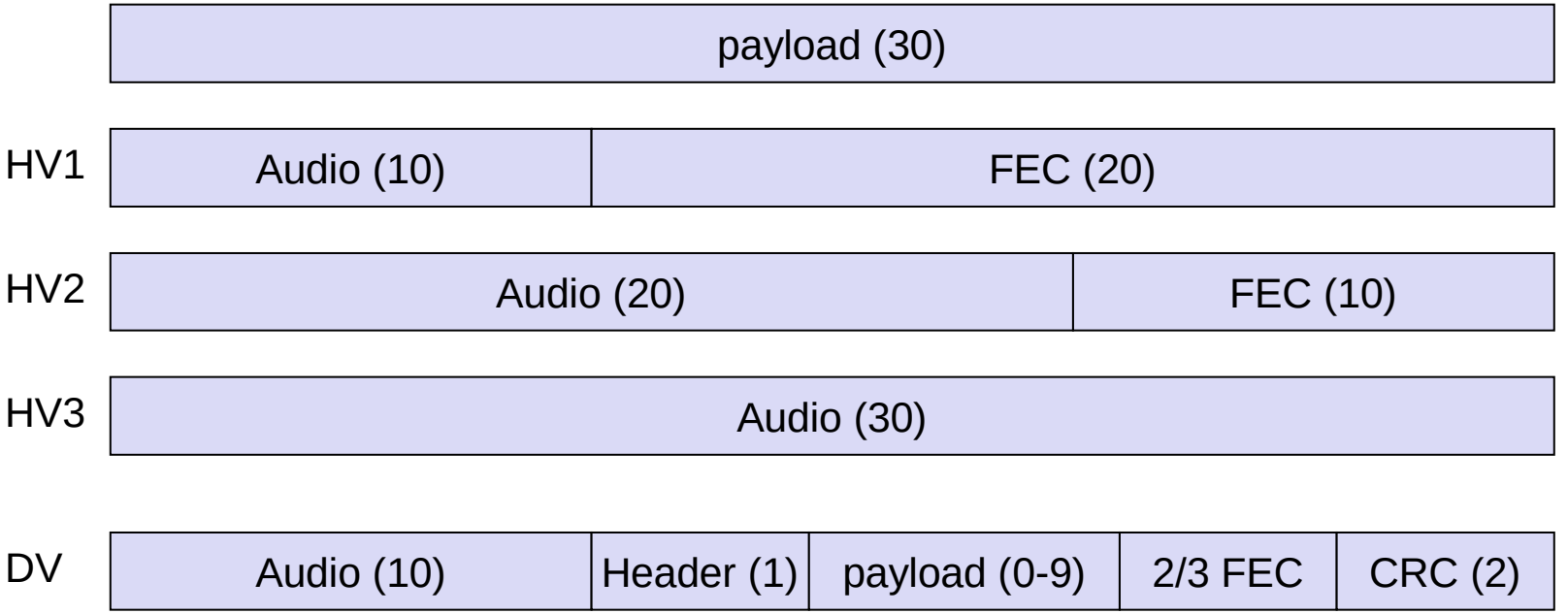
Baseband Frames

- *Access code*
  - Unique identification in the piconet, basing on device ID of the master
  - Consists of a preamble and a synchronization sequence (for hopping)
- *Header*
  - Active Member Address (1 Master, 7 Slaves)
  - Packet type, e.g. high quality voice, POLL, …
  - Flow: flow control, receiver can stop the sender
  - ARQN/SEQN: sequence and acknowledgement numbers
  - HEC: CRC checksum
- *Payload*: can use an additional FEC, if necessary (reducing the data rate)



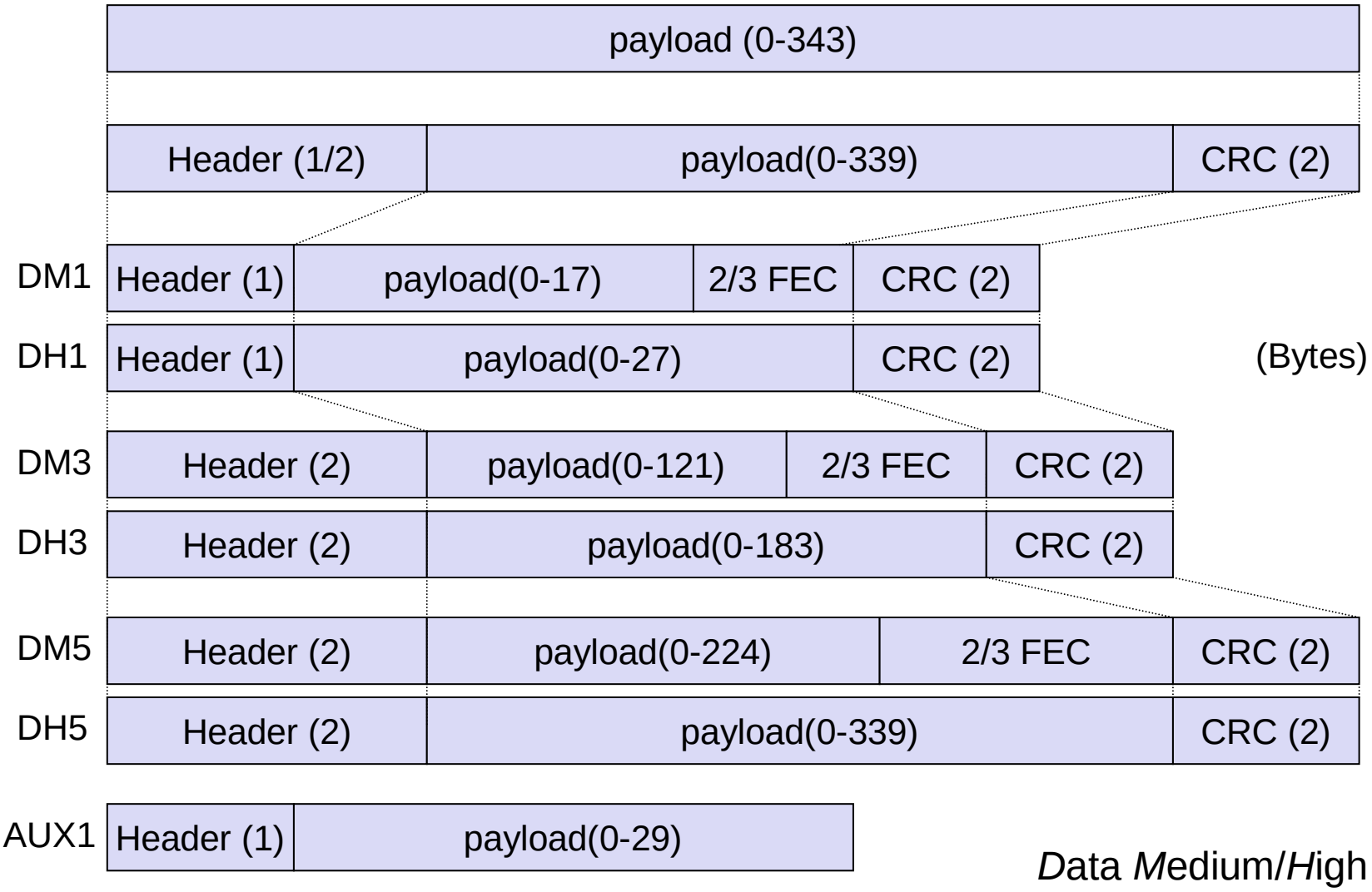
1/3-FEC: spend 2/3 of the data for error correction

SCO Payload Types



*H*igh-quality *V*oice, *D*ata and *V*oice

ACL Payload Types



*D*ata *M*edium/*H*igh rate

Baseband Data Rates

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

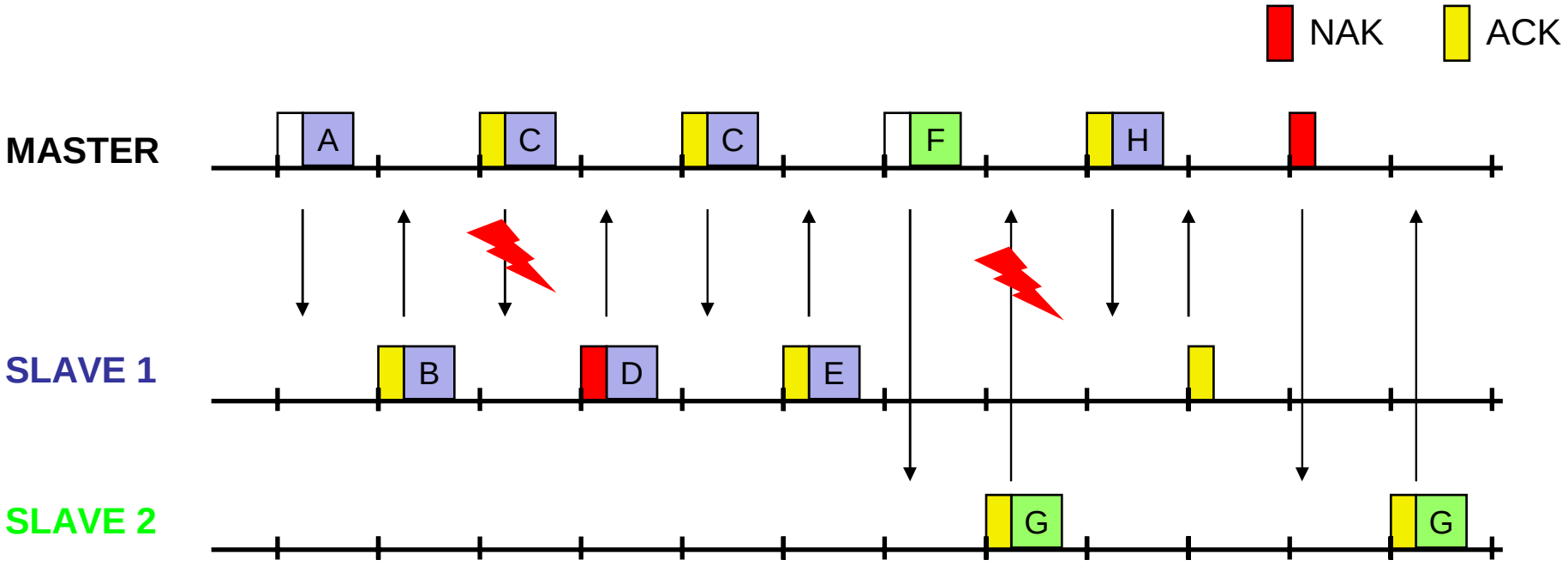
*D*ata *M*edium/*H*igh rate, *H*igh-quality *V*oice, *D*ata and *V*oice

Example for Power Consumption

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 115,2kbit/s (Master)	15,5 mA
ACL data transfer 720kbit/s (Slave)	53,0 mA
ACL data transfer 720kbit/s (Master)	53,0 mA
ACL connection , sniff mode 40ms interval, 38,4kbit/s	4,0 mA
ACL connection , sniff mode 1.28s interval, 38,4kbit/s	0,5 mA
Parked Slave, 1,28s beacon interval, 38,4kbps	0,6 mA
Standby-Modus (connected to host, no radio activity)	47,0 µA
Deep sleep mode	20,0 µA

Acknowledgement Mechanism

Retransmissions for ACL only, very fast; 1 Bit for sequence/acknowledgement numbers is enough because master and slave have to send alternating:



Link Manager Protocol

Provides additional functions to the simple baseband transmission service:

- Authentication of the communication partner, ciphering of data during transmission
- Clock synchronization (frequency hopping) by computing a clock offset added to the local time
- Switching of master/slave roles, because the master has a higher power consumption
- Switching of states (park, standby, active)
- Adaptation of transmission power regarding to measured signal strengths
- Reaction on varying transmission quality by changing the payload type (e.g. usage of a higher FEC rate when quality goes down)
- Setup of SCO connections. Default is ACL, but it can be used up to three SCO connections in parallel

Link Manager for Connection Establishment

A Bluetooth device can be in one of several states:

Standby

- Each 2048th slot (1.28s) a device listens on 32 of the 79 channels
- Incoming signals are examined, the device activates itself on demand
- Alternatively, use active connection establishment

Connection Establishment

- Process of connection establishment consists of three states
  1. *Inquiry*
  2. *Paging*
  3. *Paring*

Connected

- Device is is a piconet either as master or as slave, depending on the connection establishment phase
- Also possible to switch to a power-save mode

Connection Establishment - Inquiry

A device discovers its environment by an inquiry procedure; while no connection is established, the device switches between two states:

- *Inquiry* (“ask for connections”)

  Search for other devices by broadcasting special ID-frames on 32 defined channels (hopping through those frequencies)
- *Inquiry Scan* (“search for such asks”)

  Listen of the 32 channels for incoming inquiries (hopping)

A scanning device, on receiving an inquiry frame, answers with its B_ADDR

- After message exchange, devices know Bluetooth addresses, a common clock, Bluetooth device classes (power management)
- Human user can influence inquiry by deciding about visibility and power consumption of its device

The “inquiry” device becomes master, the “inquiry scan” device becomes slave

Afterwards: *paging*

Connection Establishment - Paging

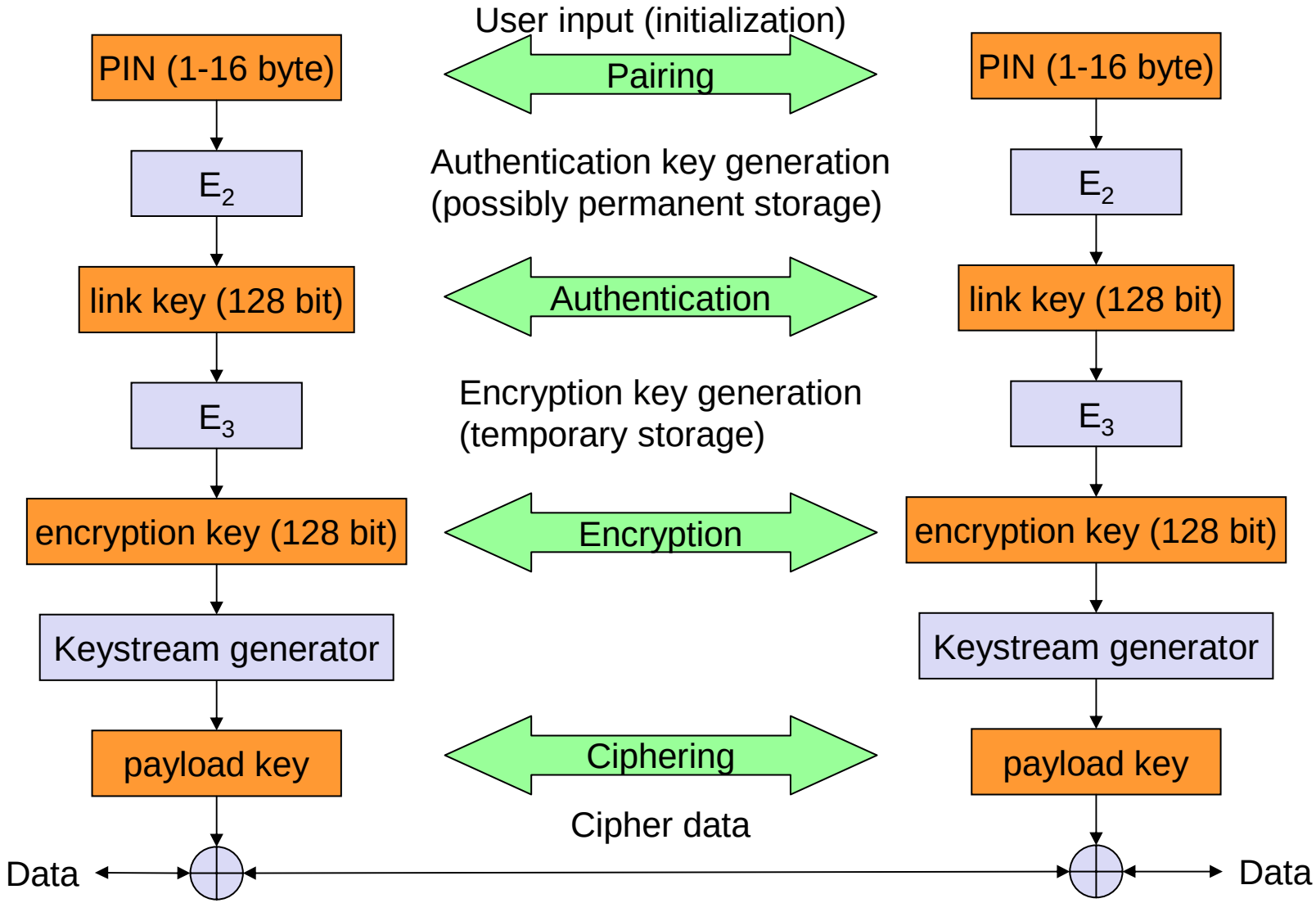
The inquiring device becomes master, but in inquiry state only the existence of other devices is tested – to really establish a connection, *paging* is done

- Master is in *page* mode: connection establishment request is sent to slave, including the address (B_ADDR) of the slave
- Slave is in *page scan* mode: listen for incoming page message
- Used in connection establishment: *page hopping sequence* – a hopping sequence based on the slave's ID
- If the slave answers in a certain time, the master sends a message including an AMA for the new slave as well as all synchronization information for joining the network
- Average time for connection establishment: 0.64 s

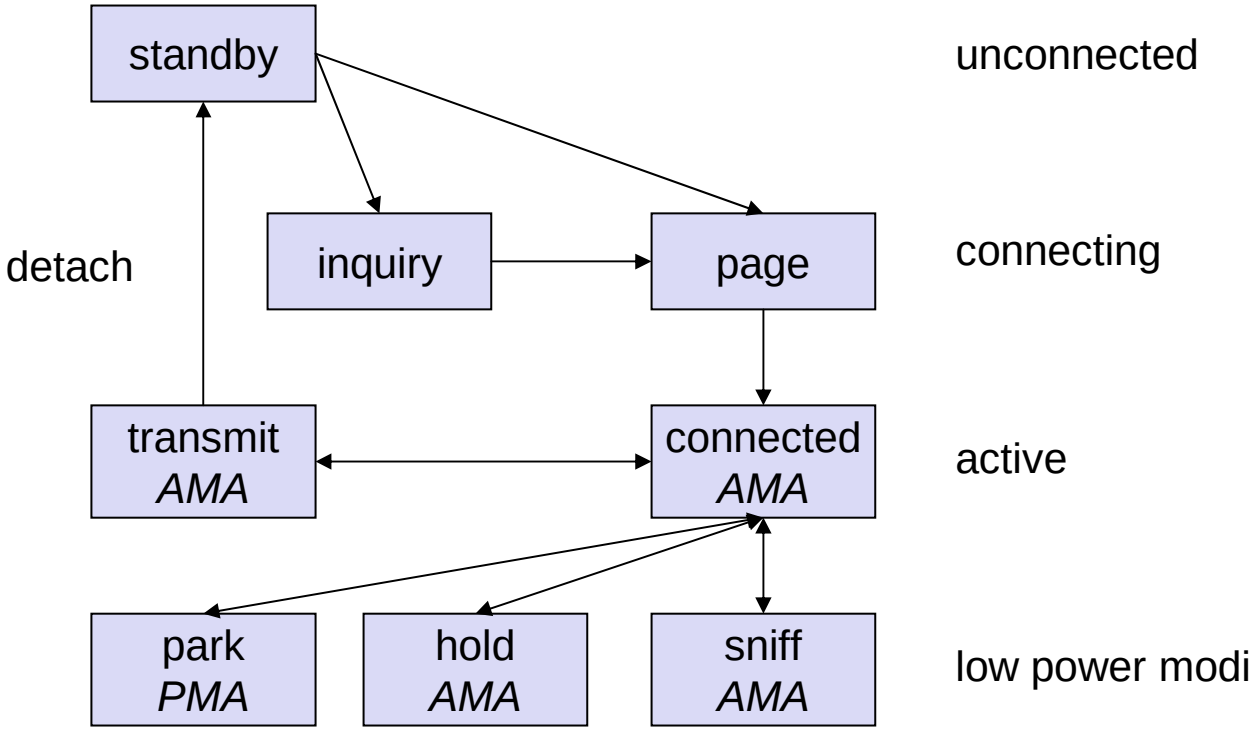
Afterwards: *Pairing (optional)*

- When connecting to a new device, check the rights of the new device for joining the network
- Used: PIN, given by the user

Pairing and following Security Mechanisms



States of a Bluetooth Device

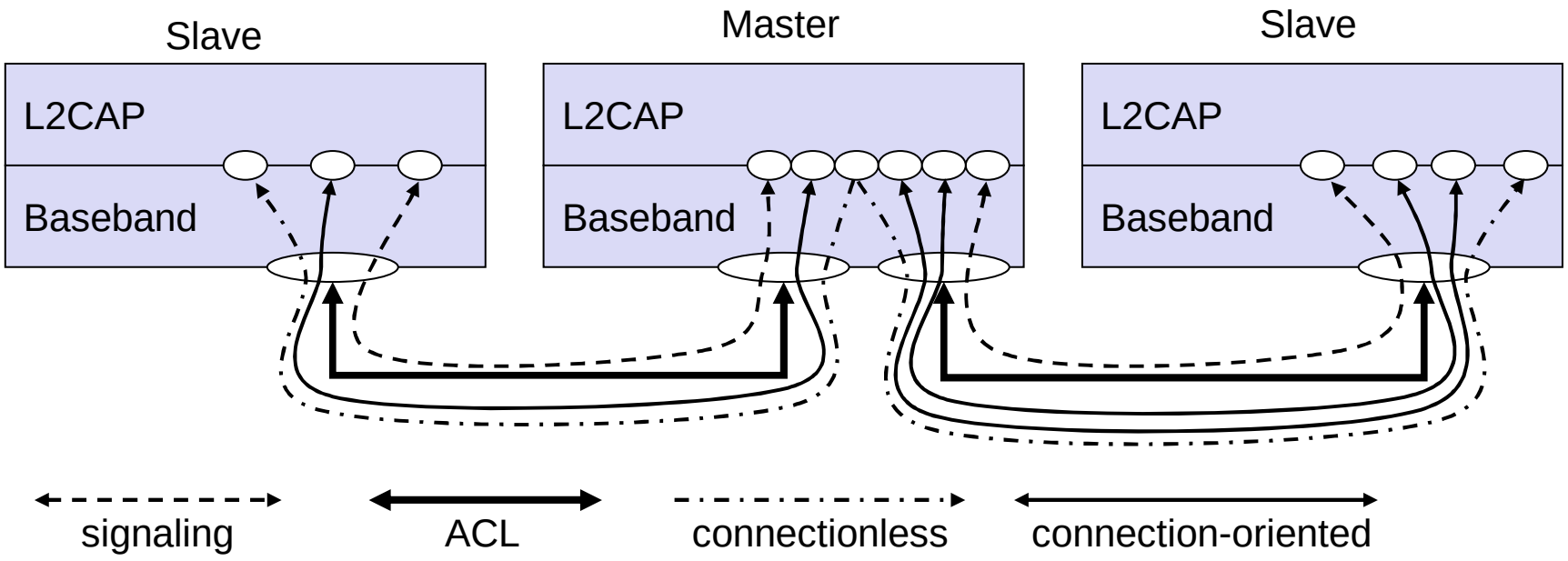


Standby: do nothing
Inquiry: search for other devices
Page: connect to a specific device
Connected: participate in a piconet

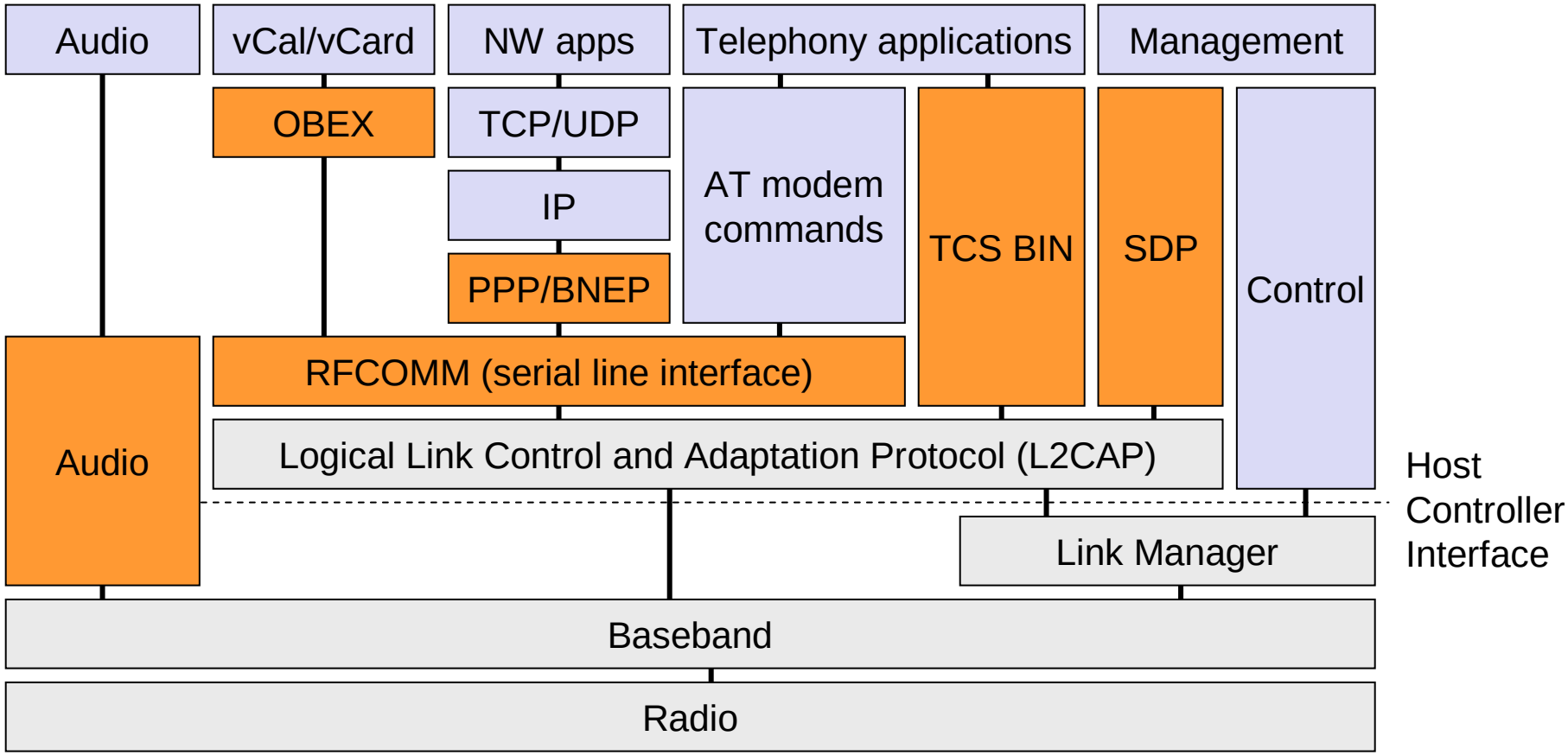
Park: release AMA, get PMA
Sniff: listen periodically, not each time slot
Hold: stop ACL, SCO still possible, possibly participate in another piconet

L2CAP - Logical Link Control and Adaptation Protocol

- Simple data link protocol on top of baseband
- Connection-oriented and connectionless (based auf ACL), additionally signaling channels
- Several logical channels on one connection (Protocol multiplex: RFCOMM, SDP, …)
- Management of QoS specifications per logical channel (delay, jitter, burst, bandwidth)
- Segmentation & reassembly of data packets up to 64Kbyte user data
- Management of communication groups



Higher Layer Protocols



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.

SDP – Service Discovery Protocol

- Protocol for the discovery of available services
  - Searching for and browsing services in radio range
  - Adapted to highly dynamic environment
  - Can be completed by other services like SLP, Jini, …
  - Only defines the discovery of services, not the usage
  - Caching of discovered services
  - Gradual discovery

- Service record format
  - Information about services provided by attributes
  - Attributes are composed of a 16 bit ID (name) and a value
  - Values may be derived from 128 bit Universally Unique Identifiers (UUID)

Protocols to support Legacy Protocols/Applications

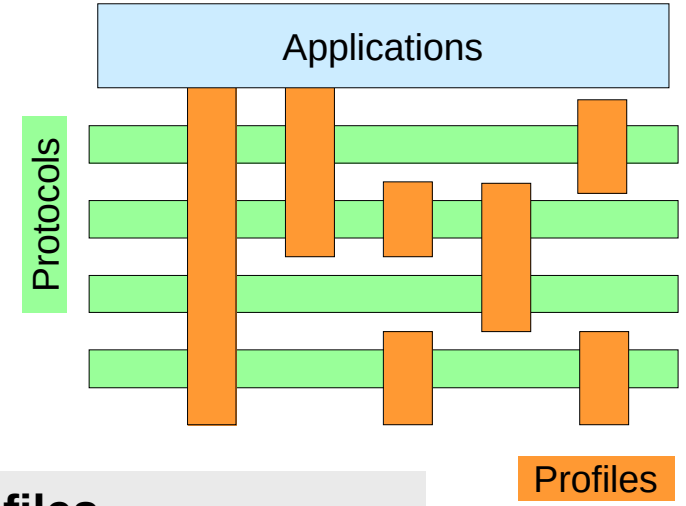
- RFCOMM
  - Emulation of a serial port (supports a large base of legacy applications)
  - Allows multiple ports over s single physical channel
- Telephony Control Protocol Specification (TCS)
  - Call control (setup, release)
  - Group management
- OBEX
  - Exchange of objects, replacement for IrDA
- WAP
  - Interactions 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 100 m
- Frequency
  - Free 2.4 GHz ISM band
- Availability
  - Integrated into several products, several vendors
- Connection setup time
  - Depends on power mode
  - Max. 2,56s, average 0,64s
- Quality of Service
  - Guarantees, ARQ/FEC
- Manageability
  - Public/private keys needed, key management not specified, simple system integration
- Advantages/disadvantages
  - Advantages: already integrated into several products, available worldwide, free ISM band, several vendors, simple system, simple ad-hoc networking, peer-to-peer
  - Disadvantages: interferences on ISM band, limited range, max. 8 devices per network, high setup latency

Bluetooth Enhancements

The Bluetooth standard is developed on till now several times:

Bluetoot h 1.2

- Adaptive frequency hopping to protect against interference on some frequencies
- New packet type for synchronous communication: eSCO (enhanced SCO) with CRC checksum, variable data rates (up to 288 kBit/s), retransmission of lost packets, variable payload size, and multislot operation

Bluetooth 2.0+ EDR

- EDR = enhanced data rate
- Up to ~ 2.1 MBit/s data rate by allowing for differential QPSK and differential 8PSK as modulation techniques

Bluetooth 2.1+ EDR

- Mechanisms for simpler pairing, lower power consumption, and increased security

Bluetooth 3.0

- Planned with 480 MBit/s
- See below: Ultra-Wideband (UWB)

WPAN: IEEE 802.15 – Further Developments

- 802.15-2: Coexistence
  - Coexistence of WPANs (802.15) and WLANs (802.11), both are using the same frequencies - quantify the mutual interference
- 802.15-3: High-Rate (UWB = Ultra Wide-Band)
  - Standard for WPANs with high data rate (20 Mbit/s or higher), while still low-power and low-cost
  - Data rates: 11, 22, 33, 44, 55 MBit/s, also as a vision: 500 MBit/s
  - 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 – Further Developments

- 802.15-4: Low-rate, very low-power (Zigbee)
  - Low data rate solution with battery life time of several month up to several years and with very low complexity
  - Potential applications are sensors, interactive toys, smart badges, remote controls, home automation, ...
  - Data rates of 2-250 kbit/s, latency down to 15 ms
  - Master/slave or peer-to-peer operation
  - Up to 254 devices
  - Support for critical latency devices, such as joysticks
  - 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

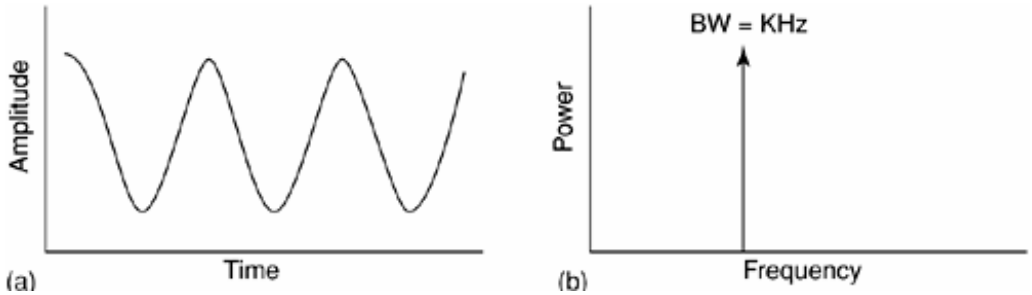
802.15.3 – UWB

The frequency spectrum is overcrowded…

… thus use all of it!

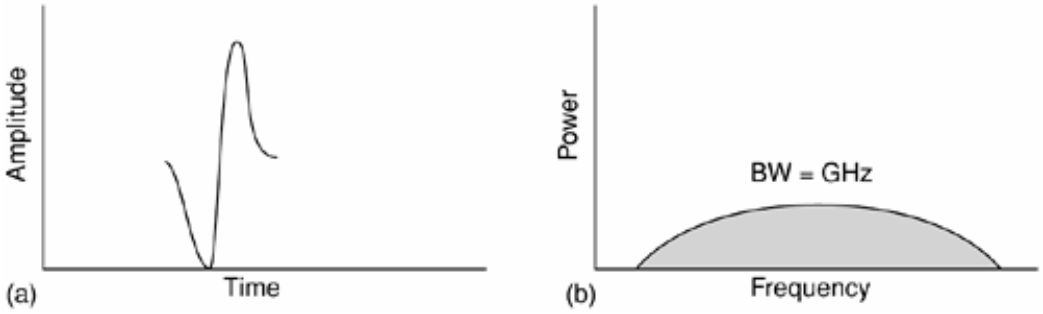
Normal narrowband signal

- Narrow frequency range
- Susceptible to jamming



UWB signal

- Broad frequency range
- Robust
- Low transmission power

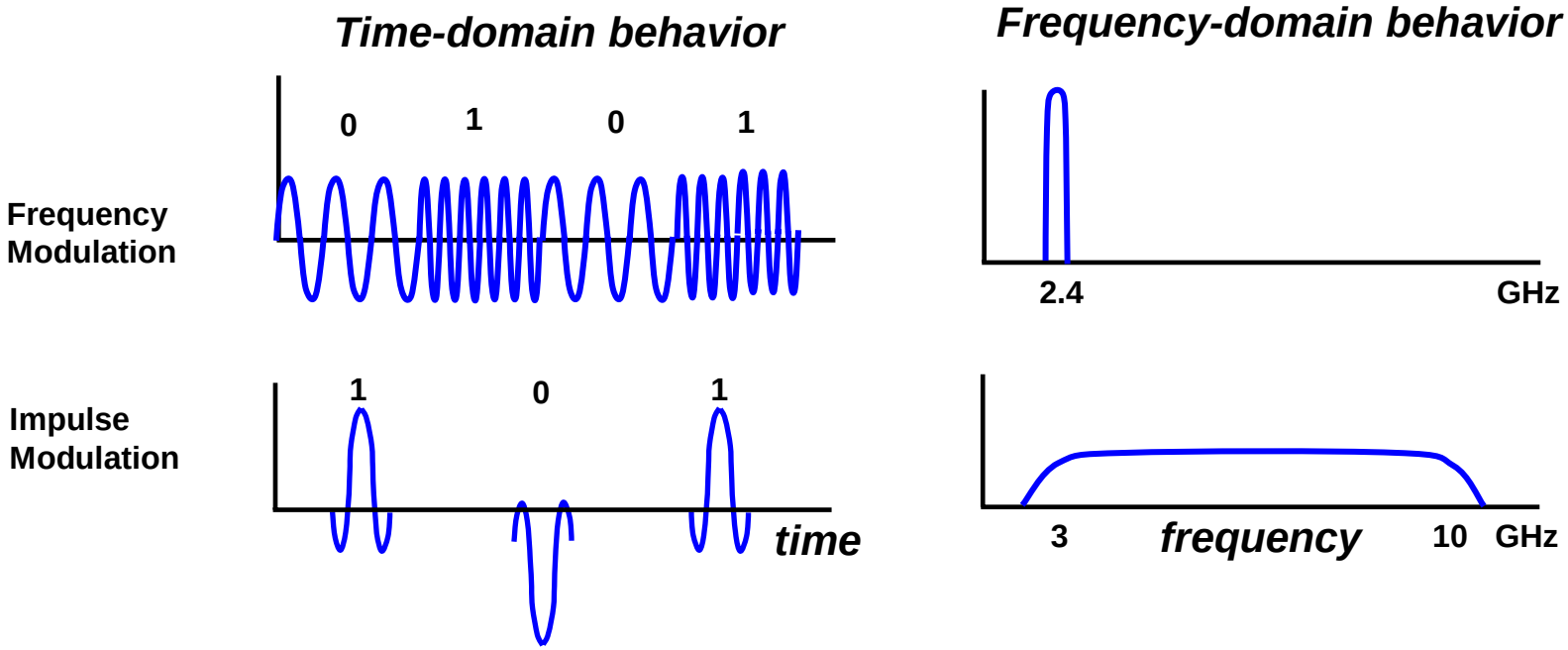


Signal is defined as an ultra wideband if

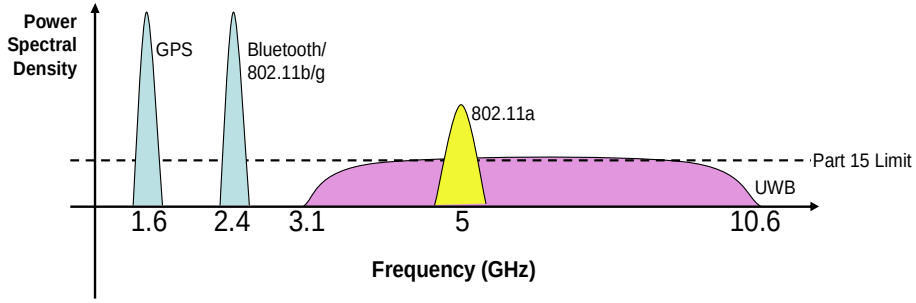
- Signal bandwidth > 500 MHz
- Fractional bandwidth $\eta > 0.20$

$$\eta = 2 \cdot \frac{f_{high} - f_{low}}{f_{high} + f_{low}}$$

UWB Definition

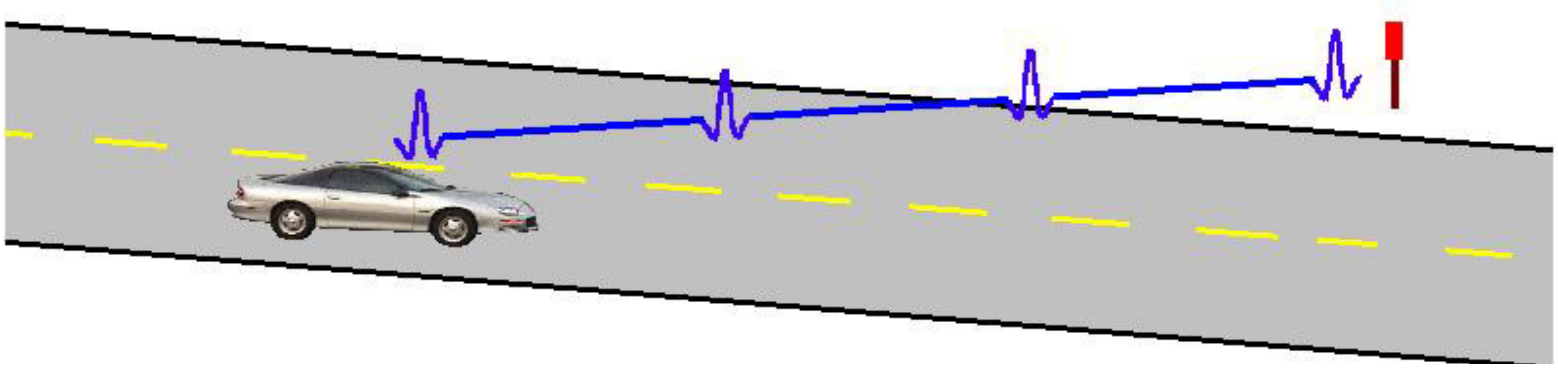


- Frequency range 3.1 GHz to 10.6 GHz
- Indoor: up to 20 meters range
- Suitable for short-distance communication with high bandwidth (100 MBit/s)



Possible Applications

- Personal Area Networking (PAN), connecting cell phones, laptops, PDAs, cameras, MP3 players with much higher data rates than Bluetooth or 802.11
- Can be integrated into automotive in-car services and entertainment
- Download driving directions from PDA/laptop for use by on-board navigation system using GPS
- Download music and videos for passenger entertainment
- Info-station concept: road side ‘markers’ containing UWB transmitters
  - Short burst of very high rate data (100s of MBit/s for 1-3 sec at a time)
  - Messages could contain road conditions, construction, weather advisories
  - Allow for emergency assistance communication

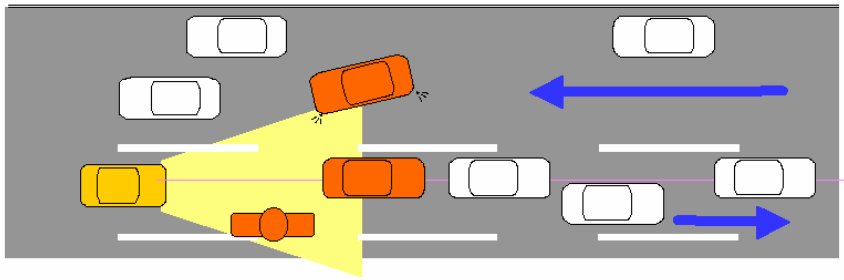


Possible Applications

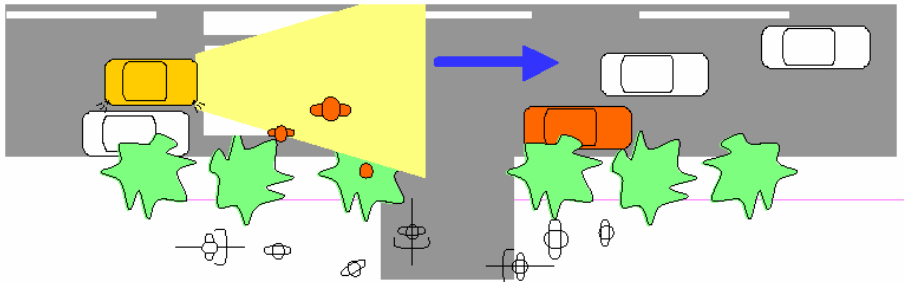
Vehicular Radar

- Collision Avoidance/Detection
- Driver aid/alert to avoid collisions.
- Aid for airbag/restraint deployment
- Resolution to distinguish cars/people/animals/poles on or near road

Dense Traffic



Street in a Residential Area



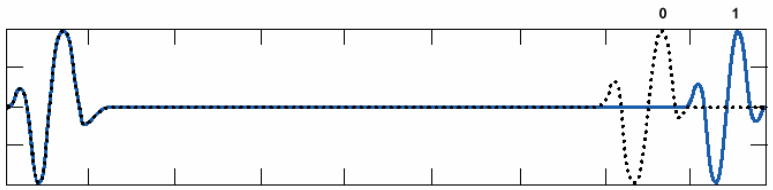
Modulation Schemes

Different coding schemes – how to do modulation with short pulses?

- Pulse length ~ 200ps
- Voltage swing ~100mV; Power ~ 10uW

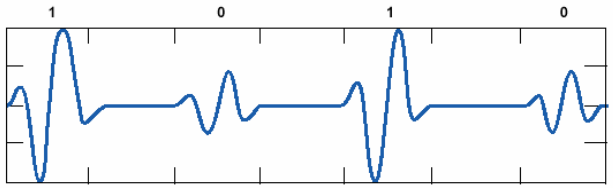
Common modulations:

- Pulse position modulation (PPM)



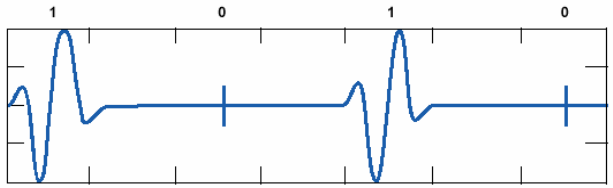
(can code *n* bit as once using 2^n positions at different times)

- Pulse Amplitude Modulation (PAM)

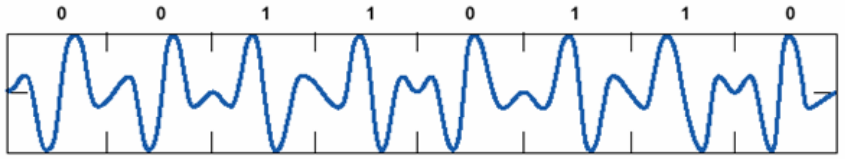


(also: *n* bit using 2^n amplitude levels)

- On/Off Keying (OOK)



- Bi-Phase Signaling (BPSK)



(Possible: combination with PPM)

Advantages and Challenges

Advantages of UWB

- Ability to share the frequency spectrum
- Large channel capacity
- Ability to work with low Signal-to-Noise-Ratios
- Low probability of interception and detection
- Resistance to jamming
- High performance in multipath channels
- Superior penetration properties
- Sub-centimeter resolution of localization
- Low transmission power

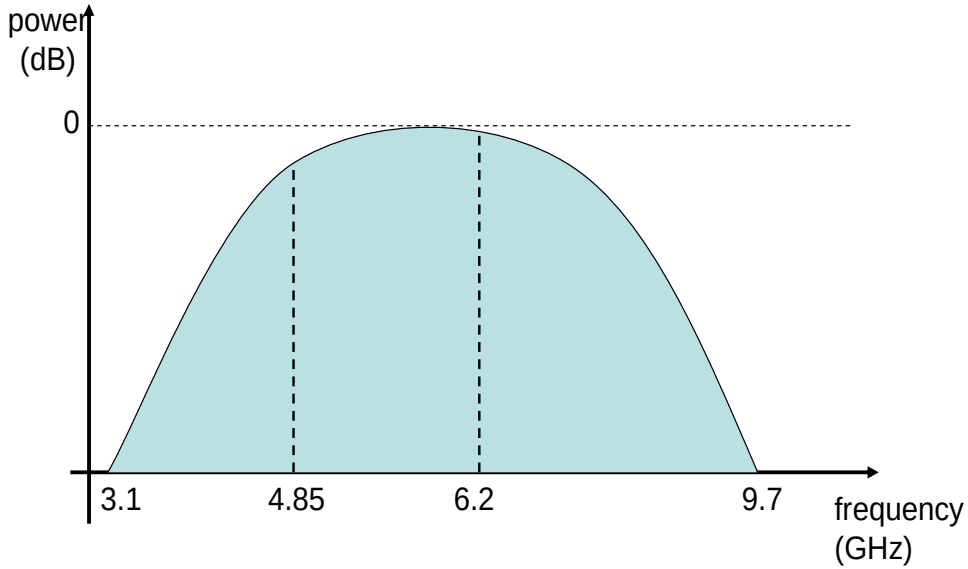
Challenges

- Pulse-shape distortion
- High-frequency synchronization
- Multiple-access interference
- Low transmission power
- New higher-layer protocols for efficient use of the new network concept

UWB Variants: Singleband Approach

Direct sequence (DS-UWB)

- Defined by 802.15.3
- Use 2 frequency bands: 3.1-4.85GHz, 6.2-9.7GHz
- CDMA has been proposed at the encoding layer
- Has no carrier frequency
- Requires wideband antennas
- Potential problem with GPS and other licensed bands



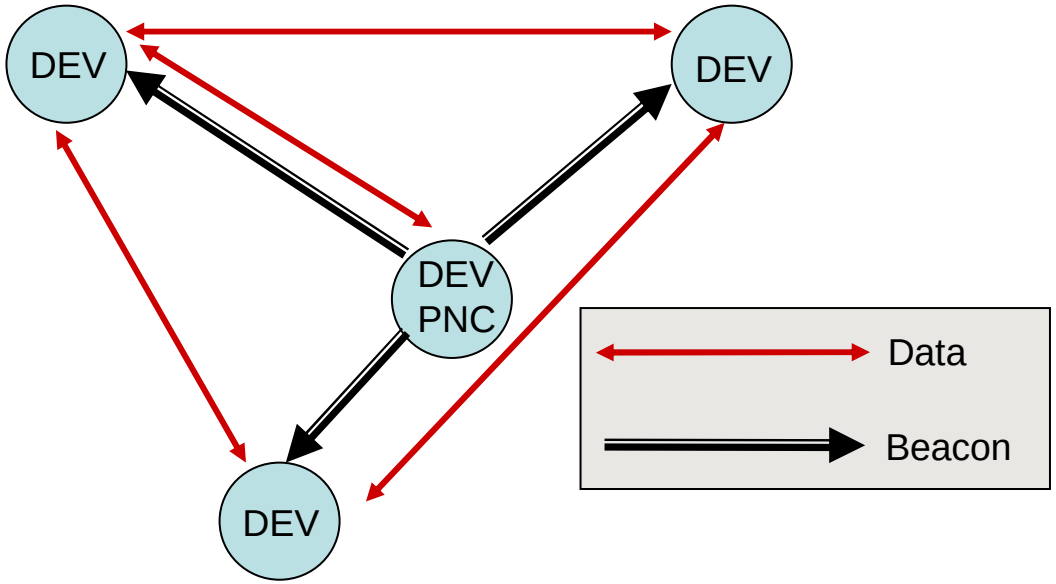
Medium Access:

- UWB systems typically use many pulse repetitions (100s) to represent each data symbol
- A uniform pulse train has spectral lines present (not a smooth spectrum)
- For multiple access this could also lead to catastrophic collisions.

DS-UWB Networks

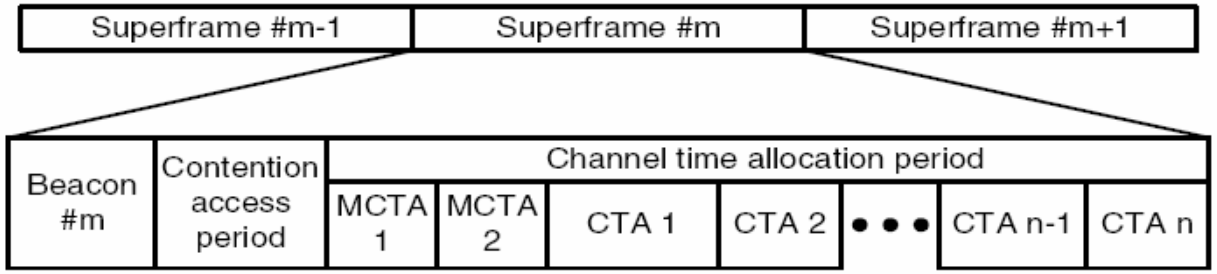
Ad-hoc communication based on Bluetooth principles: Piconet

- One Piconet Coordinator (PNC): analogous to master, provide snychronization and various management functions: power management, security, Quality of Service (QoS)
- Several devices (DEV): slaves of piconet



DS-UWB MAC Layer

On each channel: time is divided into *superframes*



- Beacon: assign channel time allocation (CTA), distribute management information
- Contention Access Period (CAP, optional): CSMA/CA mechanism for the transfer of commands and/or asynchronous data
- Channel Time Allocation Period (CTAP):
  - Dynamic TDMA protocol: each device is assigned a CTA of defined duration (QoS)
  - A device can send a CTA request to the PNC in the management CTA (MCTA)
  - PNC schedules CTAs for the next superframe based on such requests

DS-UWB Networks

"Scatternet" variants in DS-UWB:

Independent piconets:

- Bridging devices between two independent piconets (as in Bluetooth scatternets)

Neighbour piconets:

- Neighbour PNC is not member of parent piconet and parent PNC is not member of the neighbour piconet

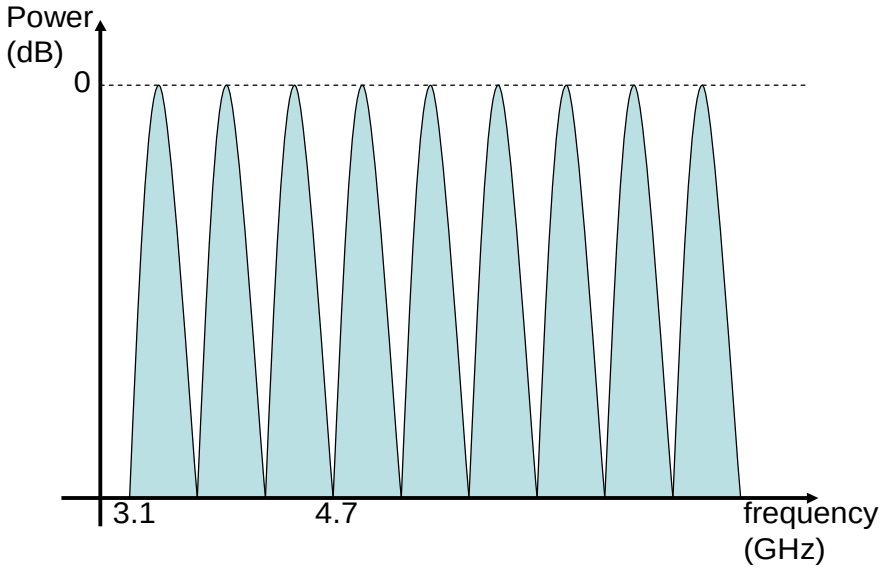
Dependent piconets (parent/*child* piconet):

- Created by a DEV of an existing piconet
- Child piconet requests a pseudo-private CTA from the parent PNC
- This CTA is used by all members of the child piconet, i.e. child piconet gets parts of the transmission capacity exclusively

UWB Variants: Multiband Approach

Multiband Orthogonal Frequency Division Multiplexing (OFDM)

- Also: multi-carrier UWB (MC-UWB)
- Similar in nature to 802.11a/g
- 14 bands of 528MHz each (simplest devices need to support 3 lowest bands, 3.1GHz – 4.7 GHz)
- Each band subdivided in 128 subbands
- Coexistence with other networks by avoiding certain bands
- Defined by Multiband OFDM Alliance (MBOA)



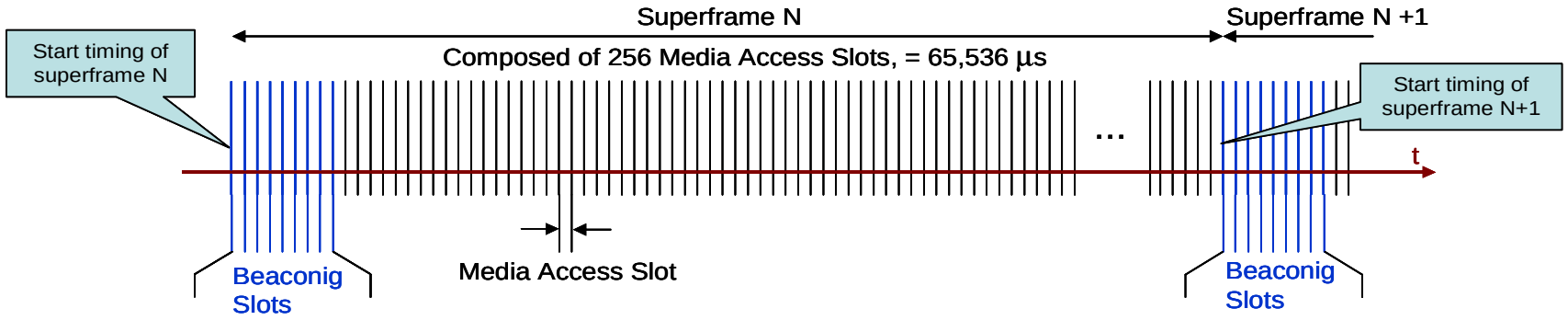
Medium Access:

- Mutually orthogonal frequency bands for parallel usage
- Interference-free transmissions
- Efficient data transmissions

MBOA MAC Layer

Beacon Group (BG) topology:

- Analogous concept to piconet, but no use of PNC (distributed MAC)
- Every device can send a beacon, common beacon group interval
- Also superframe structure



Medium Access in two variants:

- Pre-defined timeslots for isochronous traffic, i.e. making reservations using a distributed reservation protocols
- Asynchronous traffic based on CSMA/CA

Note: multiband approach seems to be more prominent than singleband approach, but development is still in progress

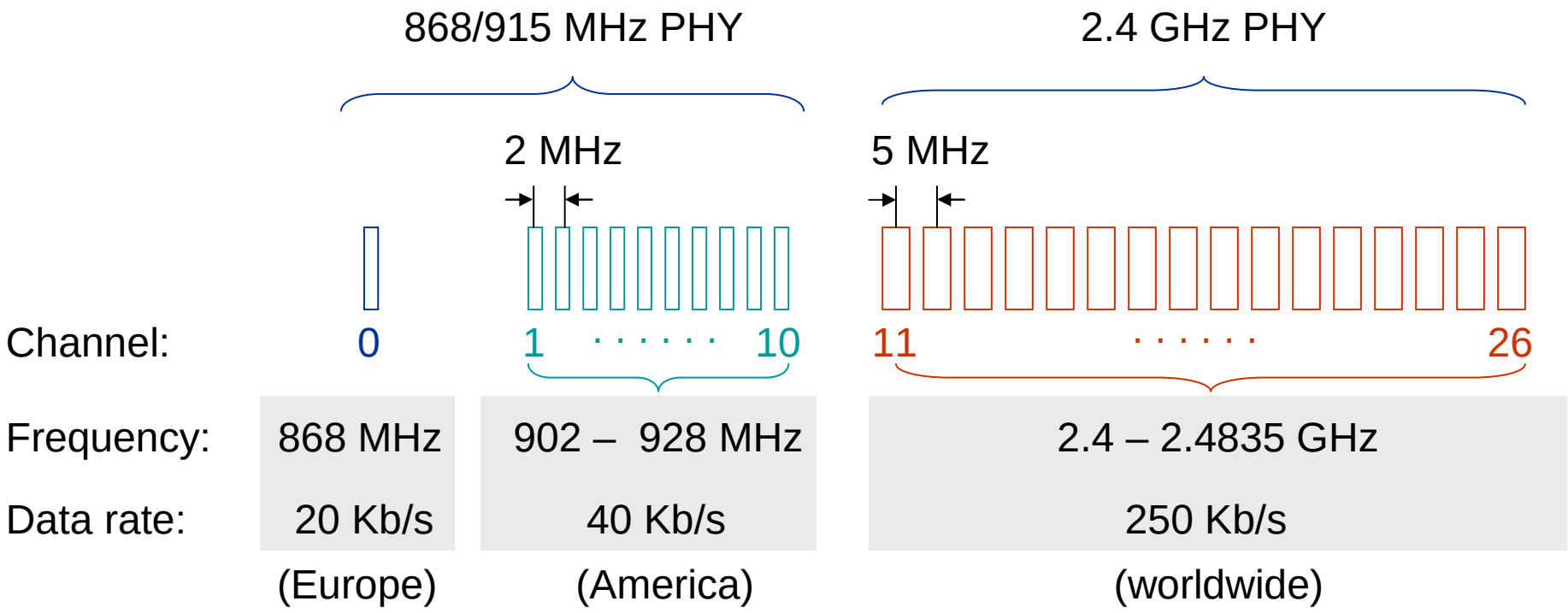
IEEE 802.15.4 – ZigBee

ZigBee was defined (and adopted as IEEE 802.15.4) for *low data rate (LR-WPAN)* – but why should we define a standard for low data rate???

- Low data rate sounds negative, but…
- Low data rate applications are closer to our daily lives than high data rate applications; they are expected to play an increasingly important role in our lives:
  - Automation and control: at home, in a factory, in a warehouse – e.g. remote control for TV
  - Monitoring: as well health as environments
  - Location technologies: e.g. real-time tracking of inventory, but maybe also military applications
  - Entertainment, e.g. learning games or interactive toys

ZigBee: Channels and Data Rates

Defined for several frequency bands, all using DSSS, but with different data rate:



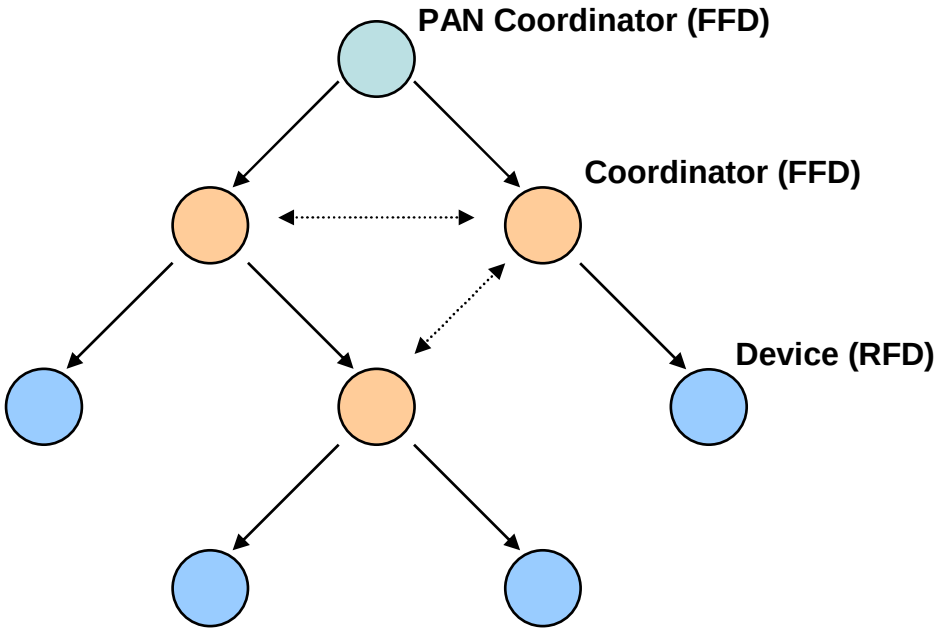
Low data rate is one characteristic, but also:

- Low power consumption (long-living batteries)
- Low cost

ZigBee: Network and MAC

Network topology:

- Range of up to 10 meters
- Piconet structure, or Multi-hop peer-to-peer structure (mesh or tree)



Two device classes:

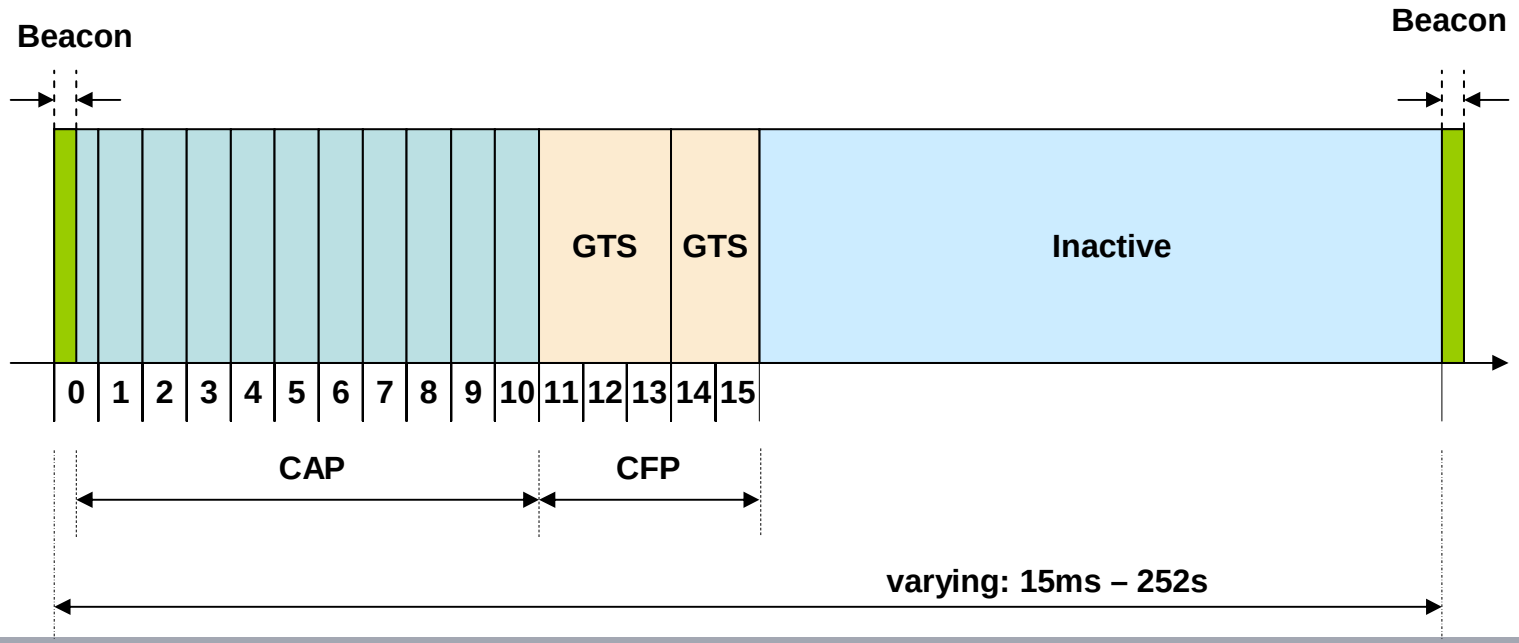
- Full function device (FFD): capable of any topology, of being network coordinator, of talking to any other device
- Reduced function device (RFD): limited to star topology, cannot become a network coordinator, talks only to a network coordinator, but very simple implementation

Communication: beacon mode with superframe structure / non-beacon enabled with CSMA/CA mechanism

ZigBee: Network and MAC

Beacon Mode:

- Beacon for synchronization / network identification, sent by coordinator
- Active and inactive (power-saving) phase; active phase subdivided in 16 slots
- Contention Access Period (CAP) with slotted CSMA/CA
- GTS (guaranteed time slots) during Contention Free Period (CFP)
- In beacon enabled mode, a device can track beacons from its parent for synchronization and failure detection



802.15.1, 2, 3, 4

Project	Data Rate	Range	Configuration	Other Features
802.15.1 (Bluetooth)	1 Mbps	10M (class 3) 100M (class 1)	8 active device Piconet/ Scatternet	Authentication, Encryption, Voice
802.15.3 High Rate	22, 33, 44, 55 Mbps	10M	256 active device Piconet/ Scatternet	FCC part 15.249 QoS, Fast Join Multi-Media
802.15.4 Low Rate	up to 250Kbps	10M nominal 1M-100M based on settings	Master/Slave (256 Devices or more) Peer to Peer	Battery Life: multi-month to infinite
802.15.2 Coexistence	Develop a Coexistence Model and Mechanisms Document as a Recommended Practice			

… and relatively new: *802.15.5: Mesh Networking in WPANs* by enhanced reliability via route redundancy, easier network configuration, better device battery life due to fewer retransmissions

Other Technology in Short Range: RFID

RFID = *Radio Frequency Identification Device*

- Holds a small amount of unique data – a serial number or other unique attribute of the item
- The data can be read from a distance – no contact or even line of sight necessary (compared to, e.g., laser scanners)
- In response to a radio interrogation signal from a reader (base station) the RFID tags transmit their ID
- RFID tags withstand difficult environmental conditions (sunlight, cold, frost, dirt etc.)
- Products available with read/write memory, smart-card capabilities
- Enables individual items to be individually tracked e.g. from manufacture to consumption

Where to use RFID?

- 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

Passive RFID Tags

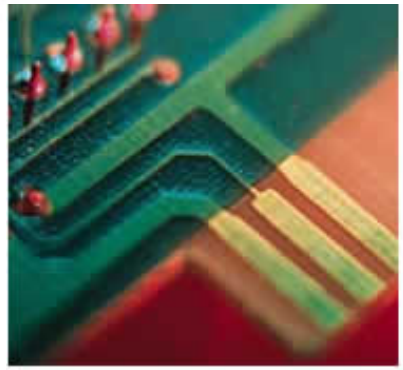
"Traditional" tags used in retail security applications:

- Tag contains an antenna, and a small chip that stores a small amount of data
- Tag can be programmed at manufacture or on installation
- Tag is powered by the high power electromagnetic field generated by the antennas (connected to a reader) – usually in doorways
- The field allows the chip/antenna to reflect back an extremely weak signal containing the data
- Collision Detection – recognition of multiple tags in the read range – is employed to separately read the individual tags
- Low prices

Performa Long Range Reader

Active RFID Tags

- Battery Powered tags
  - Have much greater range – 100m
  - Hold much more information – Kbytes
  - Can integrate sensing technology, e.g. temperature, GPS
  - Can signal at defined time
  - Multiple tags can be recorded at once
- Used for higher value items
  - Shipping containers
  - Babies
  - Electronic assets
- Much higher costs per item
- Life between 2 – 4 years



RFID Tag Attributes

	Active RFID	Passive RFID
Tag power source	Internal to tag	Energy transferred using RF from reader
Tag battery	Yes	No
Availability of power	Continuous	Only in range of reader
Required signal strength	Very Low	Very High
Range	Up to 100m	Up to 3-5m, usually less
Multi-tag reading	1000's of tags recognized – up to 160 km/h	Few hundred within 3m distance of reader
Data storage	Up to 128Kb of read/write	128 bytes of read/write

RFID – Radio Frequency Identification

- Data rate
  - Transmission of ID only (e.g. 48 bit, 64kbit, 1 Mbit)
  - 9,6 – 115 kbit/s
- Transmission range
  - Passive: up to 3 m
  - Active: up to 30-100 m
  - Simultaneous detection of up to 256 tags, scanning of 40 tags/sec – more using active tags
- Frequencies
  - 125 kHz, 13.56 MHz, 433 MHz, 2.4 GHz, 5.8 GHz and many others
- Security
  - Application dependent, typically no coding on RFID device
- Availability
  - Many products, many vendors
- Connection setup time
  - Depends on product/medium access scheme (typically 2 ms per device)
- Quality of Service
  - None
- Manageability
  - Very simple, same like serial interface
- Advantages/disadvantages
  - Advantages: extremely low cost, large experience, high volume available, for passive RFIDs no power needed, large variety of products, relative speeds up to 300 km/h), broad temperature range
  - Disadvantages: no QoS, simple DoS attacks possible, crowded ISM bands, typically simplex connection (activation, transmission of ID)

RFID – Radio Frequency Identification

- 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
- Further 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 (“Future Store” in Rheinberg)
  - Creation of „electronic manifests“ at item or package level (embedded inexpensive passive RFID tags)
  - 3D tracking of children, patients