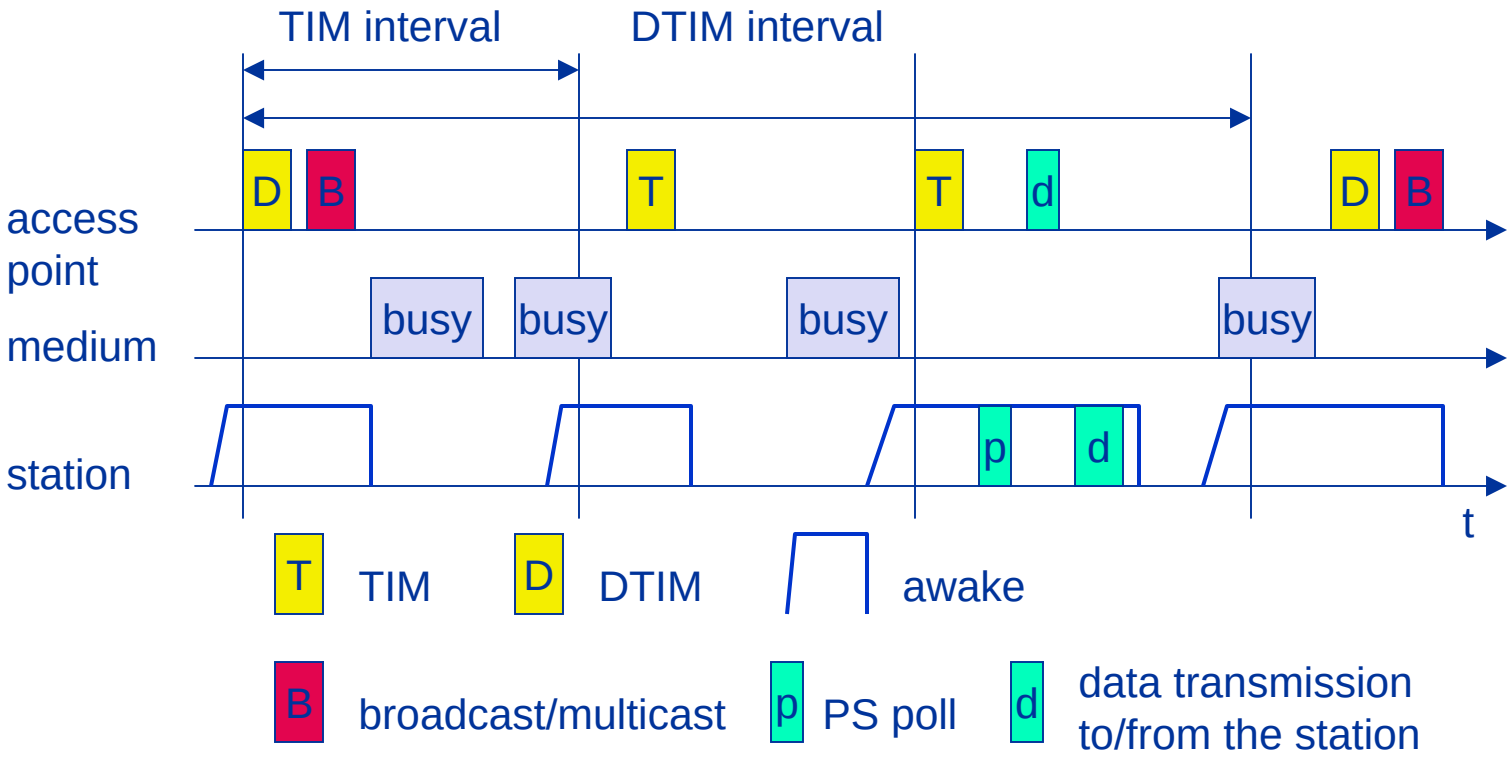
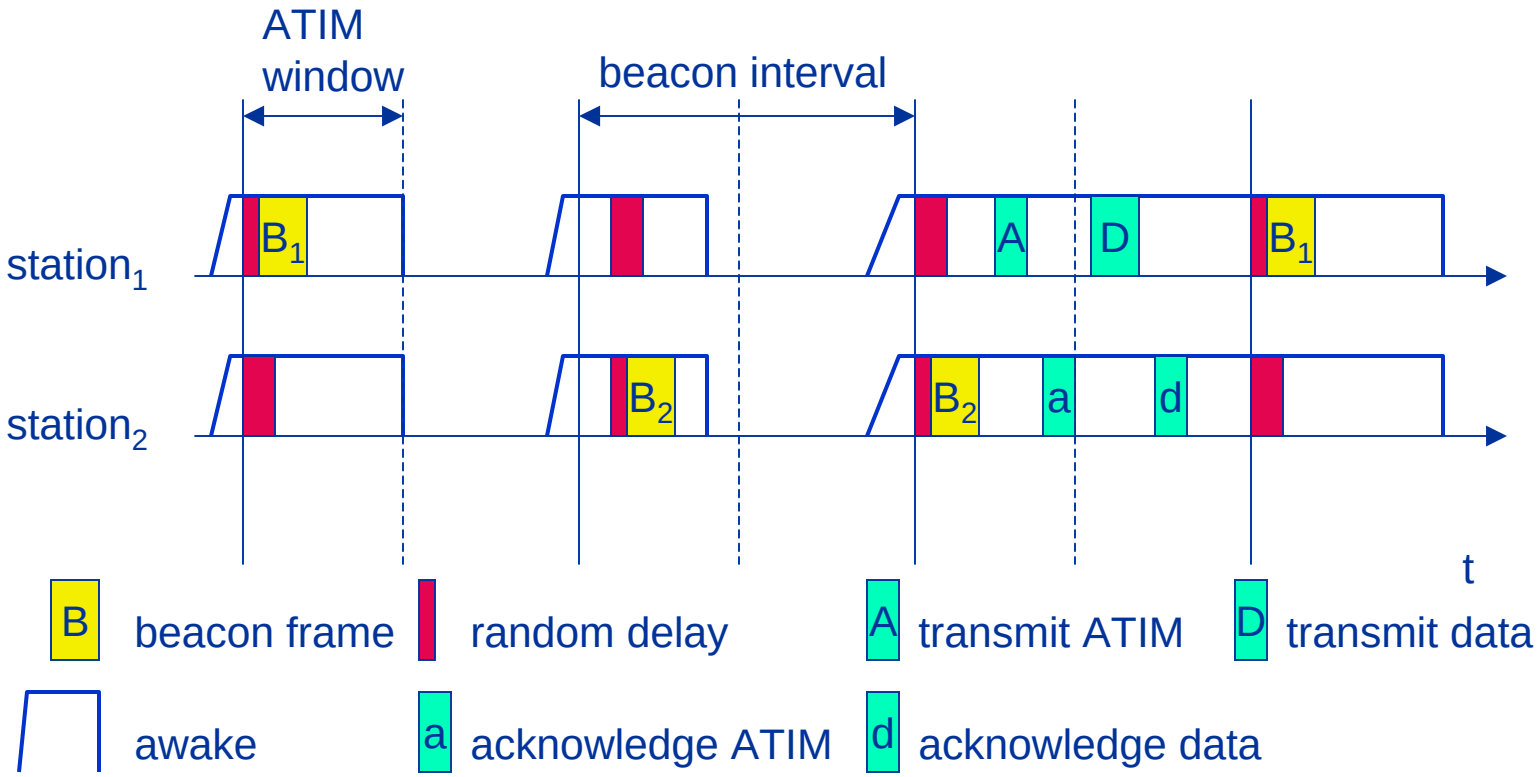
Power management

- 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 (nodes run this at all times)
- Infrastructure
  - Traffic Indication Map (TIM) sent with beacons
    - list of unicast receivers transmitted by AP
  - Delivery Traffic Indication Map (DTIM)
    - list of broadcast/multicast receivers transmitted by AP
- Ad-hoc
  - Ad-hoc Traffic Indication Map (ATIM)
    - announcement of receivers by stations buffering frames
    - more complicated - no central AP
    - collision of ATIMs possible (scalability?)
- APSD (Automatic Power Save Delivery)
  - new method in 802.11e replacing above schemes

Power saving with wake-up patterns (infrastructure)



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



802.11 - Roaming

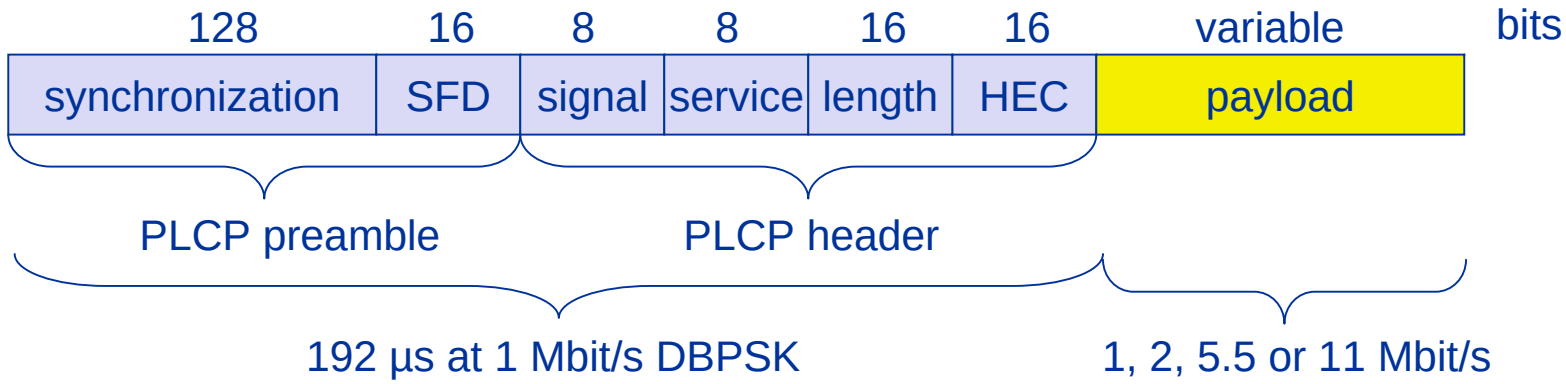
- No or bad connection? Then perform:
- Scanning
  - scan the environment, i.e., listen into the medium for beacon signals or send probes into the medium and wait for an answer
- Reassociation Request
  - station sends a request to one or several AP(s)
- Reassociation Response
  - success: AP has answered, station can now participate
  - failure: continue scanning
- AP accepts Reassociation Request
  - signal the new station to the distribution system
  - the distribution system updates its data base (i.e., location information)
  - typically, the distribution system now informs the old AP so it can release resources
- Fast roaming – 802.11r
  - e.g. for vehicle-to-roadside networks

WLAN: IEEE 802.11b

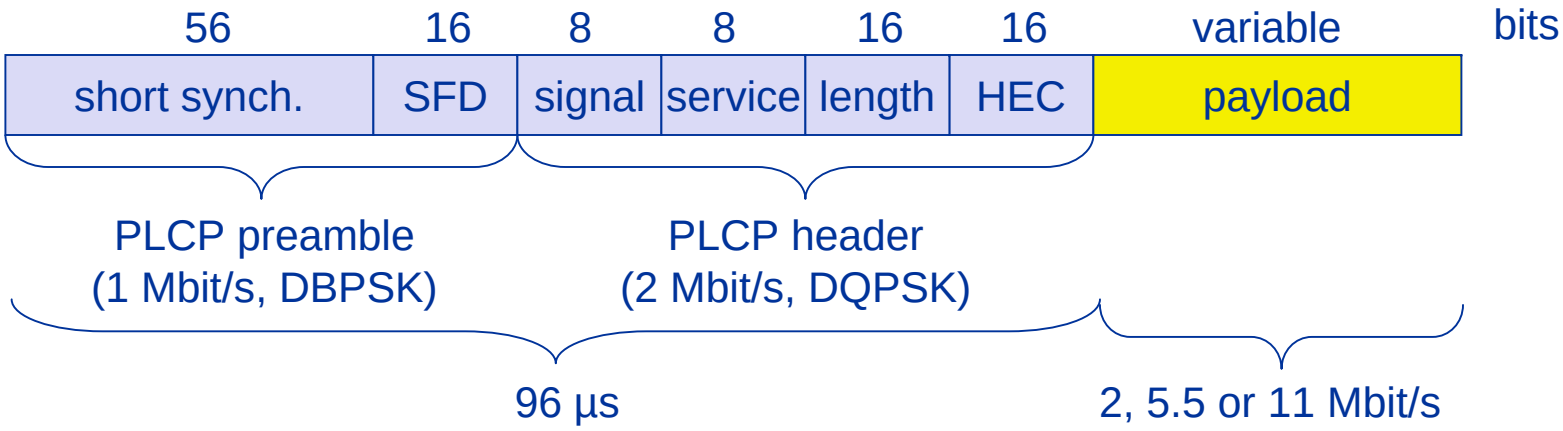
- Data rate
  - 1, 2, 5.5, 11 Mbit/s, depending on SNR
  - User data rate max. approx. 6 Mbit/s
- Transmission range
  - 300m outdoor, 30m indoor
  - Max. data rate ~10m indoor
- Frequency
  - DSSS, 2.4 GHz ISM-band
- Security
  - Limited, WEP insecure, SSID
- Availability
  - Many products, many vendors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

IEEE 802.11b – PHY frame formats

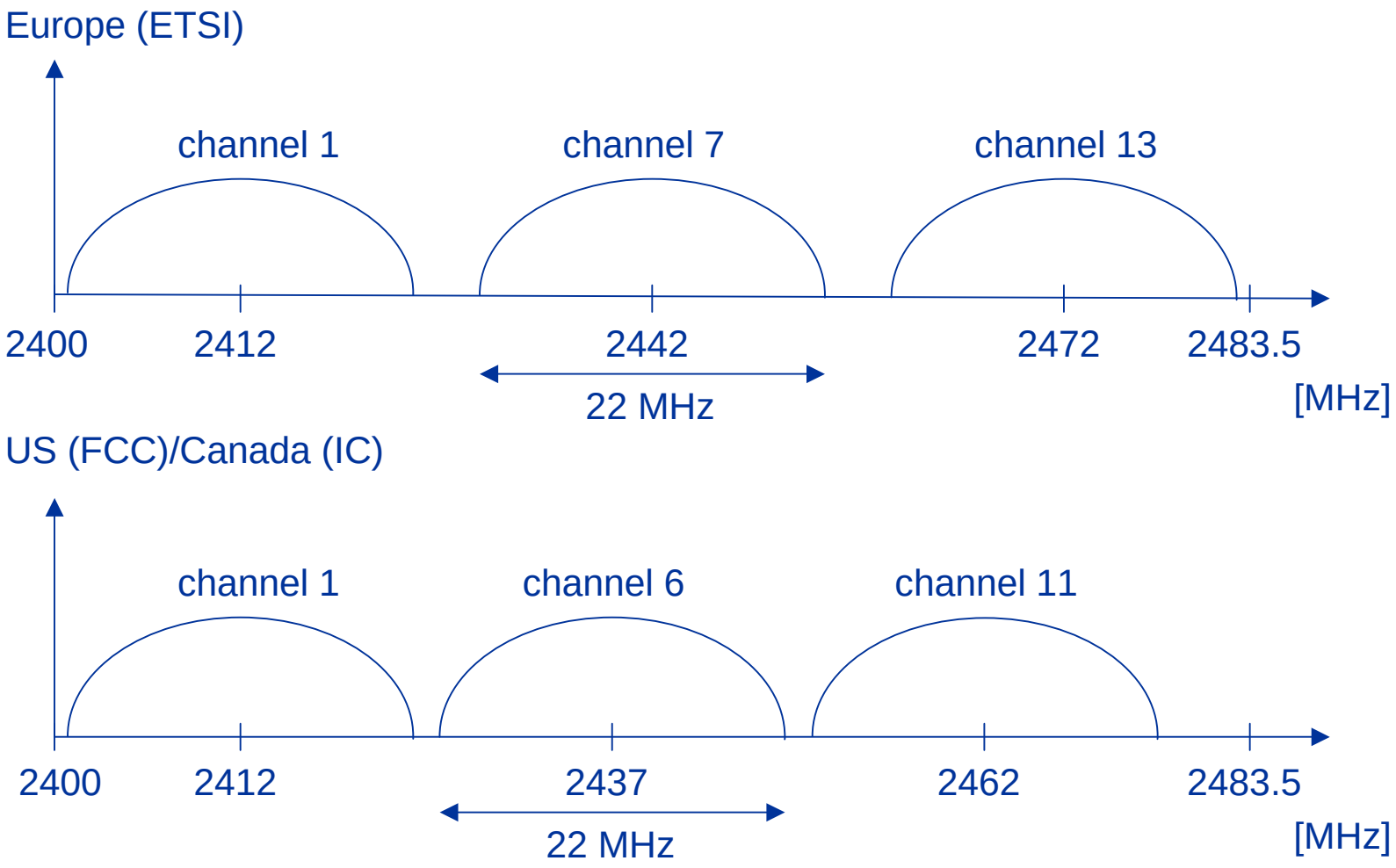
Long PLCP PPDU format



Short PLCP PPDU format (optional)



Channel selection (non-overlapping)



WLAN: IEEE 802.11 – current developments (06/2009)

- 802.11c: Bridge Support
  - Definition of MAC procedures to support bridges as extension to 802.1D
- 802.11d: Regulatory Domain Update
  - Support of additional regulations related to channel selection, hopping sequences
- **802.11e**: MAC Enhancements – QoS
  - Enhance the current 802.11 MAC to expand support for applications with Quality of Service requirements, and in the capabilities and efficiency of the protocol
  - Definition of a data flow ("connection") with parameters like rate, burst, period… supported by HCCA (HCF (Hybrid Coordinator Function) Controlled Channel Access, optional)
  - Additional energy saving mechanisms and more efficient retransmission
  - EDCA (Enhanced Distributed Channel Access): high priority traffic waits less for channel access
- 802.11F: Inter-Access Point Protocol (withdrawn)
  - Establish an Inter-Access Point Protocol for data exchange via the distribution system
- **802.11g**: Data Rates > 20 Mbit/s at 2.4 GHz; 54 Mbit/s, OFDM
  - Successful successor of 802.11b, performance loss during mixed operation with .11b

IEEE 802.11– current developments

- 802.11h: Spectrum Managed 802.11a
  - Extension for operation of 802.11a in Europe by mechanisms like channel measurement for dynamic channel selection (DFS, Dynamic Frequency Selection) and power control (TPC, Transmit Power Control)
- 802.11i: Enhanced Security Mechanisms
  - Enhance the current 802.11 MAC to provide improvements in security.
  - TKIP enhances the insecure WEP, but remains compatible to older WEP systems
  - AES provides a secure encryption method and is based on new hardware
- 802.11j: Extensions for operations in Japan
  - Changes of 802.11a for operation at 5GHz in Japan using only half the channel width at larger range
- **802.11-2007**: Current “complete” standard
  - Comprises amendments a, b, d, e, g, h, i, j
- 802.11k: Methods for channel measurements
  - Devices and access points should be able to estimate channel quality in order to be able to choose a better access point of channel
- 802.11m: Updates of the 802.11-2007 standard

IEEE 802.11– current developments

- **802.11n**: Higher data rates above 100Mbit/s
  - Changes of PHY and MAC with the goal of 100Mbit/s at MAC SAP
  - MIMO antennas (Multiple Input Multiple Output), up to 600Mbit/s are currently feasible
  - However, still a large overhead due to protocol headers and inefficient mechanisms
- 802.11p: Inter car communications
  - Communication between cars/road side and cars/cars
  - Planned for relative speeds of min. 200km/h and ranges over 1000m
  - Usage of 5.850-5.925GHz band in North America
- 802.11r: Faster Handover between BSS
  - Secure, fast handover of a station from one AP to another within an ESS
  - Current mechanisms (even newer standards like 802.11i) plus incompatible devices from different vendors are massive problems for the use of, e.g., VoIP in WLANs
  - Handover should be feasible within 50ms in order to support multimedia applications efficiently
- 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

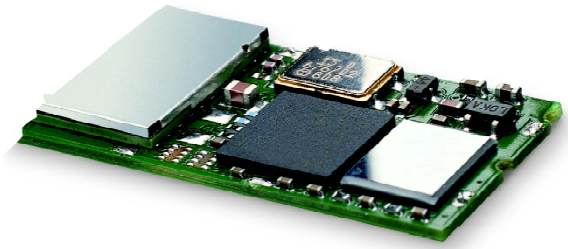
IEEE 802.11– current developments

- 802.11T: Performance evaluation of 802.11 networks
  - Standardization of performance measurement schemes
- 802.11u: Inter-working with additional external networks
- 802.11v: Network management
  - Extensions of current management functions, channel measurements
  - Definition of a unified interface
- 802.11w: Securing of network control
  - Classical standards like 802.11, but also 802.11i protect only data frames, not the control frames. Thus, this standard should extend 802.11i in a way that, e.g., no control frames can be forged.
- 802.11y: Extensions for the 3650-3700 MHz band in the USA
- 802.11z: Extension to direct link setup
- 802.11aa: Robust audio/video stream transport
- 802.11ac: Very High Throughput <6Ghz
- 802.11ad: Very High Throughput in 60 GHz

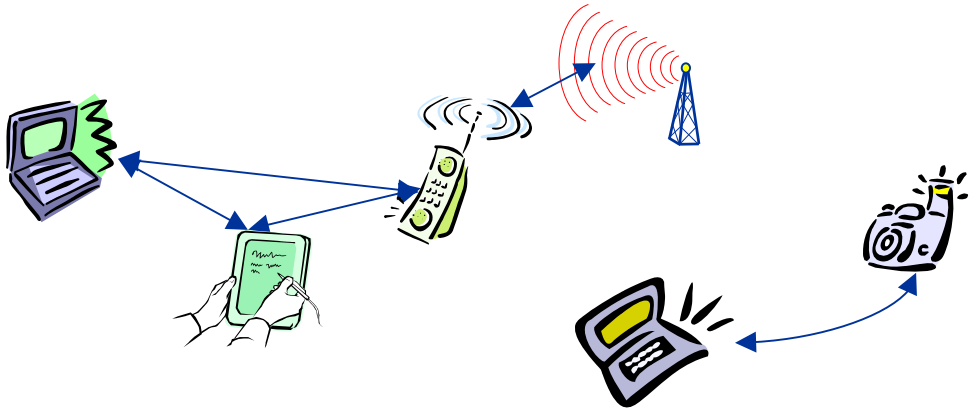
- Note: Not all “standards” will end in products, many ideas get stuck at working group level
- Info: www.ieee802.org/11/, 802wirelessworld.com, standards.ieee.org/getieee802/

Bluetooth

- Basic idea
  - Universal radio interface for ad-hoc wireless connectivity
  - Interconnecting computer and peripherals, handheld devices, tablets, cell phones – replacement of IrDA
  - Embedded in other devices



One of the first modules (Ericsson).



Bluetooth - contd

- Available globally for unlicensed users
- Devices within 10 m can share up to 720 kbps of capacity
- Supports open-ended list of applications
  - Data, audio, graphics, video

Applications

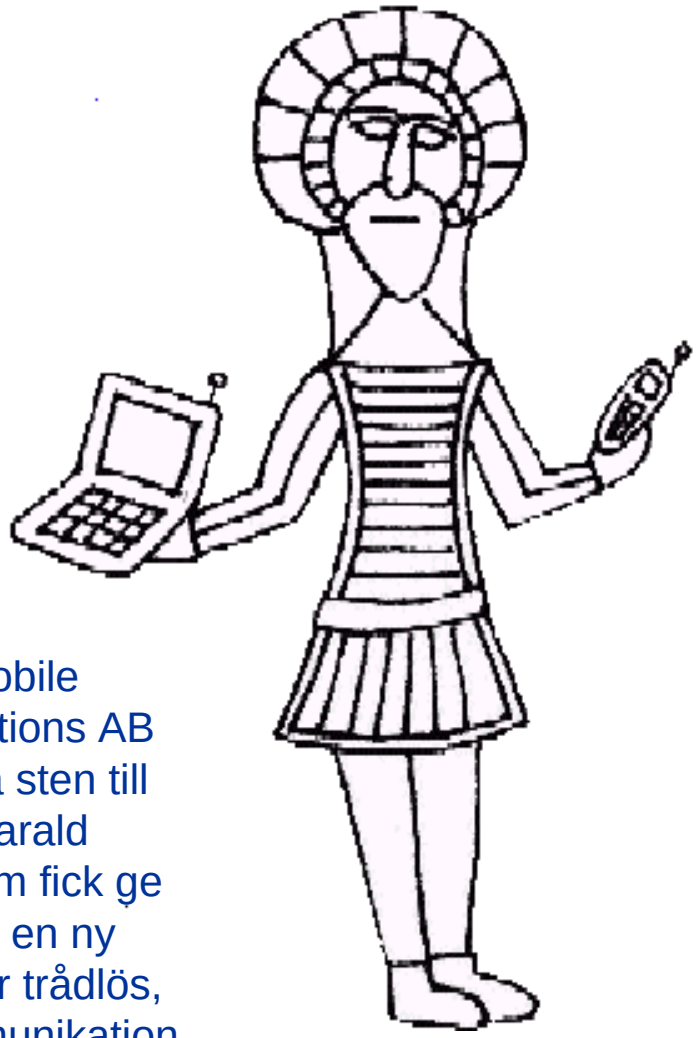
- Data and voice access points
  - Real-time voice and data transmissions
- Cable replacement
  - Eliminates need for numerous cable attachments for connection
- Ad hoc networking
  - Device with Bluetooth radio can establish connection with another when in range

Bluetooth - history

- 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
  - 2001: first consumer products for mass market, spec. version 1.1 released
  - 2005: 5 million chips/week

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

History and hi-tech…



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.

…and the real rune stone

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

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

Blåtand means “of dark complexion”
(not having a blue tooth…)

This could be the “original” colors of the stone.
Inscription:
“auk tani karthi kristna” (and made the Danes Christians)

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 Connection Less)
  - 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

Standards Documents

- Core specifications
  - Details of various layers of Bluetooth protocol architecture
- Profile specifications
  - Use of Bluetooth technology to support various applications

Protocol Architecture

- Bluetooth is a layered protocol architecture
  - Core protocols
  - Cable replacement and telephony control protocols
  - Adopted protocols
- Core protocols
  - Radio
  - Baseband
  - Link manager protocol (LMP)
  - Logical link control and adaptation protocol (L2CAP)
  - Service discovery protocol (SDP)

Protocol Architecture

- Cable replacement protocol
  - RFCOMM
- Telephony control protocol
  - Telephony control specification – binary (TCS BIN)
- Adopted protocols
  - PPP
  - TCP/UDP/IP
  - OBEX
  - WAE/WAP

Usage Models

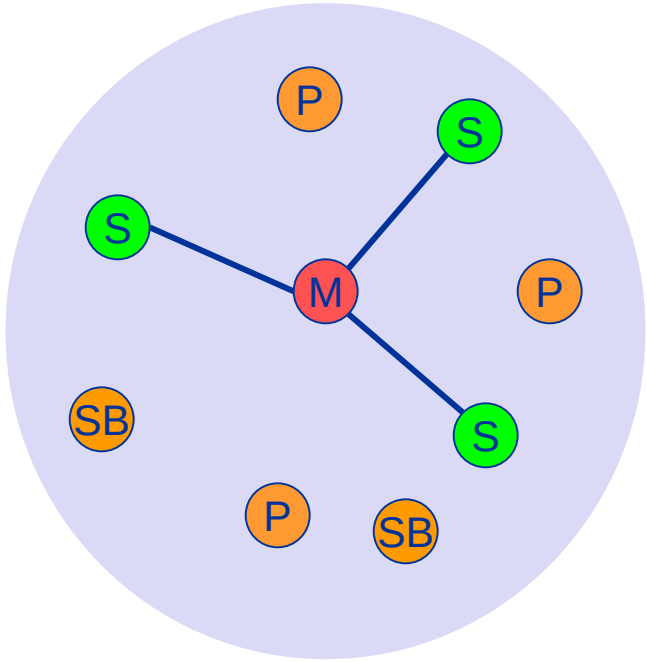
- File transfer
- Internet bridge
- LAN access
- Synchronization
- Three-in-one phone
- Headset

Piconets and Scatternets

- Piconet
  - Basic unit of Bluetooth networking
  - Master and one to seven slave devices
  - Master determines channel and phase
- Scatternet
  - Device in one piconet may exist as master or slave in another piconet
  - Allows many devices to share same area
  - Makes efficient use of bandwidth

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)

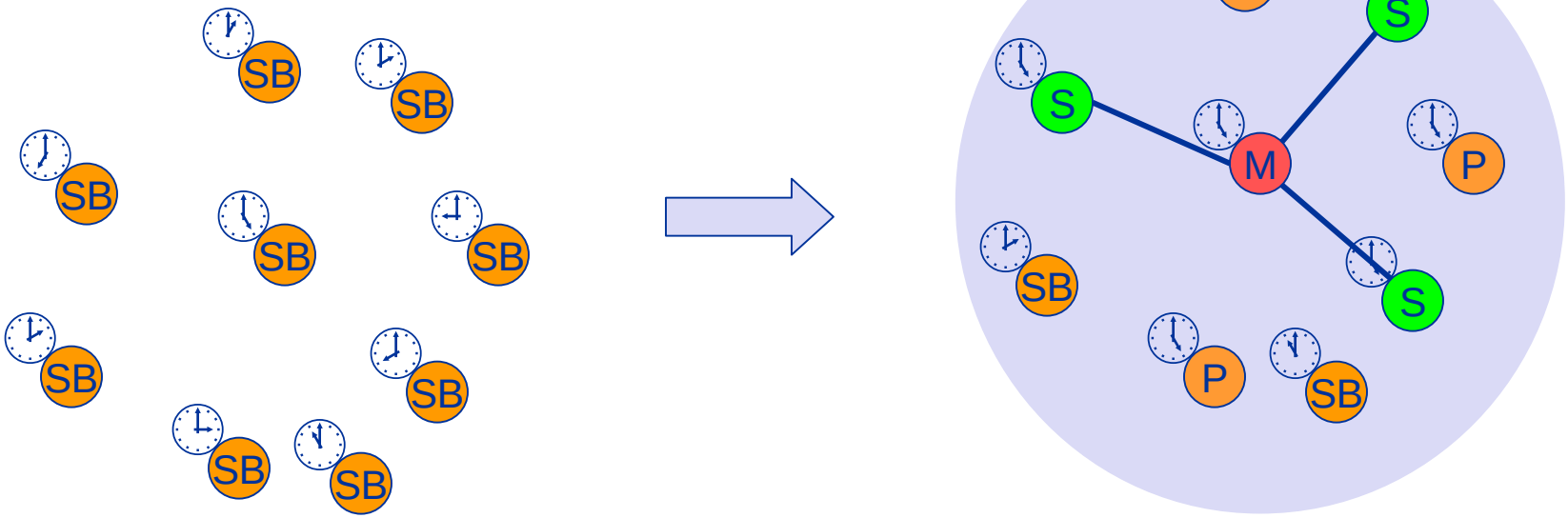


M=Master
S=Slave

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)



Radio Specification

- Classes of transmitters
  - Class 1: Outputs 100 mW for maximum range
    - Power control mandatory
    - Provides greatest distance
  - Class 2: Outputs 2.4 mW at maximum
    - Power control optional
  - Class 3: Nominal output is 1 mW
    - Lowest power

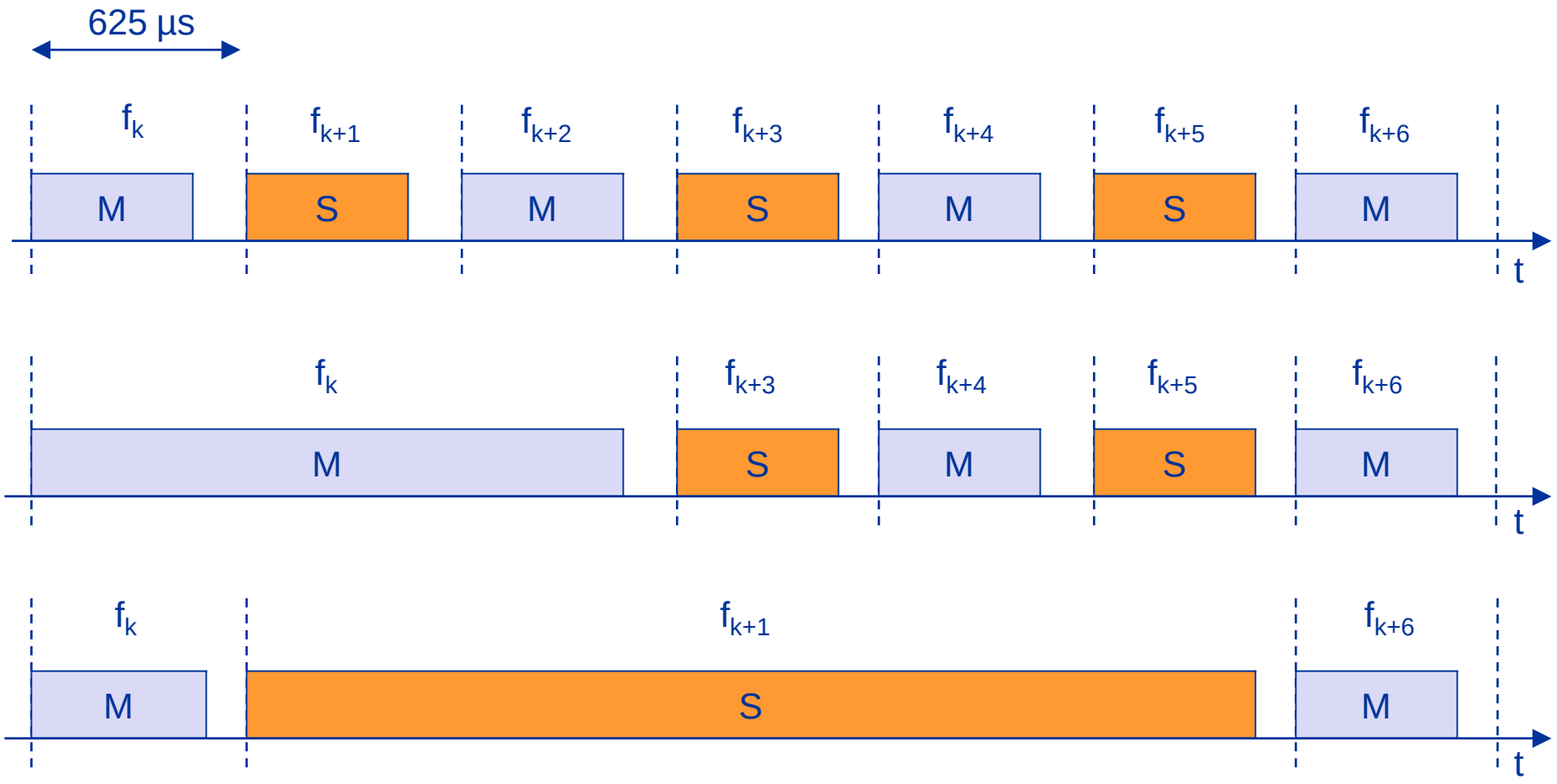
Frequency Hopping in Bluetooth

- Provides resistance to interference and multipath effects
- Provides a form of multiple access among co-located devices in different piconets

Frequency Hopping

- Total bandwidth divided into 1MHz physical channels
- FH occurs by jumping from one channel to another in pseudorandom sequence
- Hopping sequence shared with all devices on piconet
- Piconet access:
  - Bluetooth devices use time division duplex (TDD)
  - Access technique is TDMA
  - FH-TDD-TDMA

Frequency selection during data transmission

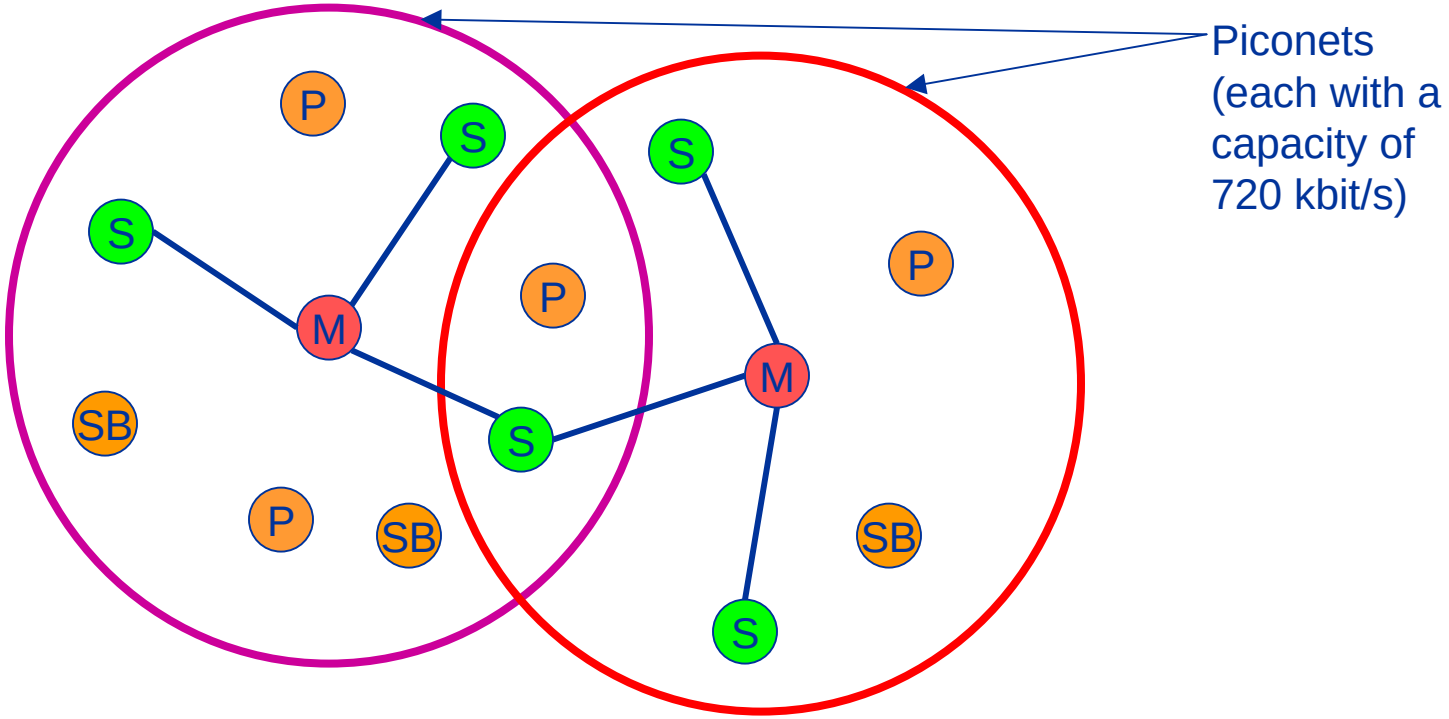


Physical Links between Master and Slave

- Synchronous connection oriented (SCO)
  - Allocates fixed bandwidth between point-to-point connection of master and slave
  - Master maintains link using reserved slots
  - Master can support three simultaneous links
- Asynchronous connectionless (ACL)
  - Point-to-multipoint link between master and all slaves
  - Only single ACL link can exist

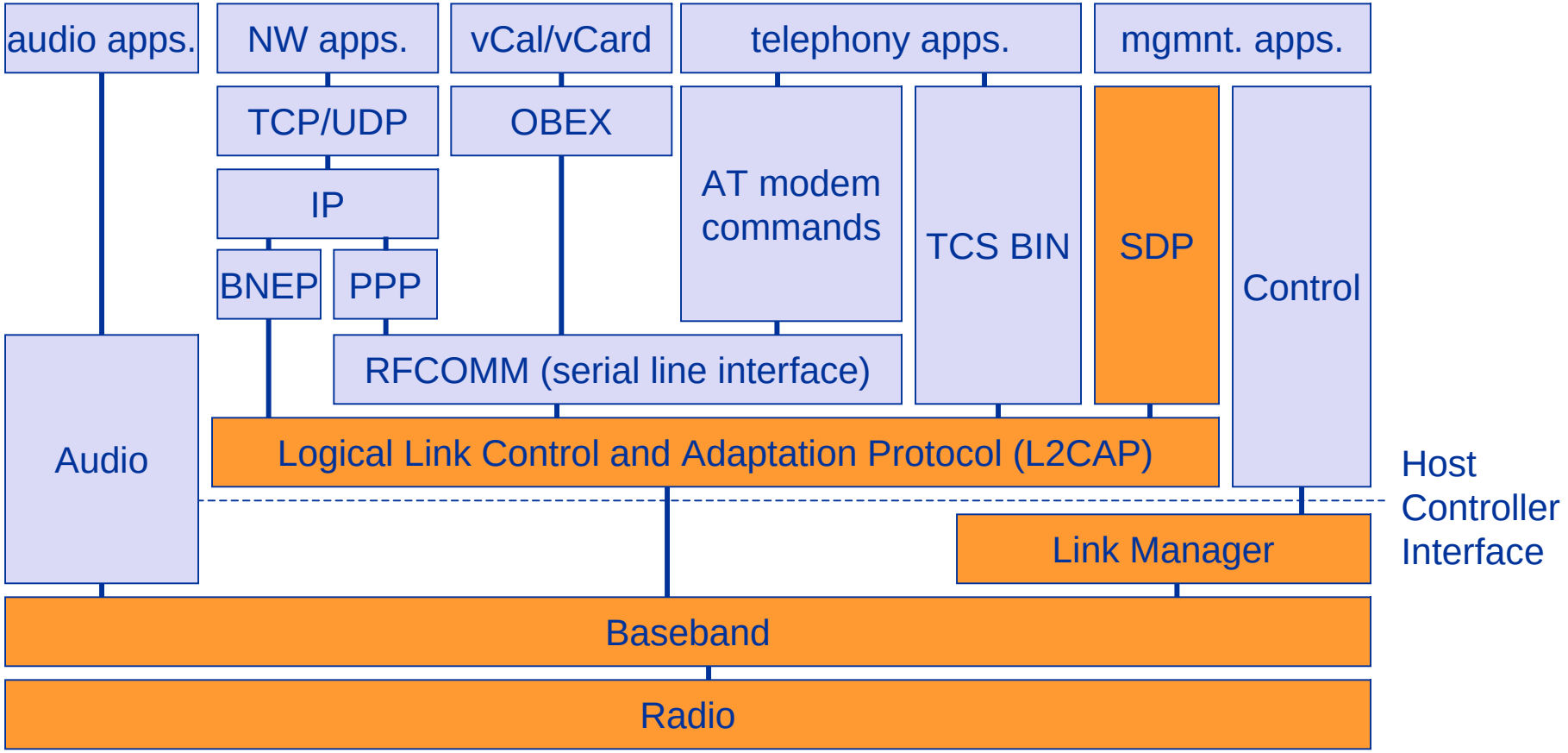
Scatternet

- 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.

Bluetooth Packet Fields

- Access code – used for timing synchronization, offset compensation, paging, and inquiry
- Header – used to identify packet type and carry protocol control information
- Payload – contains user voice or data and payload header, if present

Types of Access Codes

- Channel access code (CAC) – identifies a piconet
- Device access code (DAC) – used for paging and subsequent responses
- Inquiry access code (IAC) – used for inquiry purposes

Access Code

- Preamble – used for DC compensation
  - 0101 if LSB of sync word is 0
  - 1010 if LSB of synch word is 1
- Sync word – 64-bits, derived from:
  - 7-bit Barker sequence
  - Lower address part (LAP)
  - Pseudonoise (PN) sequence
- Trailer
  - 0101 if MSB of sync word is 1
  - 1010 if MSB of sync word is 0

Packet Header Fields

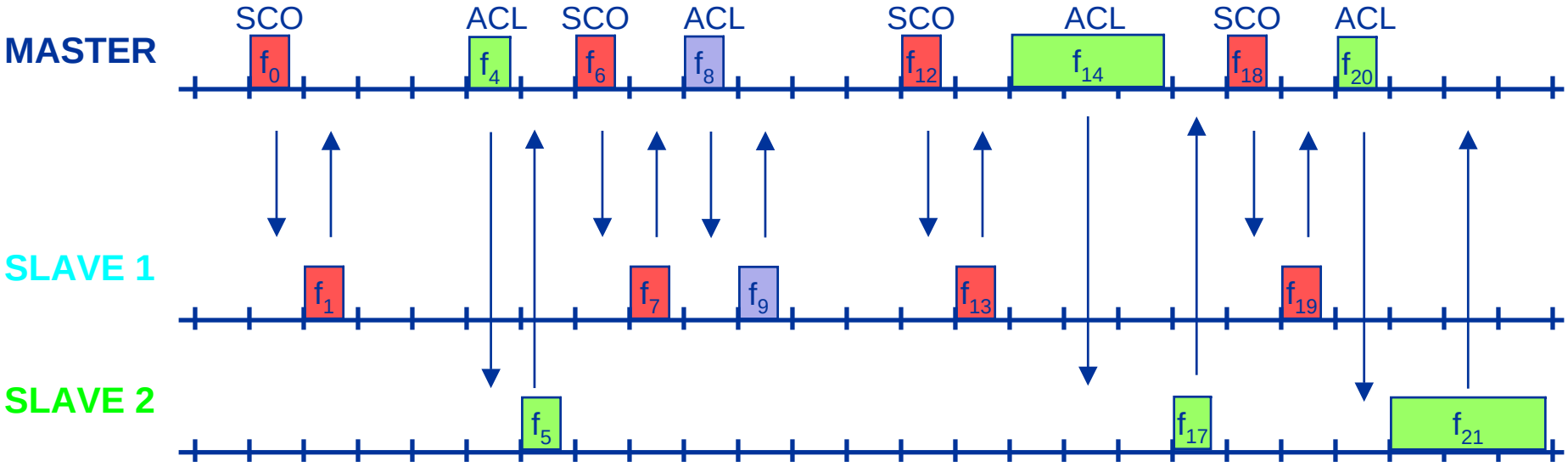
- AM_ADDR – contains “active mode” address of one of the slaves
- Type – identifies type of packet
- Flow – 1-bit flow control
- ARQN – 1-bit acknowledgment
- SEQN – 1-bit sequential numbering schemes
- Header error control (HEC) – 8-bit error detection code

Payload Format

- Payload header
  - L_CH field – identifies logical channel
  - Flow field – used to control flow at L2CAP level
  - Length field – number of bytes of data
- Payload body – contains user data
- CRC – 16-bit CRC code

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



Error Correction Schemes

- 1/3 rate FEC (forward error correction)
  - Used on 18-bit packet header, voice field in HV1 packet
- 2/3 rate FEC
  - Used in DM packets, data fields of DV packet, FHS packet and HV2 packet
- ARQ
  - Used with DM and DH packets

ARQ Scheme Elements

- Error detection – destination detects errors, discards packets
- Positive acknowledgment – destination returns positive acknowledgment
- Retransmission after timeout – source retransmits if packet unacknowledged
- Negative acknowledgment and retransmission – destination returns negative acknowledgement for packets with errors, source retransmits

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