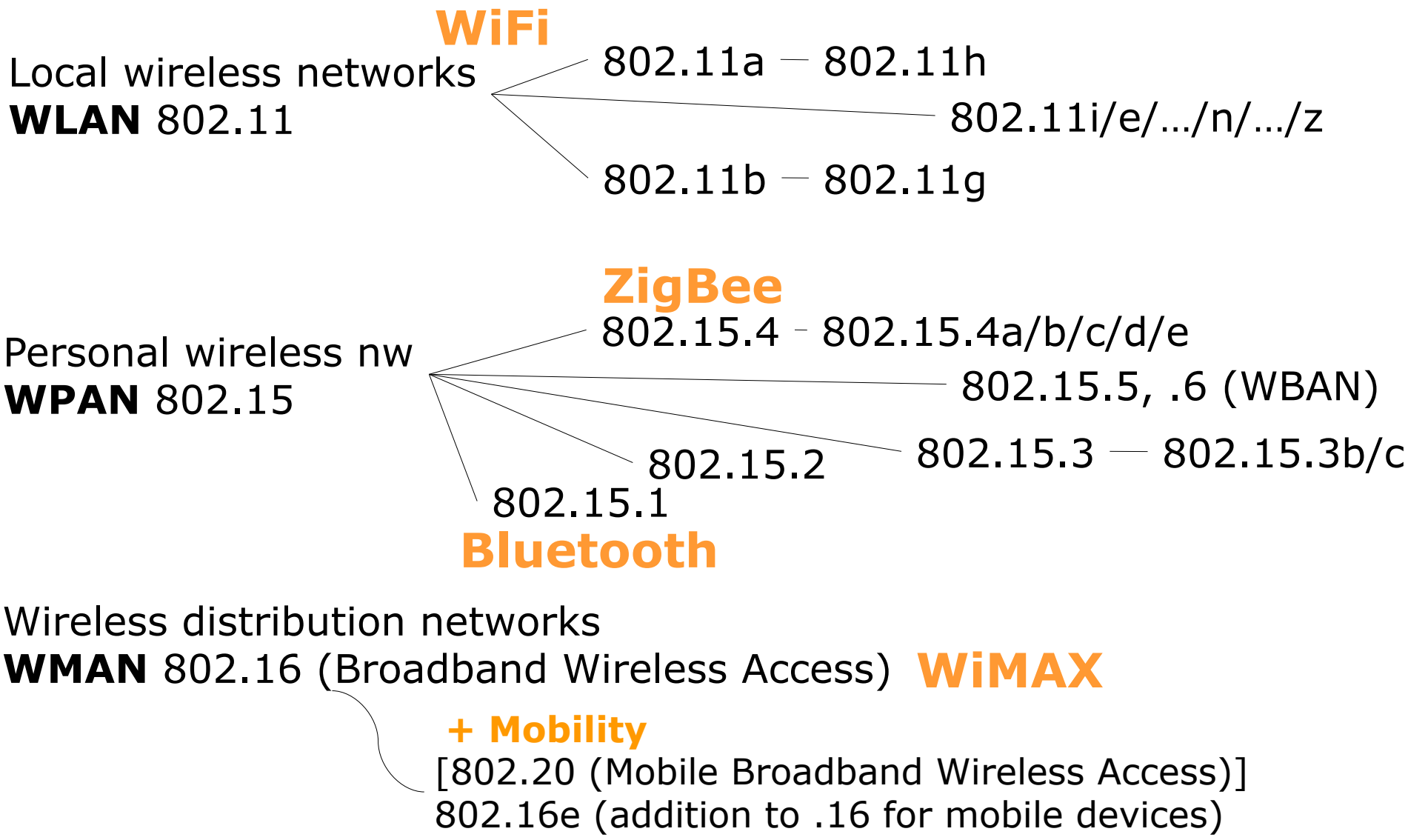
Mobile Communications
Chapter 7: Wireless LANs

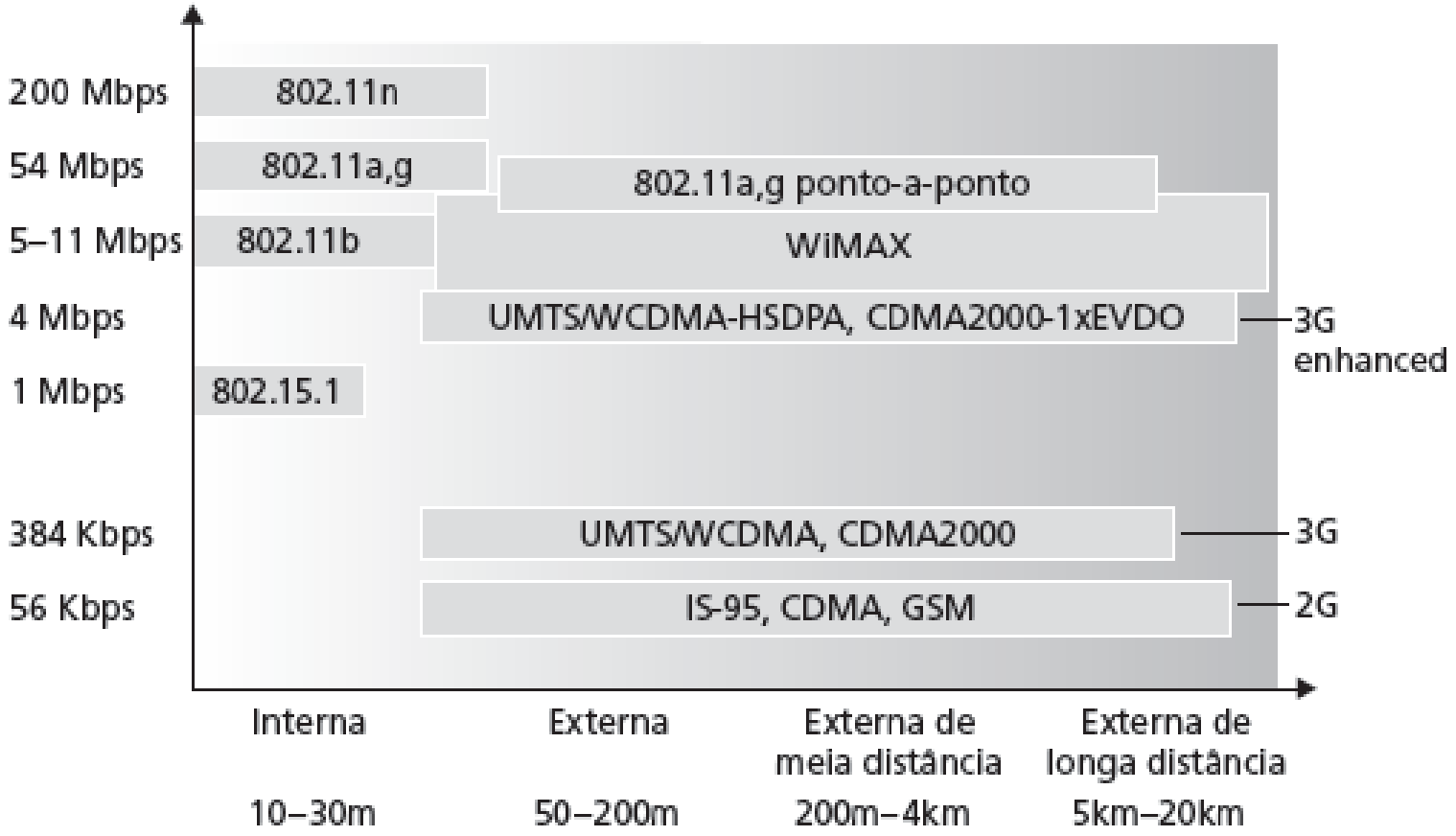
- Characteristics
- IEEE 802.11 (PHY, MAC, Roaming, .11a, b, g, h, i, n … z)
- Bluetooth / IEEE 802.15.x
- IEEE 802.16/.20/.21/.22
- RFID
- Comparison

Prof. Jó Ueyama

Mobile Communication Technology according to IEEE (examples)



Main features of the existing wireless technologies



Why is 802.11n faster?

- MIMO technology
  - Multiple Output Multiple Input
  - Signal processing smart antenna
  - Transmits multiple data streams through multiple antennas
  - The result?
  - Up to five times the performance
  - Achieves twice the range to that of 802.11g
- Simultaneous dual band: 2.4/5 GHz frequencies
- Range 175 feet
- Typically up to 450 Mbps

Why is 802.11n faster?

- MIMO is also employed in WiMax
- 802.11g typically achieves up to 54Mbps
- MIMO can simultaneously transmit three streams of data and receive two
- Three non overlapping channels at 2.4 GHz (1, 6 and 11)
- Payload optimization: more data being transmitted in each packet
- 802.11n is ideal for video streaming
- If your 802.11n working with 802.11g laptop will result in slower 802.11g speeds

Characteristics of wireless LANs

- Advantages
  - very flexible within the reception area
  - Ad-hoc networks without previous planning possible
  - (almost) no wiring difficulties (e.g. historic buildings, firewalls)
  - more robust against disasters like, e.g., earthquakes, fire - or users pulling a plug...
- Disadvantages
  - typically very low bandwidth compared to wired networks (1-450 Mbit/s) due to shared medium
  - many patented proprietary solutions, especially for higher bit-rates, standards take their time (e.g. IEEE 802.11n)
  - products have to follow many national restrictions such as frequencies that are permitted within a country (e.g. police, aircraft control, etc.)

Design goals for wireless LANs

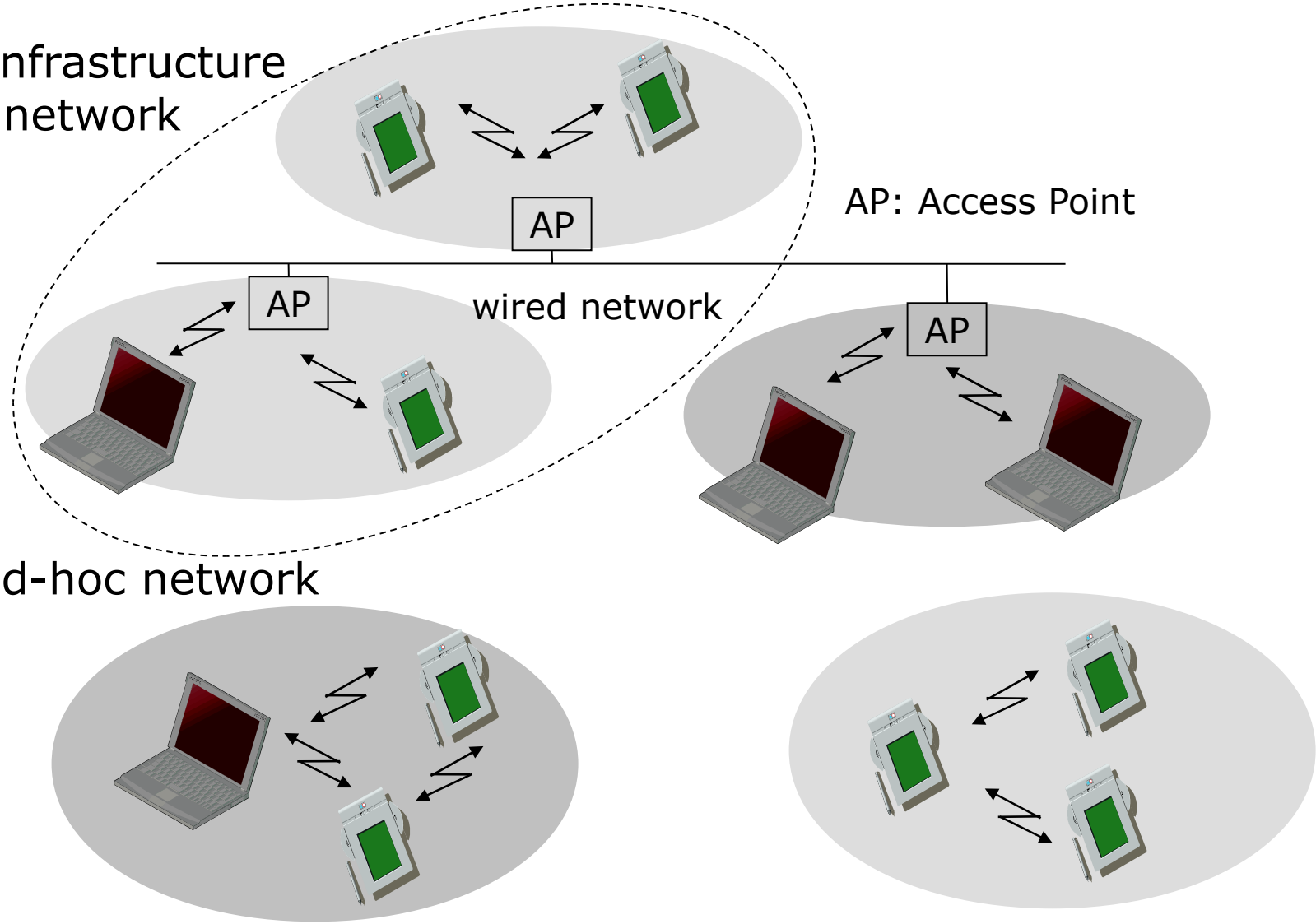
- global, seamless operation
- low power for battery use (e.g. WSNs and cell phones)
- no special permissions or licenses needed to use the LAN
- robust transmission technology
- simplified spontaneous cooperation at meetings
- easy to use for everyone, simple management
- protection of investment in wired networks (i.e. interoperable with wired LANs)
- 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

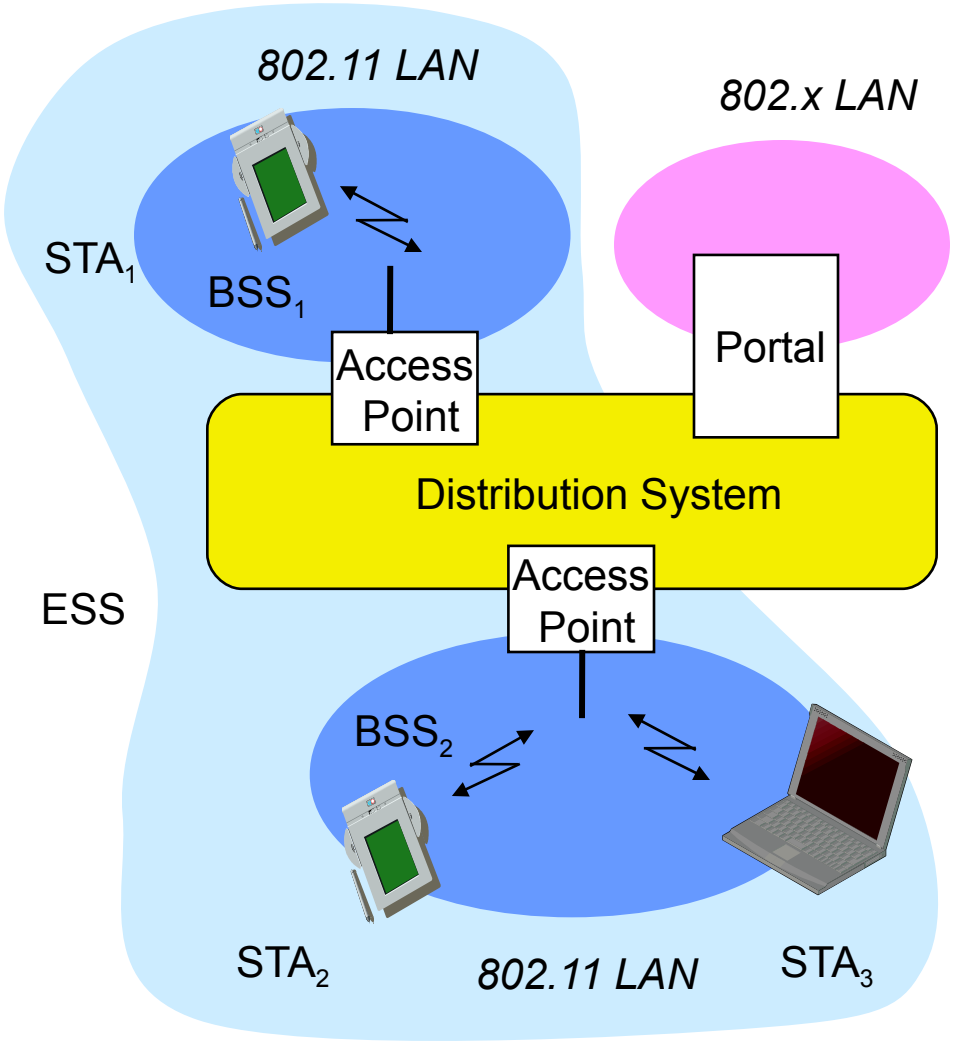
- Infrared
  - uses IR diodes, multiple reflections (walls, furniture etc.)
- Advantages
  - simple, cheap, available in many mobile devices
  - no licenses needed
  - simple shielding possible
- Disadvantages
  - interference by sunlight, heat sources etc.
  - many things shield or absorb IR light
  - low bandwidth
- Example
  - IrDA (Infrared Data Association) interface available everywhere

- Radio
  - typically using the license free ISM band at 2.4 GHz
- Advantages
  - experience from wireless WAN and mobile phones can be used
  - coverage of larger areas possible (radio can penetrate walls, furniture etc.)
- Disadvantages
  - very limited license free frequency bands
  - shielding more difficult, interference with other electrical devices
- Example
  - Many different products

Comparison: infrastructure vs. ad-hoc networks

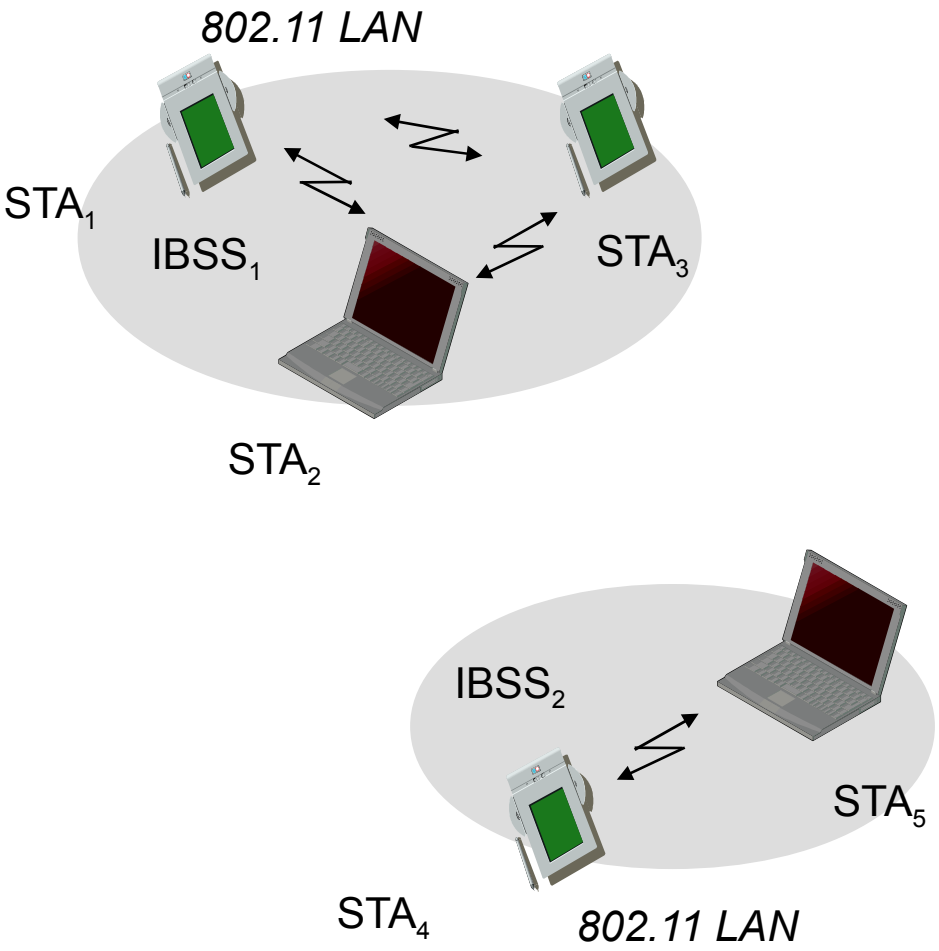


802.11 - Architecture of an infrastructure network



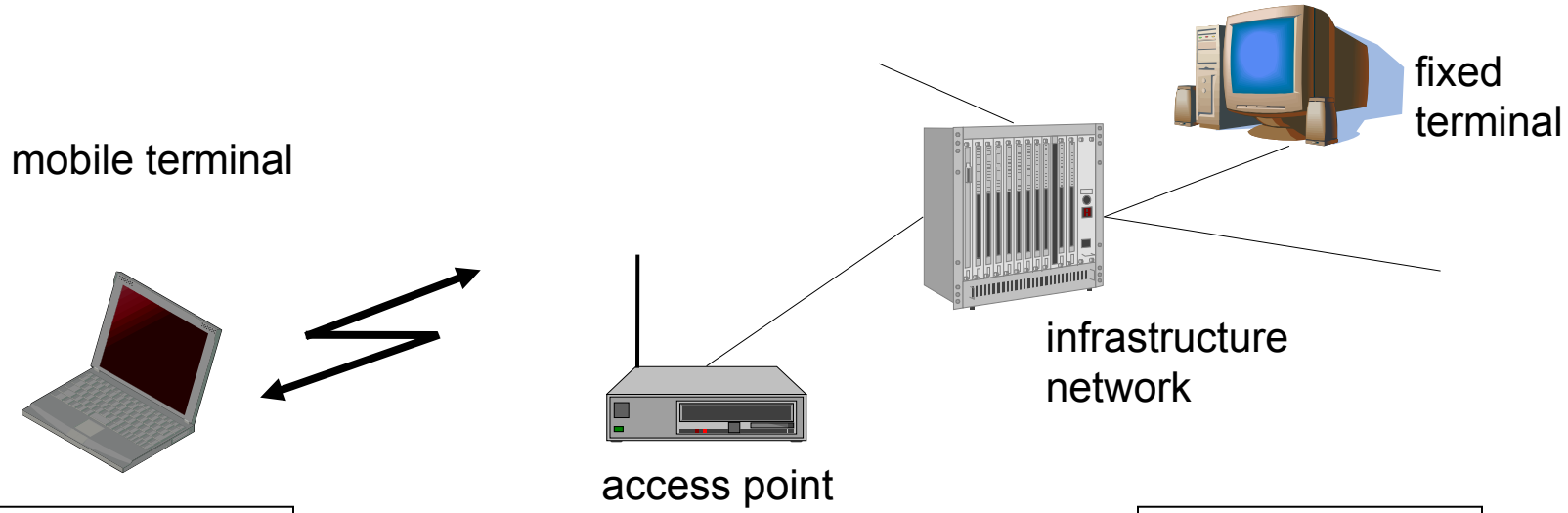
- Station (STA)
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- Basic Service Set (BSS)
  - group of stations using the same radio frequency
- Access Point
  - station integrated into the wireless LAN and the distribution system
- Portal
  - bridge to 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

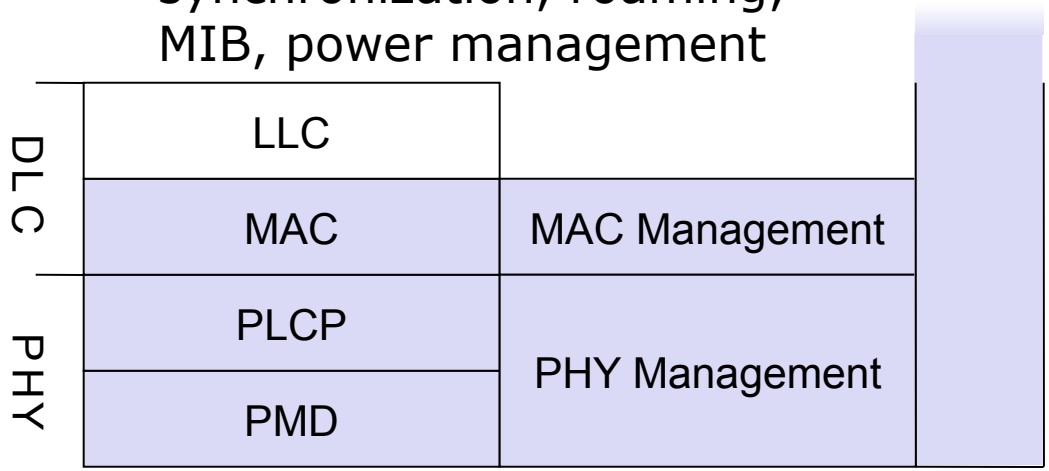


application		application
TCP		TCP
IP		IP
LLC	LLC	LLC
802.11 MAC	802.11 MAC / 802.3 MAC	802.3 MAC
802.11 PHY	802.11 PHY / 802.3 PHY	802.3 PHY

LLC – Logical Link Control – interface between different medias

802.11 - Layers and functions

- MAC
  - access mechanisms, fragmentation, encryption
- MAC Management
  - synchronization, roaming, MIB, power management



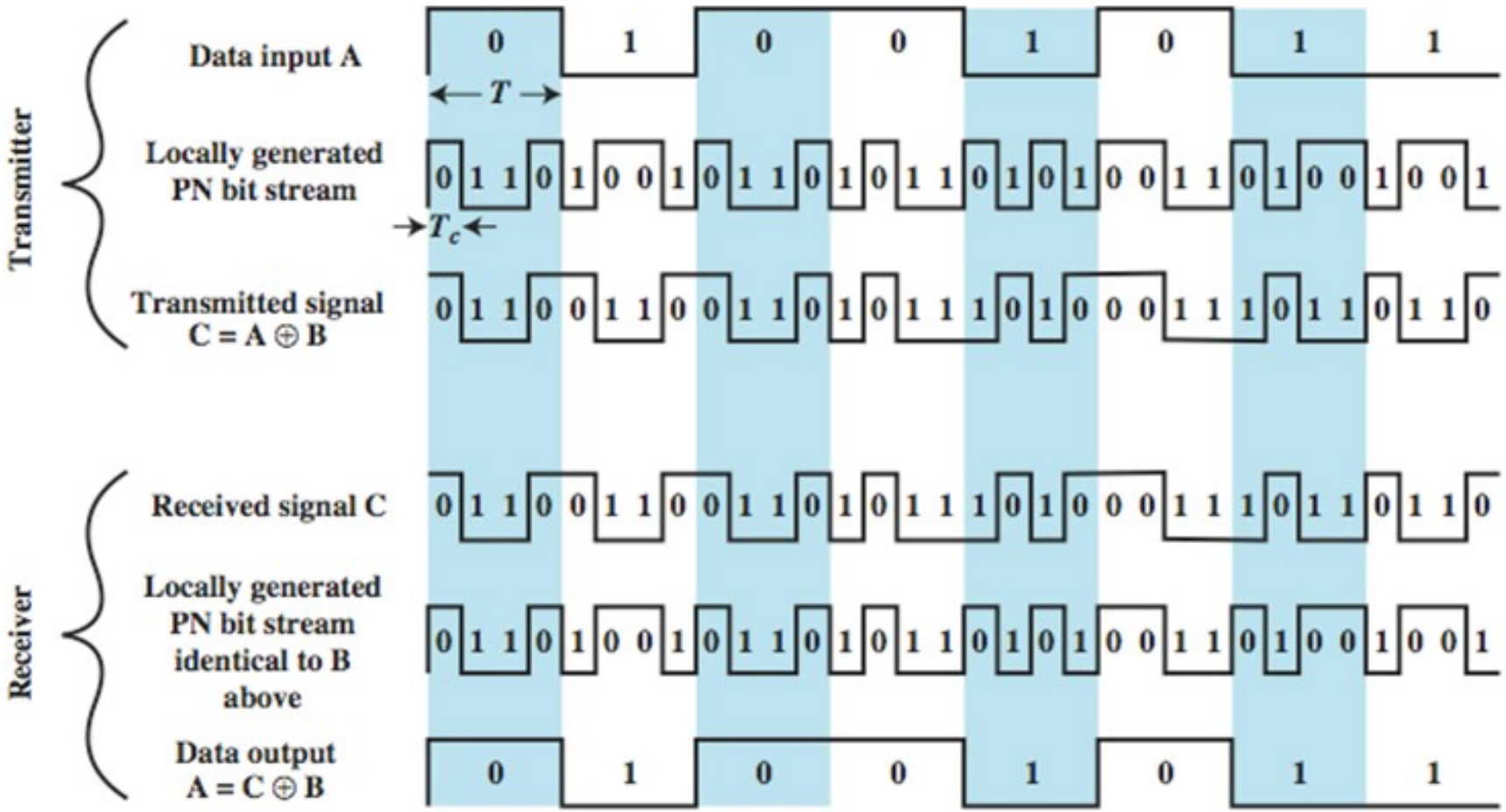
- PHY Management includes
  - PLCP Physical Layer Convergence Protocol
    - clear channel assessment signal (carrier sense)
    - Medium currently idle?
  - PMD Physical Medium Dependent
    - modulation, coding, transforms bits into signals
- Station Management
  - coordination of all management functions

802.11 - Physical layer (legacy)

- 3 versions: 2 radio (typ. 2.4 GHz), 1 IR
  - data rates 1 or 2 Mbit/s
- FHSS (Frequency Hopping Spread Spectrum) only up to 2Mbs
  - spreading, despreading
  - Frequency multiplexing
- DSSS (Direct Sequence Spread Spectrum) → 802.11b/g/n
  - Multiplexes by code (i.e. using a chipping code)
  - Implementation is more complex than FHHS
  - chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
  - DATA XOR chipping code
- Infrared
  - Wavelength around 850-950 nm, diffuse light, typ. 10 m range
  - uses near visible light
  - carrier detection, up to 4Mbits/s data rate

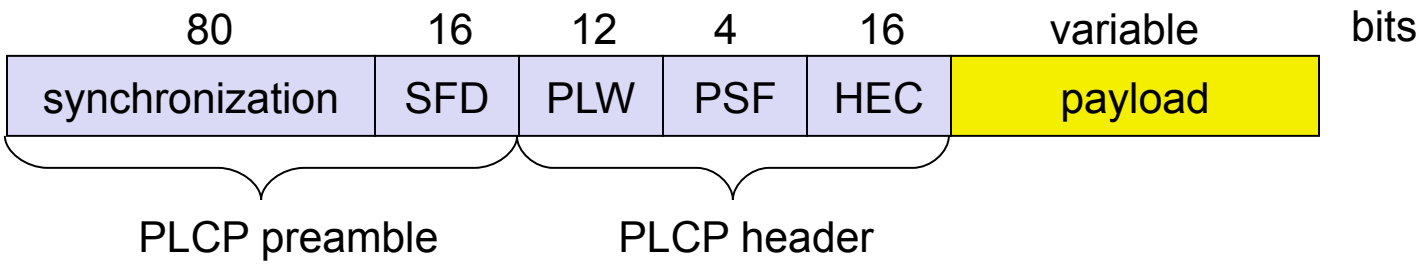
802.11 – DSSS, how does it work?

x	y	x XOR y
0	0	0
0	1	1
1	0	1
1	1	0



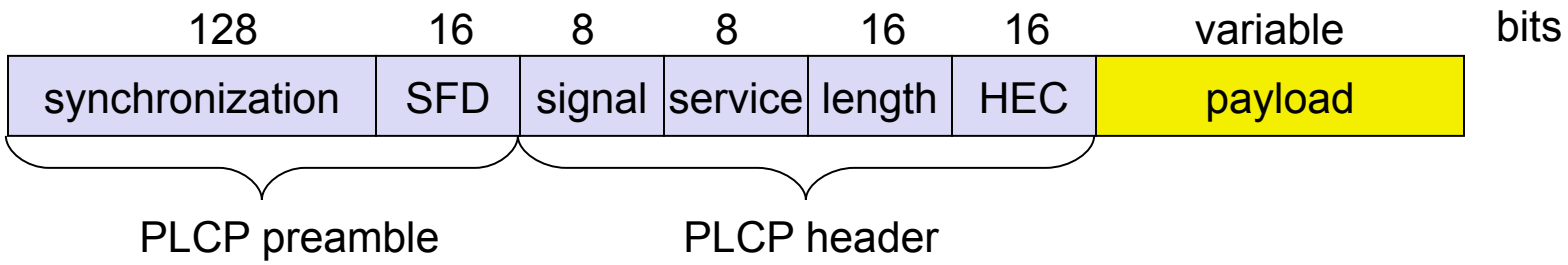
FHSS PHY packet format (legacy)

- Synchronization
  - synch with 010101... pattern
- SFD (Start Frame Delimiter)
  - 0000110010111101 start pattern
- PLW (PLCP_PDU Length Word)
  - length of payload incl. 32 bit CRC of payload, PLW < 4096
- PSF (PLCP Signaling Field)
  - data rate of the payload (0000 -> the lowest data rate 1Mbs)
- HEC (Header Error Check)
  - checksum with the standard ITU-T polynomial generator



DSSS PHY packet format (legacy)

- Synchronization
  - synch., gain setting, energy detection, frequency offset compensation
- SFD (Start Frame Delimiter)
  - 1111001110100000
- Signal
  - data rate of the payload (0A: 1 Mbit/s)
- Service
  - future use, 00: 802.11 compliant
- Length
  - length of the payload
- HEC (Header Error Check)
  - protected by checksum using ITU-T standard polynomial error check



802.11 - MAC layer I - DFWMAC

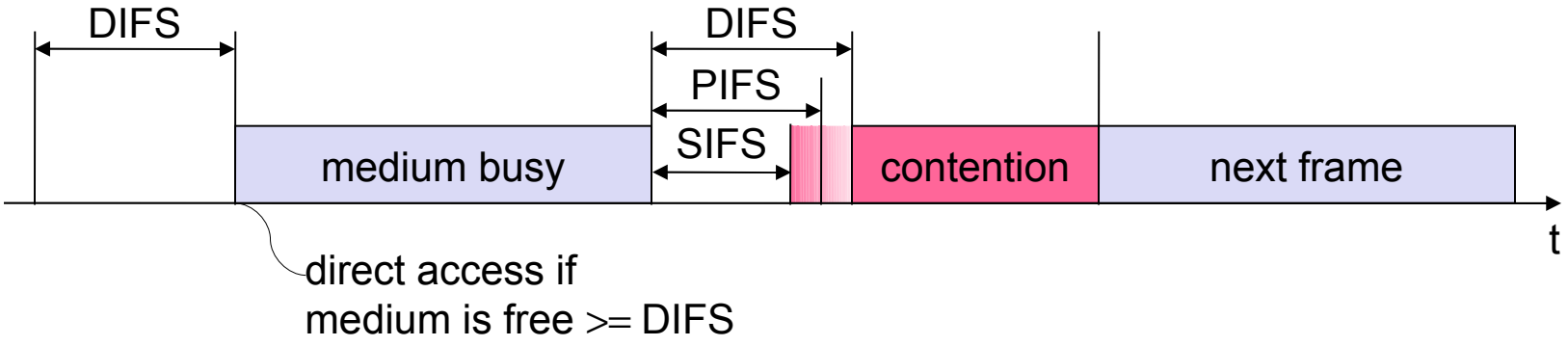
- MAC layer has to fulfill several tasks including:
  - control medium access
  - support for roaming
  - authentication
  - power conservation
- In summary, it has two key tasks:
  - traffic services
  - access control

802.11 - MAC layer I - DFWMAC

- Traffic services (two implementations)
  - 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

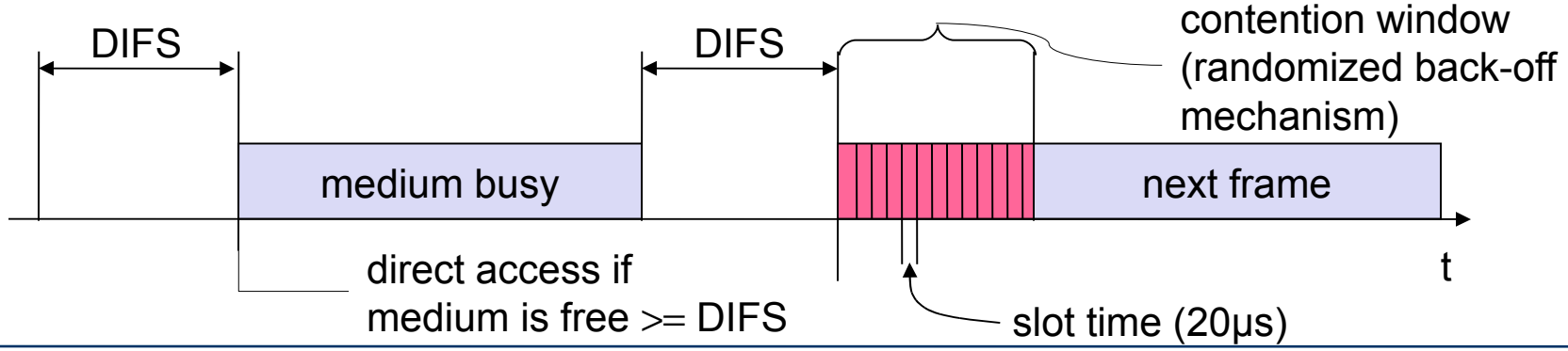
802.11 - MAC layer II

- Priorities
  - defined through different inter frame spaces
  - no guarantee, hard priorities
  - SIFS (Short Inter Frame Spacing)
    - highest priority, for ACK, CTS, polling response
    - DSSS SIFS 10 micro seconds
  - PIFS (PCF IFS)
    - medium priority, for time-bounded service using PCF
  - DIFS (DCF Inter frame spacing)
    - lowest priority, for asynchronous data service

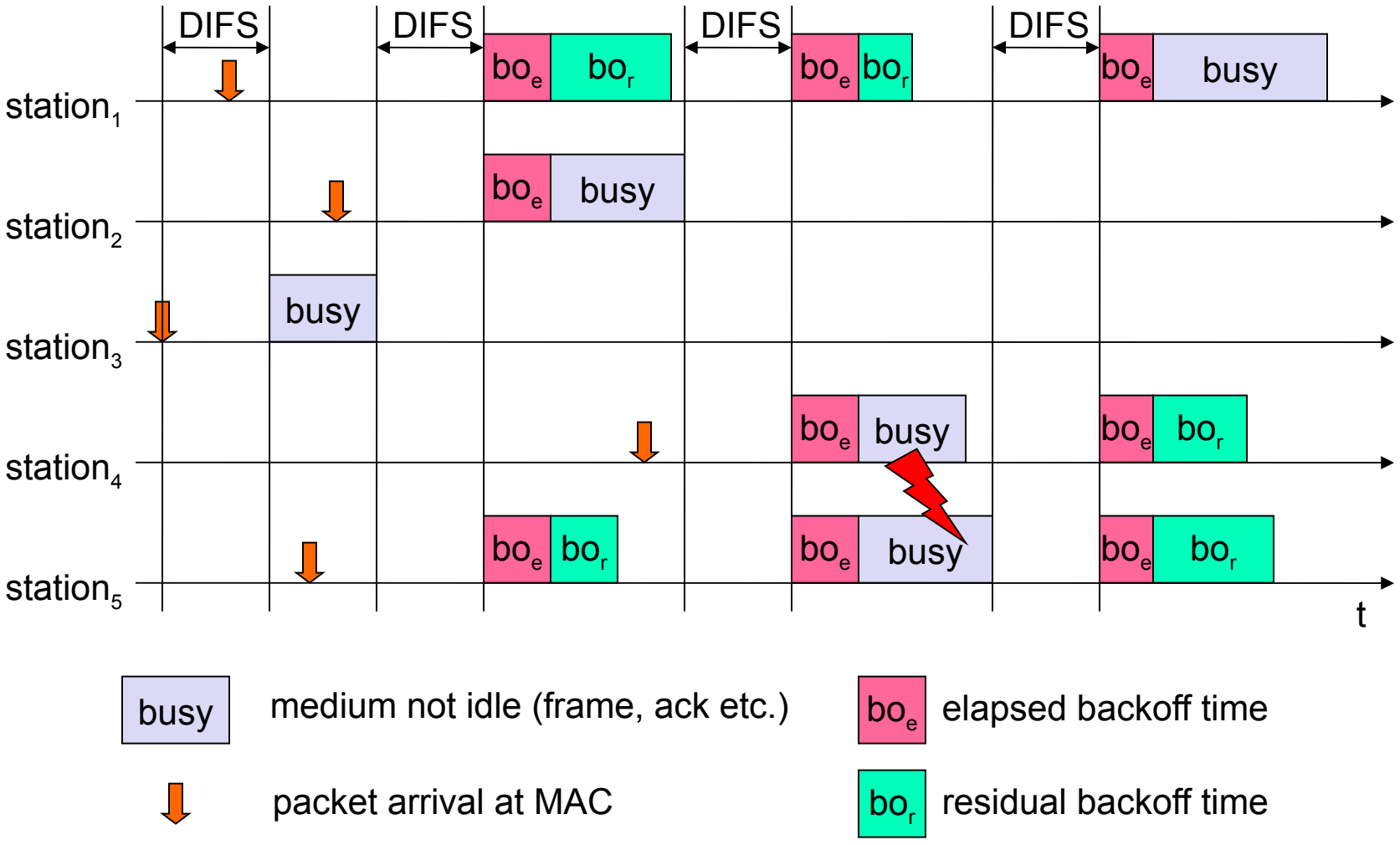


802.11 - CSMA/CA access method I

- station ready to send starts sensing the medium (Carrier Sense based on CCA - Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)

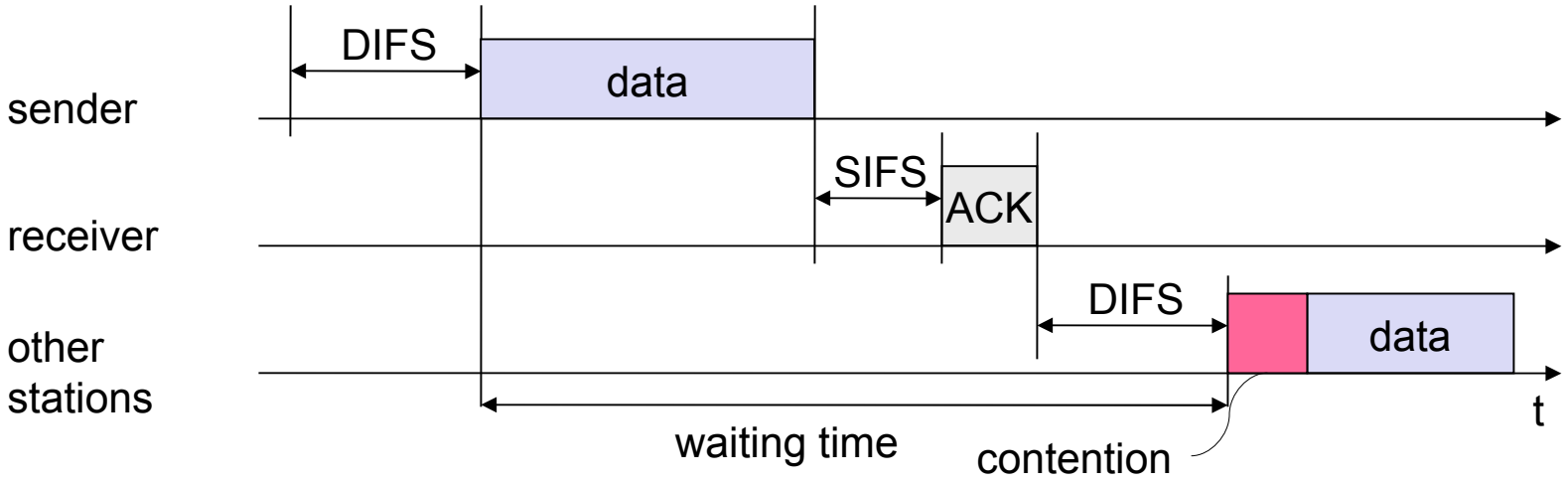


802.11 - competing stations - simple version



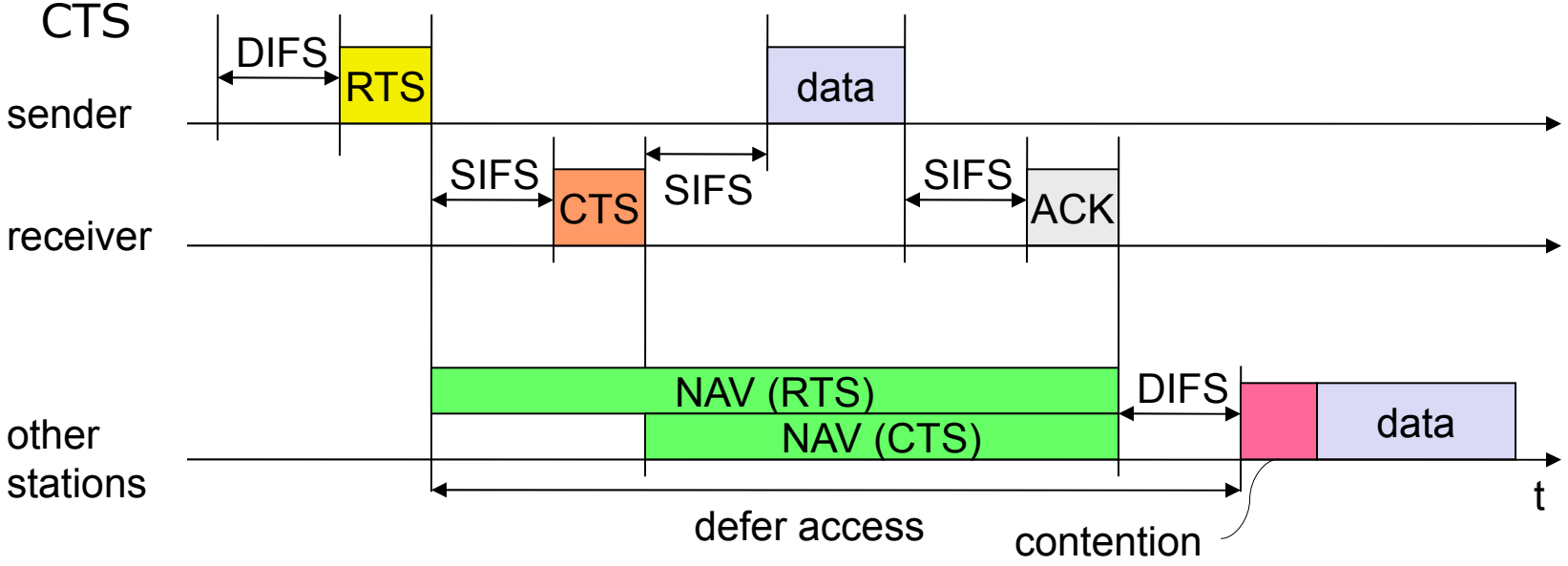
802.11 - CSMA/CA access method II

- Sending unicast packets
  - station has to wait for DIFS before sending data
  - receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
  - automatic retransmission of data packets in case of transmission errors

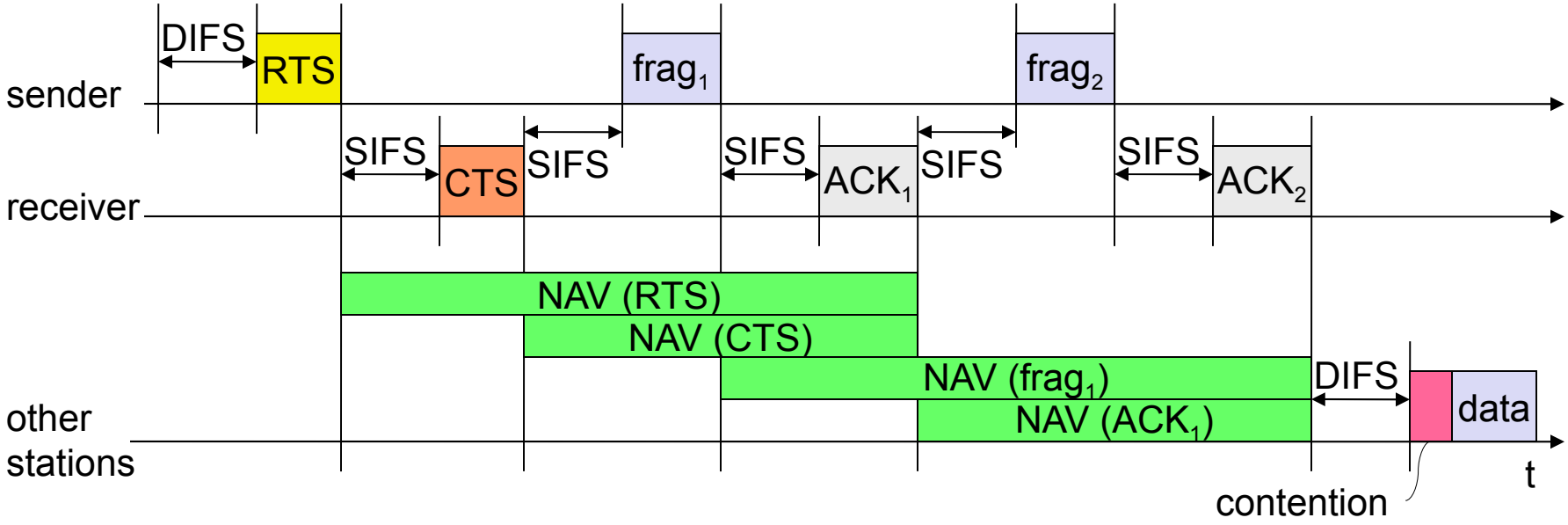


802.11 – Access scheme details (NAV-net allocat. vect.)

- 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

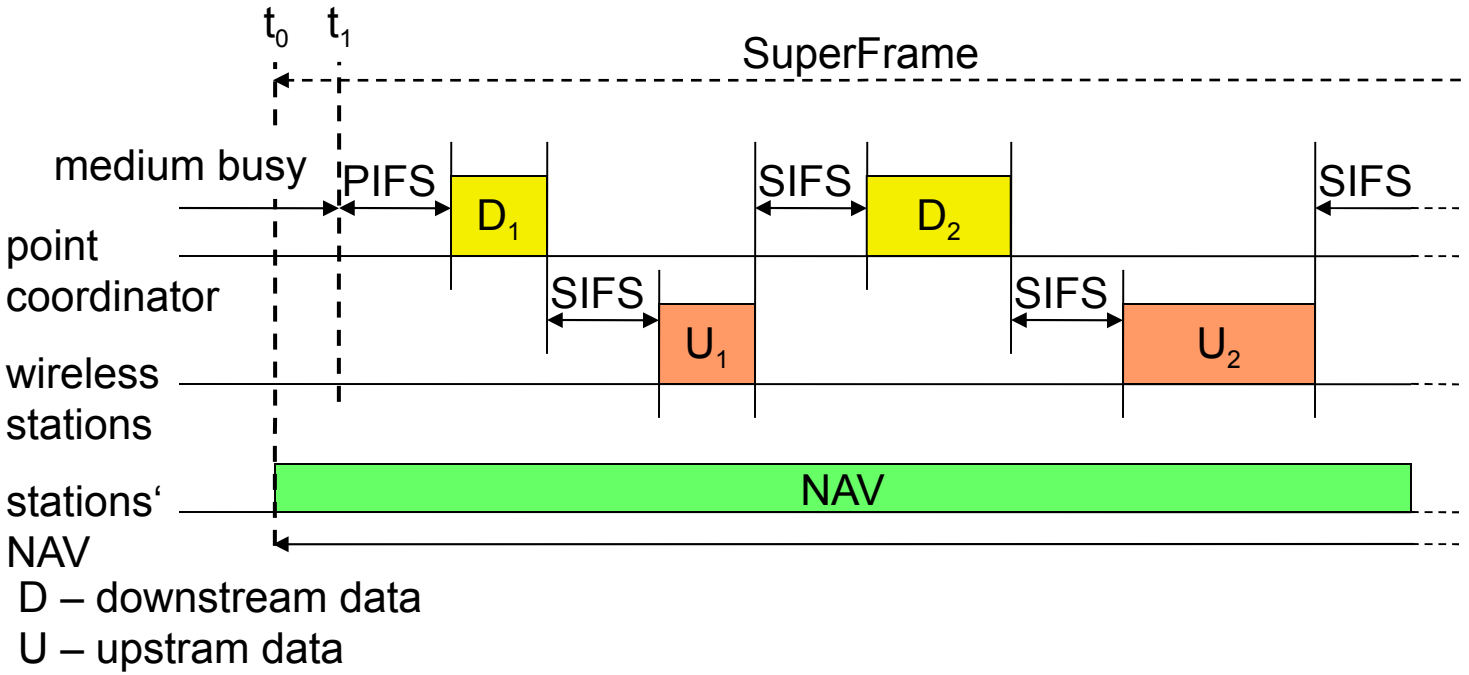


Fragmentation (advantages?)



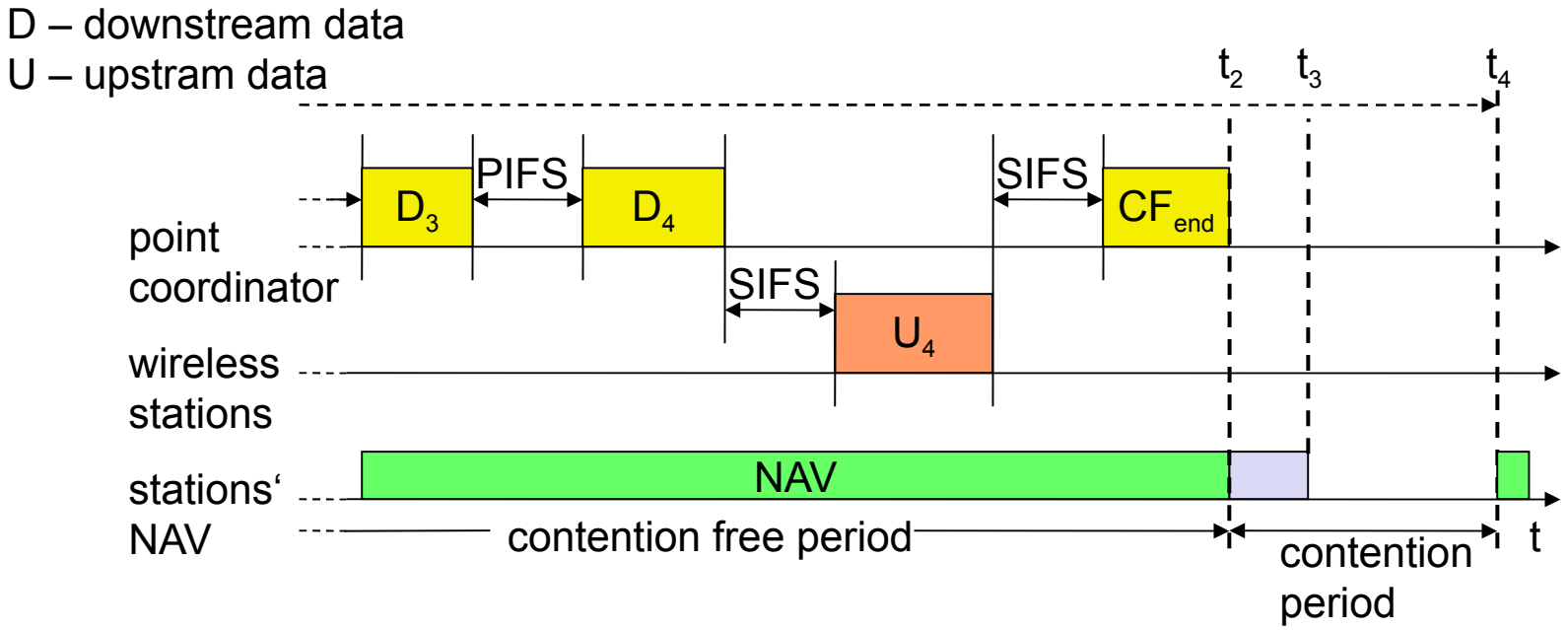
DFWMAC-PCF I (almost never used)

- The two previous mechanisms cannot guarantee QoS
- PCF on top of the standard DCF
- Using PCF → AP controls medium access and polls single nodes
- Super frame → comprises contention-free + contention period
- Contention period can be used for the two mechanisms



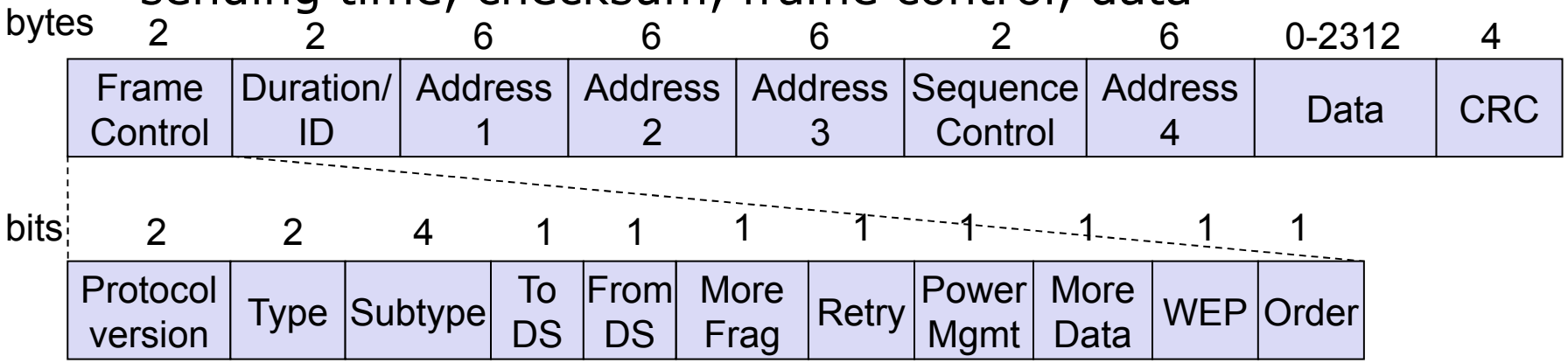
DFWMAC-PCF II

- As PIFS is smaller than DIFS no station can start sending earlier
- Node 3 has nothing to answer and AP will not receive a packet after SIFS



802.11 - Frame format

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



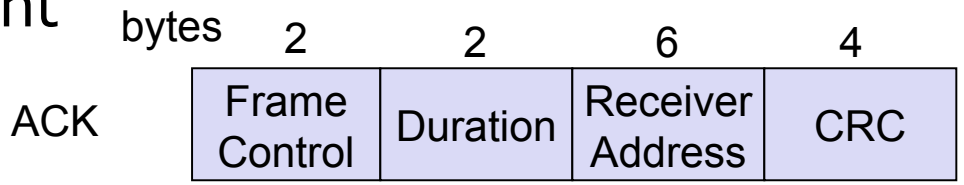
MAC address format

scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

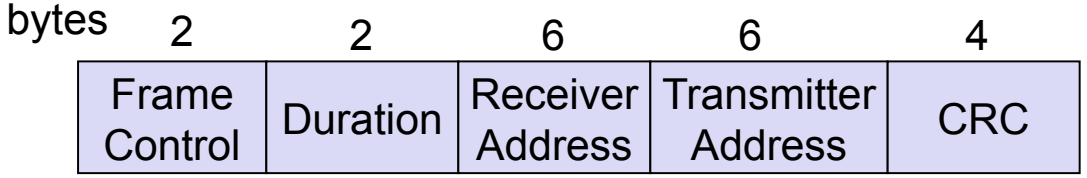
DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Basic Service Set Identifier
RA: Receiver Address
TA: Transmitter Address
Address1 – destination
Address2 – source (ACK will be sent to)
Address3 – filter (often it will carry BSSID addr)
Address4 – Address of the source Access Point

Special Frames: ACK, RTS, CTS

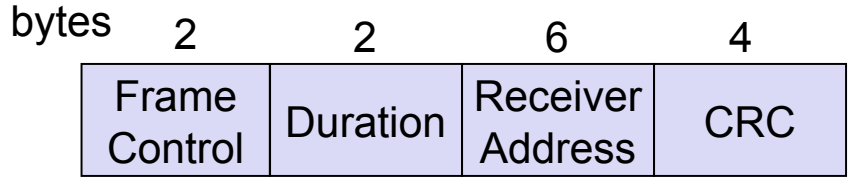
- Acknowledgement



- Request To Send



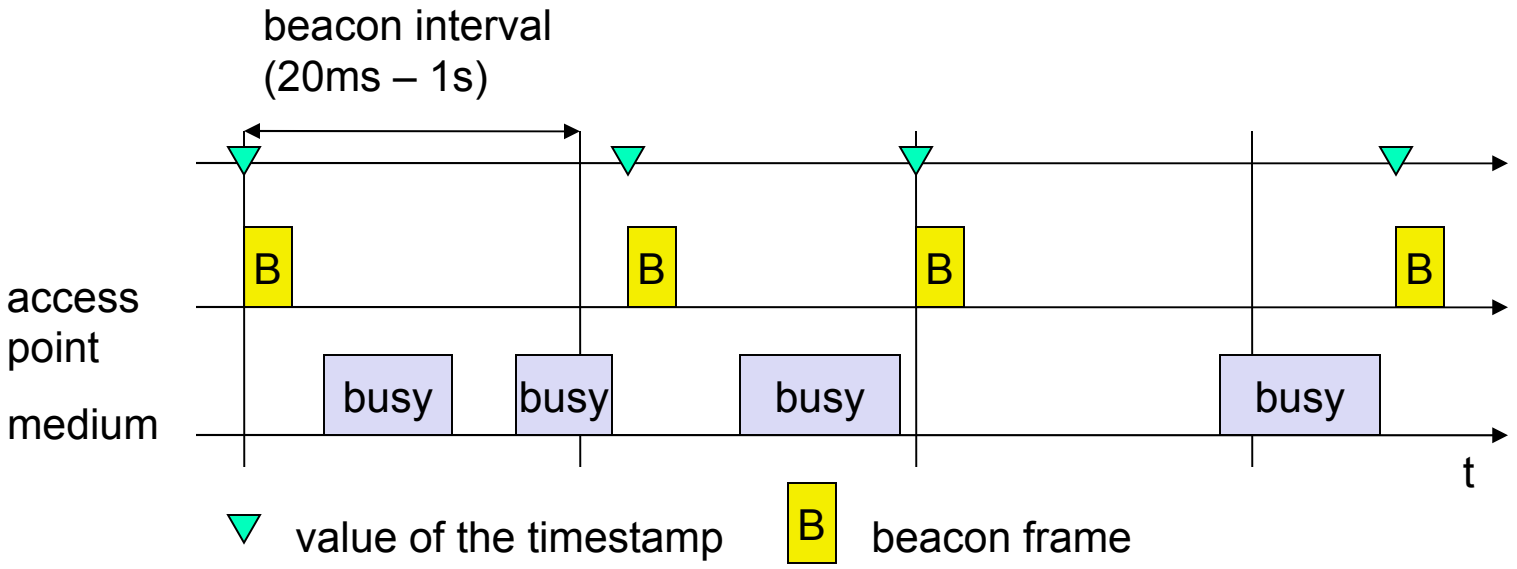
- Clear To Send



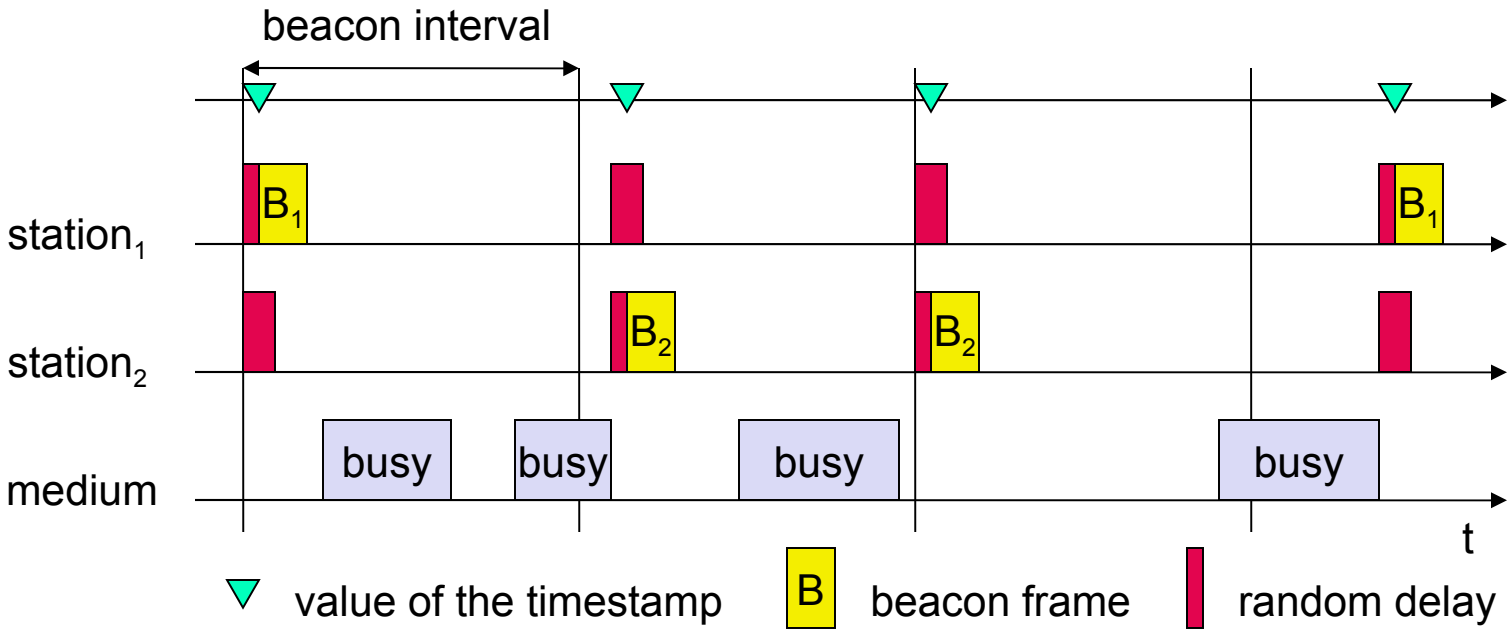
802.11 - MAC management

- Synchronization
  - try to find a LAN, try to stay within a LAN
  - timer etc.
- Power management
  - sleep-mode without missing a message
  - periodic sleep, frame buffering, traffic measurements
- Association/Reassociation
  - integration into a LAN
  - roaming, i.e. change networks by changing access points
  - scanning, i.e. active search for a network
- MIB - Management Information Base
  - managing, read, write

Synchronization using a Beacon (infrastructure)



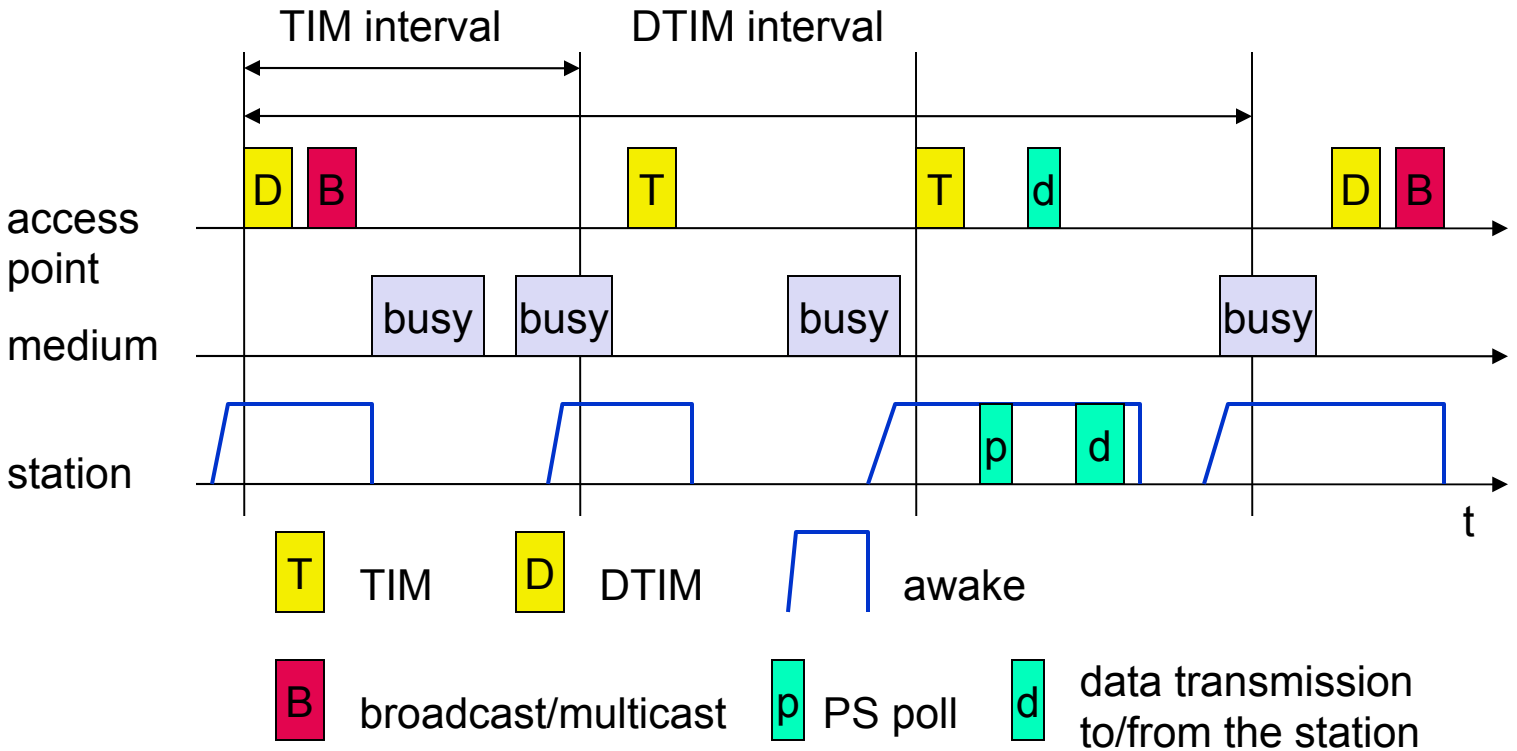
Synchronization using a Beacon (ad-hoc)



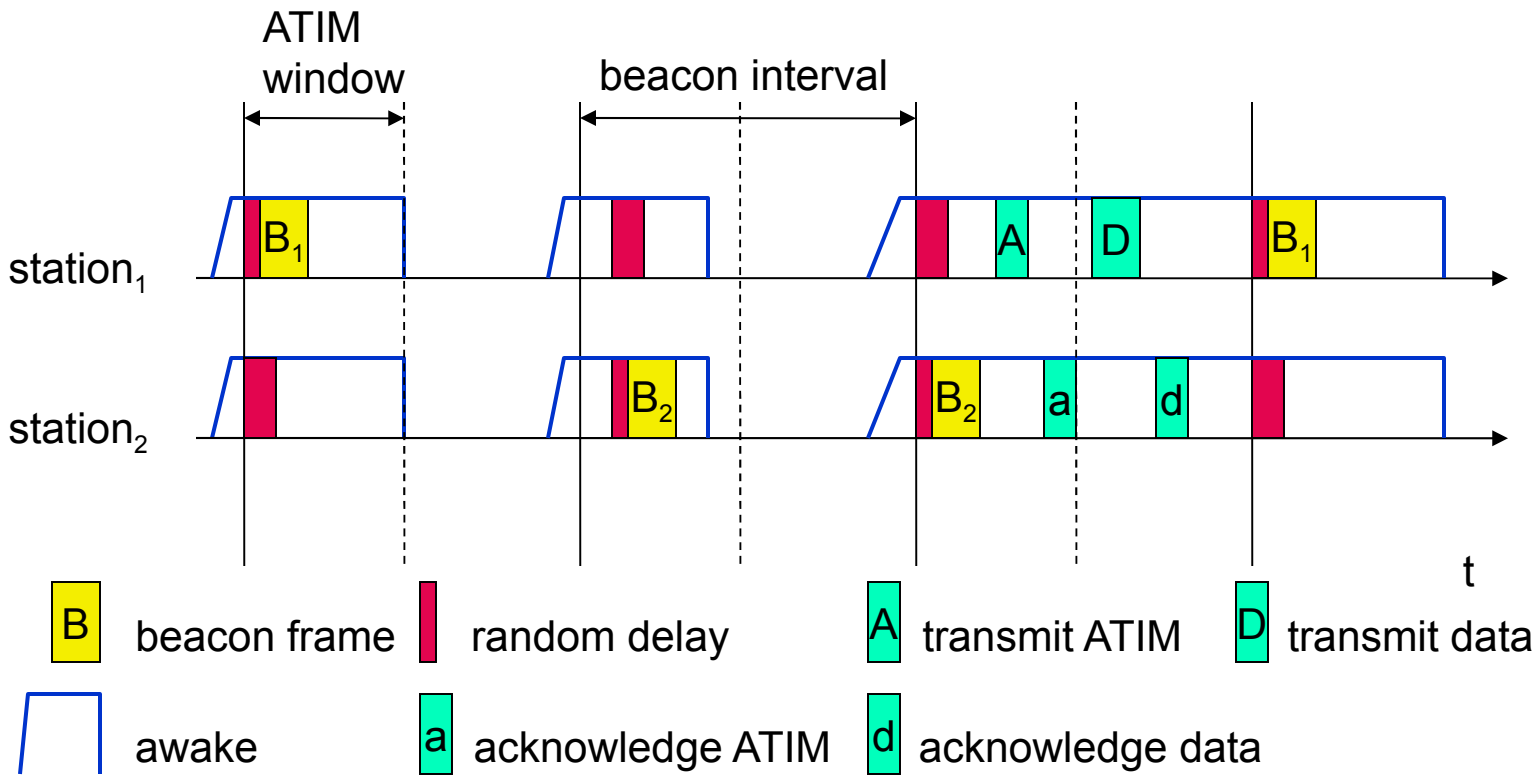
Power management

- Idea: switch the transceiver off if not needed
- States of a station: sleep and awake
- Timing Synchronization Function (TSF)
  - stations wake up at the same time
- Infrastructure
  - Traffic Indication Map (TIM)
    - list of unicast receivers transmitted by AP
  - Delivery Traffic Indication Map (DTIM)
    - list of broadcast/multicast receivers transmitted by AP
- Ad-hoc
  - Ad-hoc Traffic Indication Map (ATIM)
    - announcement of receivers by stations buffering frames
    - more complicated - no central AP
    - collision of ATIMs possible (scalability?)
- APSD (Automatic Power Save Delivery)
  - new method in 802.11e replacing above schemes

Power saving with wake-up patterns (infrastructure)



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



802.11 - Roaming

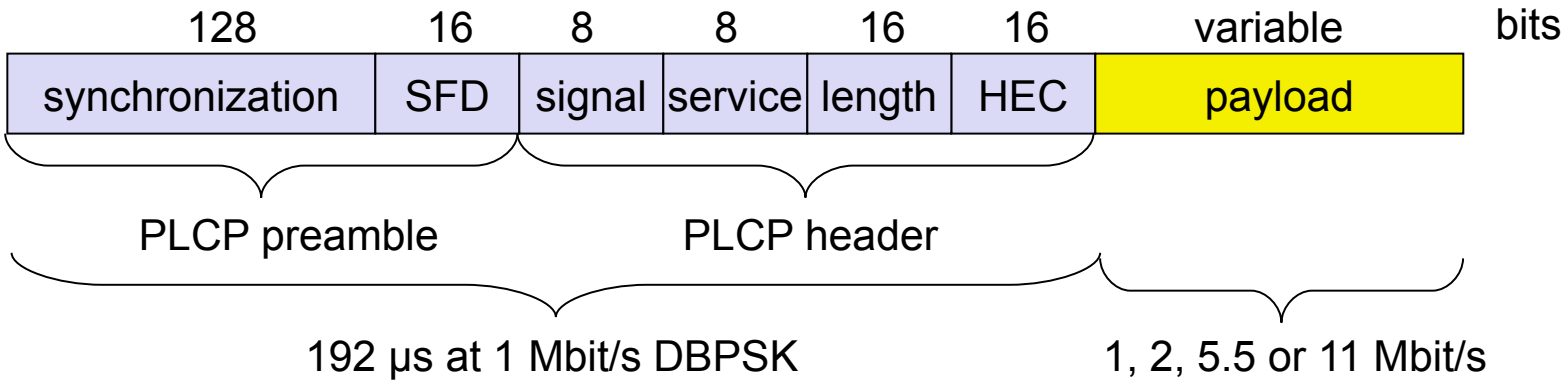
- No or bad connection? Then perform:
- Scanning
  - scan the environment, i.e., listen into the medium for beacon signals or send probes into the medium and wait for an answer
- Reassociation Request
  - station sends a request to one or several AP(s)
- Reassociation Response
  - success: AP has answered,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

WLAN: IEEE 802.11b

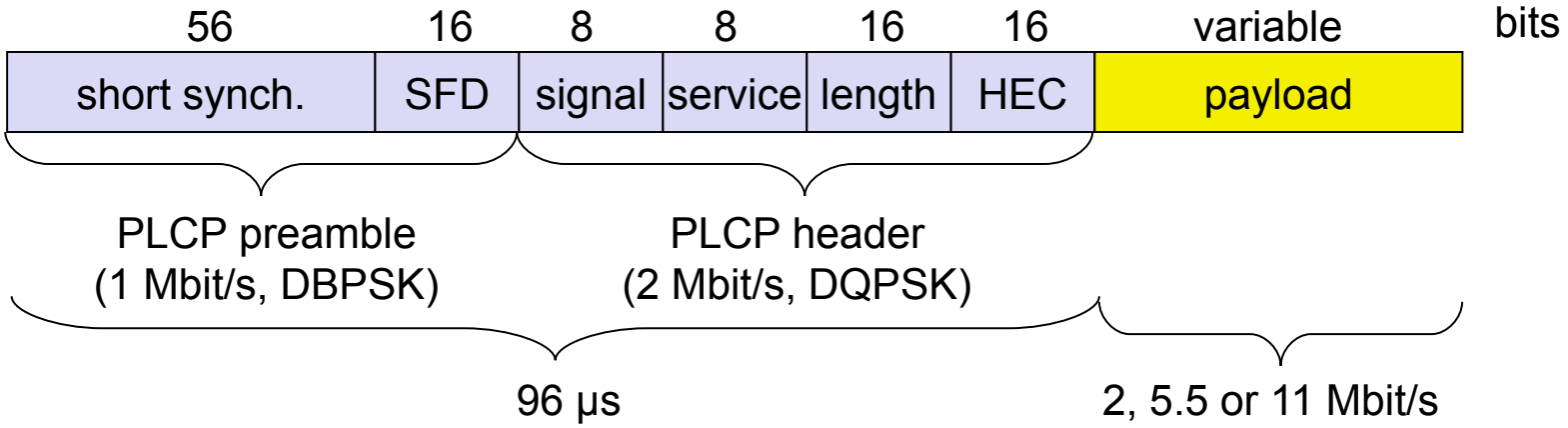
- Data rate
  - 1, 2, 5.5, 11 Mbit/s, depending on SNR
  - User data rate max. approx. 6 Mbit/s
- Transmission range
  - 300m outdoor, 30m indoor
  - Max. data rate ~10m indoor
- Frequency
  - DSSS, 2.4 GHz ISM-band
- Security
  - Limited, WEP insecure, SSID
- Availability
  - Many products, many vendors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

IEEE 802.11b – PHY frame formats

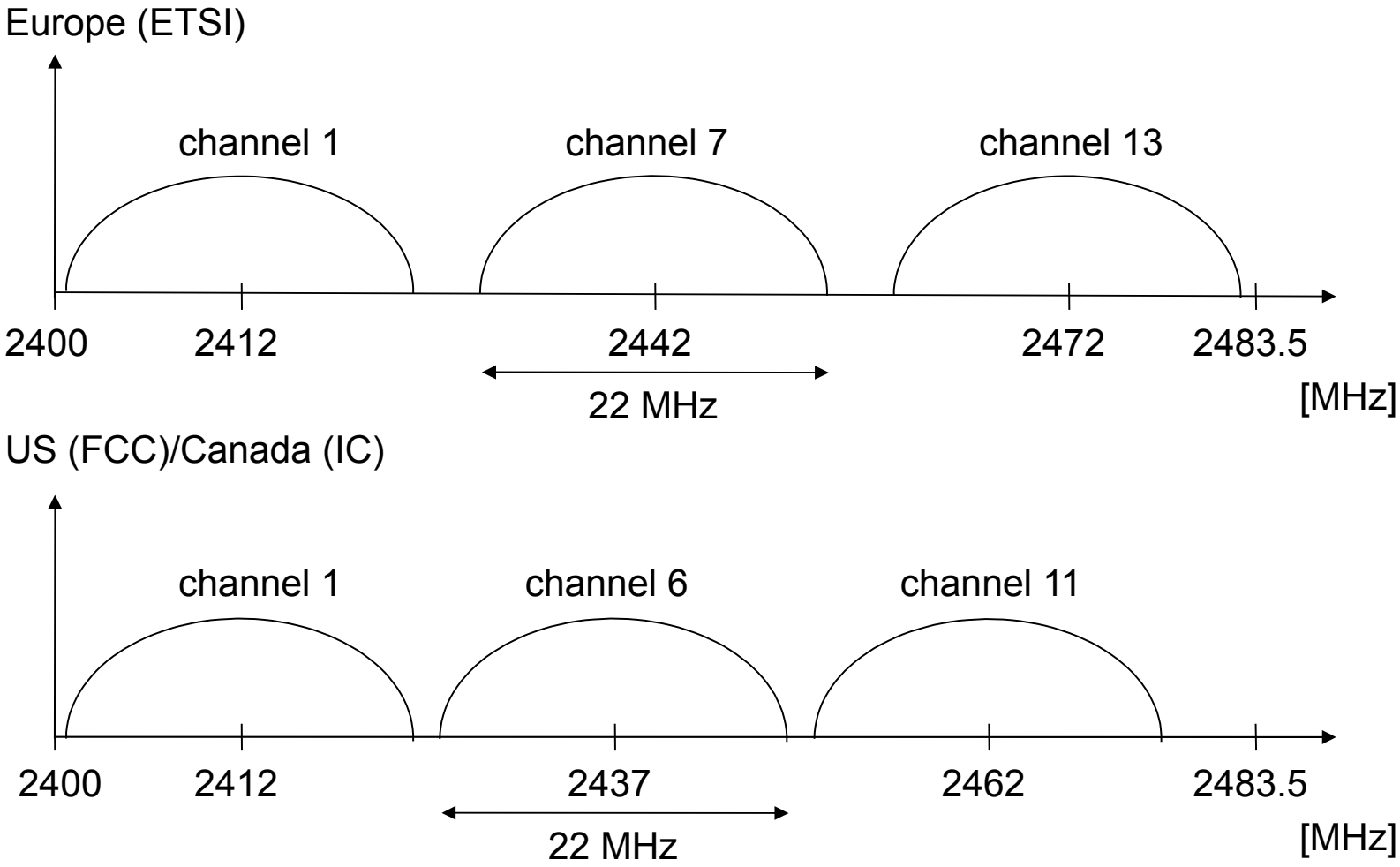
Long PLCP PPDU format



Short PLCP PPDU format (optional)



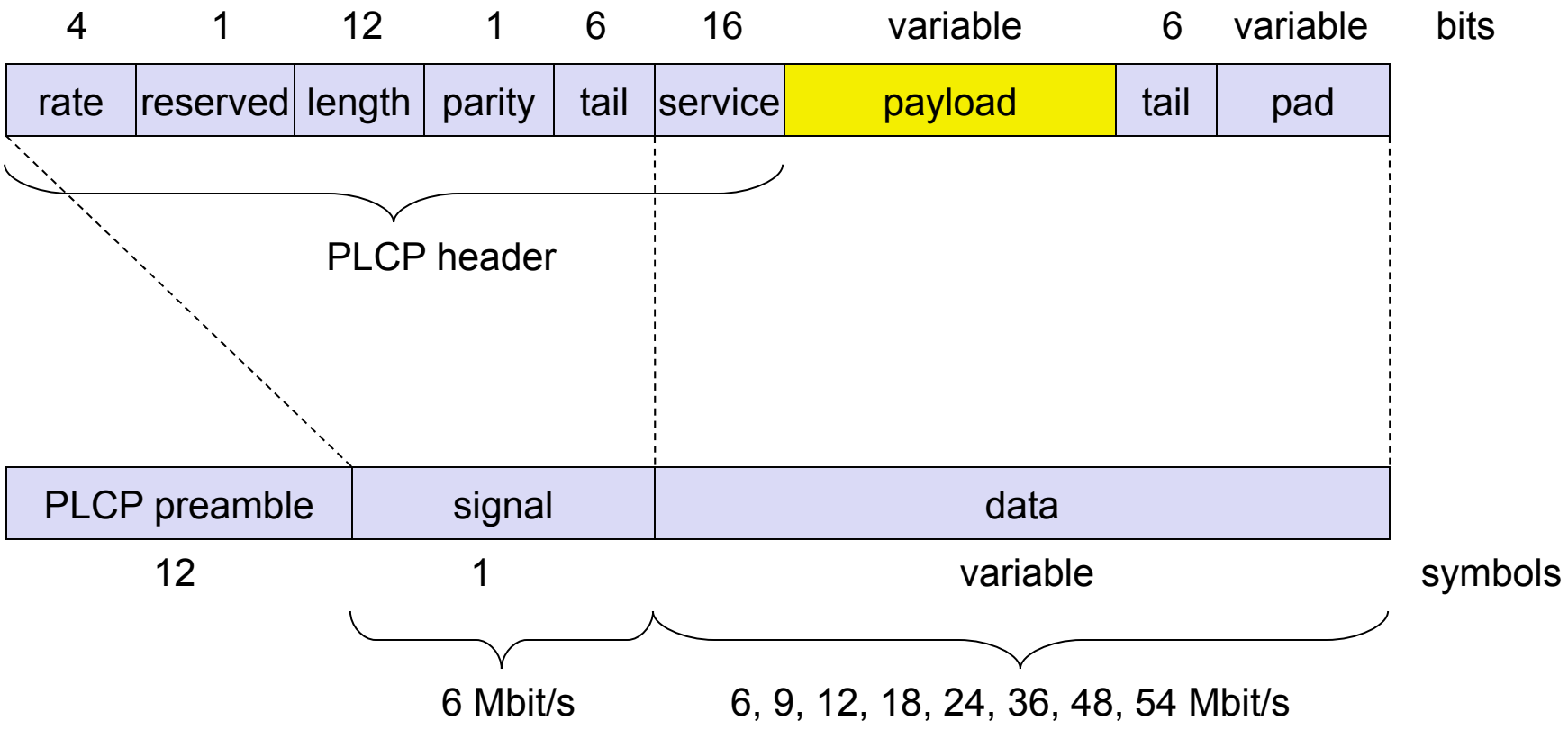
Channel selection (non-overlapping)



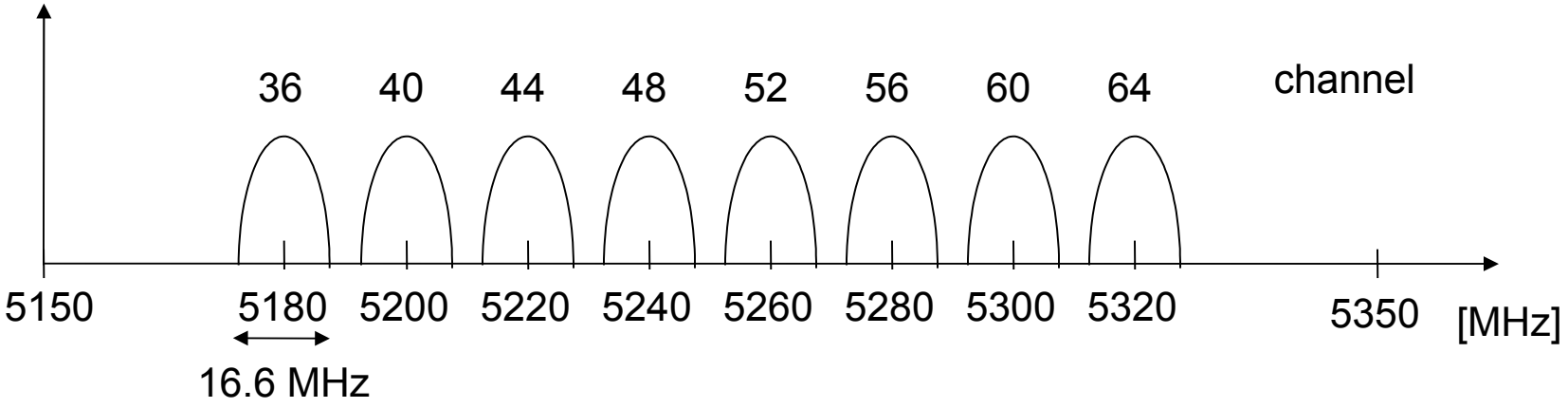
WLAN: IEEE 802.11a

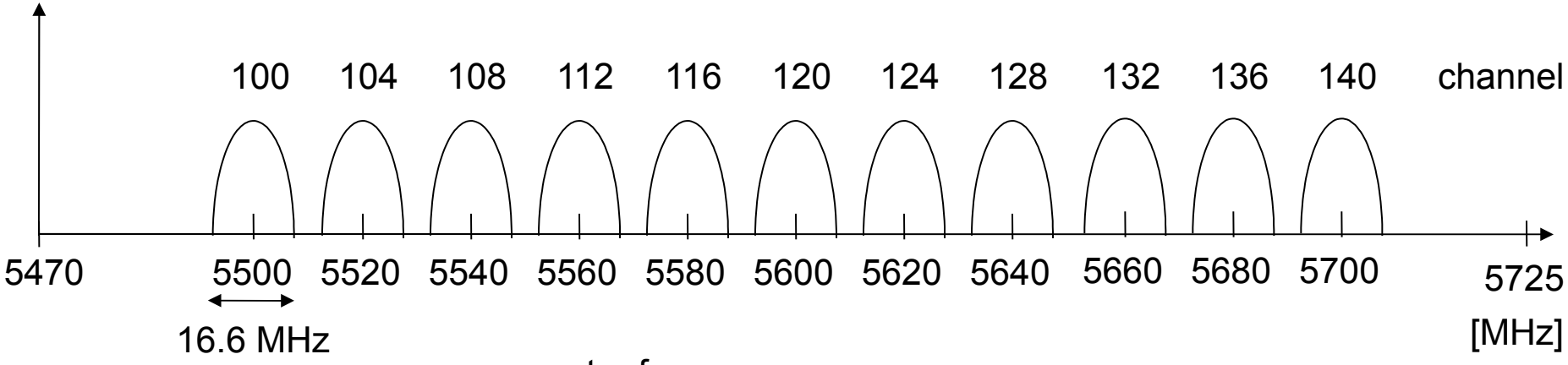
- Data rate
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, depending on SNR
  - User throughput (1500 byte packets): 5.3 (6), 18 (24), 24 (36), 32 (54)
  - 6, 12, 24 Mbit/s mandatory
- Transmission range
  - 100m outdoor, 10m indoor
    - E.g., 54 Mbit/s up to 5 m, 48 up to 12 m, 36 up to 25 m, 24 up to 30m,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

IEEE 802.11a – PHY frame format



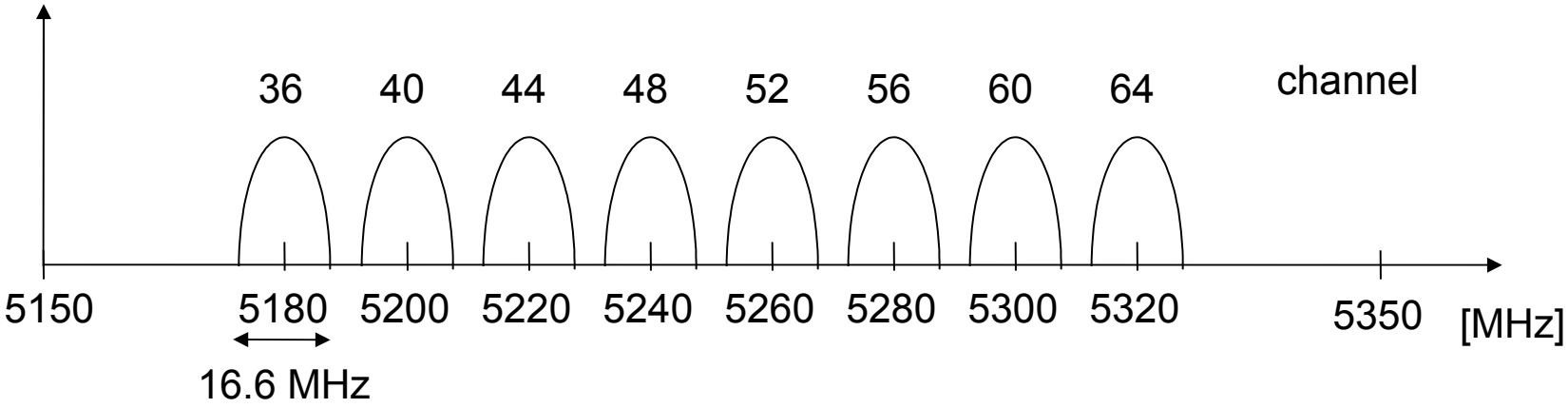
Operating channels of 802.11a in Europe

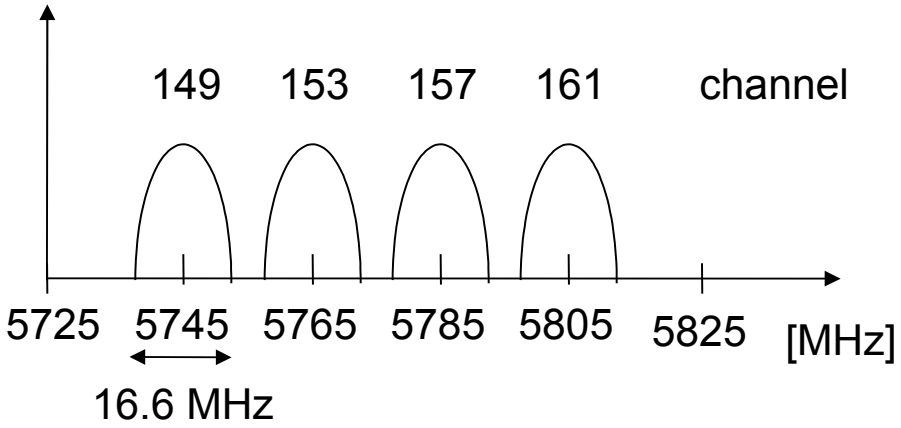




center frequency =
5000 + 5*channel number [MHz]

Operating channels for 802.11a / US U-NII

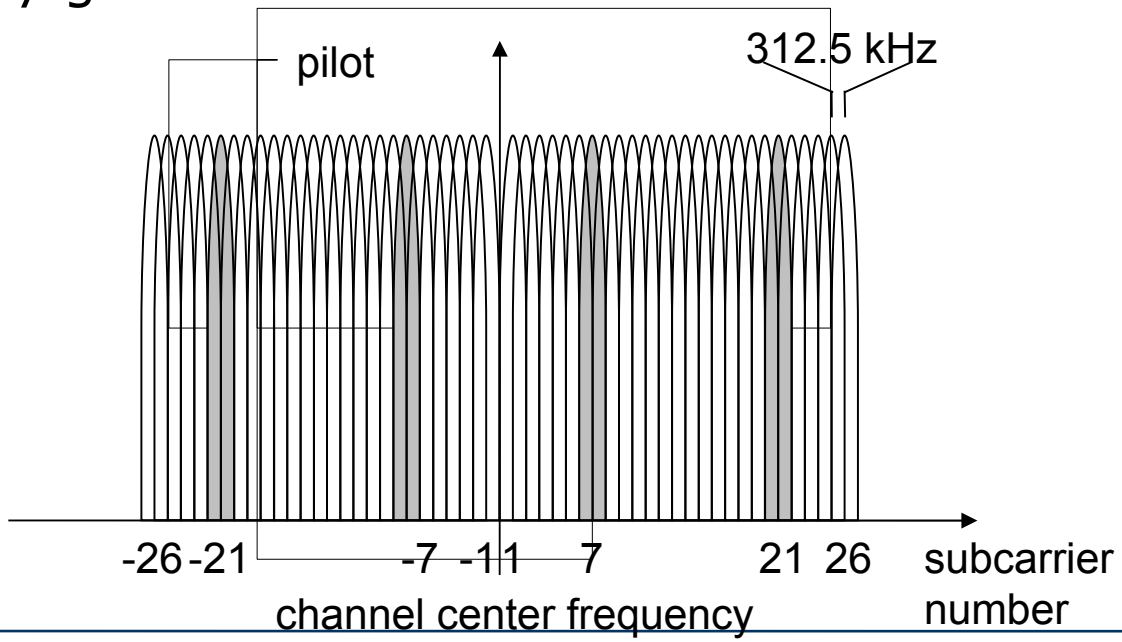




center frequency =
5000 + 5*channel number [MHz]

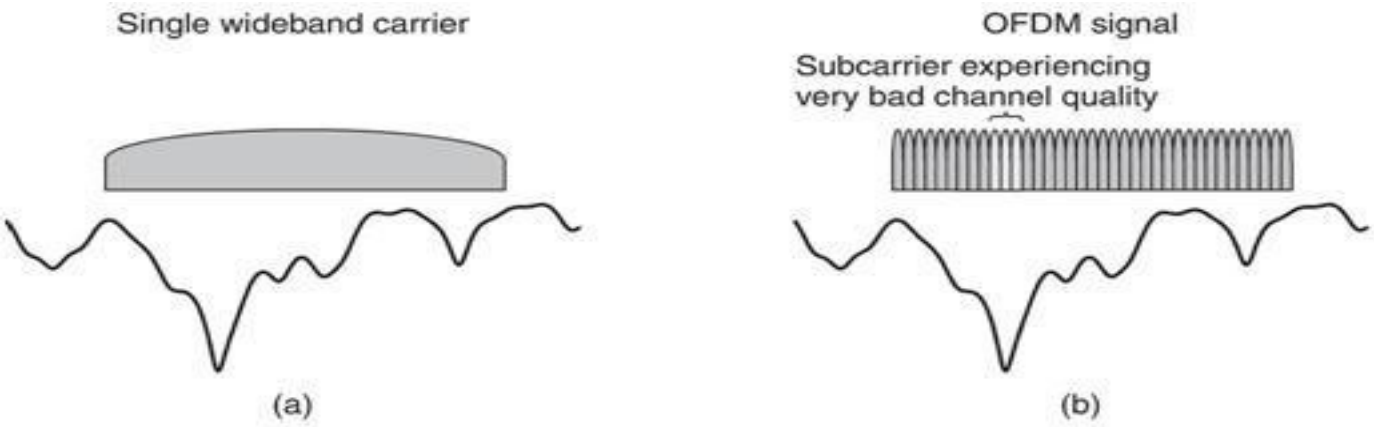
OFDM in IEEE 802.11a

- OFDM may have less than a hundred to several hundreds of subcarriers
  - Splits a high data rate into N parallel streams which are then transmitted by distinct subcarriers
  - Typically 312.5 kHz spacing
  - FDM style → information is spread by hopping in the time-frequency grid



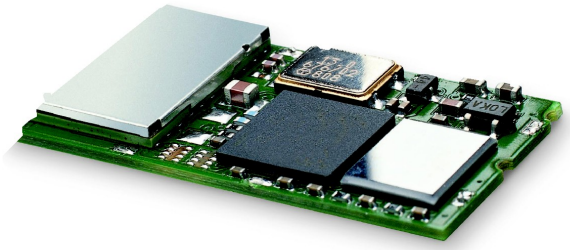
OFDM in 4G/LTE

- OFDM is employed by 4G LTE
  - One such an implementation has around 600 subcarriers and subcarrier spacing of 15kHz
- Frequency interleaving → distributing code bits in the frequency domain
- OFMD disadvantages
  - More complex than a single carrier modulation
  - Demands strict synchronization

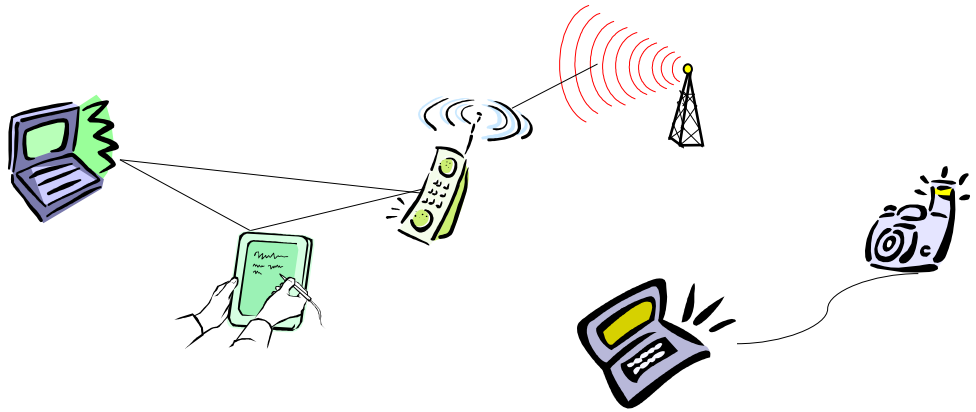


Bluetooth

- Basic idea
  - Universal radio interface for ad-hoc wireless connectivity
  - Interconnecting computer and peripherals, handheld devices, PDAs, cell phones – replacement of IrDA
  - Embedded in other devices, goal: 5€/device (already < 1€)
  - 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).

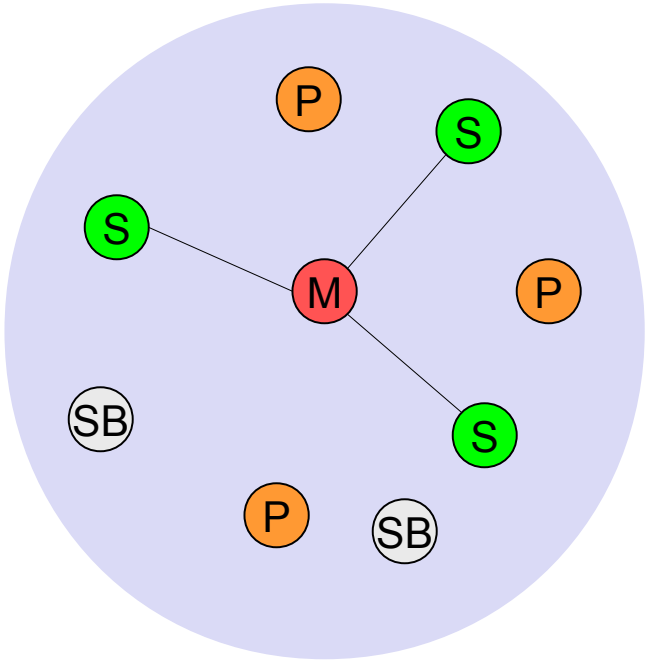


Characteristics

- 2.4 GHz ISM band, 1 MHz carrier spacing
  - Channel 0: 2402 MHz … channel 78: 2480 MHz
  - 1-100 mW transmit power
- FHSS and TDD
  - Frequency hopping
  - Hopping sequence in a pseudo random fashion, determined by a master
  - TDD (time division duplex) – data is transmitted in one direction at a time with transmission alternating between two directions
- Voice link – SCO (Synchronous Connection Oriented)
  - FEC (forward error correction), no retransmission
  - Connection explicitly set up prior to transmitting
- Data link – ACL (Asynchronous ConnectionLess)
  - Asynchronous, packets must be acknowledged
- Topology
  - Overlapping piconets (stars) forming a scatternet

Piconet

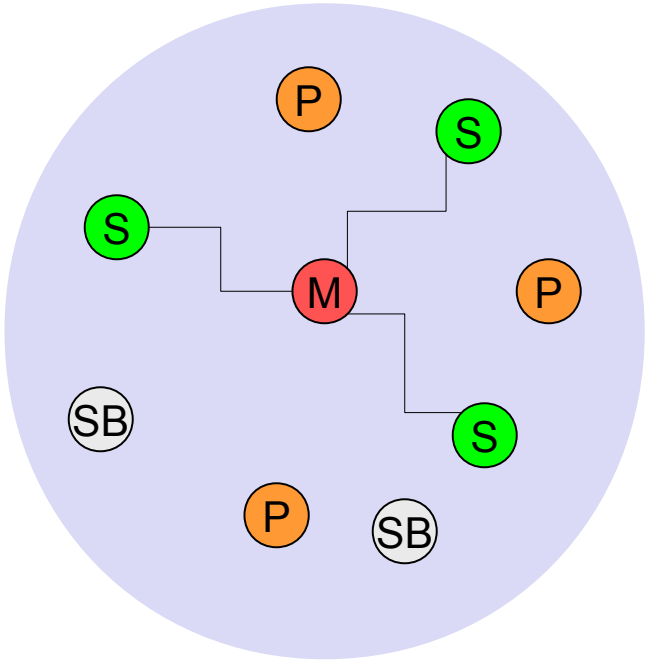
- Collection of devices connected in an ad hoc fashion
- One unit acts as master and the others as slaves for the lifetime of the piconet
- Master determines hopping pattern, slaves have to synchronize
- Each piconet has a unique hopping pattern
- Participation in a piconet = synchronization to hopping sequence
- Each piconet has one master and up to 7 simultaneous slaves (> 200 could be parked)



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

Piconet

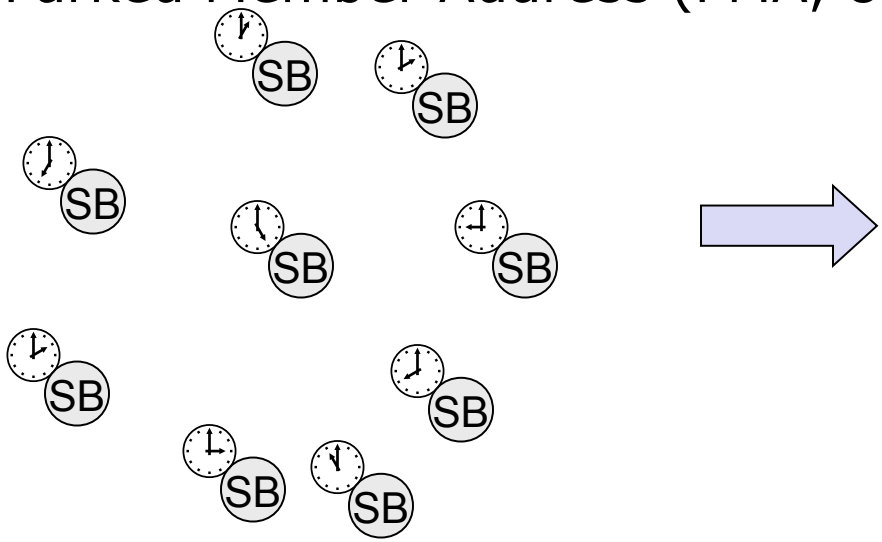
- The Standby state is the default low power state in the Bluetooth unit. Only the native clock is runnning and there is no interaction with any device whatsoever

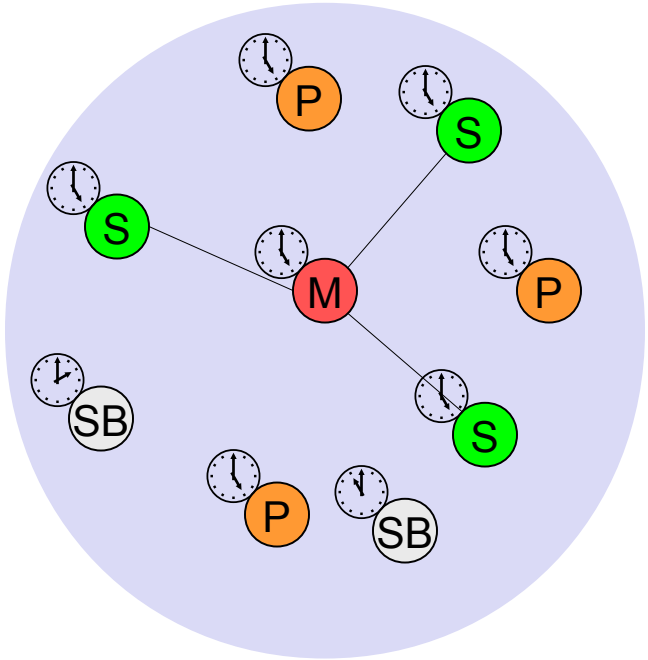


M=Master
S=Slave
P=Parked
SB=Standby

Forming a piconet

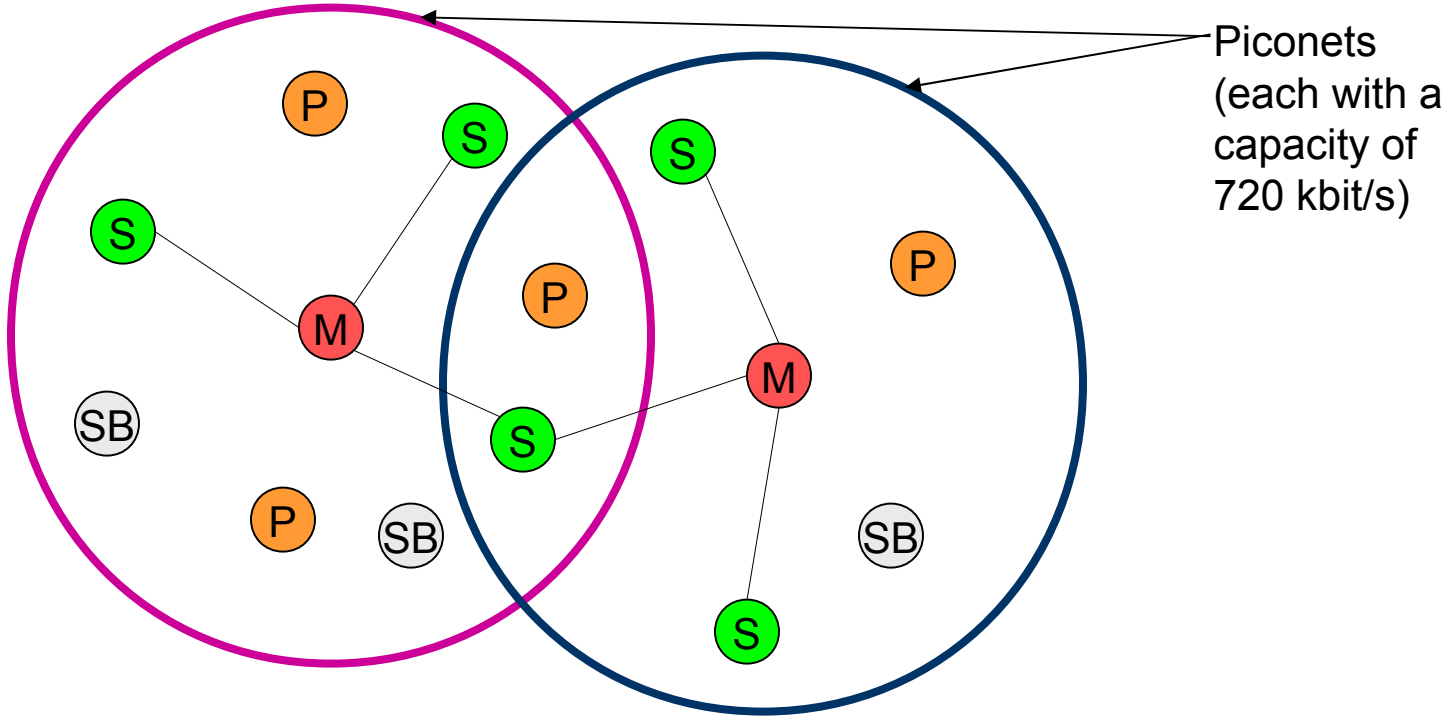
- All devices in a piconet hop together
  - Master gives slaves its clock and device ID
    - Hopping pattern: determined by device ID (48 bit, unique worldwide)
    - Phase in hopping pattern determined by clock
- Addressing
  - Active Member Address (AMA, 3 bit)
  - Parked Member Address (PMA, 8 bit)



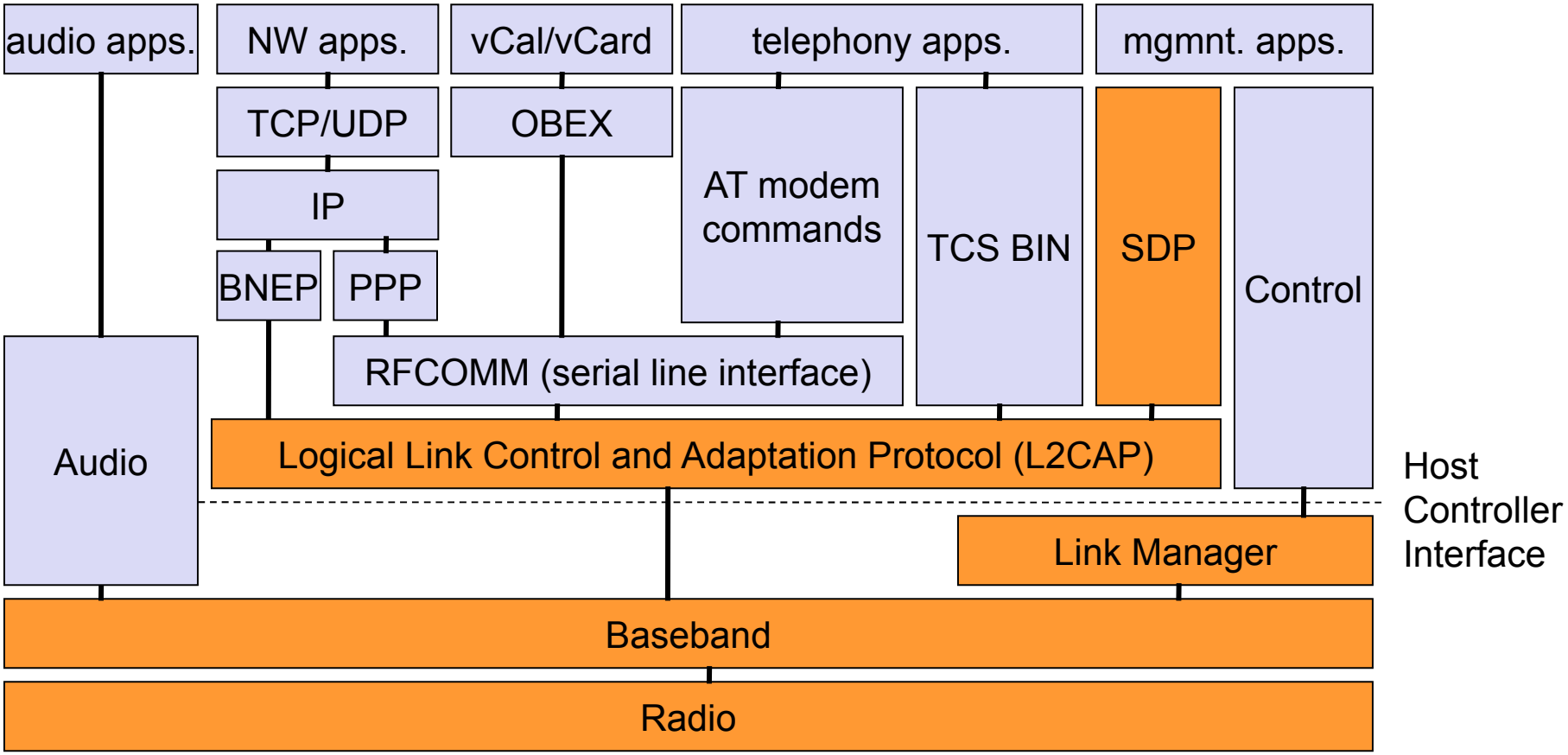


Scatternet

- 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



Bluetooth protocol stack



AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol

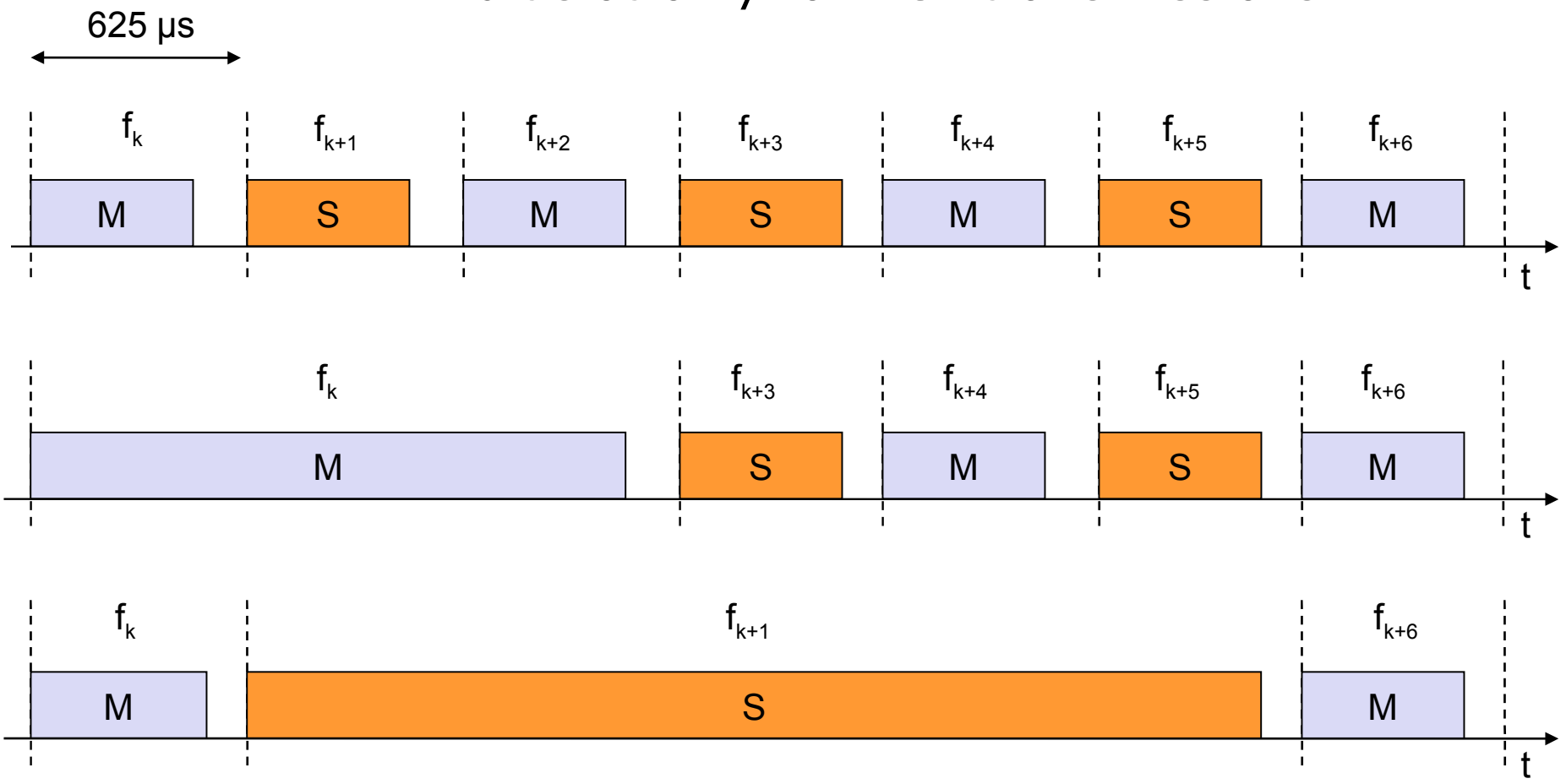
SDP: service discovery protocol
RFCOMM: radio frequency comm.

Radio Layer

- Rather a short document
- Only defines the carrier frequencies and output power
- Bluetooth is targeted to low power devices
- And yes, for interoperable licensed channels
  - So 2.4 GHz
- Uses FHSS for transmission
- The time between hops is 625 microseconds
- Bluetooth power is available in three classes
  - Power class 1 (1~100mW, 100m range)
  - Power class 2 (0.25~2.5mW, typically 1mW, 10m range)
  - Power class 3 (max 1mW, 10m range)

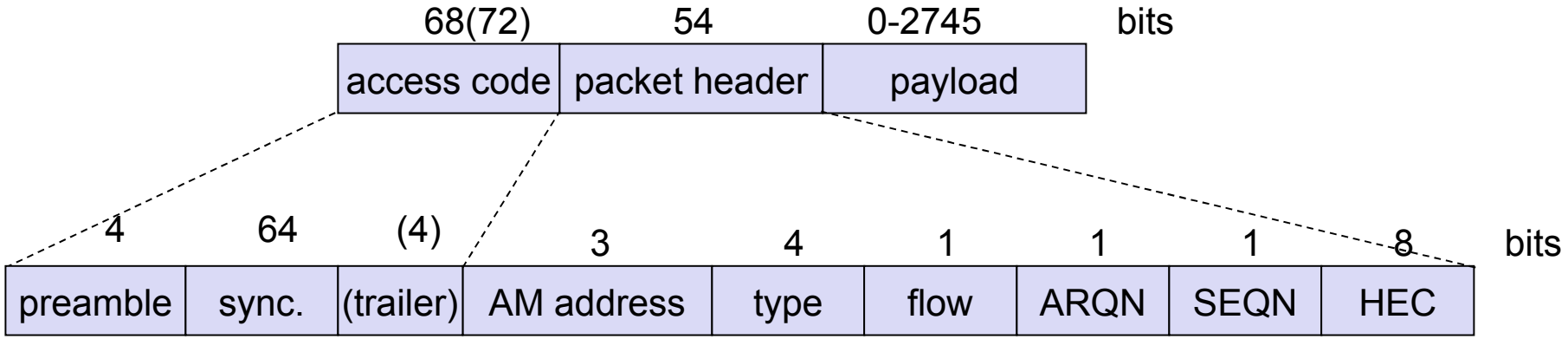
Baseband Layer: Frequency selection during data transmission

multislot only for ACL transmissions



Baseband

- Piconet/channel definition
- Low-level packet definition
  - Access code
    - Channel, device access, trailer (0101 if rightmost bit is 1, 0 otherwise)
  - Packet header
    - 1/3-FEC, active member address (broadcast + 7 slaves), link type, alternating bit ARQ/SEQ, checksum



Packet Header Framing

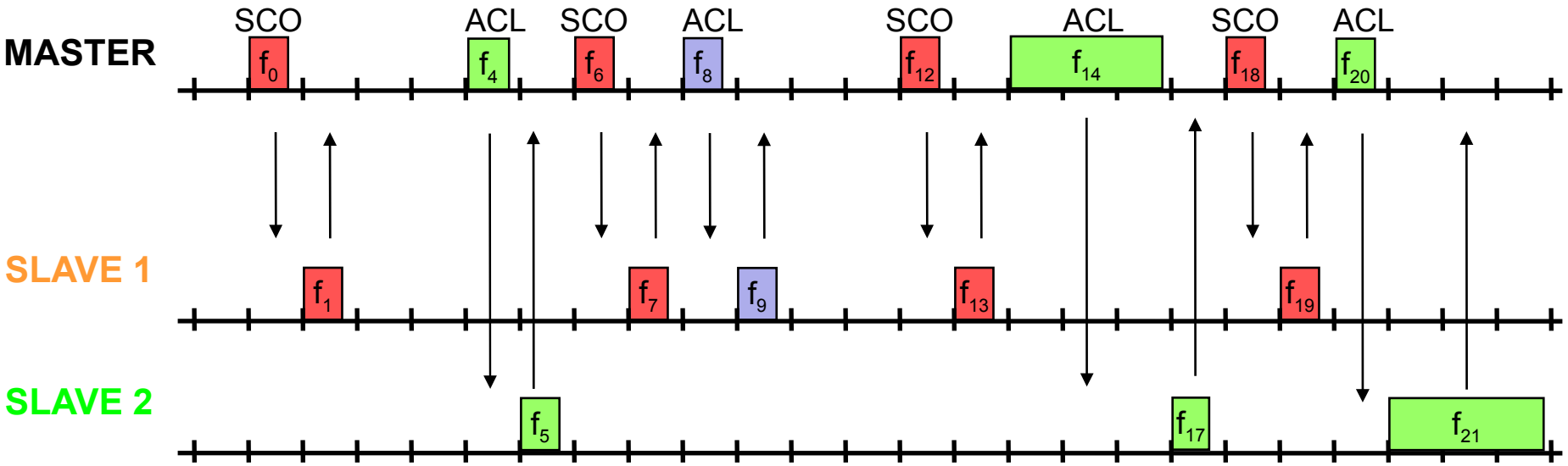
- “AM address” is a 3 bit active member address
- Master to slave → the address is the receiver address
- Slave to master → the address is the sender address
- 0000 value → broadcast
- Type → type of packet (e.g. control packets)
- Flow (1 halt ACL transmission, 0 resume)
- ARQN (1 – ACK, 0 NACK) for ACL transmissions
- SEQN (Sequential number) – packets are labeled between 0/1
- HEC – header error control

Bluetooth link types

- Synchronous connection oriented link (SCO)
  - Similar to phone calls
  - Point to point connections
  - A master can support up to three simultaneous links to the same slave
  - Data and voice
  - No retransmissions
  - Time critical applications
  - Single slot packets
- Asynchronous connectionless link (ACL)
  - Multi point and broadcast transfer mechanisms
  - Retransmission if packet is lost
  - ACK and NACK
  - 1, 3, 5 slot packets allowed

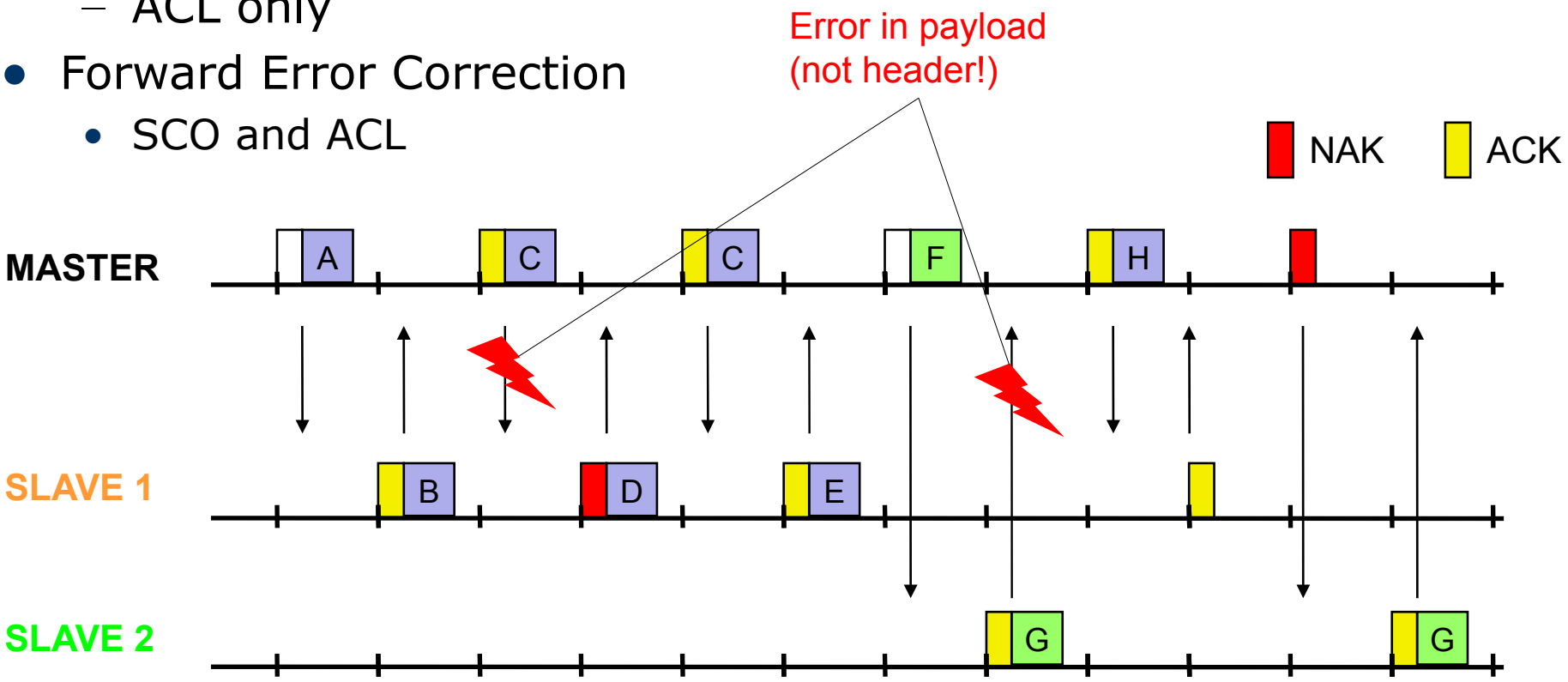
Baseband link types

- Polling-based TDD (time division duplex) 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

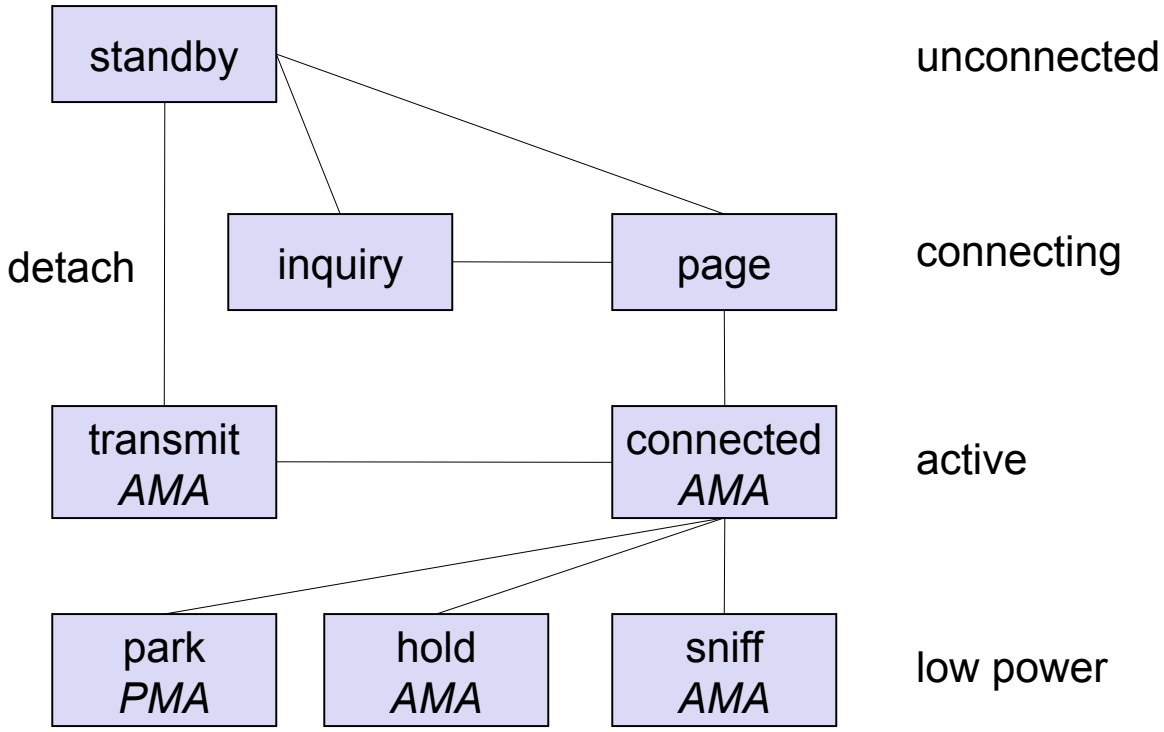
- Slow frequency hopping with hopping patterns determined by a master
  - Protection from interference on certain frequencies
- Retransmission
  - ACL only
- Forward Error Correction
  - SCO and ACL



Link Manager Roles

- Authentication – sets the encryption mode (e.g. no encryption), key size, etc.
- Synchronization – clock offset is updated
- Capability negotiation – Not all features are supported, so devices need to agree the usage of e.g. multi-slot packets, etc.
- Quality of service negotiation – e.g. limit number of slots for slave answers, latency control, FEC protection or no protection, etc.
- Power control – Decrease transmissions according to battery power
- Link supervision – set up new SCO links, destroy
- State transition – changing from unconnected, connected, active and low power modes

Baseband states of a Bluetooth device



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

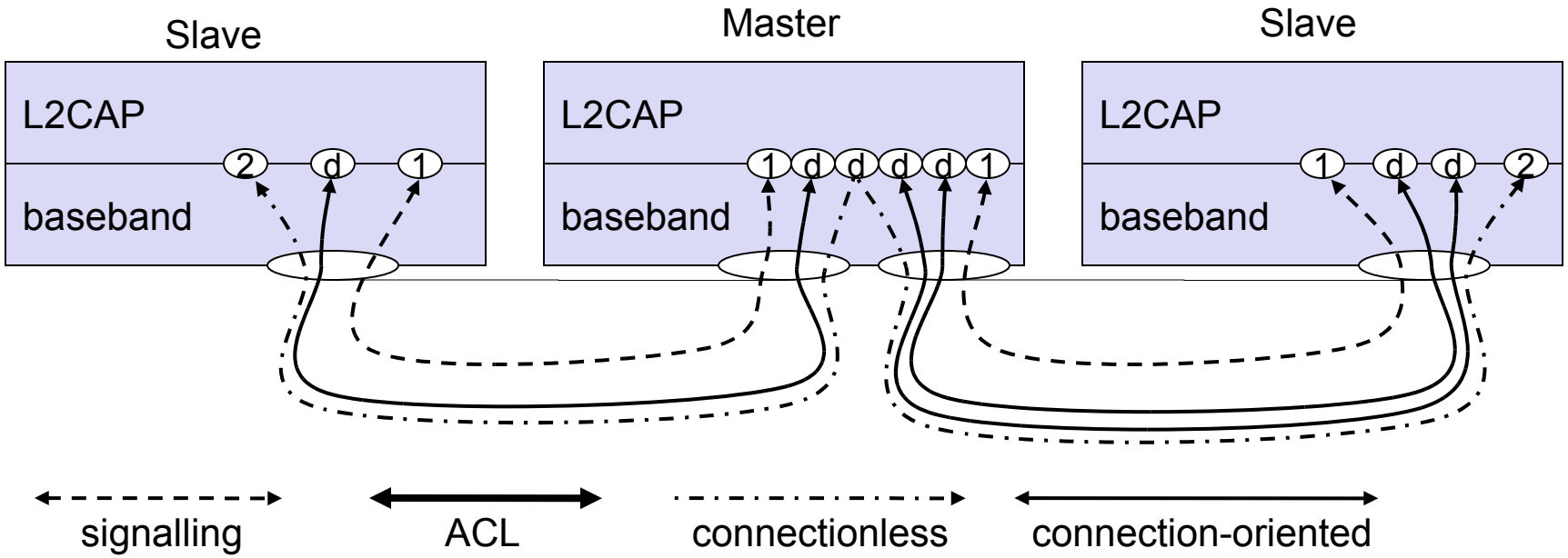
Park: release AMA, get PMA
Sniff: listen periodically, not each slot
Hold: stop ACL, SCO still possible, possibly participate in another piconet

L2CAP - Logical Link Control and Adaptation Protocol

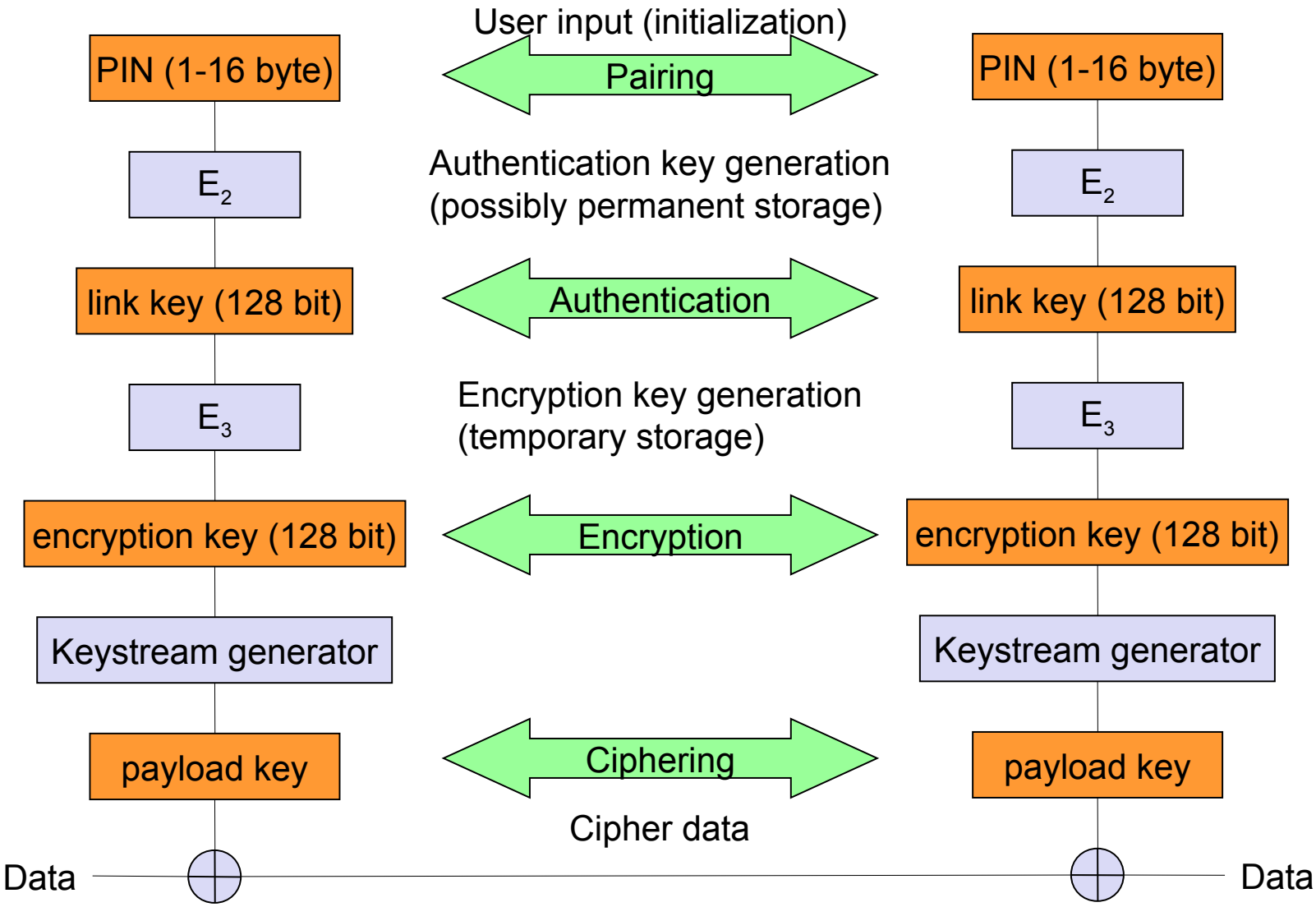
- Simple data link protocol on top of baseband
- Connection oriented, connectionless, and signaling channels
  - Employed to send messages between L2CAP entities
- Segmentation & reassembly
- QoS flow specification per channel
  - Specifies delay, bandwidth, etc.
- Group abstraction
  - Create/close group, add/remove member

L2CAP logical channels

- Why are connectionless links unidirectional?



Security

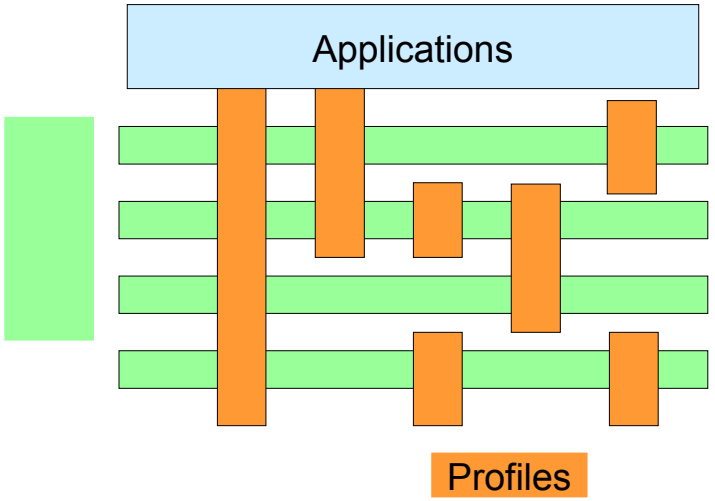

User input (initialization)
PIN (1-16 byte)
Pairing
PIN (1-16 byte)
E2
Authentication key generation
(possibly permanent storage)
E2
link key (128 bit)
Authentication
link key (128 bit)
E3
Encryption key generation
(temporary storage)
E3
encryption key (128 bit)
Encryption
encryption key (128 bit)
Keystream 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,
  - Defines discovery only, not the usage of services
  - Caching of discovered services
  - Gradual discovery

Profiles

- Represent default solutions for a certain usage model
  - Vertical slice through the protocol stack
  - Basis for interoperability
- Service Discovery Application Profile
- Cordless Telephony 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
PAN
Audio Video Remote Control
Basic Printing
Basic Imaging
Extended Service Discovery

Finalizando o Bluetooth

- Leiam o capítulo 7