Unit 3
Wireless Transmission Fundamentals

Preeti Godabole

Topics

- Introduction to narrow and wideband systems;
- Spread spectrum;
- Frequency hopping;
- Introduction to MIMO;
  - MIMO Channel Capacity and diversity gain;
- Introduction to OFDM; MIMO-OFDM system;
- Multiple access control (FDMA, TDMA, CDMA, SDMA);
- **Wireless local area network;**
- Wireless personal area network (Bluetooth and ZigBee)

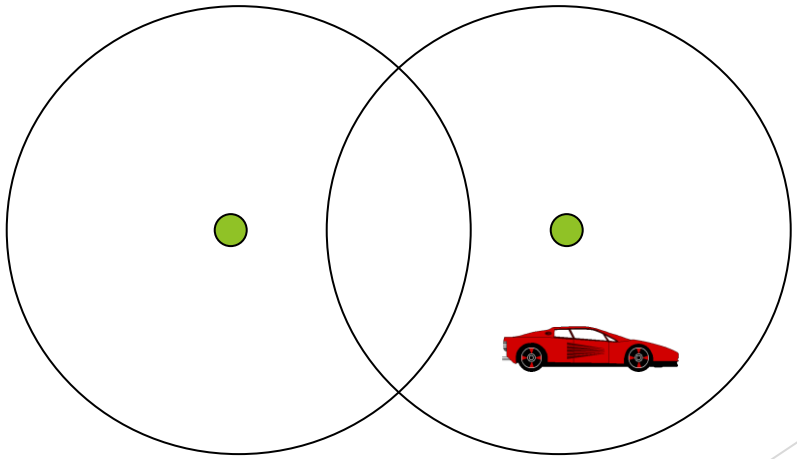
Goal of WLANs is to replace office cabling, to enable tetherless access to the internet and, to introduce a higher flexibility for ad-hoc communication in, e.g., group meetings.

Wireless networks

- Access computing/communication services, on the move
- Cellular Networks
  - traditional base station infrastructure systems
- Wireless LANs
  - infrastructure as well as ad-hoc networks possible
  - very flexible within the reception area
  - low bandwidth compared to wired networks (1-10 Mbit/s)
- Multihop Ad hoc Networks
  - useful when infrastructure not available, impractical, or expensive
  - military applications, rescue, home networking

Cellular Wireless

- Single hop wireless connectivity to the wired world
  - Space divided into cells, and hosts assigned to a cell
  - A base station is responsible for communicating with hosts/nodes in its cell
  - Mobile hosts can change cells while communicating
  - Hand-off occurs when a mobile host starts communicating via a new base station



Evolution of cellular networks

- First-generation: Analog cellular systems (450-900 MHz)
  - Frequency shift keying; FDMA for spectrum sharing
  - NMT (Europe), AMPS (US)
- Second-generation: Digital cellular systems (900, 1800 MHz)
  - TDMA/CDMA for spectrum sharing; Circuit switching
  - GSM (Europe), IS-136 (US), PDC (Japan)
  - <9.6kbps data rates
- 2.5G: Packet switching extensions
  - Digital: GSM to GPRS; Analog: AMPS to CDPD
  - <115kbps data rates
- 3G: Full-fledged data services
  - High speed, data and Internet services
  - IMT-2000, UMTS
  - <2Mbps data rates

Characteristics of wireless LANs

Advantages

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

Disadvantages

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

Design goals for wireless LANs

- global, seamless operation
- low power for battery use
- no special permissions or licenses needed to use the LAN
- robust transmission technology
- simplified spontaneous cooperation at meetings
- easy to use for everyone, simple management
- protection of investment in wired networks
- security (no one should be able to read my data), privacy (no one should be able to collect user profiles), safety (low radiation)
- transparency concerning applications and higher layer protocols, but also location awareness if necessary

Comparison: infrared vs. radio transmission

- **Infrared**
  - uses IR diodes, diffuse light, multiple reflections (walls, furniture etc.)

Advantages

- simple, cheap, available in many mobile devices
- no licenses needed
- simple shielding possible

Disadvantages

- interference by sunlight, heat sources etc.
- many things shield or absorb IR light
- low bandwidth
- Example
- IrDA (Infrared Data Association) interface available everywhere

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

Advantages

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

Disadvantages

- very limited license free frequency bands
- shielding more difficult, interference with other electrical devices
- Example
- WaveLAN, HIPERLAN, Bluetooth

Wireless LANs

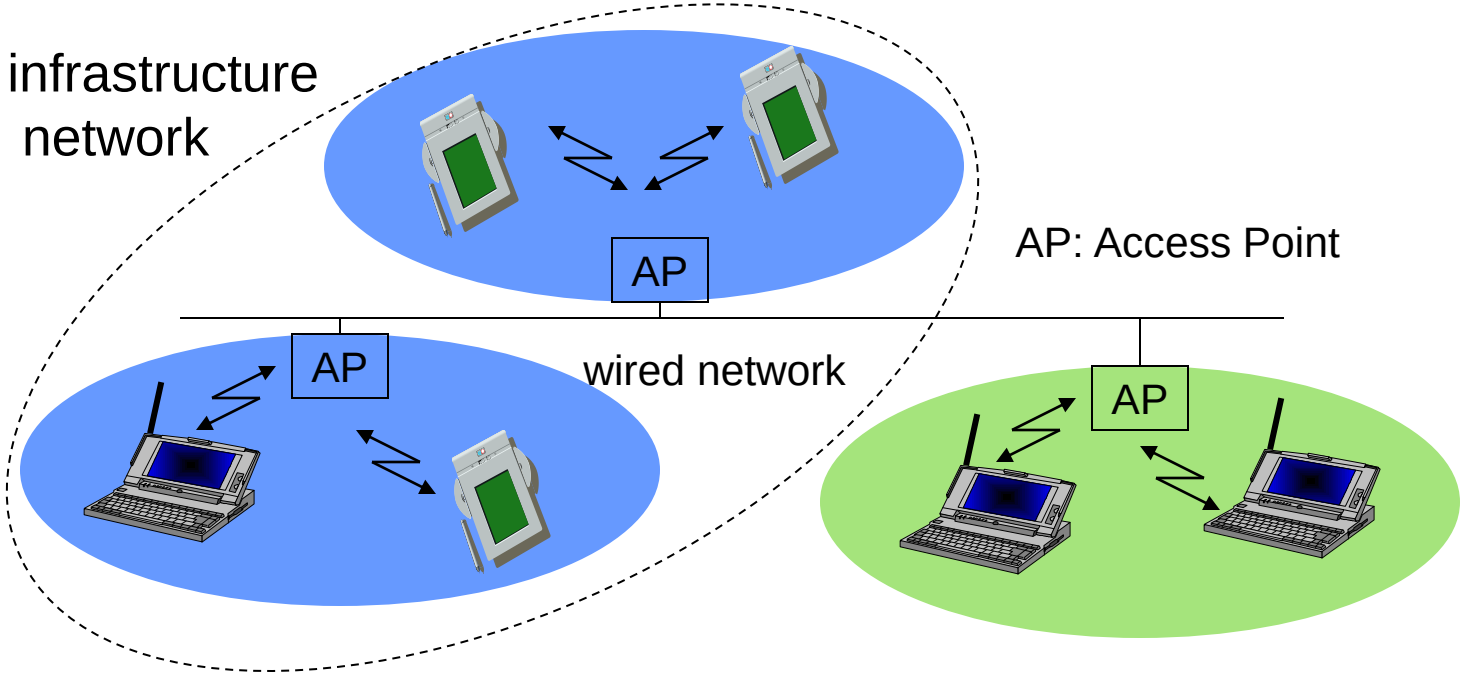
- Infrared (IrDA) or radio links (Wavelan)

- Advantages
  - very flexible within the reception area
  - Ad-hoc networks possible
  - (almost) no wiring difficulties
- Disadvantages
  - low bandwidth compared to wired networks
  - many proprietary solutions
    - Bluetooth, HiperLAN and IEEE 802.11

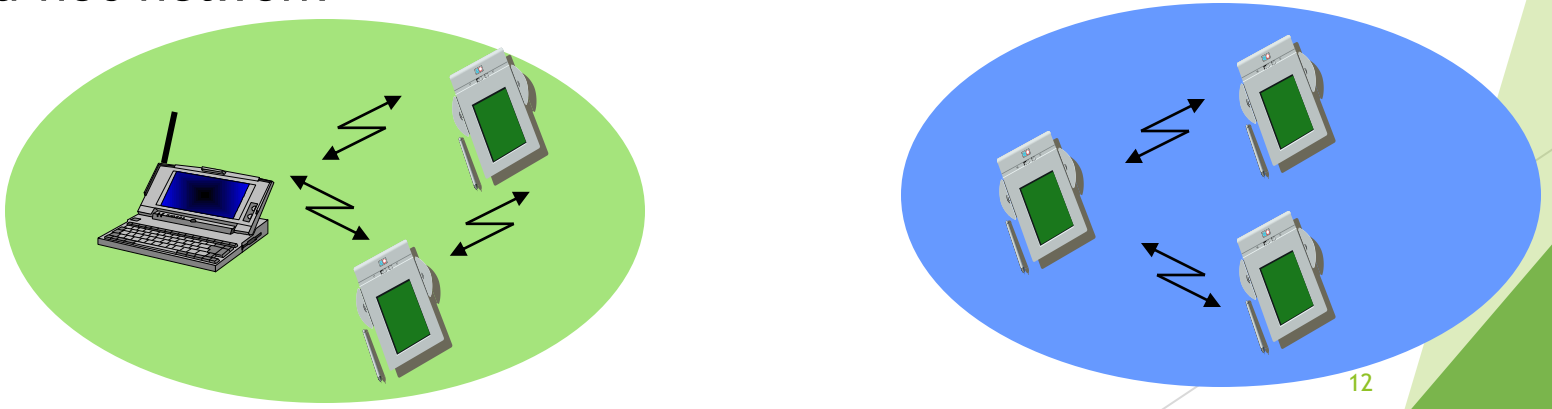
Wireless LANs vs. Wired LANs

- Destination address does not equal destination location
- The media impact the design
- wireless LANs intended to cover reasonable geographic distances must be built from basic coverage blocks
- Impact of handling mobile (and portable) stations
- Propagation effects
- Mobility management
- Power management

Infrastructure vs. Ad hoc WLANs



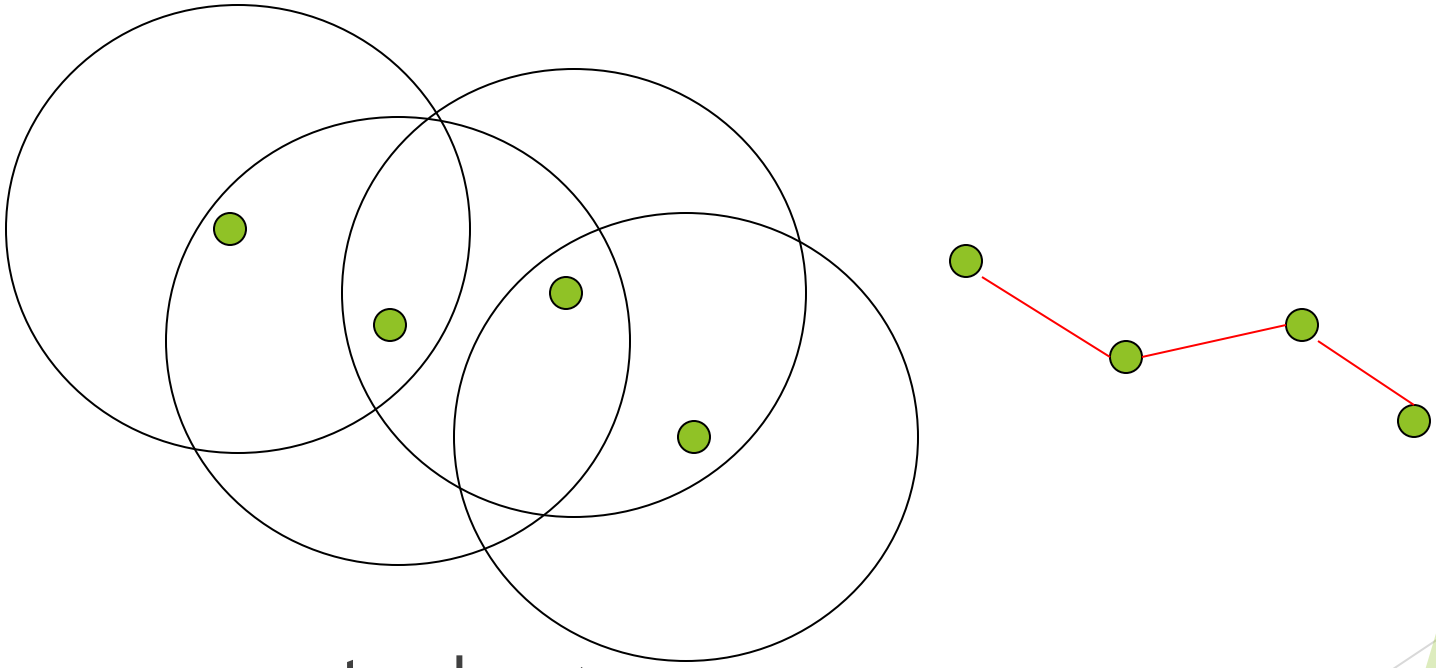
ad-hoc network



Source: Schiller

Multi-Hop Wireless

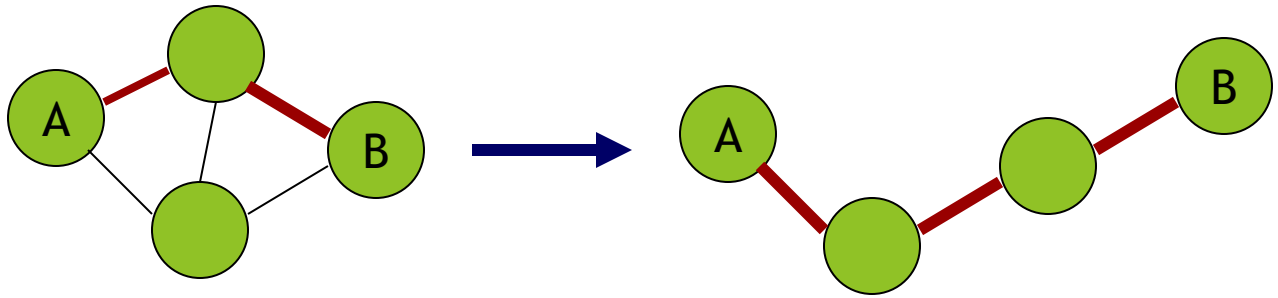
- May need to traverse multiple links to reach destination



- Mobility causes route changes

Mobile Ad Hoc Networks (MANET)

- Do not need backbone infrastructure support
- Host movement frequent
- Topology change frequent

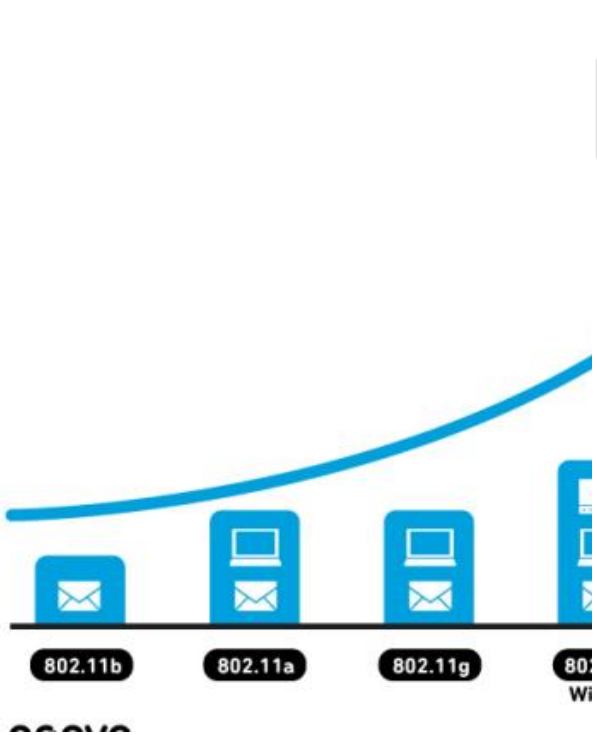


- Multi-hop wireless links
- Data must be routed via intermediate nodes

Applications of MANETS

- Military - soldiers at Kargil, tanks, planes
- Disaster Management – Orissa, Gujarat
- Emergency operations – search-and-rescue, police and firefighters
- Sensor networks
- Taxicabs and other closed communities
- airports, sports stadiums etc. where two or more people meet and want to exchange documents
- Presently MANET applications use 802.11 hardware
- Personal area networks - Bluetooth

Wireless Lan 802.11 Evolution



IEEE 802.11 Protocol	Release Date	Frequency Band(s)	Bandwidth	Max Throughput
802.11-1997	1997	2.4	22	2 Mbps
11b	1999	2.4	22	11 Mbps
11a	1999	5	20	54 Mbps
11g	2003	2.4	20	54 Mbps
11n (Wi-Fi 4)	2009	2.4/5	20/40	600 Mbps
11ac (Wi-Fi 5)	2013	2.4/5	20/40/ 80/160	6.8 Gbps
11ax (Wi-Fi 6)	2019	2.5/5	20/40/ 80/160	10 Gbps

Challenges of Wireless Communications

Wireless Media

- Physical layers used in wireless networks

- have neither absolute nor readily observable boundaries outside which stations are unable to receive frames are unprotected from outside signals
- communicate over a medium significantly less reliable than the cable of a wired network

- have dynamic topologies

- lack full connectivity and therefore the assumption normally made that every station can hear every other station in a LAN is invalid (i.e., STAs may be “hidden” from each other)

- have time varying and asymmetric propagation properties

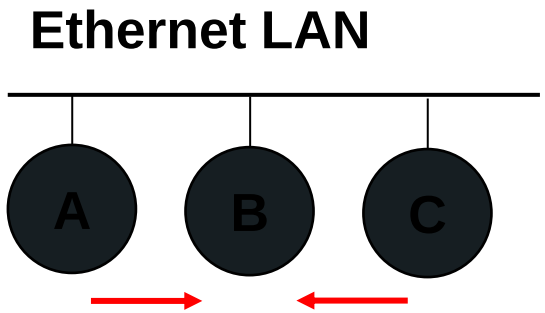
Limitations of the mobile environment

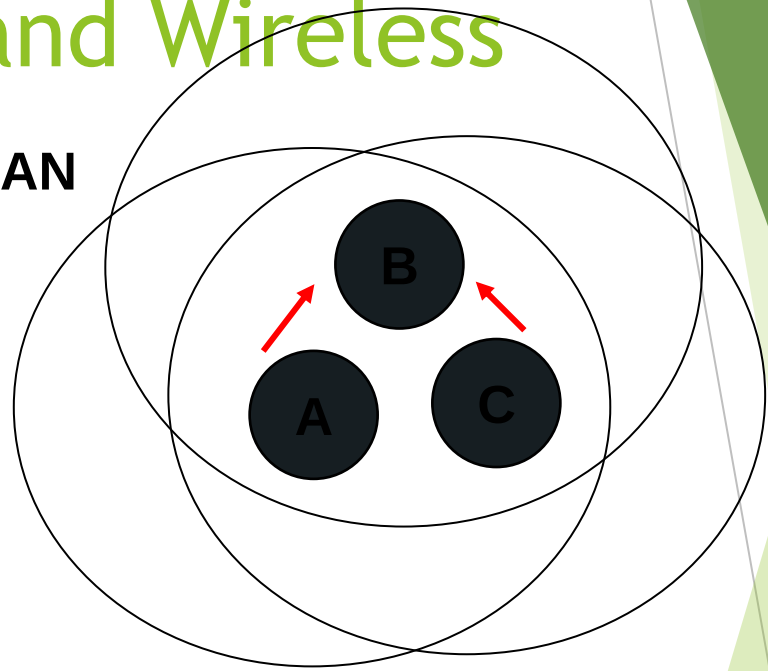
- Limitations of the Wireless *Network*
  - limited communication bandwidth
  - frequent disconnections
  - heterogeneity of fragmented networks
- Limitations Imposed by *Mobility*
  - route breakages
  - lack of mobility awareness by system/applications
- Limitations of the Mobile *Device*
  - short battery lifetime
  - limited capacities

Wireless v/s Wired networks

- Regulations of frequencies
  - Limited availability, coordination is required
  - useful frequencies are almost all occupied
- Bandwidth and delays
  - Low transmission rates
    - few Kbps to some Mbps.
  - Higher delays
    - several hundred milliseconds
  - Higher loss rates
    - susceptible to interference, e.g., engines, lightning
- Always shared medium
  - Lower security, simpler active attacking
  - radio interface accessible for everyone
  - Fake base stations can attract calls from mobile phones
  - secure access mechanisms important

Difference Between Wired and Wireless





- If both A and C sense the channel to be idle at the same time, they send at the same time.
- Collision can be detected *at sender* in Ethernet.
- Half-duplex radios in wireless cannot detect collision at sender.

Effect of mobility on protocol stack

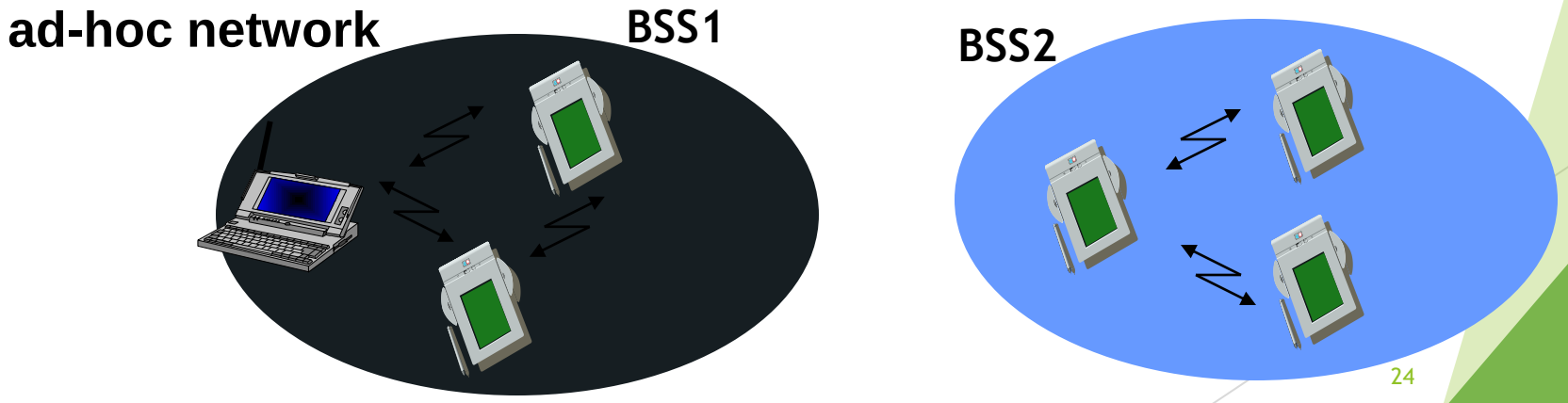
- Application
  - new applications and adaptations
- Transport
  - congestion and flow control
- Network
  - addressing and routing
- Link
  - media access and handoff
- Physical
  - transmission errors and interference

802.11-based Wireless LANs Architecture and Physical Layer

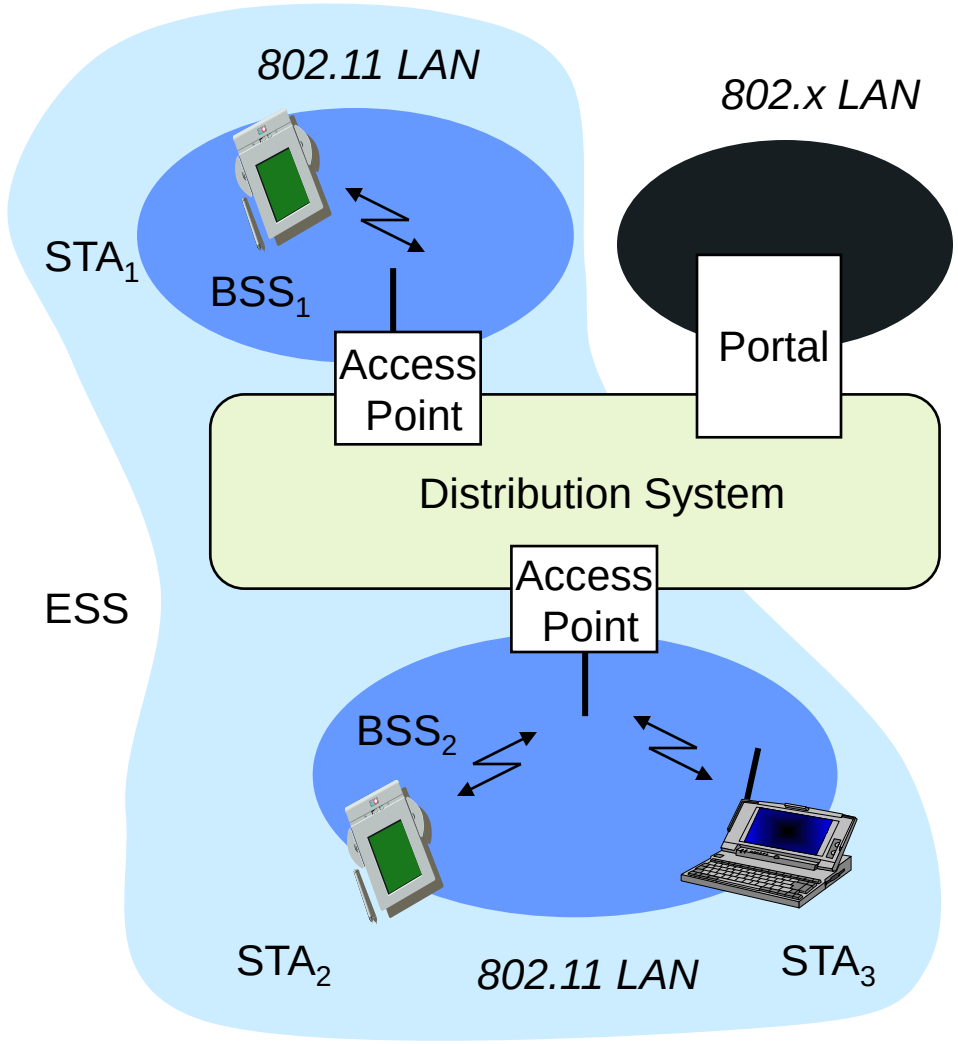
The **primary goal** of the standard was the specification of a simple and robust WLAN which offers time-bounded and asynchronous services. The MAC layer should be able to operate with multiple physical layers, each of which exhibits a different medium sense and transmission characteristic

Components of IEEE 802.11 architecture

- The basic service set (BSS) is the basic building block of an IEEE 802.11 LAN
- The ovals can be thought of as the coverage area within which member stations can directly communicate
- The Independent BSS (IBSS) is the simplest LAN. It may consist of as few as two stations



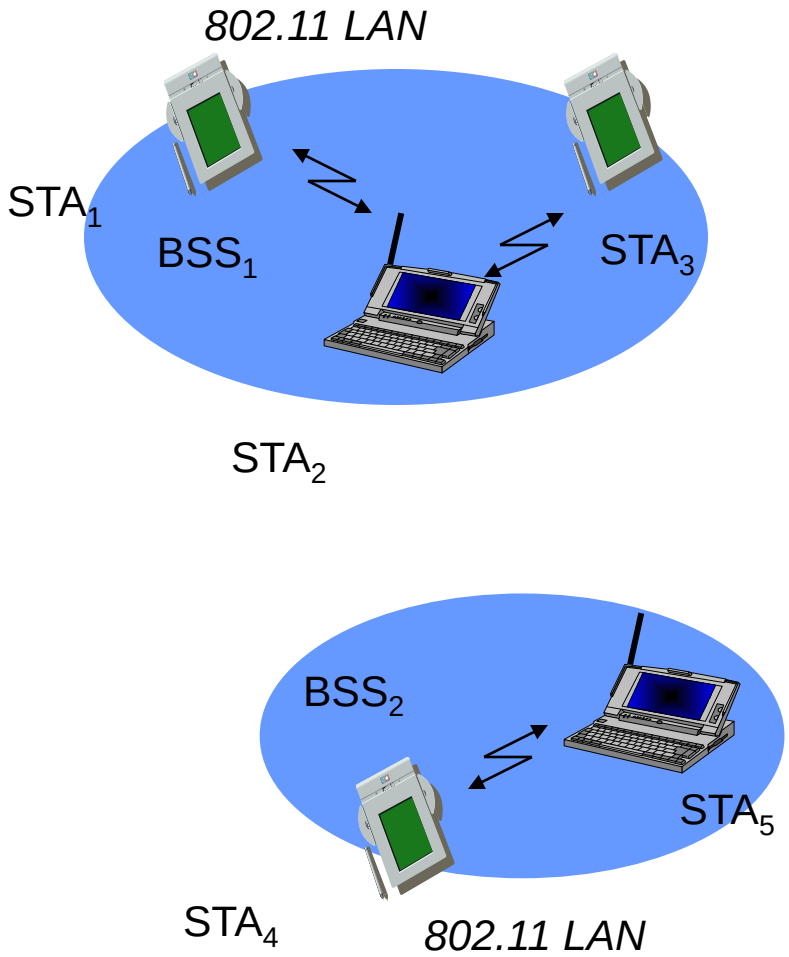
802.11 - infrastructure network



- 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

Source: Schiller

802.11 - ad-hoc network



- Direct communication within a limited range
  - Station (STA):
    terminal with access mechanisms to the wireless medium
  - Basic Service Set (BSS):
    group of stations using the same radio frequency

Source: Schiller

Distribution System (DS) concepts

- The Distribution system interconnects multiple BSSs
- 802.11 standard logically separates the wireless medium from the distribution system – it does not preclude, nor demand, that the multiple media be same or different
- An Access Point (AP) is a STA that provides access to the DS by providing DS services in addition to acting as a STA.
- Data moves between BSS and the DS via an AP
- The DS and BSSs allow 802.11 to create a wireless network of arbitrary size and complexity called the Extended Service Set network (ESS)

Extended Service Set network

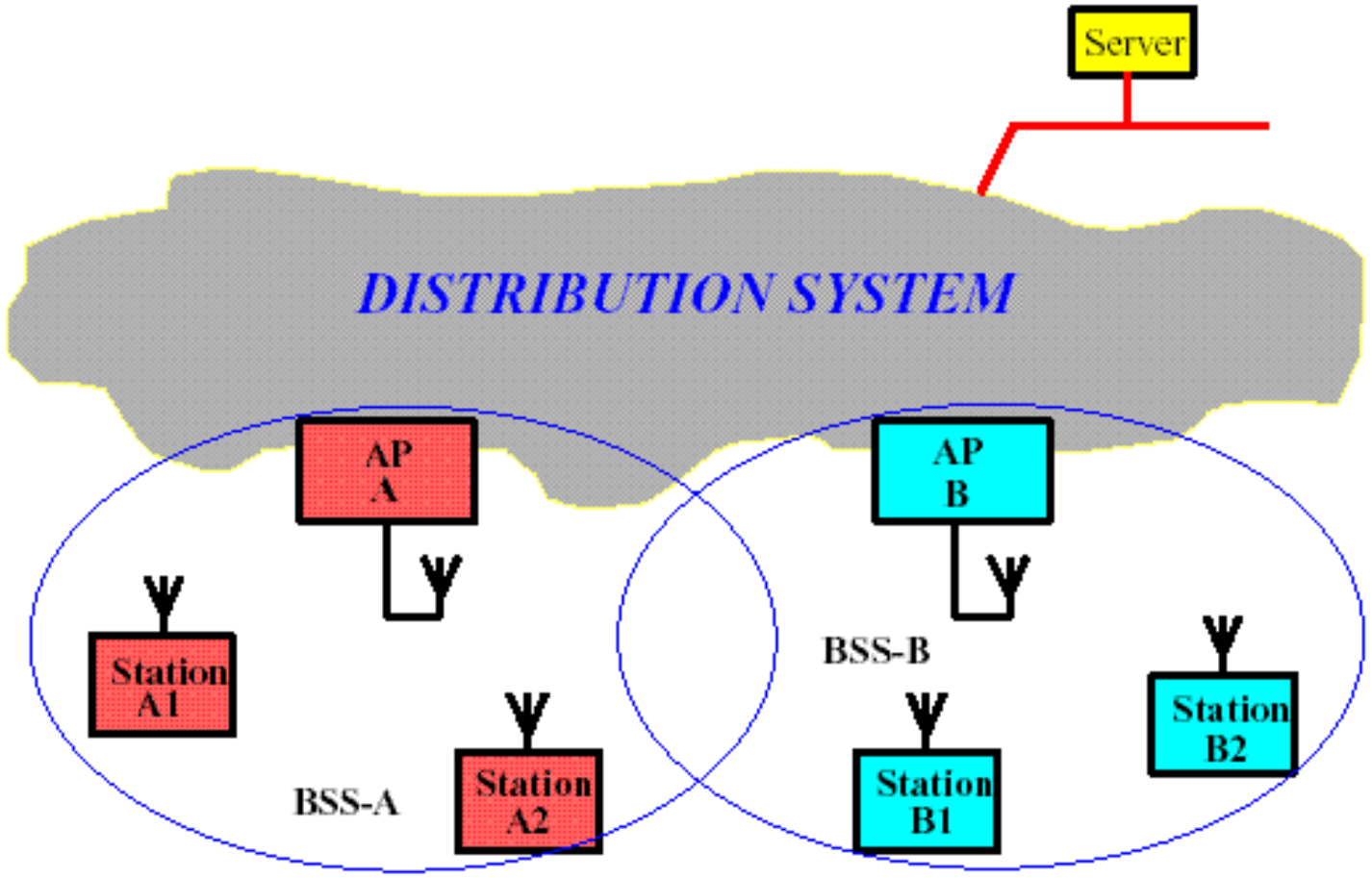
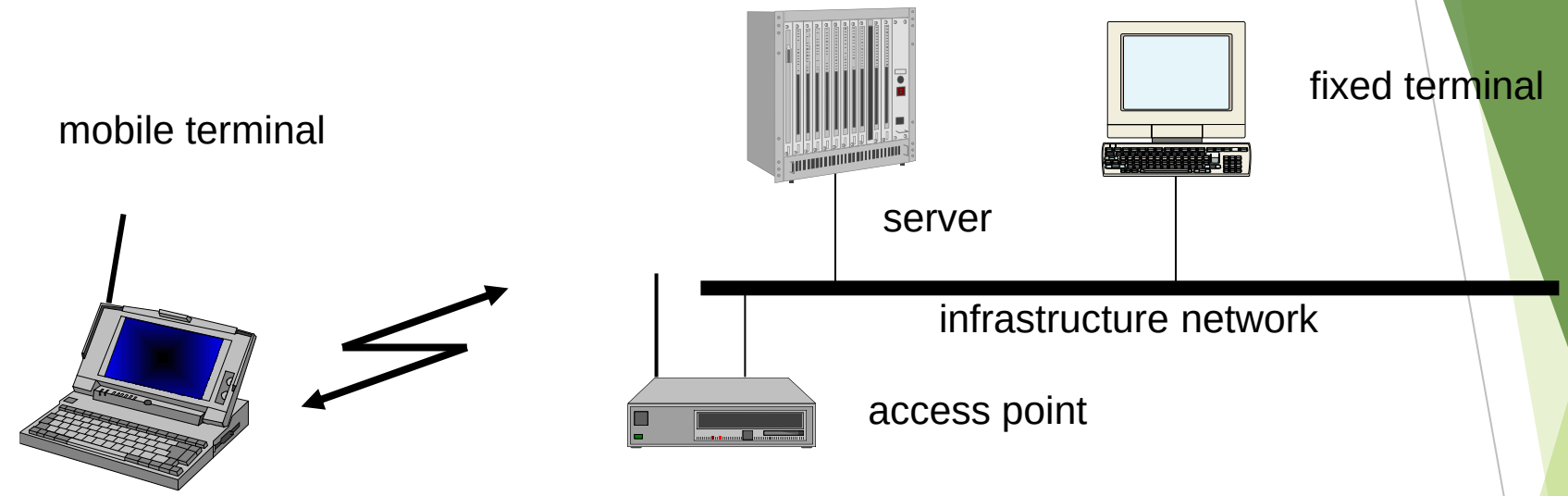
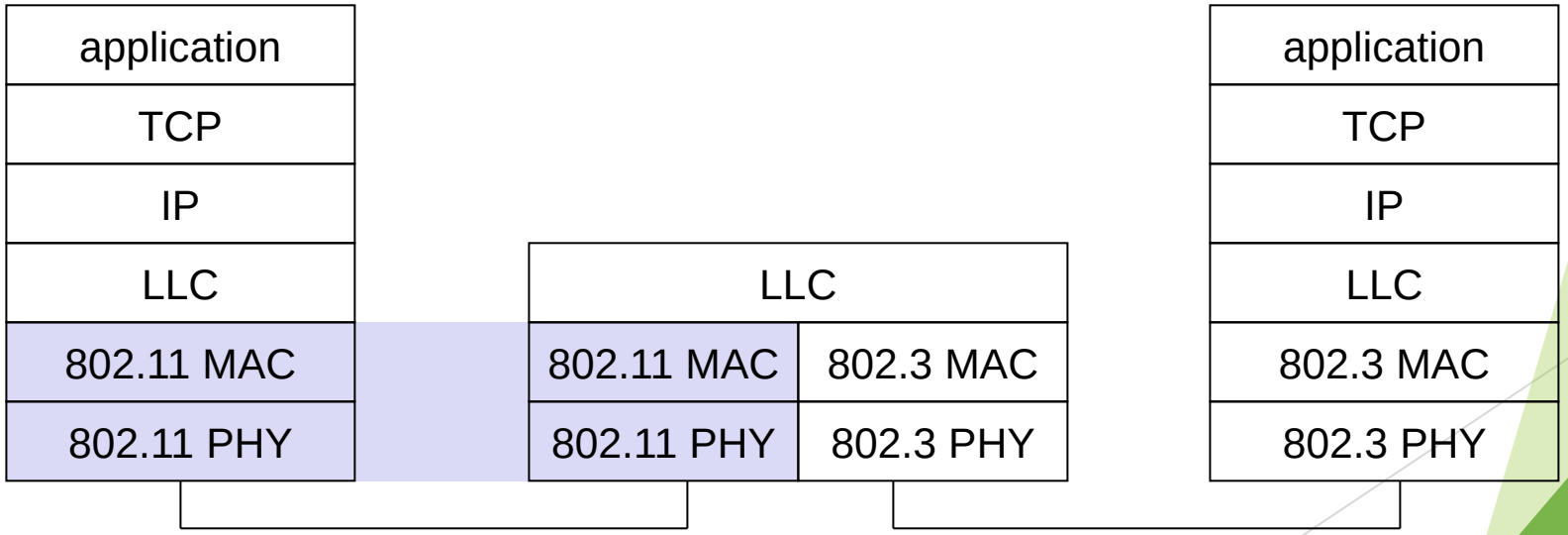


Figure 2 ESS Provides Campus-Wide Coverage

Source: Intersil

802.11- in the TCP/IP stack

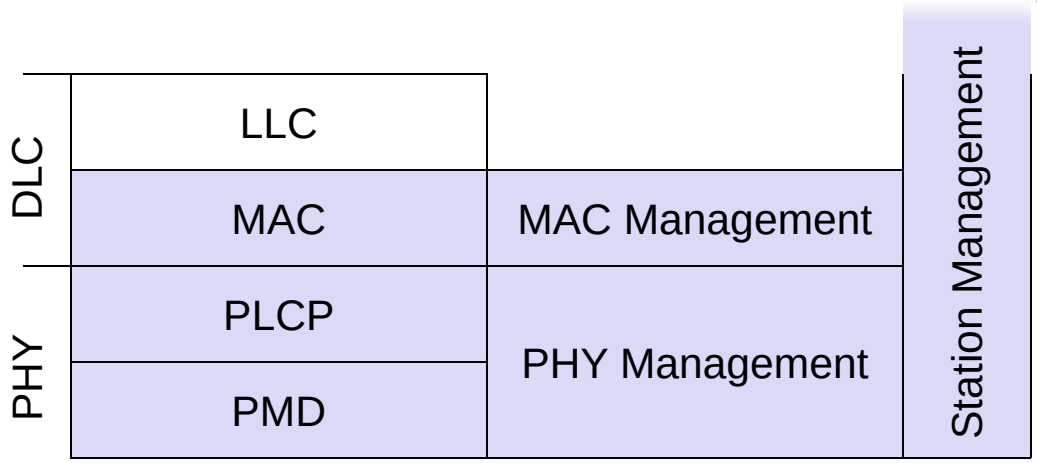




802.11 - Layers and functions

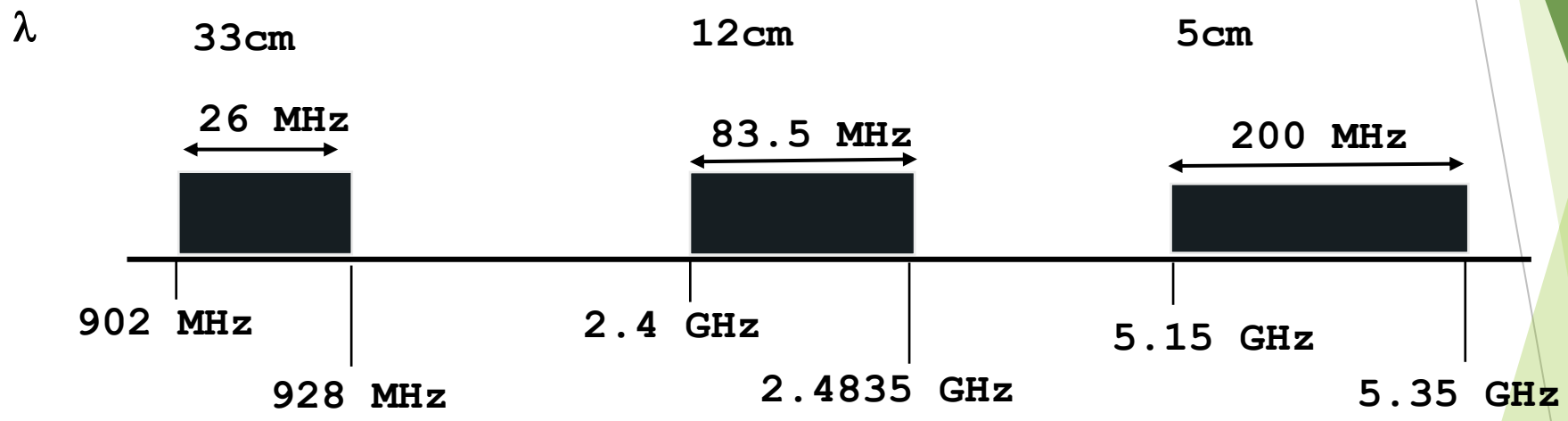
- MAC
  - access mechanisms, fragmentation, encryption
- MAC Management
  - synchronization, roaming, MIB, power management

- PLCP Physical Layer Convergence Protocol
  - clear channel assessment signal (carrier sense)
- PMD
- Physical Medium Dependent modulation, coding
- PHY Management
  - channel selection, MIB
- Station Management
  - coordination of all management functions



IEEE 802.11

- Wireless LAN standard defined in the unlicensed spectrum (2.4 GHz and 5 GHz U-NII bands)



- Standards covers the MAC sublayer and PHY layers
- Three different physical layers in the 2.4 GHz band
  - FHSS, DSSS and IR
- OFDM based Phys layer in the 5 GHz band (802.11a)

802.11 - Physical layer

- All PHY variants include the provision of the clear channel assessment signal (CCA). This is needed for the MAC mechanisms controlling medium access and indicates if the medium is currently idle
- The PHY layer offers a service access point (SAP) with 1 or 2 Mbit/s transfer rate to the MAC layer (basic version of the standard).

3 versions of spread spectrum:

2 radio (typ. 2.4 GHz),

1 IR data rates 1 or 2 Mbps

1.FHSS (Frequency Hopping Spread Spectrum)

- spreading, despreading, signal strength, typically 1 Mbps min. 2.5 frequency hops/s (USA), two-level GFSK modulation

FHSS PHY packet format

- Synchronization

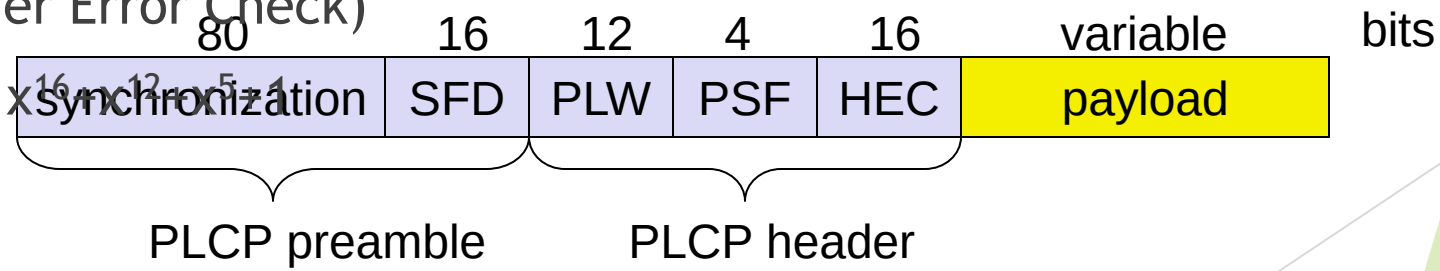
  synch with 010101... pattern
- SFD (Start Frame Delimiter)

  0000110010111101 start pattern
- PLW (PLCP_PDU Length Word)

  length of payload incl. 32 bit CRC of payload, PLW < 4096
- PSF (PLCP Signaling Field)

  data of payload (1 or 2 Mbit/s)
- HEC (Header Error Check)

  CRC with x



2.DSSS (Direct Sequence Spread Spectrum)

- DBPSK modulation for 1 Mbps (Differential Binary Phase Shift Keying), DQPSK for 2 Mbps (Differential Quadrature PSK)
- preamble and header of a frame is always transmitted with 1 Mbps, rest of transmission 1 or 2 Mbps
- chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
- max. radiated power 1 W (USA), 100 mW (EU), min. 1mW

3.Infrared

- 850-950 nm, diffuse light, typ. 10 m range
- carrier detection, energy detection, synchronization

DSSS PHY packet format

- Synchronization

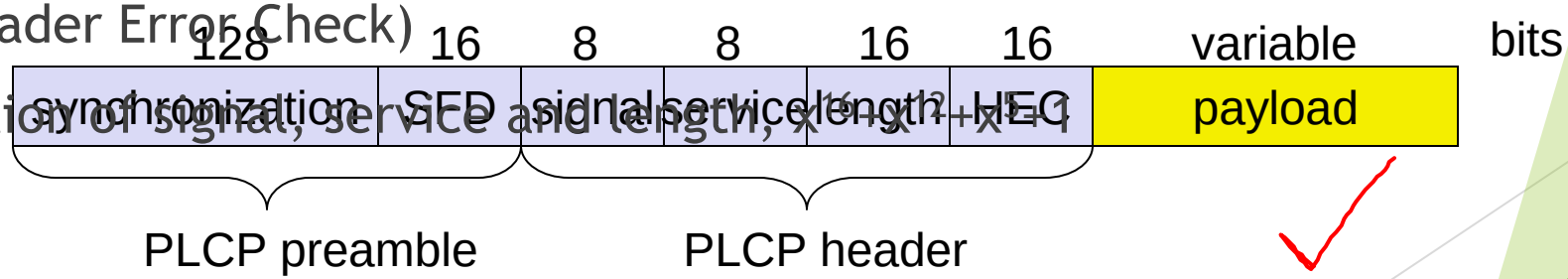
  synch., gain setting, energy detection, frequency offset compensation
- SFD (Start Frame Delimiter)

  1111001110100000
- Signal

  data rate of the payload (0A: 1 Mbit/s DBPSK; 14: 2 Mbit/s DQPSK)
- Service Length

  future use, 00: 802.11 compliant length of the payload
- HEC (Header Error Check)

  protection of signal, service and length, $x^{16}+x^{12}+x^5+1$



Hardware

- Original WaveLAN card (NCR)
  - 914 MHz Radio Frequency
  - Transmit power 281.8 mW
  - Transmission Range ~250 m (outdoors) at 2Mbps
  - SNRT 10 dB (capture)
- WaveLAN II (Lucent)
  - 2.4 GHz radio frequency range
  - Transmit Power 30mW
  - Transmission range 376 m (outdoors) at 2 Mbps (60m indoors)
  - Receive Threshold = - 81dBm
  - Carrier Sense Threshold = -111dBm
- Many others….Agere, Cisco,……

802.11-based Wireless LANs
MAC functional spec - DCF

802.11 - MAC layer I - DFWMAC

Traffic services

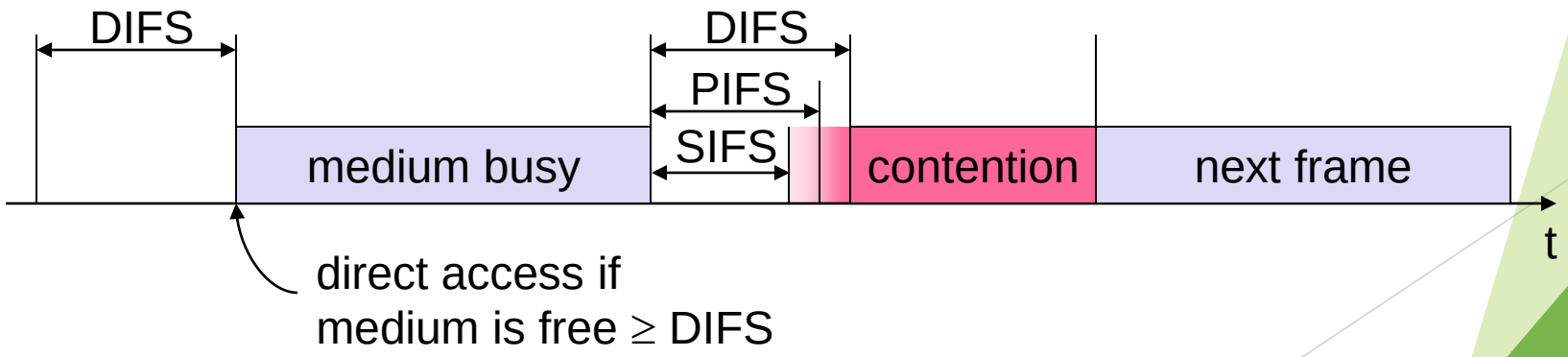
- Asynchronous Data Service (mandatory)
  - exchange of data packets based on “best-effort”
  - support of broadcast and multicast
- Time-Bounded Service (optional)
  - implemented using PCF (Point Coordination Function)

Access methods

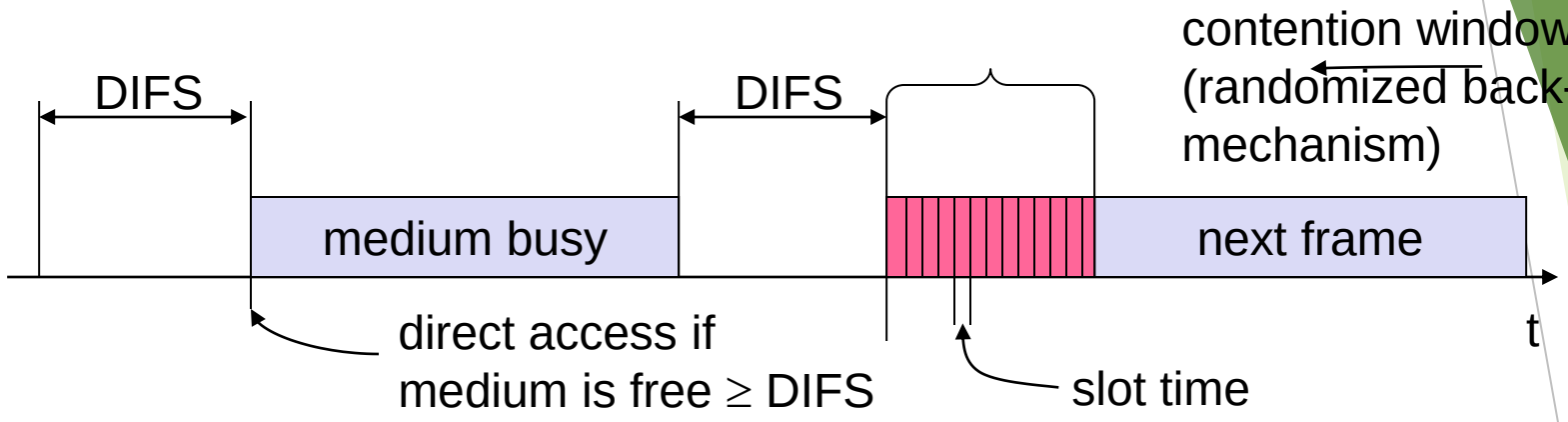
- DFWMAC-DCF CSMA/CA (mandatory)
  - collision avoidance via randomized „back-off“ mechanism
  - minimum distance between consecutive packets
  - ACK packet for acknowledgements (not for broadcasts)
- DFWMAC-DCF w/ RTS/CTS (optional)
  - Distributed Foundation Wireless MAC
  - avoids hidden terminal problem
- DFWMAC- PCF (optional)
  - access point polls terminals according to a list

802.11 - MAC layer II

- Priorities
  - defined through different inter frame spaces
  - no guaranteed, hard priorities
- SIFS (Short Inter Frame Spacing)
  - highest priority, for ACK, CTS, polling response
- PIFS (PCF IFS)
  - medium priority, for time-bounded service using PCF
- DIFS (DCF, Distributed Coordination Function IFS)
  - lowest priority, for asynchronous data service



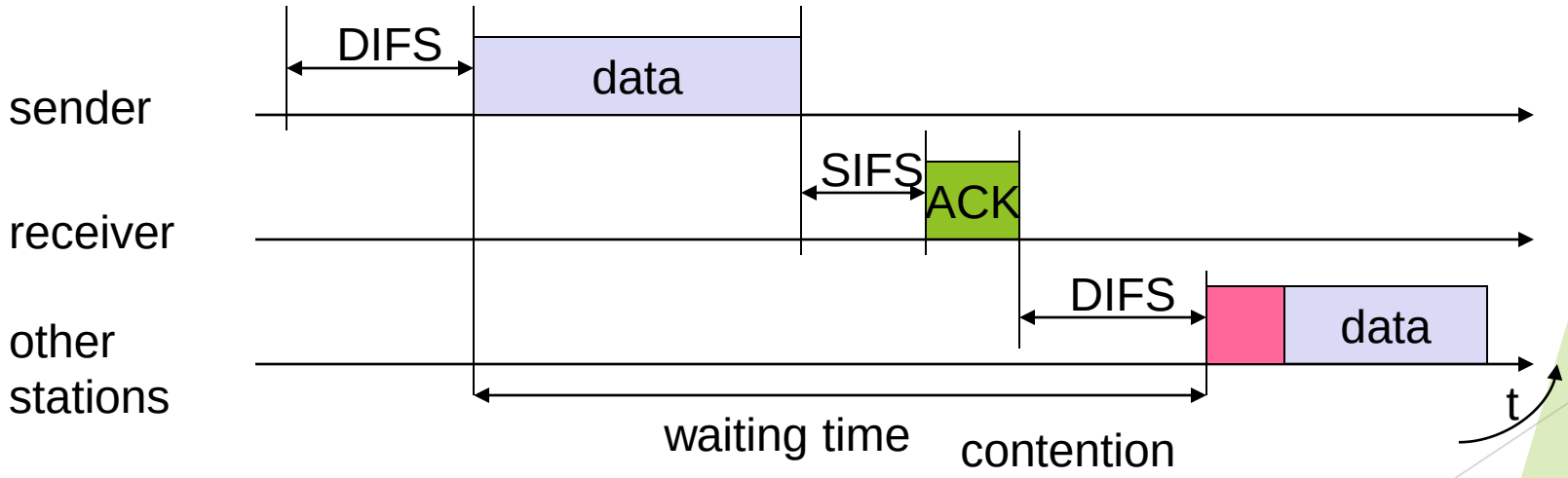
802.11 - CSMA/CA access method I



- station ready to send 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)

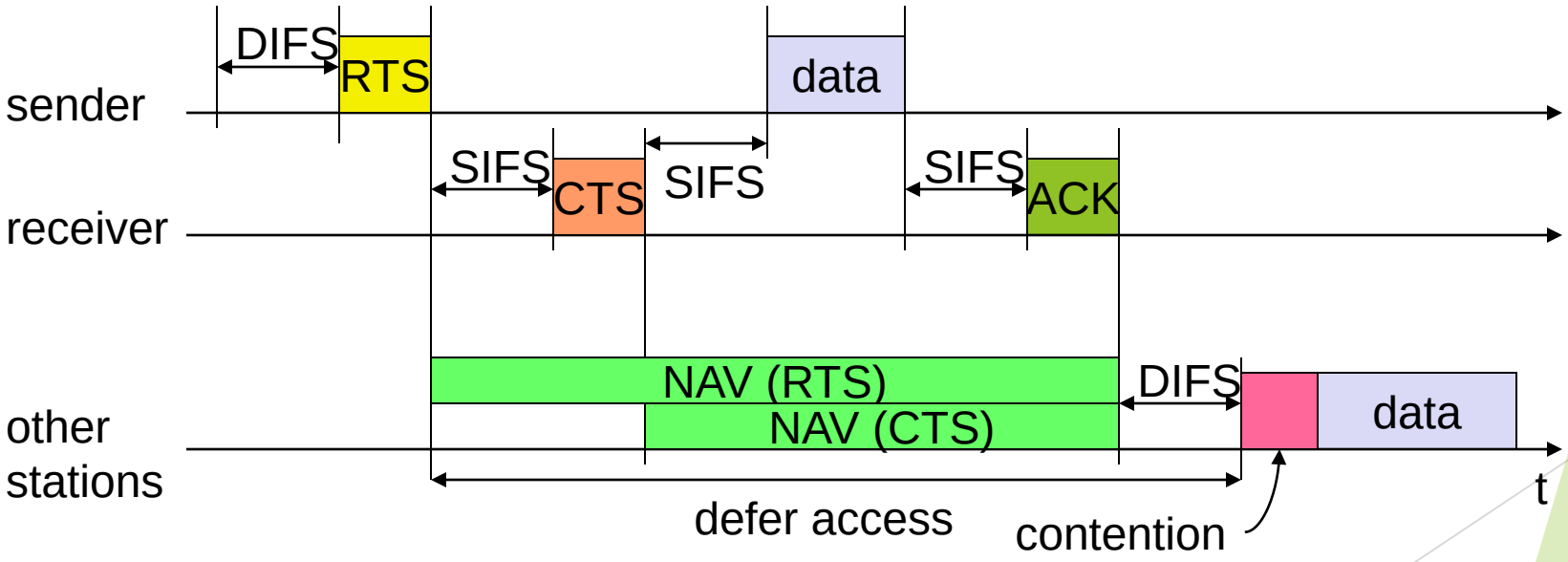
802.11 - CSMA/CA access method II

- 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 - DFWMAC

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



802.11 - Carrier Sensing

- **In IEEE 802.11, carrier sensing is performed**
  - at the air interface (*physical carrier sensing*), and
  - at the MAC layer (*virtual carrier sensing*)
- **Physical carrier sensing**
  - detects presence of other users by analyzing all detected packets
  - Detects activity in the channel via relative signal strength from other sources
- **Virtual carrier sensing** is done by sending MPDU duration information in the header of RTS/CTS and data frames
- Channel is busy if **either** mechanisms indicate it to be
- Duration field indicates the amount of time (in microseconds) required to complete frame transmission
- Stations in the BSS use the information in the duration field to adjust their network allocation vector (NAV)

802.11 - Collision Avoidance

- If medium is not free during DIFS time..
- Go into Collision Avoidance: Once channel becomes idle, wait for DIFS time plus a randomly chosen backoff time before attempting to transmit
- For DCF the backoff is chosen as follows:
  - When first transmitting a packet, choose a backoff interval in the range [0,cw]; cw is contention window, nominally 31
  - Count down the backoff interval when medium is idle
  - Count-down is suspended if medium becomes busy
  - When backoff interval reaches 0, transmit RTS
  - If collision, then double the cw up to a maximum of 1024
- Time spent counting down backoff intervals is part of MAC overhead

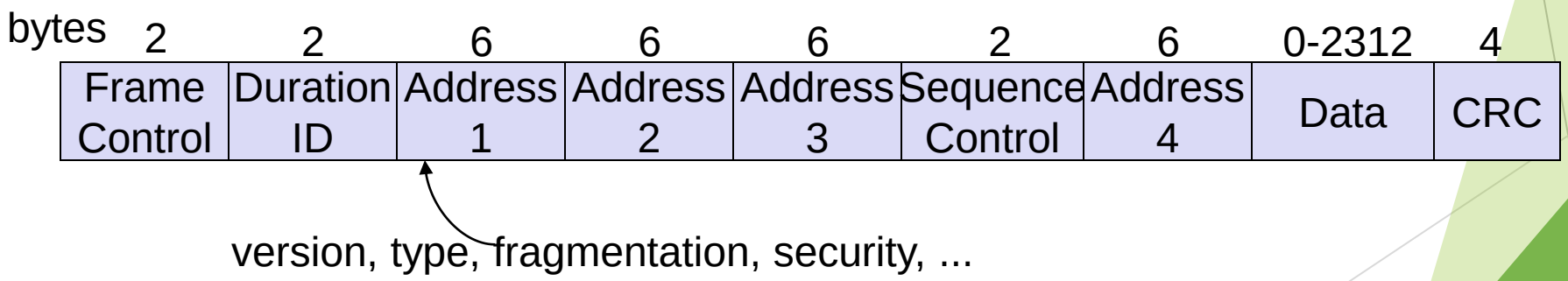
802.11 - Congestion Control

- Contention window (cw) in DCF: Congestion control achieved by dynamically choosing cw
- *large* cw leads to larger backoff intervals
- *small* cw leads to larger number of collisions

- Binary Exponential Backoff in DCF:
  - When a node fails to receive CTS in response to its RTS, it increases the contention window
    - cw is doubled (up to a bound cwmax =1023)
  - Upon successful completion data transfer, restore cw to cwmin=31

802.11 - Frame format

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



Types of Frames

- Control Frames
  - RTS/CTS/ACK
  - CF-Poll/CF-End
- Management Frames
  - Beacons
  - Probe Request/Response
  - Association Request/Response
  - Dissociation/Reassociation
- Authentication/Deauthentication
  - ATIM
- Data Frames

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

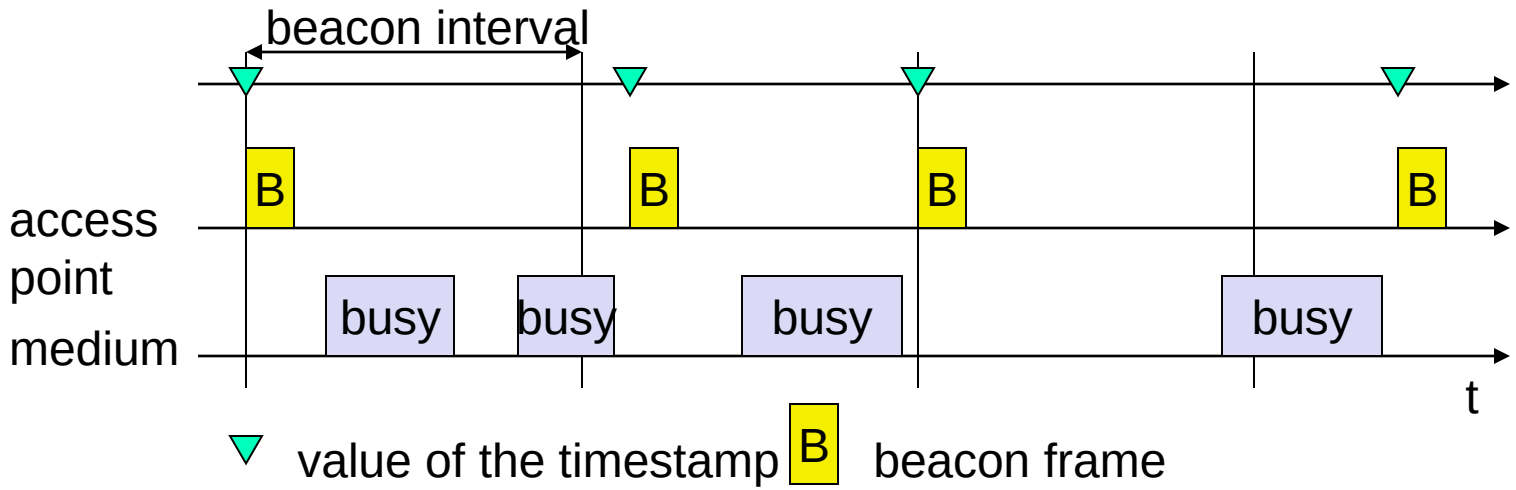
  managing, read, write

802.11 - Synchronization

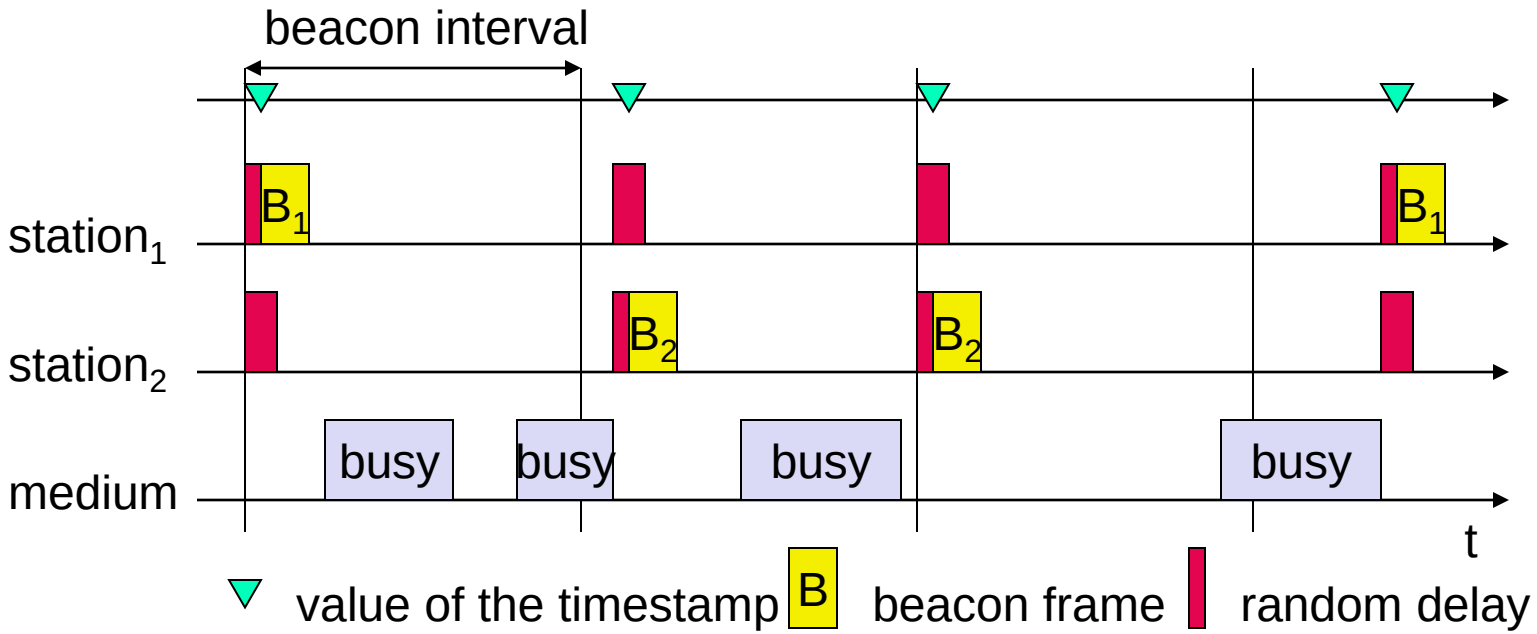
- All STAs within a BSS are synchronized to a common clock
- Infrastructure mode: AP is the timing master
  - periodically transmits Beacon frames containing Timing Synchronization function (TSF)
  - Receiving stations accepts the timestamp value in TSF
- Ad hoc mode: TSF implements a distributed algorithm
  - Each station adopts the timing received from any beacon that has TSF value later than
  - its own TSF timer

- This mechanism keeps the synchronization of the TSF timers in a BSS to within 4 μs plus the maximum propagation delay of the PHY layer

Synchronization using a Beacon (infrastructure)



Synchronization using a Beacon (ad-hoc)



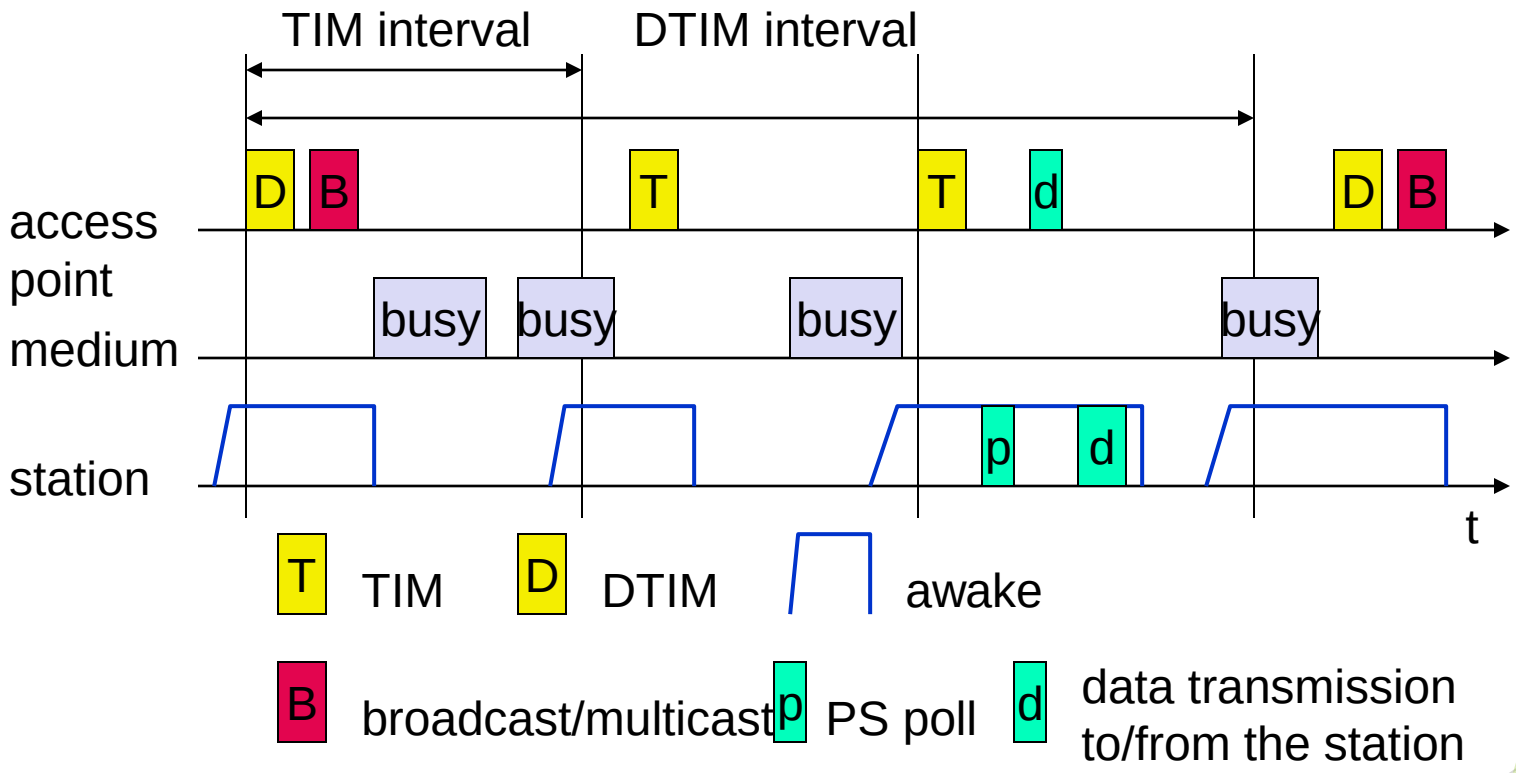
Power management

- Idea: switch the transceiver off if not needed

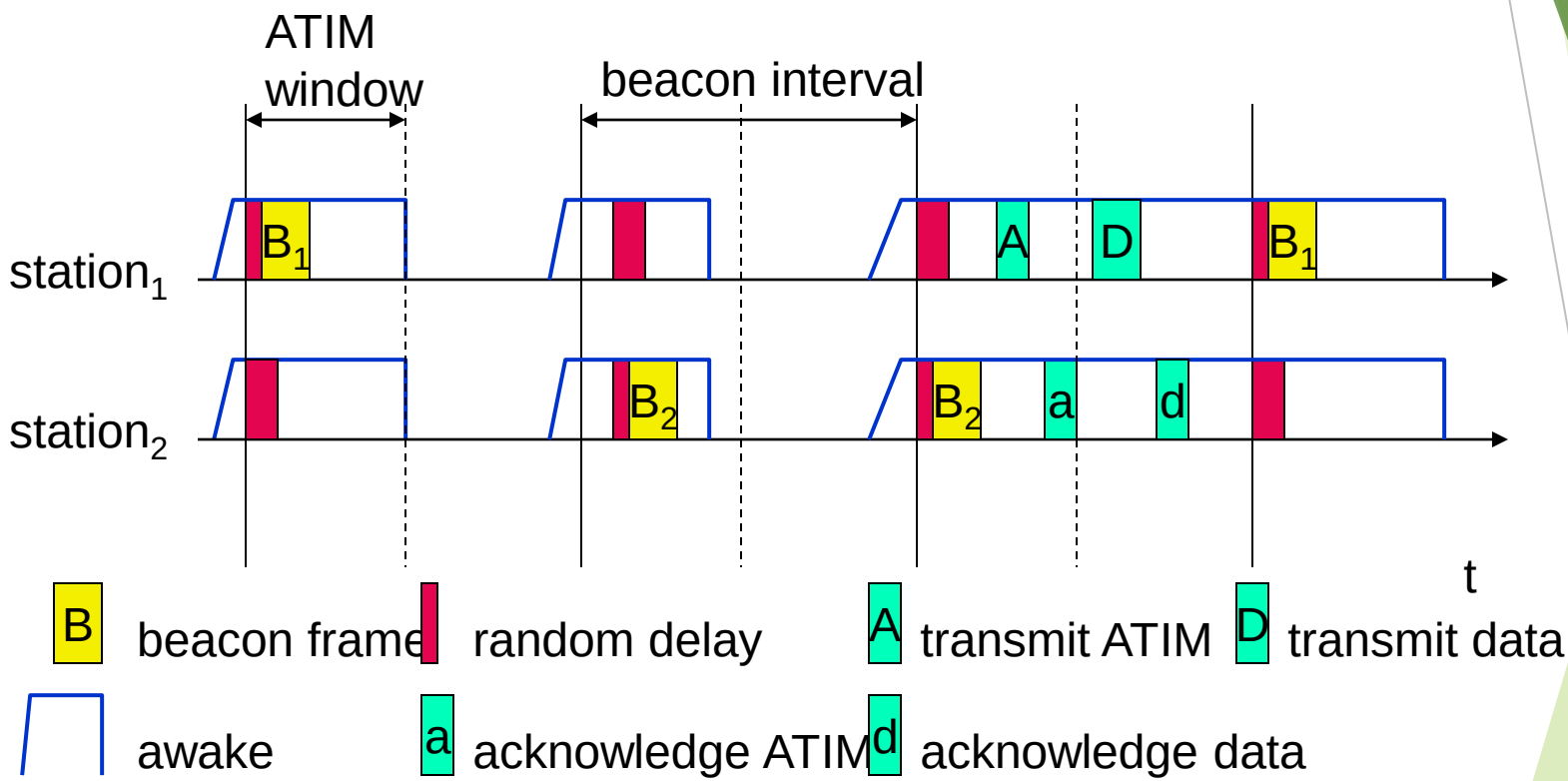
  States of a station: sleep and awake
- Timing Synchronization Function (TSF)

  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?)

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

IEEE 802.11 Summary

- Infrastructure and ad hoc modes using DCF
- Carrier Sense Multiple Access
- Binary exponential backoff for collision avoidance and congestion control
- Acknowledgements for reliability
- Power save mode for energy conservation
- Time-bound service using PCF
- Signaling packets for avoiding Exposed/Hidden terminal problems, and for reservation
  - Medium is reserved for the duration of the transmission
  - RTS-CTS in DCF
  - Polls in PCF

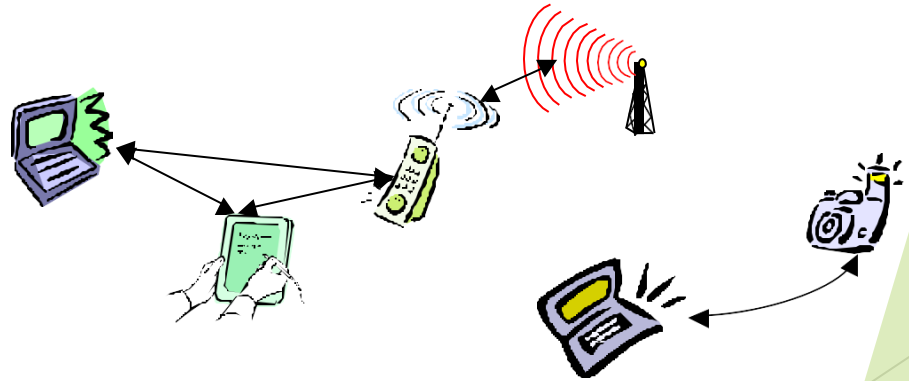
- IEEE WPAN (Wireless Personal Area Networks)
  - market potential
  - compatibility
  - low cost/power, small form factor
  - technical/economic feasibility
    - Bluetooth
    - Zigbee

Bluetooth

Idea

- Universal radio interface for ad-hoc wireless connectivity
- Interconnecting computer and peripherals, handheld devices, PDAs, cell phones – replacement of IrDA
- Embedded in other devices, goal: 5€/device (2005: 40€/USB bluetooth)
- Short range (10 m), low power consumption, license-free 2.45 GHz ISM
- Voice and data transmission, approx. 1 Mbit/s gross data rate

One of the first modules (Ericsson).



Bluetooth

History

- 1994: Ericsson (Mattison/Haartsen), “MC-link” project
- Renaming of the project: Bluetooth according to Harald “Blåtand” Gormsen [son of Gorm], King of Denmark in the 10th century
- 1998: foundation of Bluetooth SIG, www.bluetooth.org (was: )
- 1999: erection of a rune stone at Ercisson/Lund ;-)
- 2001: first consumer products for mass market, spec. version 1.1 released
- 2005: 5 million chips/week

Special Interest Group

- Original founding members: Ericsson, Intel, IBM, Nokia, Toshiba
- Added promoters: 3Com, Agere (was: Lucent), Microsoft, Motorola
- > 2500 members
- Common specification and certification of products

Characteristics

4. GHz ISM band, 79 (23) RF channels, 1 MHz carrier spacing
   - Channel 0: 2402 MHz … channel 78: 2480 MHz
   - G-FSK modulation, 1-100 mW transmit power

FHSS and TDD
   - Frequency hopping with 1600 hops/s
   - Hopping sequence in a pseudo random fashion, determined by a master
   - Time division duplex for send/receive separation

Voice link – SCO (Synchronous Connection Oriented)
   - FEC (forward error correction), no retransmission, 64 kbit/s duplex, point-to-point, circuit switched

Data link – ACL (Asynchronous ConnectionLess)
   - Asynchronous, fast acknowledge, point-to-multipoint, up to 433.9 kbit/s symmetric or 723.2/57.6 kbit/s asymmetric, packet switched

Topology
   - Overlapping piconets (stars) forming a scatternet

Piconet

Collection of devices connected in an ad hoc fashion

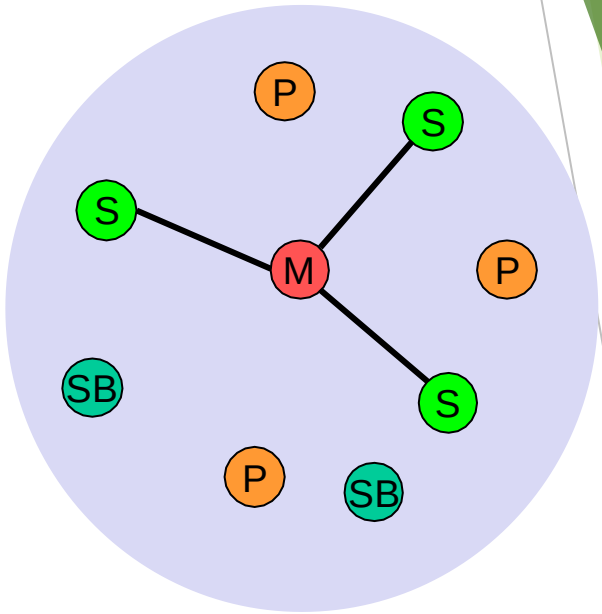
One unit acts as master and the others as slaves for the lifetime of the piconet

Master determines hopping pattern, slaves have to synchronize

Each piconet has a unique hopping pattern

Participation in a piconet = synchronization to hopping sequence

Each piconet has one master and up to 7 simultaneous slaves (> 200 could be parked)



M=Master
S=Slave

P=Parked
SB=Standby

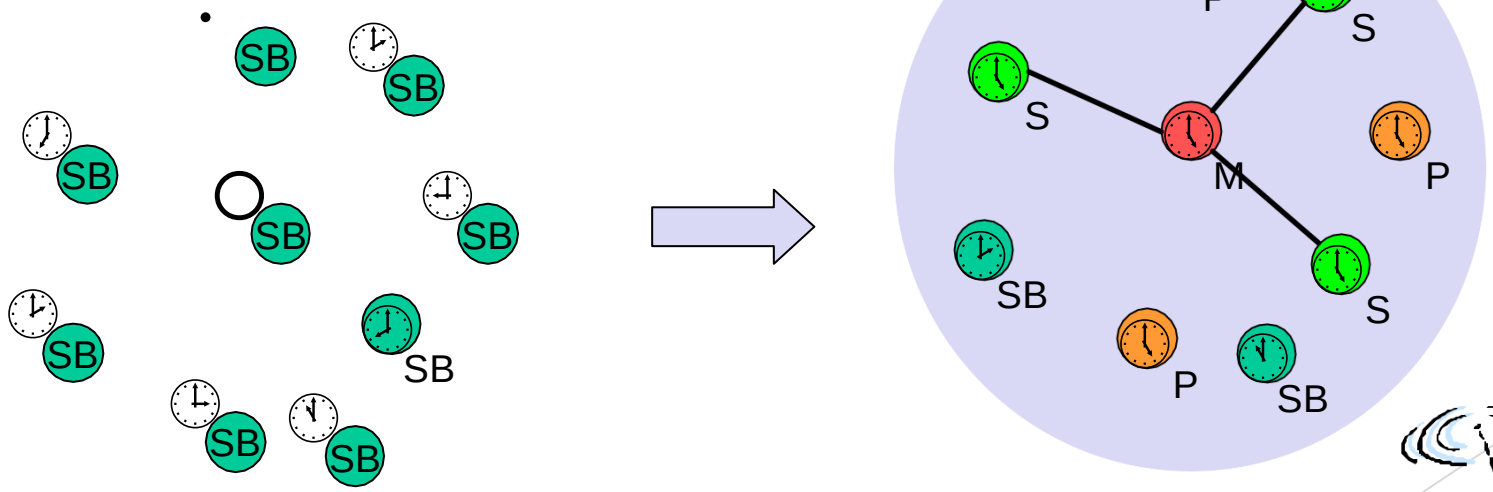
Forming a piconet

All devices in a piconet hop together

- Master gives slaves its clock and device ID
  - Hopping pattern: determined by device ID (48 bit, unique worldwide)
  - Phase in hopping pattern determined by clock

Addressing

- Active Member Address (AMA, 3 bit)
- Parked Member Address (PMA, 8 bit)



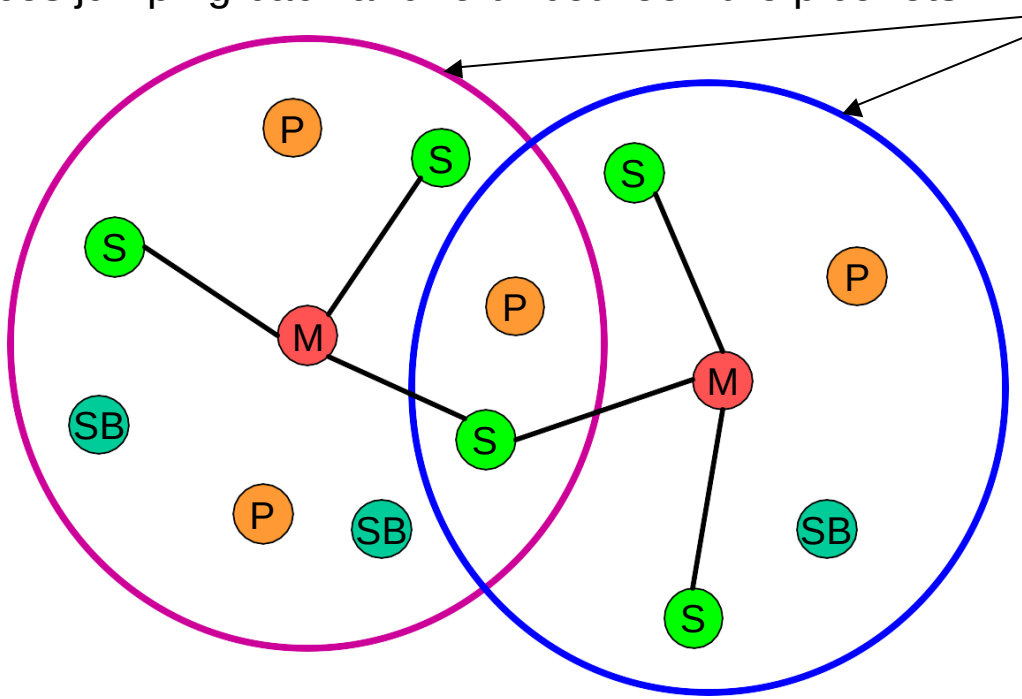
Scatternet

Linking of multiple co-located piconets through the sharing of common master or slave devices

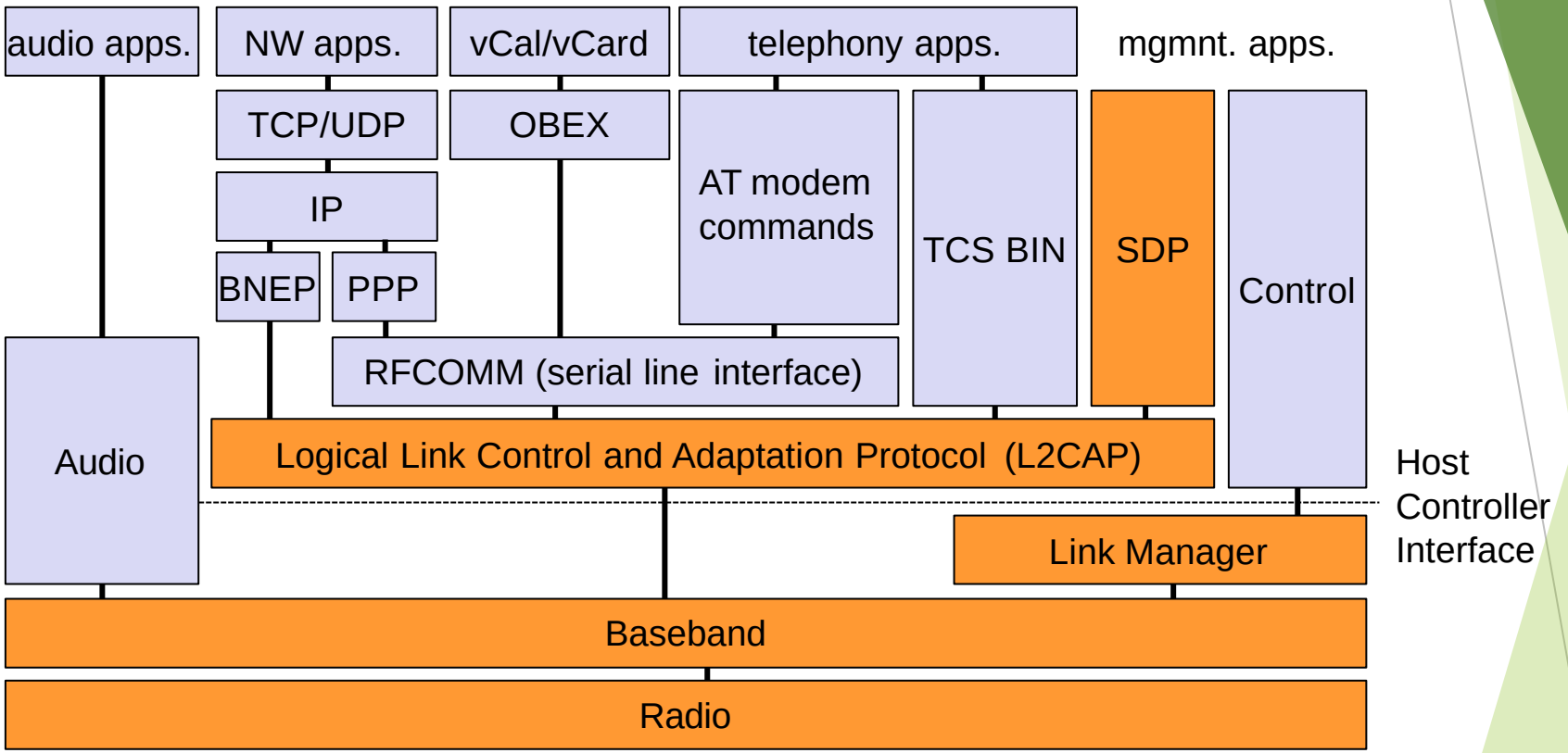
- Devices can be slave in one piconet and master of another

Communication between piconets

- Devices jumping back and forth between the piconets



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.

Prof. Dr.-Ing. Jochen Schiller, http://www.jochenschiller.de/

Bluetooth Protocol Stack

- Radio: Specification of the air interface, i.e., frequencies, modulation, and transmit power
- Baseband: Description of basic connection establishment, packet formats, timing, and basic QoS parameters
- Link manager protocol: Link set-up and management between devices including security functions and parameter negotiation
- Logical link control and adaptation protocol (L2CAP): Adaptation of higher layers to the baseband (connectionless and connection-oriented services,
- Service discovery protocol: Device discovery in close proximity plus querying of service characteristics

Bluetooth Protocol Stack

- Cable replacement protocol RFCOMM that emulates a serial line interface following the EIA-232 (formerly RS-232) standards. RFCOMM supports multiple serial ports over a single physical channel.
- The telephony control protocol specification – binary (TCS BIN) describes a bit-oriented protocol that defines call control signaling for the establishment of voice and data calls between Bluetooth devices. It also describes mobility and group management functions. The host controller interface (HCI) between the baseband and L2CAP provides a command interface to the baseband controller and link manager, and access to the hardware status and control registers. The HCI can be seen as the hardware/software boundary.

L2CAP - Logical Link Control and Adaptation Protocol

Simple data link protocol on top of baseband

Connection oriented, connectionless, and signalling channels

Protocol multiplexing

- RFCOMM, SDP, telephony control

Segmentation & reassembly

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

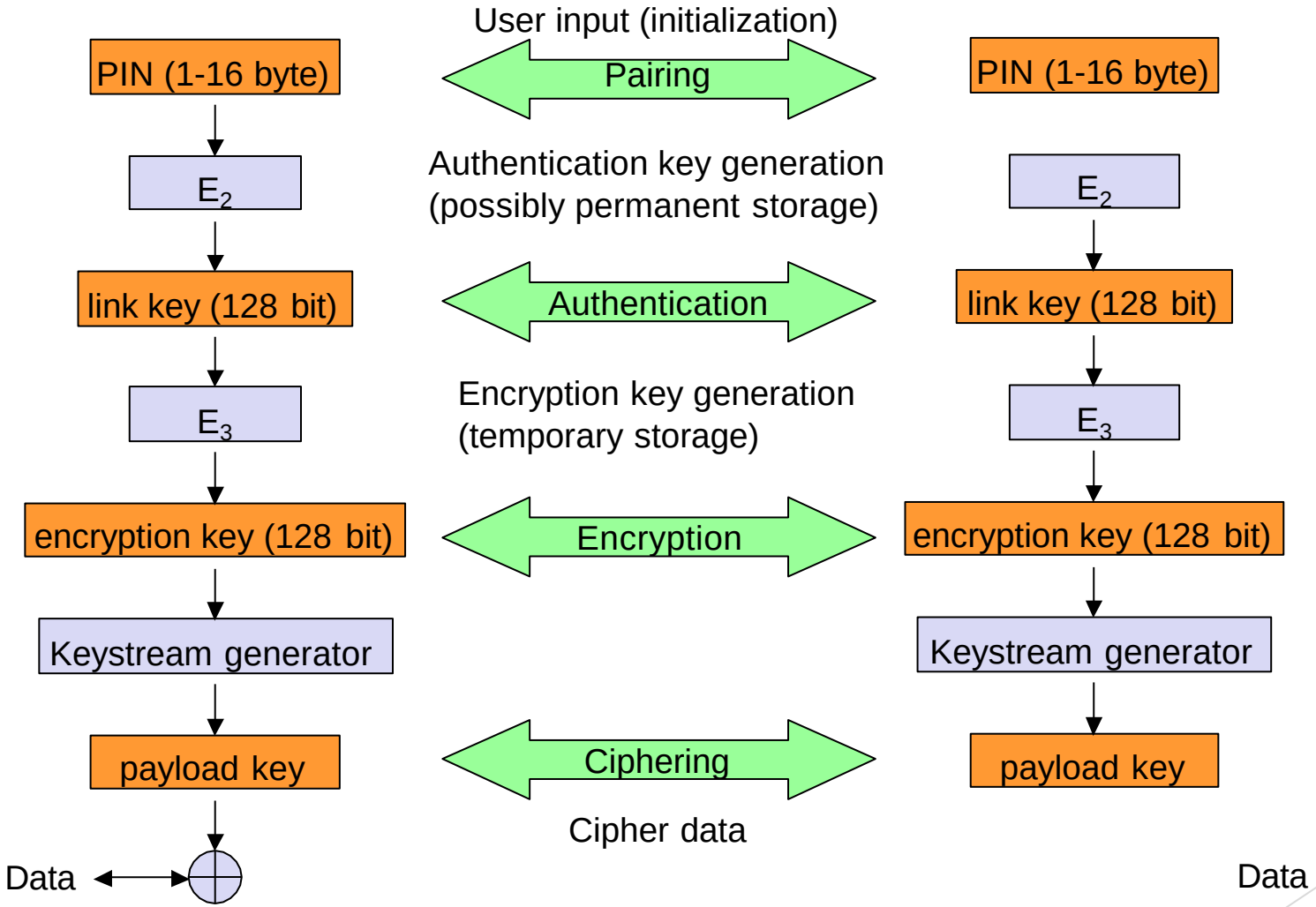
QoS flow specification per channel

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

Group abstraction

- Create/close group, add/remove member

Security architecture of Bluetooth



Prof. Dr.-Ing. Jochen Schiller, http://www.jochenschiller.de/

LMP

- Authentication, pairing, and encryption: Although basic authentication is handled in the baseband, LMP has to control the exchange of random numbers and signed responses.
- Synchronization: Precise synchronization is of major importance within a Bluetooth network. The clock offset is updated each time a packet is received from the master. Additionally, special synchronization packets can be received.
- Capability negotiation: Not all Bluetooth devices will support all features that are described in the standard, so devices have to agree the usage of, e.g., multi-slot packets, encryption, SCO links, voice encoding, park/sniff/hold mode (explained below), HV2/HV3 packets etc.
- Quality of service negotiation: Different parameters control the QoS of a Bluetooth device at these lower layers. The poll interval, i.e., the maximum time between transmissions from a master to a particular slave, controls the latency and transfer capacity. Depending on the quality of the channel, DM or DH packets may be used (i.e., 2/3 FEC protection or no protection).
- Power control: A Bluetooth device can measure the received signal strength. Depending on this signal level the device can direct the sender of the measured signal to increase or decrease its transmit power.

SDP – Service Discovery Protocol

Inquiry/response protocol for discovering services

- Searching for and browsing services in radio proximity
- Adapted to the highly dynamic environment
- Can be complemented by others like SLP, Jini, Salutation, …
- Defines discovery only, not the usage of services
- Caching of discovered services
- Gradual discovery

Additional protocols to support legacy protocols/apps.

RFCOMM

- Emulation of a serial port (supports a large base of legacy applications)
- Allows multiple ports over a single physical channel

Telephony Control Protocol Specification (TCS)

- Call control (setup, release)
- Group management

OBEX

- Exchange of objects, IrDA replacement

WAP

- Interacting with applications on cellular phones

Power management

- . All devices being active must have the 3-bit active member address (AMA).
- To save battery power, a Bluetooth device can go into one of three low power states:
  - Sniff state: The sniff state has the highest power consumption of the low power states. Here, the device listens to the piconet at a reduced rate (not on every other slot as is the case in the active state).
  - Hold state: The device does not release its AMA . If there is no activity in the piconet, the slave may either reduce power consumption or participate in another piconet.
  - Park state: In this state the device has the lowest duty cycle and the lowest power consumption. The device releases its AMA and receives a parked member address (PMA). The device is still a member of the piconet, but gives room for another device to become active

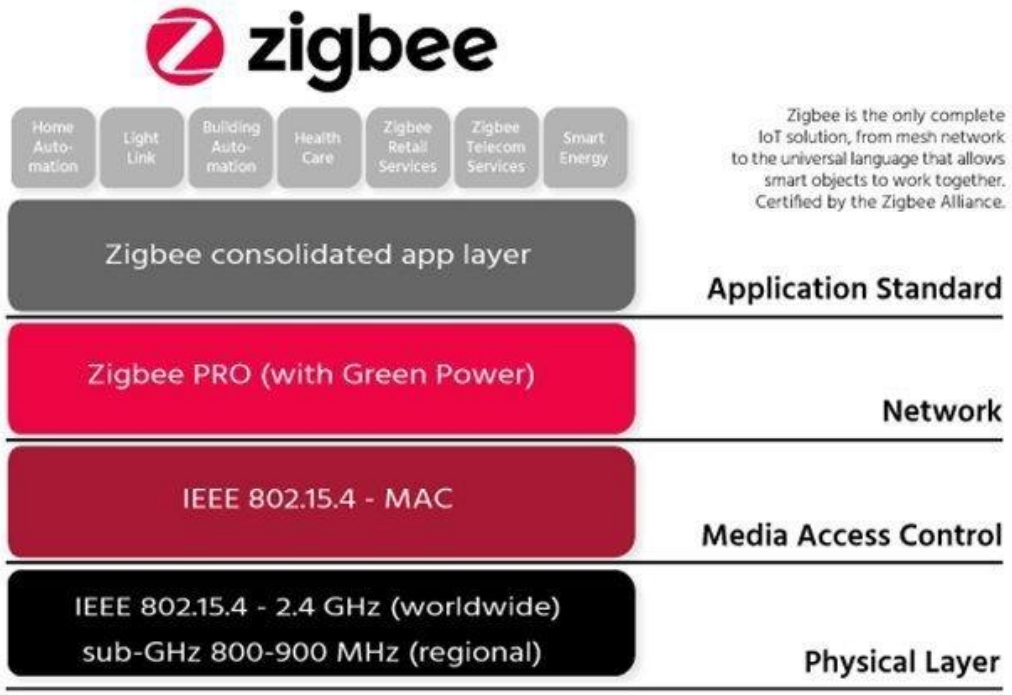
Zigbee

- Zigbee is a standards-based wireless technology developed to enable low-cost, low-power wireless machine-to-machine (M2M) and internet of things (IoT) networks.
- Zigbee is for low-data rate, low-power applications and is an open standard.
- Zigbee products have been extended and customized by vendors and, thus, plagued by interoperability issues.
- In contrast to Wi-Fi networks used to connect endpoints to high-speed networks, Zigbee supports much lower data rates and uses a mesh networking protocol to avoid hub devices and create a self-healing architecture.
- IEEE 802.15.4 wireless standard for wireless personal area networks (WPANs). The Zigbee WPANs operate on 2.4 Ghz, 900 MHz and 868 MHz frequencies.

ZigBee Architecture

Zigbee Applications:

1.Home Automation
2.Medical Data Collection
3.Industrial Control Systems
4.meter reading system
5.light control system



Bluetooth v/s Zigbee

- **Bluetooth** was developed under IEEE 802.15.1, which is used for providing wireless communication through radio signals. The frequency range supported in Bluetooth varies from 2.4 GHz to 2.483 GHz. It covers less distance than Zigbee. In Bluetooth, GFSK modulation technique is used.
- **Zigbee**, BPSK and QPSK modulation techniques are used like UWB (Ultra-Wide Band). the frequency range supported in Zigbee is mostly 2.4 GHz worldwide, which means 2.4 GHz is not supported at all times. It covers more distance as compared with Bluetooth.

Bluetooth networks can be built using the point-to-point master-slave approach in which there is one master and up to seven slaves form a piconet, which leads to forming a scatter net which is a linking of two or more piconets.

Zigbee devices can be networked in a variety of generic topologies, including a star, mesh, and others. A cluster can be created by connecting different Zigbee-based network topologies. Zigbee Coordinator, Zigbee Router, and Zigbee Endpoint nodes make up any Zigbee network.