# CS480: MOBILE NETWORKS

Wireless LANs

14th March 2017

# Topics Covered

- Introduction
- Design goals for wireless LANs
- Infra red vs radio transmission
- Infrastructure and ad-hoc networks
- IEEE 802.11
- Bluetooth
- HIPERLAN

# Introduction

# Introduction

- Wireless LAN (WLAN) technologies constitute a fast-growing market introducing the flexibility of wireless access into office, home, or production environments.
- WLANs are typically restricted to buildings, a campus, single rooms etc.
- WLANs are operated by individuals, not by large-scale network providers.
- The global goal of wireless LANs (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.

# Advantages of WLANs (1)

- *Flexibility*
  - very flexible within the reception area.
  - Radio waves can penetrate walls, senders and receivers can be placed anywhere.
- *Planning*
  - only ad-hoc networks allow for communication without previous planning.
  - Any wired network needs wiring planning. For wired networks, additional cabling with the right plugs and probably interworking units (such as switches) have to be provided.
- *Design*
  - Wireless networks allow for the design of small, independent devices which for example can be put into a pocket.
  - Cables not only restrict users but also designers of small PDAs, notepads, etc. (Almost) no wiring difficulties (e.g. historic buildings, firewalls)

# Advantages of WLANs (2)

- *Robustness*
  - Wireless networks can survive disasters, e.g. earthquakes or users pulling a plug.
  - Networks requiring a wired infrastructure will usually break down completely.
- *Cost*
  - After providing wireless access to the infrastructure via an access point for the first user, adding additional users to a wireless network will not increase cost.
    - Important in lecture halls, hotel lobbies or gate areas in airports where number of users using the network may vary significantly.

# Disadvantages of WLANs (1)

- *Quality of service*
  - WLANs typically offer lower quality than their wired counterparts.
  - This is because of lower bandwidth due to limitations in radio transmission (1-10 Mbit/s user data rate),
  - higher error rates due to interference
  - and higher delay/delay variation due to extensive error correction and detection mechanisms.
- *Proprietary solutions*:
  - Due to slow standardization procedures, many companies provide proprietary solutions offering standardized functionality plus many enhanced features (higher bit rates).
  - These additional features only work in a homogeneous environment, i.e. adapters from the same vendors are used for all wireless nodes.
  - Standards take time (e.g. IEEE 802.11n).

# Disadvantages of WLANs (2)

- *Restrictions*
  - All wireless products have to comply with national regulations.
  - These restrict frequencies to minimize interference.
  - It takes a very long time to establish global solutions like e.g, IMT-2000.
  - WLANs are limited to low-power senders and certain license-free frequency bands, which are not the same worldwide.
- *Safety and security*
  - Using radio waves for data transmission might interfere with other high-tech equipment in, e.g. hospitals.
  - Senders and receivers are operated by laymen and radiation has to be low.
  - Special precautions have to be taken to prevent safely hazards.
  - The open radio interface makes eavesdropping much easier in WLANs.
  - All standards must offer encryption, privacy mechanisms.

# Design Goals of WLANs (1)

For WLANs to ensure their commercial success, the following design goals have to be taken into account:

- *Global operation*
  - WLAN products should sell in all countries. National and international frequency regulations have to be considered.
- *Low power*
  - Devices communicating via a WLAN are typically also wireless devices running on battery power.
  - The LAN design should take this into account and implement special power-saving modes and power management functions.
  - The future lies in small handheld devices with no restricting wire.
- *License-free operation*
  - LAN operators do not want to apply for a special license to be able to use the product.
  - The equipment must operate in a license-free band.

# Design Goals of WLANs (2)

- *Robust transmission technology*
  - Compared to their wired counterparts, WLANs operate under difficult conditions.
  - If they use radio transmission, many other electrical devices can interfere with them (vacuum cleaners, hairdryers, train engines etc.).
  - WLAN transceivers cannot be adjusted for perfect transmission in a standard office or production environment. Senders and receivers can move.
- *Simplified spontaneous cooperation*
  - To be useful in practice, WLANs should not require complicated setup routines but should operate spontaneously after power-up.
  - These LANs would not be useful for supporting e.g., ad-hoc meetings.

# Design Goals of WLANs (3)

- *Easy to use*
  - In contrast to huge and complex wireless WANs, wireless LANs are made for simple use.
  - They should not require complex management, but rather work on a plug-and-play basis.
- *Protection of investment*
  - A lot of money has already been invested into wired LANs.
  - These new WLANs should protect this investment by being interoperable with existing networks.
  - This means that simple bridging between the different LANs should be enough to interoperate.
- *Safety and security*
  - WLANs should be safe to operate, especially regarding low radiation if used, e.g. in hospitals.
  - Users cannot keep safety distances to antennas.

# Design Goals of WLANs (4)

  - The equipment has to be safe for pacemakers.
  - Users should not be able to read personal data during transmission, i.e., encryption mechanisms should be integrated.
  - The networks should also take into account user privacy, i.e., it should not be possible to collect roaming profiles for tracking persons if they do not agree.
- *Transparency for applications*:
  - Existing applications should continue to run over WLANs, the only difference being higher delay and lower bandwidth.
  - The fact of wireless access and mobility should be hidden if it is not relevant, but the network should also support location aware applications, e.g., by providing location information.

# Infra Red vs Radio Transmission

# Infra Red vs Radio Transmission (1)

- Today, two basic transmission technologies can be used to set up WLANs.
- One technology is based on the transmission of infra red light (e.g at 900nm wavelength).
  - An example is the IrDA (Infrared Data Association) interface available everywhere.
- The other one, which is more popular, uses radio transmission in the GHz range.
  - Examples include WaveLAN, HIPERLAN (High-PERformance LAN) and Bluetooth.
- Both technologies can be used to
  - set up ad-hoc connections for workgroups,
  - connect, e.g. a desktop with a printer without a wire,
  - or to support mobility within a small area.

# Infra red vs radio transmission (2)

- Infra red technology uses diffuse light reflected at walls, etc. or directed light if a line-of-sight (LOS) exists between sender and receiver.
  - Senders can be simple light emitting diodes (LEDs) or laser diodes.
  - Photodiodes act as receivers.

# Advantages of infra red technology

- The main advantages are its simple and extremely cheap senders and receivers which are integrated into nearly all mobile devices available today.
  - PDAs, laptops, notebooks, mobile phones have an infra red data association (IrDA) interface.
- No licenses are needed for infra red technology
- Shielding is very simple
- Electrical devices do not interfere with infra red transmission

# Disadvantages of infra red technology

- Infra red transmission is quite easily shielded
  - Cannot penetrate walls or other obstacles
- Interference by light, heat sources etc.
- Low bandwidth compared to other LAN technologies
  - Typically, IrDA devices are internally connected to a serial port limiting transfer rates to 115 kbit/s.

# Advantages of radio transmission

- Long-term experiences made with radio transmission for wide area networks (e.g., microwave links) and mobile cellular phones.
- Can cover larger areas and can penetrate (thinner) walls, furniture.
- Additional coverage is gained by reflection.
- Radio typically does not need a LOS if the frequencies are not too high.
- Current radio-based products offer much higher transmission rates (e.g. 54 Mbits/s) than infra red.

# Disadvantages of radio transmission

- Shielding is not so simple.
- Can interfere with other senders or electrical devices can destroy data transmitted via radio.
- Only permitted in certain frequency bands
  - Very limited ranges of license-free bands

# Infrastructure and ad-hoc networks

# Infrastructure and ad-hoc networks (1)

- Many WLANs of today need an infrastructure network.
- Infrastructure networks not only provide access to other networks, but also include forwarding functions.
- In infrastructure networks, communication typically takes place only between the wireless nodes and the access point (see Figure 1) but not directly between the wireless nodes.
- The access point does not just control medium access, but also acts as a bridge to other wireless or wired networks.
- Figure 1 shows three access points with their three wireless networks and a wired network.

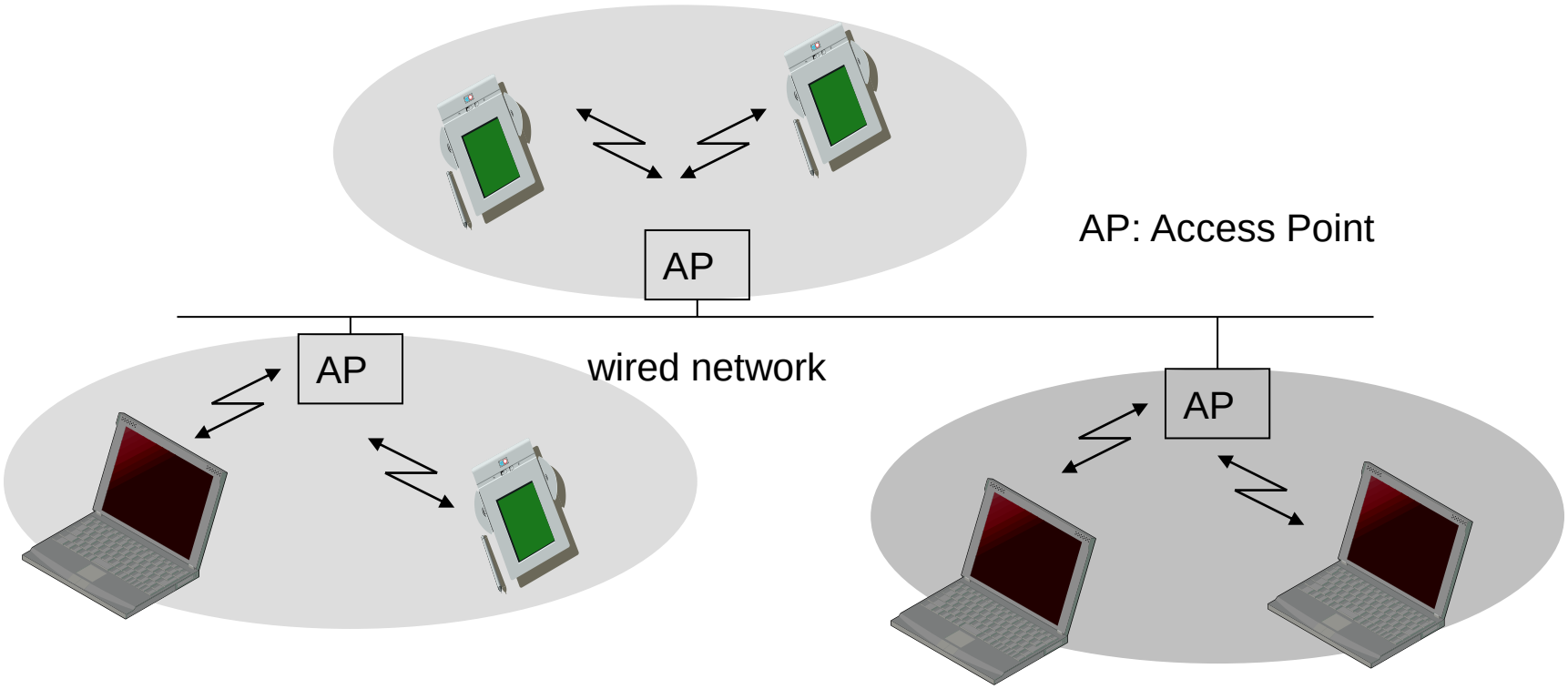



**Figure 1: Example of three infrastructure- based wireless networks**

# Infrastructure and ad-hoc networks (2)

- Design of infrastructure based wireless networks is simple
  - most of the network functionality lies within access point whereas wireless clients can remain quite simple
- Infrastructure-based networks lose some of the flexibility wireless networks can offer
  - e.g. they cannot be used for disaster relief in cases where no infrastructure is left.
- Examples of infrastructure-based networks for wide area include
  - cellular phone networks
  - and satellite-based cellular phones.

# Infrastructure and ad-hoc networks (3)

- Ad-hoc wireless networks do not need any infrastructure to work
  - Each node can communicate directly with other nodes, no access point controlling medium access is necessary
- Figure 2 shows two ad-hoc networks with three nodes each.
  - Nodes within an ad-hoc network can only communicate if they can reach each other physically i.e. if they are within each other's radio range.
  - Nodes from the two networks cannot communicate if they are not within the same radio coverage.
- In ad-hoc networks, complexity of each node is higher
  - because every node implements medium access mechanisms, mechanisms to handle hidden or exposed terminal problems.

**Figure 2: Example of two ad-hoc wireless networks**

# Infrastructure and ad-hoc networks (4)

- Ad-hoc networks exhibit the greatest possible flexibility
  - Needed for unexpected meetings
  - Quick replacements of infrastructure
- IEEE 802.11 and HiperLAN2 are infrastructure-based networks which additionally support ad-hoc networking
- Bluetooth is a typical wireless ad-hoc network

# IEEE 802.11

# IEEE 802.11 (1)

- The IEEE standard 802.11 specifies the most famous family of WLANs in which many products are available.
- The standard belongs to the group of 802.x LAN standards
  - E.g 802.3 Ethernet or 802.2.5 Token Ring
- The standard specifies the physical and medium access layer adapted to special requirements of wireless LANs
  - Offers the same interface as the others to higher layers to maintain interoperability
- The primary goal of the standard was the specification of a simple and robust WLAN which offers time-bounded and asynchronous services

# IEEE 802.11 (2)

- The MAC layer should be able to operate with multiple physical layers, each of which exhibits a different medium sense and transmission characteristic.
  - Candidates for physical layers were infra red and spread spectrum radio transmission techniques
- Additional features of the WLAN should include
  - support of power management to save battery power,
  - the handling of hidden nodes,
  - and the ability to operate worldwide.

# System architecture (1)

- Wireless networks can exhibit two different basic system architectures: infrastructure-based or ad-hoc
- Figure 3 shows the components of an infrastructure and wireless part as specified by IEEE 802.11
- Several nodes, called stations ($STA_i$), are connected to access points (AP).
- Stations are terminals with access mechanisms to the wireless medium and radio contact to the AP
- The stations and the AP which are within the same radio coverage form a basic service set ($BSS_i$)
- A distribution system connects several BSSs via the AP to form a single network and thereby extends the wireless coverage area
  - Such a network is called an extended service set (ESS) and has its own identifier, the ESSID.

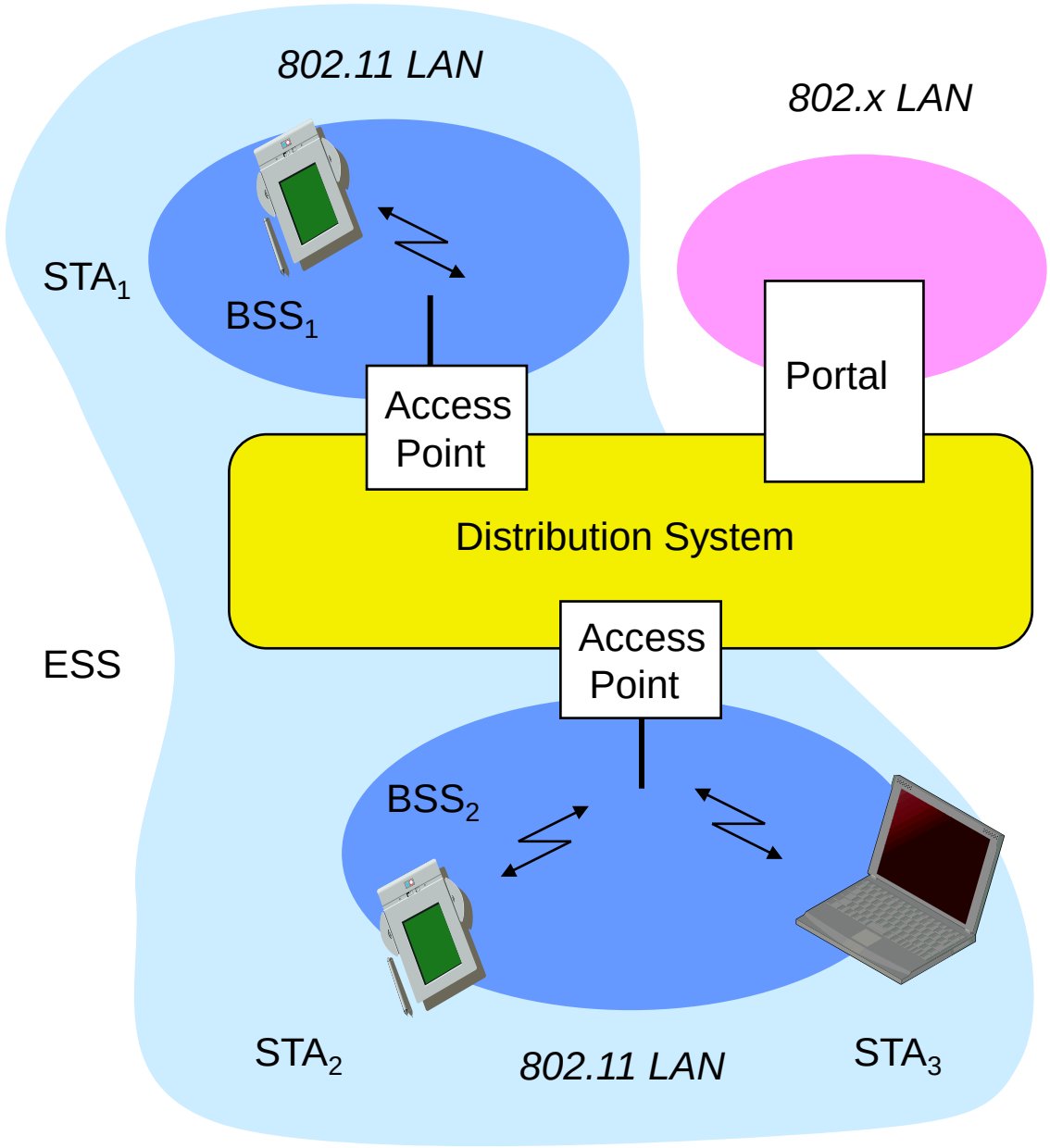



**Figure 3: Architecture of an infrastructure-based IEEE 802.11**

# System architecture (2)

- The distribution system connects the wireless networks via the APs with a portal, which forms the interworking unit to other LANs
- Stations can select an AP and associate with it.
- The APs support roaming (i.e. changing access points), power management and control medium access to support time–bounded service
- The distribution system handles data transfer between the different APs
- IEEE 802.11 allows the building of ad-hoc networks between stations, thus forming one or more independent BSSs (IBSS) as shown in Figure 4.

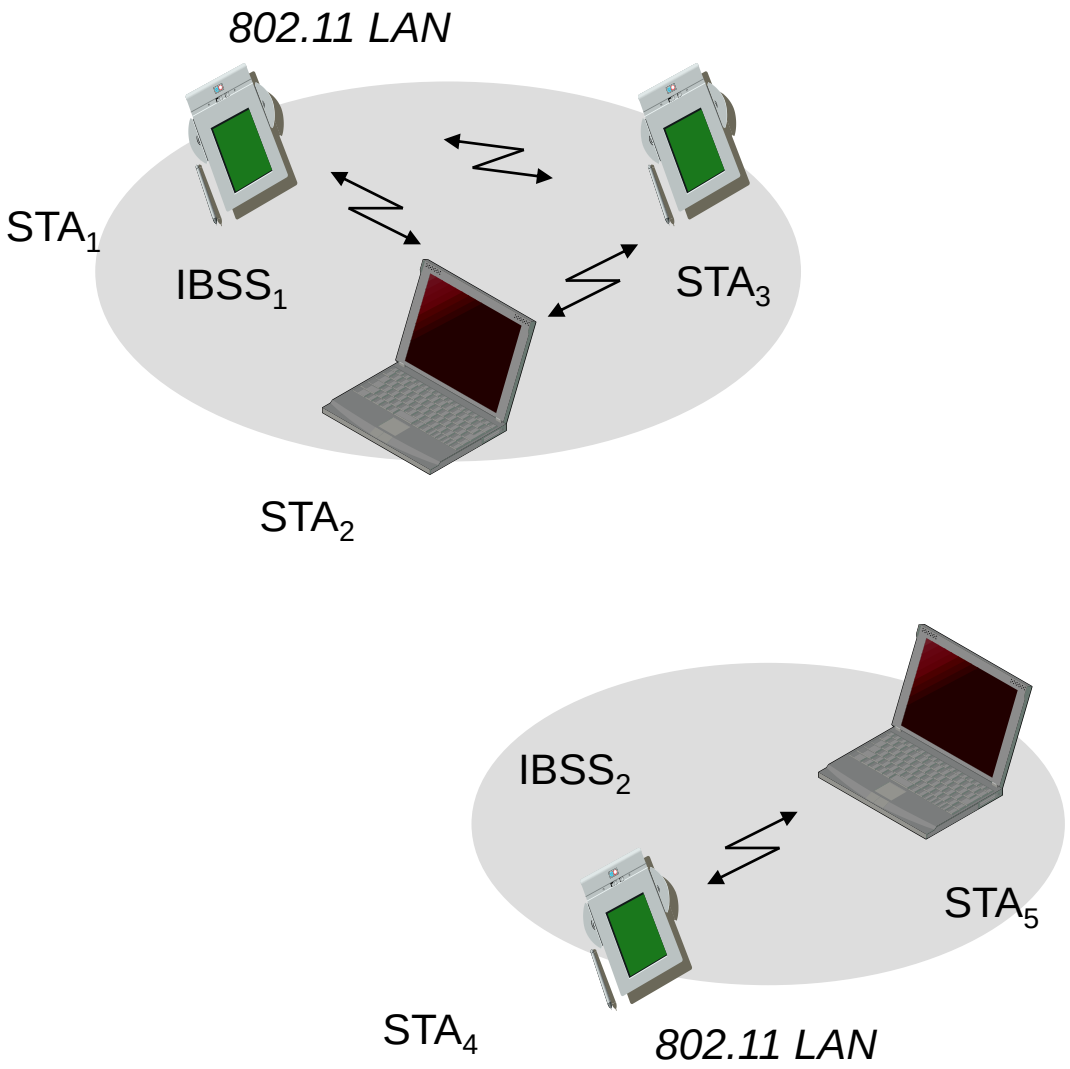



**Figure 4: Architecture of IEEE 802.11 ad-hoc wireless LANs**

# System architecture (2)

- An IBSS comprises a group of stations using the same radio frequency
- Stations $STA_1$, $STA_2$ and $STA_3$ are in $IBSS_1$ whereas $STA_4$ and $STA_5$ are in $IBSS_2$.
- This means that $STA_3$ can communicate directly with $STA_2$ but not with $STA_5$

# Protocol architecture (1)

- IEEE 802.11 fits seamlessly into the other 802.x standards for wired LANs.
- Figure 5 shows the protocol architecture of IEEE 802.11 wireless LAN
- Here the IEEE wireless LAN is connected to a switched IEEE 802.3 Ethernet via a bridge
- Applications should not notice any difference apart from the lower bandwidth and perhaps higher access time from the wireless LAN.
- The higher layers (application, TCP, IP) look the same for wireless nodes as for wired nodes

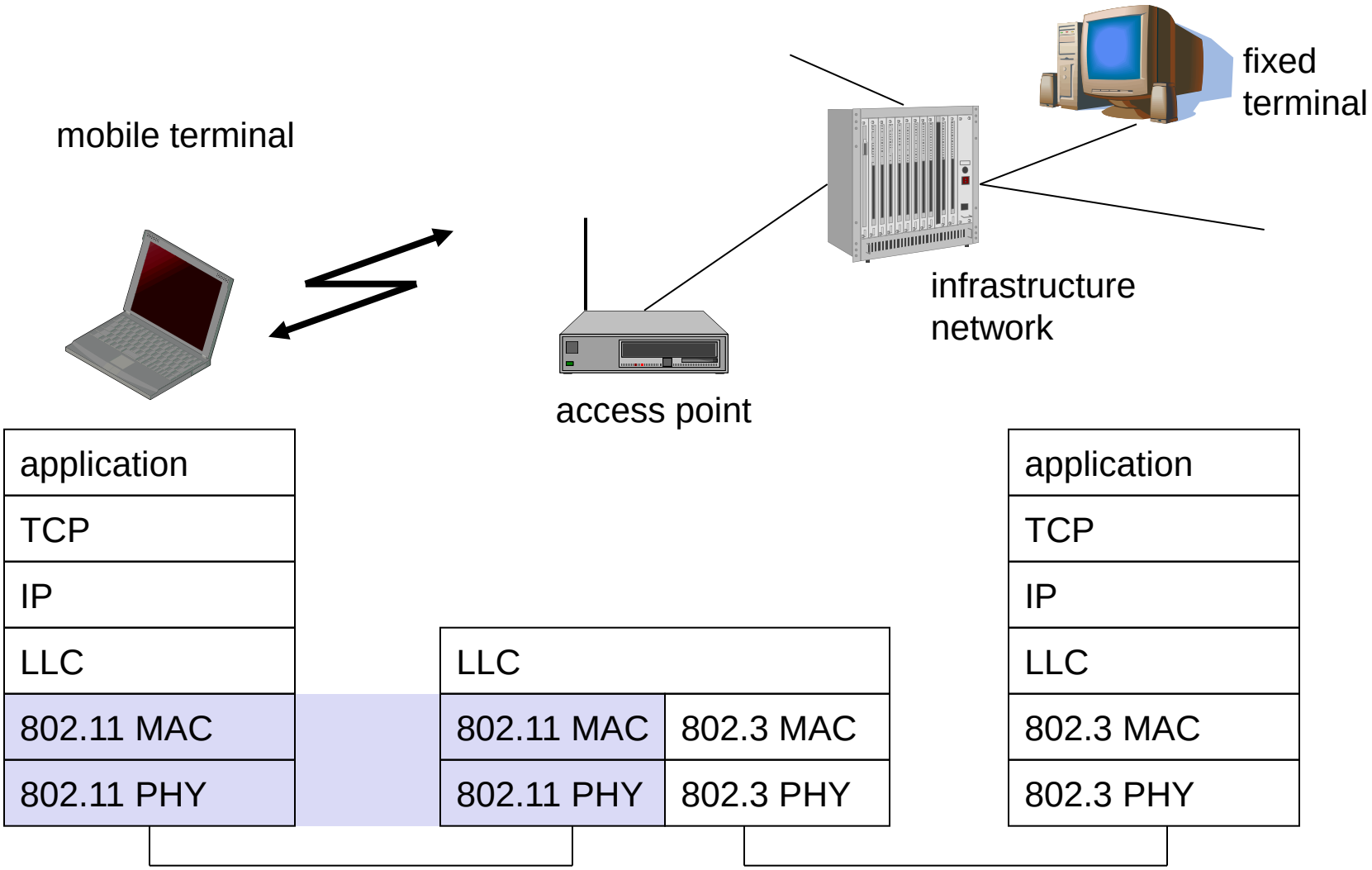



**Figure 5: IEEE 802.11 protocol architecture and bridging**

# Protocol architecture (2)

- The upper part of the data link control layer, the logical link control (LLC), covers the differences of the medium access control layers needed for the different media.
- The IEEE 802.11 standard only covers the physical layer, PHY, and the medium access layer MAC like the 802.x LANs
- The physical layer is subdivided into the physical layer convergence protocol (PLCP) and the physical medium dependent sublayer, PMD (see Figure 6)
- The basic tasks of the MAC layer comprise medium access, fragmentation of user data, and encryption.
- The PLCP sublayer provides a carrier sense signal and provides common PHY service access point (SAP) independent of the transmission technology

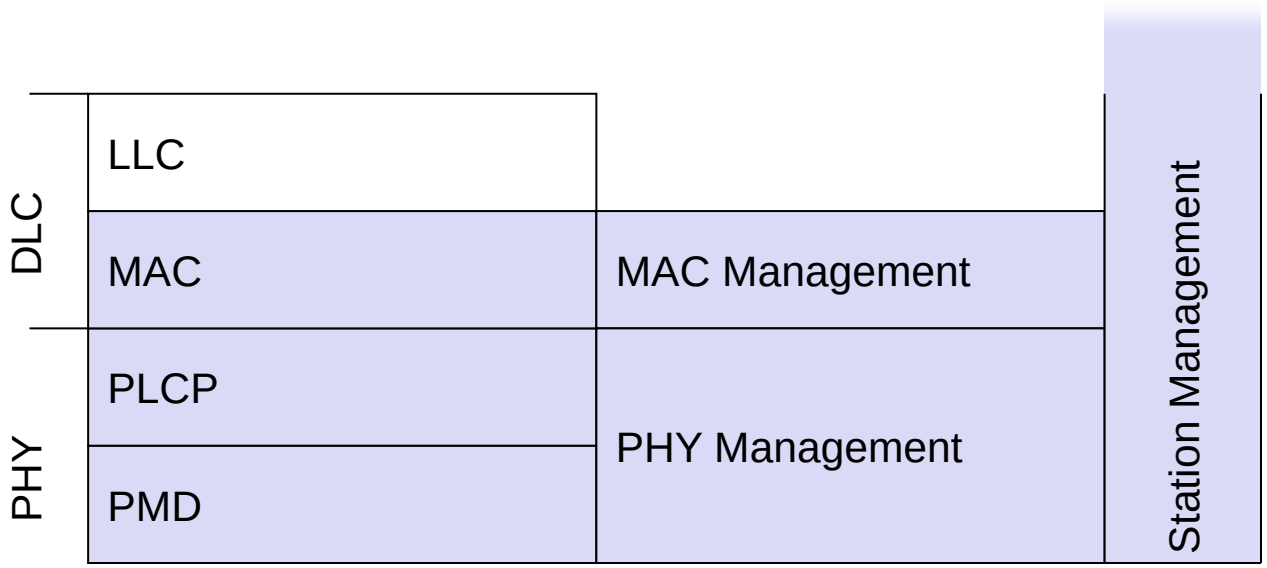



**Figure 6: Detailed IEEE 802.11 protocol architecture and management**

# Protocol architecture (3)

- .The PMD sublayer handles modulation and encoding/decoding of signals
- Apart from protocol sublayers, the standard also specifies management layers and station management
  - The MAC management supports the association and re-association of a station to an access point and roaming between different access points. It also controls authentication mechanisms, encryption etc.
  - The main tasks of the PHY management include channel tuning and PHY MIB (management information base) maintenance.
  - The station management interacts with both management layers and is responsible for additional higher layer functions
    - e.g. control of bridging and interaction with the distribution system in the case of an access point.

# Physical layer (PHY) (1)

- IEEE 802.11 supports three different physical layers:
- One layer based on infra red
  - Uses near visible light at 850-950nm
  - Infra red light is not regulated apart from safety restrictions
  - The standard allows for point-to-multipoint communication
  - Maximum range is about 10 m if there is no interference
- Two layers based on radio transmission (primarily in the ISM band at 2.4 GHz)
  - Frequency hopping spread spectrum (FHSS)
  - Direct sequence spread spectrum (DSSS)

# Frequency hopping spread spectrum (FHSS) (1)

- Spread spectrum techniques involve spreading the bandwidth needed to transmit data
- FHSS is a spread spectrum technique which allows for the coexistence of multiple networks in the same area by separating different networks using different hopping sequences
- In FHSS, the total available bandwidth is split into many channels of smaller bandwidth plus guard spaces between the channels
- Transmitter and receiver stay on one of these channels for a certain time and then hop to another channel
- The pattern of channel usage is called the hopping sequence and the time spent on a channel with a certain frequency is called the *dwell time*.

# Frequency hopping spread spectrum (FHSS) (2)

- The selection of a particular pattern is achieved by using a pseudo-random hopping pattern
- The standard specifies Gaussian shaped frequency shift keying (GFSK) as a modulation for the FHSS PHY.
  - The simplest form of FSK assigns one frequency to the binary 1 and another frequency to the binary 0.
  - In GFSK the pulse is first passed through a Gaussian filter to make it smother so as to limit its spectral width before FSK is applied.
- Fig. 7 shows a frame of the physical layer used in FHSS.
- The frame consists of two basic parts, the PLCP part and the payload (actual data) part

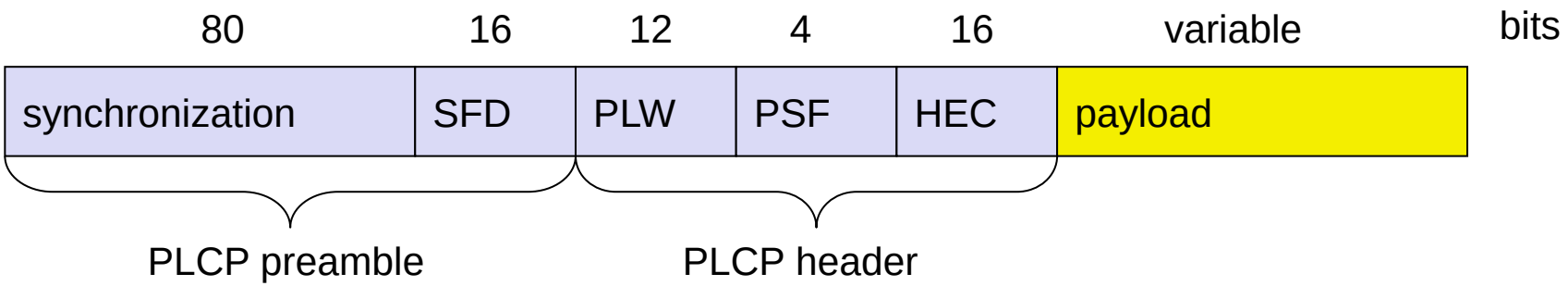



**Figure 7: Format of an IEEE 802.11 PHY frame using FHSS**

# Frequency hopping spread spectrum (FHSS) (3)

- *Synchronization*: the PLCP preamble starts with 80 bit synchronization, which is 010101… bit pattern.
  - This pattern is used for synchronization of potential receivers and signal detection by *clear channel assessment* signal (CCA)
- *Start frame delimiter (SFD)*: the following 16 bits indicate the start of the frame and provide frame synchronization.
  - The SFD pattern is 0000110010111101.
- *PLCP_PDU (Protocol Data Unit) length word (PLW)*:
  - indicates the length of the payload in bytes including the 32-bit CRC (Cyclic Redundancy Check) at the end of the payload
- PLCP signaling field (PSF):
  - This 4-bit field indicates the data rate of the payload following.
- Header error check (HEC):
  - The PLCP header is protected by a 16 bit checksum with the standard ITU-T generator polynomial $G(x) = x^{16} + x^{12} + x^5 + 1$

# Direct sequence spread spectrum (DSSS) (1)

- DSSS systems take a user bit stream and performs an XOR with a *chipping sequence*
- The chipping sequence consists of smaller pulses, called *chips* whose duration is less than that of the bit
- DSSS is the alternative spread spectrum method separating by code and not by frequency
- IEEE 802.11 DSSS PHY uses differential binary phase shift keying (DBPSK) for 1Mbit/s transmission
  - and differential quadrature phase shift keying (DQPSK) (phase shift relative to phase of previous two bits) for 2Mbit/s as modulation schemes.
- Figure 8 shows a frame of the physical layer used in DSSS.

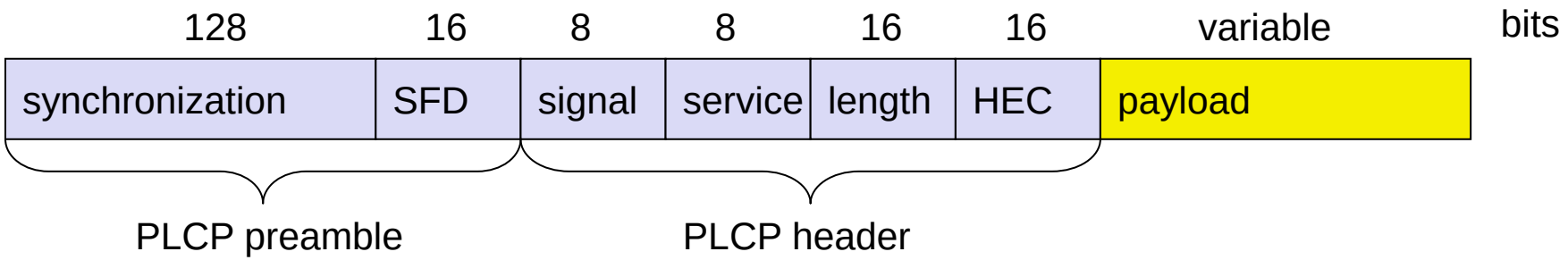



**Figure 8: Format of an IEEE 802.11 PHY frame using DSSS**

# Direct sequence spread spectrum (DSSS) (2)

- *Synchronization*: The first 128 bits are not only used for synchronization,
  - but also gain setting, energy detection (for CCA) and frequency offset compensation
- *Start frame delimiter (SFD)*: This 16 bit field is used for synchronization at the beginning of the frame
  - and consists of a pattern 1111001110100000.
- *Signal*: originally two values have been defined for this field to indicate the data rate of the payload.
  - 0x0A indicates 1Mbit/s, 0x14 indicates 2Mbit/s. other values have been reserved for future use, i.e. higher bit rates
- *Service*: This field is reserved for future use; 0x00 indicates an IEEE 802.11 compliant frame

# Direct sequence spread spectrum (DSSS) (3)

- *Length*: 16 bits are used in this case for length indication of the payload in microseconds
- *Header error check (HEC)*: signal, service and length fields are protected by this checksum
  - using the ITU-T CRC-16 standard polynomial
- 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 transmission technology determines exactly how this signal is obtained
- The PHY layer offers a service access point (SAP) with 1 or 2 Mbit/s transfer rate to the MAC layer

# IEEE 802.11b (1)

- Supplement to the original standard and the most successful version of IEEE 802.11
- Data rate
  - 1, 2, 5.5, 11 Mbit/s, depending on SNR
  - User data rate max. approx. 6 Mbit/s
- Transmission range
  - 300m outdoor, 30m indoor
  - Max. data rate ~10m indoor
- Frequency
  - Free 2.4 GHz ISM-band
- Security
  - Limited, WEP insecure, SSID

# IEEE 802.11b (2)

- Cost
  - 100€ adapter, 250€ base station, dropping
- 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)

# IEEE 802.11b (3)

- 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
- The standard describes a new PHY layer
- All MAC schemes, management procedures described in IEEE 802.11 are still used
- IEEE 802.11b systems offer 11, 5.5, 2 or 1 Mbit/s
  - depending on current interference and distance between sender and receiver
- The standard defines several packet formats for the physical layer

# IEEE 802.11a (1)

- Initially aimed at the US 5GHz UNII (Unlicensed National Information Infrastructure) bands
- 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 25m, 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

# IEEE 802.11a (2)

- Cost
  - 280€ adapter, 500€ base station
- 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

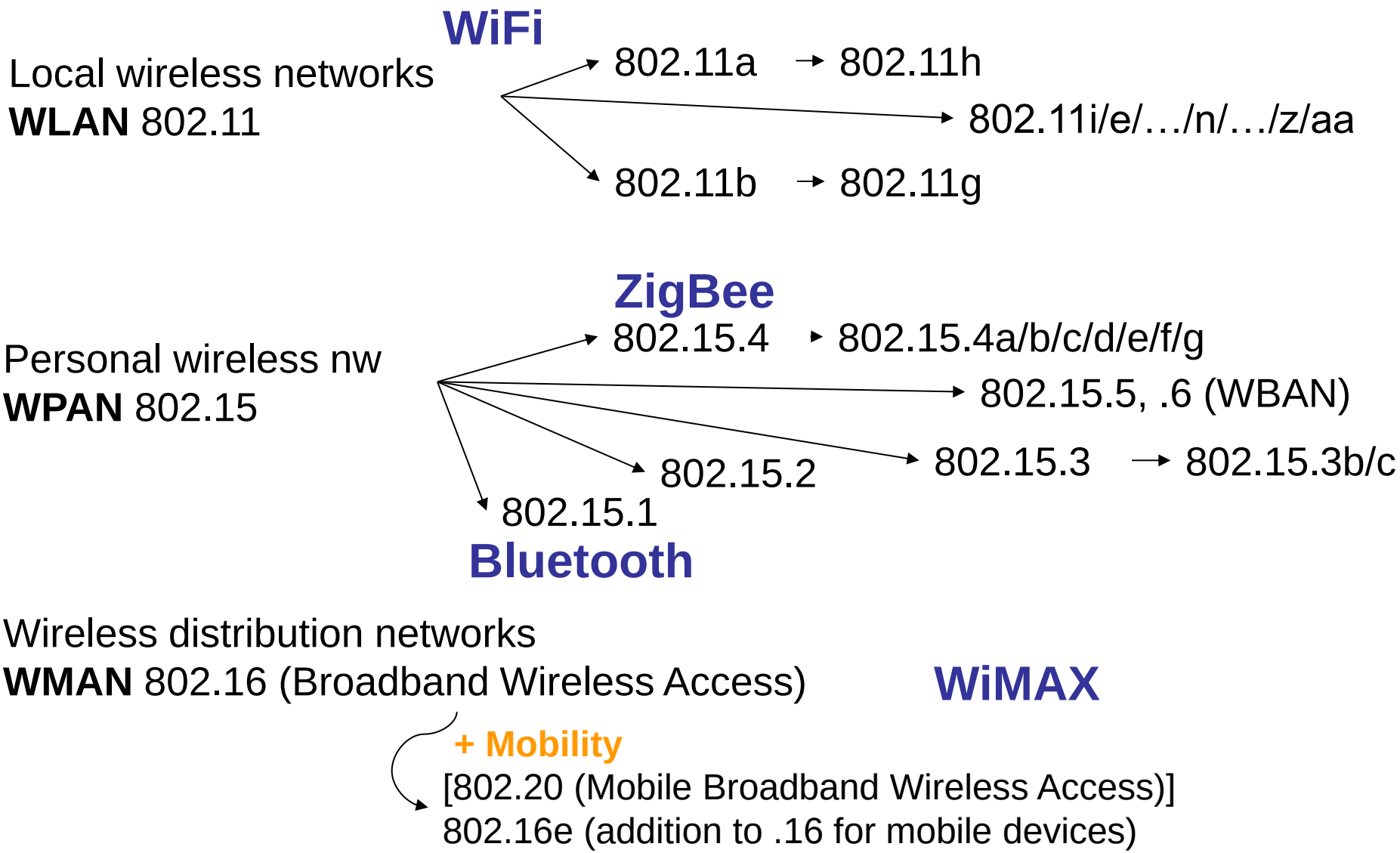



**Figure 9: Mobile Communication Technology according to IEEE (examples)**

# Bluetooth

# Introduction (1)

- Initiated by Ericsson, a Swedish company in 1994 on multi-communicator link.
- Bluetooth consortium founded in 1998 which involved Ericsson, Intel, IBM, Nokia, Toshiba.
- The goal was to develop a single-chip, low cost, radio-based wireless network technology.
- By the end of 1999, many other companies and research institutions joined the special interest group on Bluetooth
  - The goal was the development of mobile phones, laptops, notebooks, headsets etc which include Bluetooth technology.
- In 2001, first products hit the mass market,
  - and today many mobile phones, laptops, PDAs, video cameras are equipped with Bluetooth technology.

# Introduction (2)

- Bluetooth is a short-range technology to set-up wireless personal area networks (WPANs) with gross data rates less than 1Mbit/s.
- Aims at so-called ad-hoc piconets, which are LANs with a very limited coverage and without the need for an infrastructure
- Ad-hoc piconets connect different small devices in close proximity (about 10m) without expensive wiring or the need for a wireless infrastructure.

# User scenarios for wireless piconets or WPANs (1)

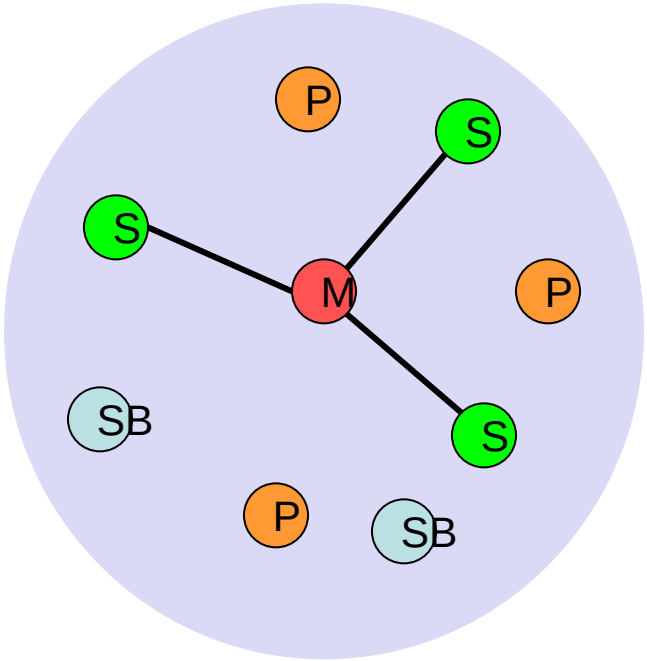
- Connection to peripheral devices:
  - Today, most devices are connected to a desktop computer via wires (e.g keyboard, mouse, joystick, headset, speakers).
  - Connection via wires has several disadvantages:
    - each device has its own type of cable, different plugs are needed, and wires block office space.
  - In a wireless network no wires are needed for data transmission
    - Batteries have to replace power supply, as the wires not only transfer data but also supply the peripheral devices with power
- Support of ad-hoc networking:
  - imagine several people coming together, discussing issues, exchanging data (schedules, sales figures etc.).
    - For instance, students might join a lecture, with the teacher distributing data to their personal digital assistants (PDAs).
  - Wireless networks can support this type of interaction.

# User scenarios for wireless piconets or WPANs (2)

- Bridging of networks:
  - Using wireless piconets, a mobile phone can be connected to a PDA or laptop in a simple way.
  - Mobile phones will not have full WLAN adapters built in, but could have a Bluetooth chip.
  - The mobile phone can act as a bridge between the local piconet and e.g. the global GSM network.
    - For instance, on arrival at an airport, a person's mobile phone could receive e-mail via GSM, and forward it to the laptop which is still in a suitcase.
    - Via a piconet, a fileserver could update local information stored on a laptop or PDA while the person is walking into the office.

# Architecture (1)

- Like the IEEE 802.11b, Bluetooth operates in the 2.4 GHz ISM (Industrial, Scientific, Medical) band.
- MAC and physical layer and the offered services are completely different
- Bluetooth operates on 79 channels in the 2.4 GHz band with 1MHz carrier spacing.
- Each device performs frequency hopping with 1,600 hops/s in a pseudo random fashion
  - For interference mitigation
- A piconet is a collection of Bluetooth devices which are synchronized to the same hopping sequence (Figure 10)
- One device can act as a master (M) and the others as slaves (S) for the lifetime of the piconet




M=Master
S=Slave

P=Parked
SB=Standby

**Figure 10: Simple Bluetooth piconet**

# Architecture (2)

- The master determines the hopping pattern in the piconet and the slaves synchronize to this pattern
- Each piconet has a unique hopping pattern
- If a device wants to participate, it has to synchronize to this
- Parked devices (P) cannot actively participate in the piconet (have no connection) but are known and can be reactivated within milliseconds
- Devices in stand-by (SB) do not participate in the piconet
- Each piconet has one master and up to 7 simultaneous slaves (> 200 could be parked)
  - Due to 3-bit addresses used in Bluetooth

# Architecture (3)

- In order to form a piconet (see Figure 11) active devices must be synchronized
  - Master gives slaves its clock and device ID
  - The hopping pattern is determined by the device ID
  - The phase in hopping pattern is determined by the master's clock
- Addressing
  - All active devices are assigned a 3–bit active member address (AMA)
  - All parked devices use an 8-bit parked member address (PMA).
  - Devices in stand-by mode do not need an address

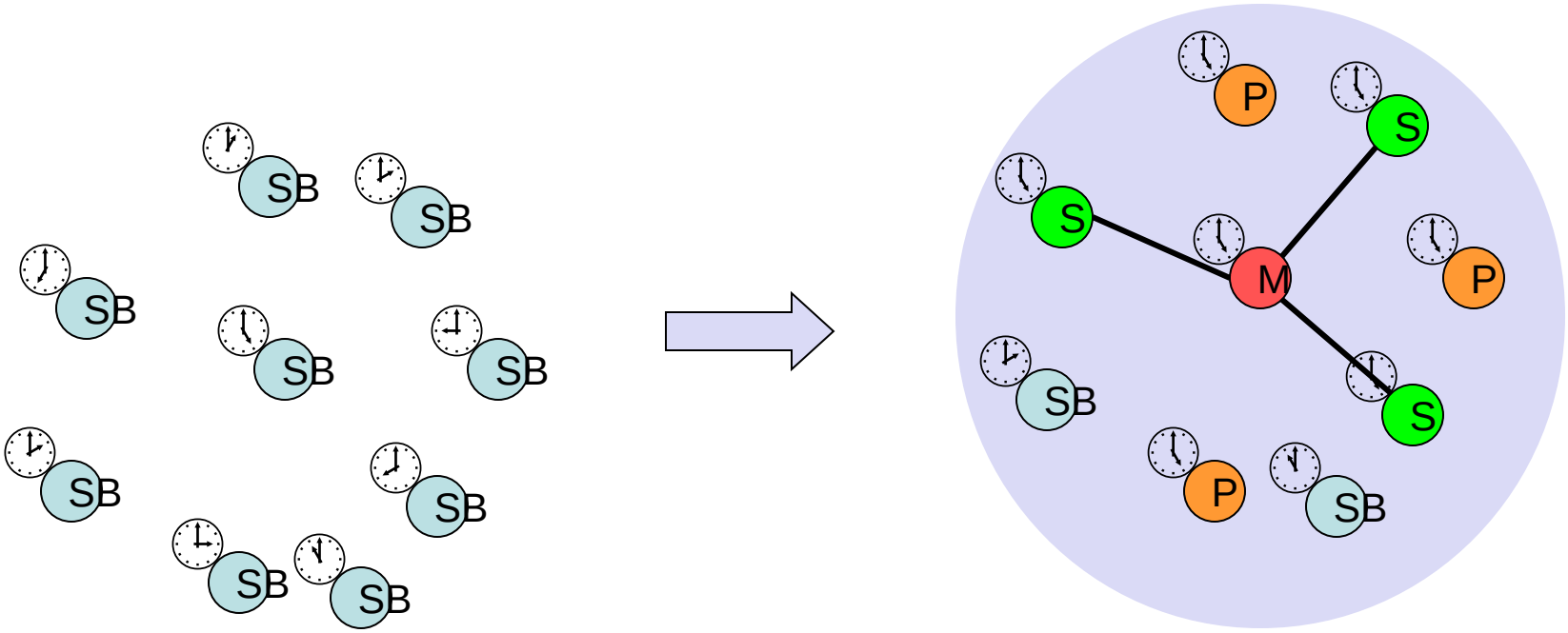



**Figure 11: Forming a Bluetooth piconet**

# Architecture (4)

- As more users join the piconet, the throughput per user drops quickly.
- This led to the idea of forming groups of piconets called scatternet (see Figure 12)
  - This involves 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 involves devices jumping back and forth between the piconets

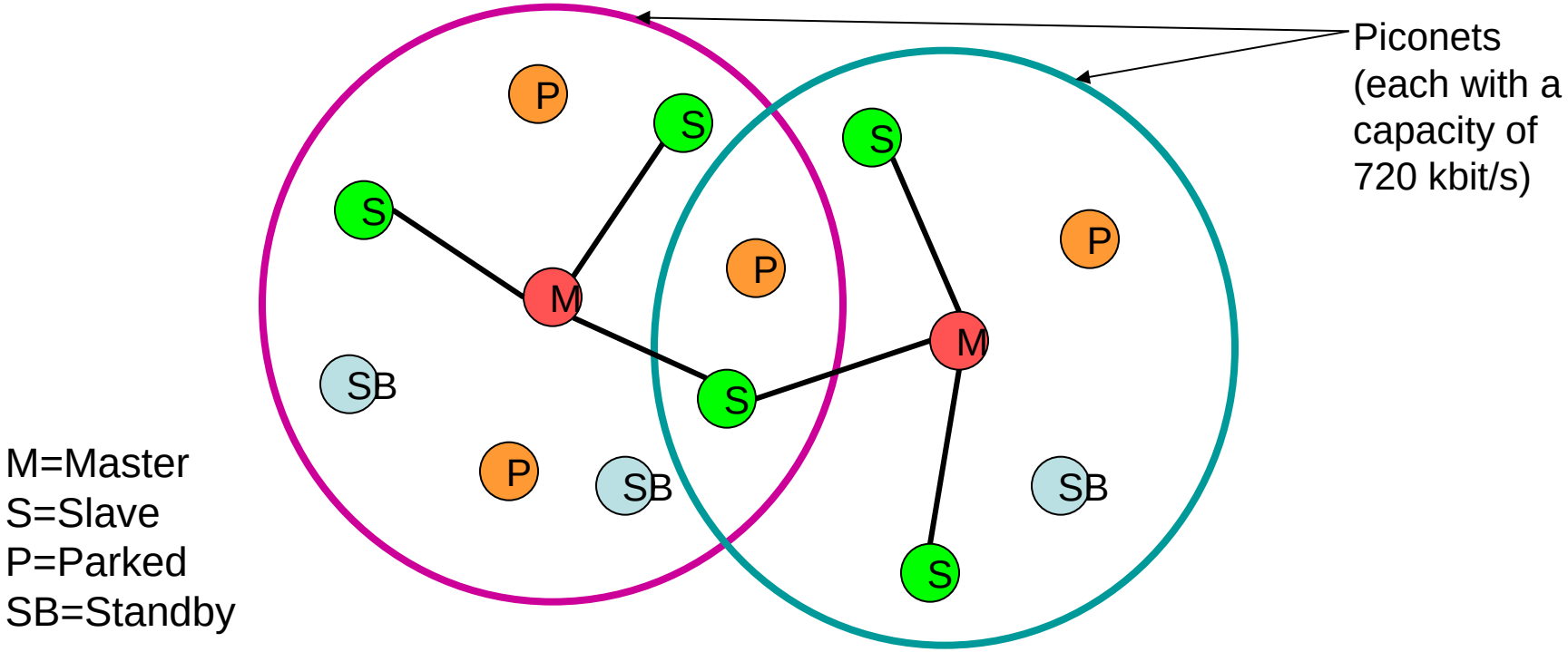
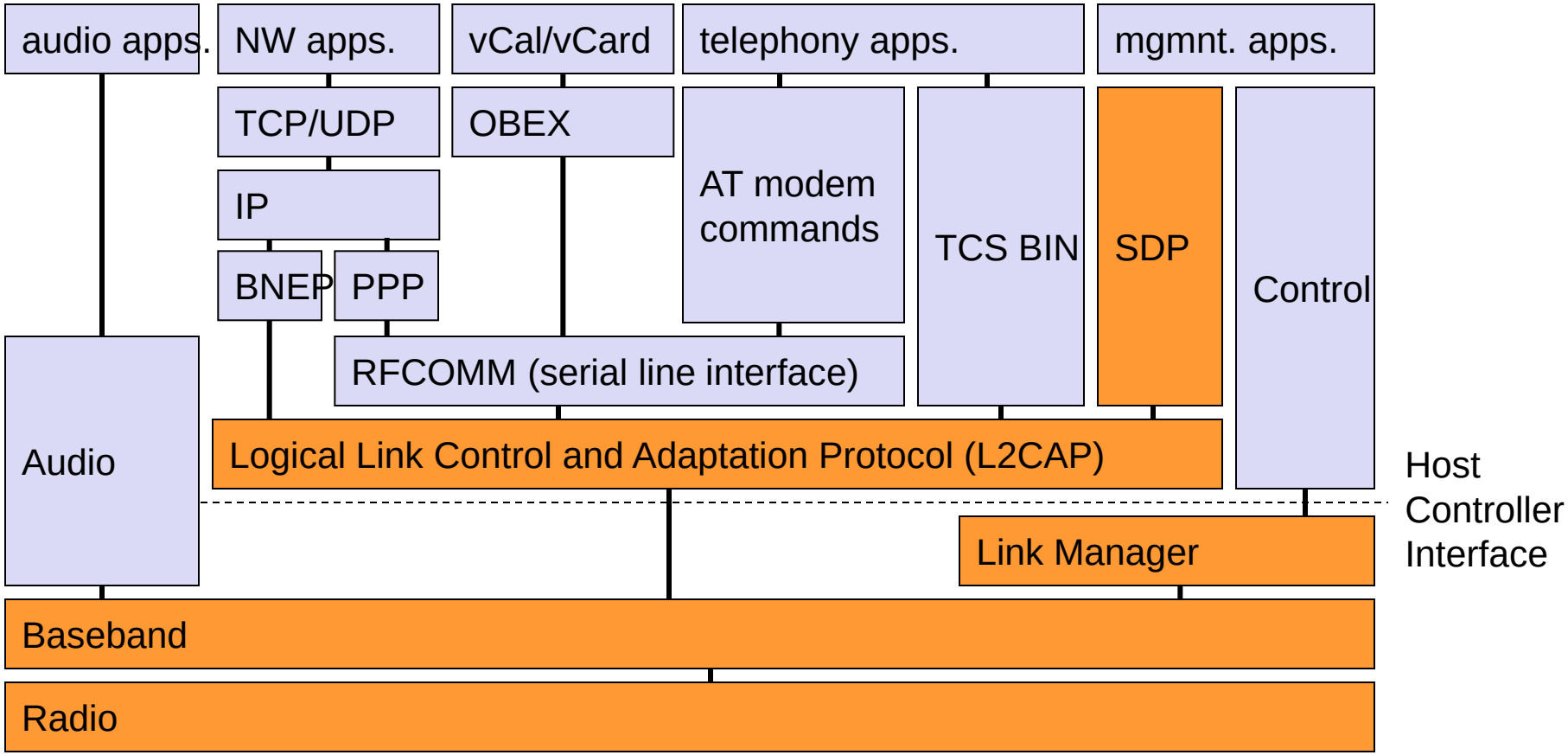



**Figure 12: Bluetooth scatternet**

# Bluetooth protocol stack (1)

- The Bluetooth protocol stack (see Figure 13) can be divided into
  - *core specification*, which describes the protocols from physical layer to the data link control together with management functions
  - *profile specifications* which describes many protocols and functions needed to adapt the wireless Bluetooth technology to legacy and new applications
- The core protocols of Bluetooth comprise the following elements:
  - 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




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.

**Figure 13: Bluetooth protocol stack**

# Bluetooth protocol stack (2)

  - 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.
- On top of L2CAP is the *cable replacement protocol* (RFCOMM)
  - this emulates a serial line interface following the EIA-232 (formally RS-232) standards.
- *Telephony control protocol specification –binary* (TCS BIN)
  - This describes a bit-oriented protocol that defines call control signaling for the establishment of voice and data calls between Bluetooth devices.
- *Host controller interface* (HCI)
  - Lies between the baseband and L2CAP

# Bluetooth protocol stack (3)

  - 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 a hardware/software boundary.
- Many protocols have been adopted in the Bluetooth standard.
  - Classical Internet applications can still use the standard TCP/IP stack running over PPP (Point-to-Point Protocol) or use more efficient Bluetooth network encapsulation protocol (BNEP)
  - Telephony applications can use the AT modem commands as if they are using a standard modem.
  - Calendar and business card objects (vCalendar/vCard) can be exchanged using the object exchange protocol (OBEX) as common with IrDA interfaces.
- A real difference to other protocols is the support of audio. Audio applications directly use the baseband layer after encoding the audio signals.

# HIPERLAN (High Performance LAN)

# HIPERLAN (1)

- In 1996 ETSI standardized HIPERLAN 1 as a WLAN
  - allowing for node mobility and supporting ad-hoc and infrastructure based topologies.
- HIPERLAN stands for high performance local area network.
- It is a European alternative for IEEE 802.11 standards
- HIPERLAN 1 was originally one out of four HIPERLANs envisaged, as ETSI decided to have different types of networks for different purposes.
  - The key feature of all four networks is their integration of time-sensitive data transfer services
  - Over time, names have changed and the former HIPERLANs 2, 3, and 4 are now called HIPERLAN2, HIPERACCESS, and HIPERLINK.

# HIPERLAN (2)

- HIPERLAN 1:
  - This high-speed WLAN supports mobility at data rates above 20Mbit/s.
  - Range is 50m, connections are multi-point-to-multi-point using ad-hoc or infrastructure networks
- HIPERLAN/2:
  - This technology can be used for wireless access to ATM or IP networks and supports up to 25MBit/s user data rate in a point-to-multi-point configuration.
  - Transmission range is 50m with support of slow (<10m/s) mobility.
  - This standard has been modified over time and can now be considered as a high performance WLAN with QoS support.

# HIPERLAN (3)

- HIPERACCESS:
  - This technology could be used to cover the ‘last mile’ to a customer via a fixed radio link, so could be an alternative to cable modems.
  - Transmission range is 5km, data rates of up to 25Mbit/s are supported.
  - However many proprietary products already offer 155Mbit/s and more, plus QoS.
- HIPERLINK:
  - To connect different HIPERLAN access points to HIPERACCESS nodes with a high-speed link, HIPERLINK technology can be chosen.
  - HIPERLINK provides a fixed point-to-point connection with up to 155Mbits/s.

# HIPERLAN (4)

- The current focus is on HiperLAN2,
  - a standard that comprises many elements from ETSI's BRAN (broadband radio access networks) and wireless ATM activities.
- HIPERLAN 1 was a wireless LAN supporting priorities and packet life for data transfer at 23.5 MBit/s,
  - including forward mechanisms, user data encryption, network identification and power conservation mechanisms.

# Architecture of an infrastructure-based HiperLAN2 (1)

- Figure 14 shows the standard architecture of an infrastructure-based HiperLAN2 network.
- Two access points (AP) are attached to a core network.
- Core networks might be Ethernet LANs, firewire connections between audio and video equipment, ATM networks etc.
- Each AP consists of an *access point controller* (APC) and one or more access point transceivers (APT)
- An APT can comprise one or more sectors (shown as cells here)
- Four mobile terminals (MT) are also shown.
- MTs can move around in the cell area as shown.

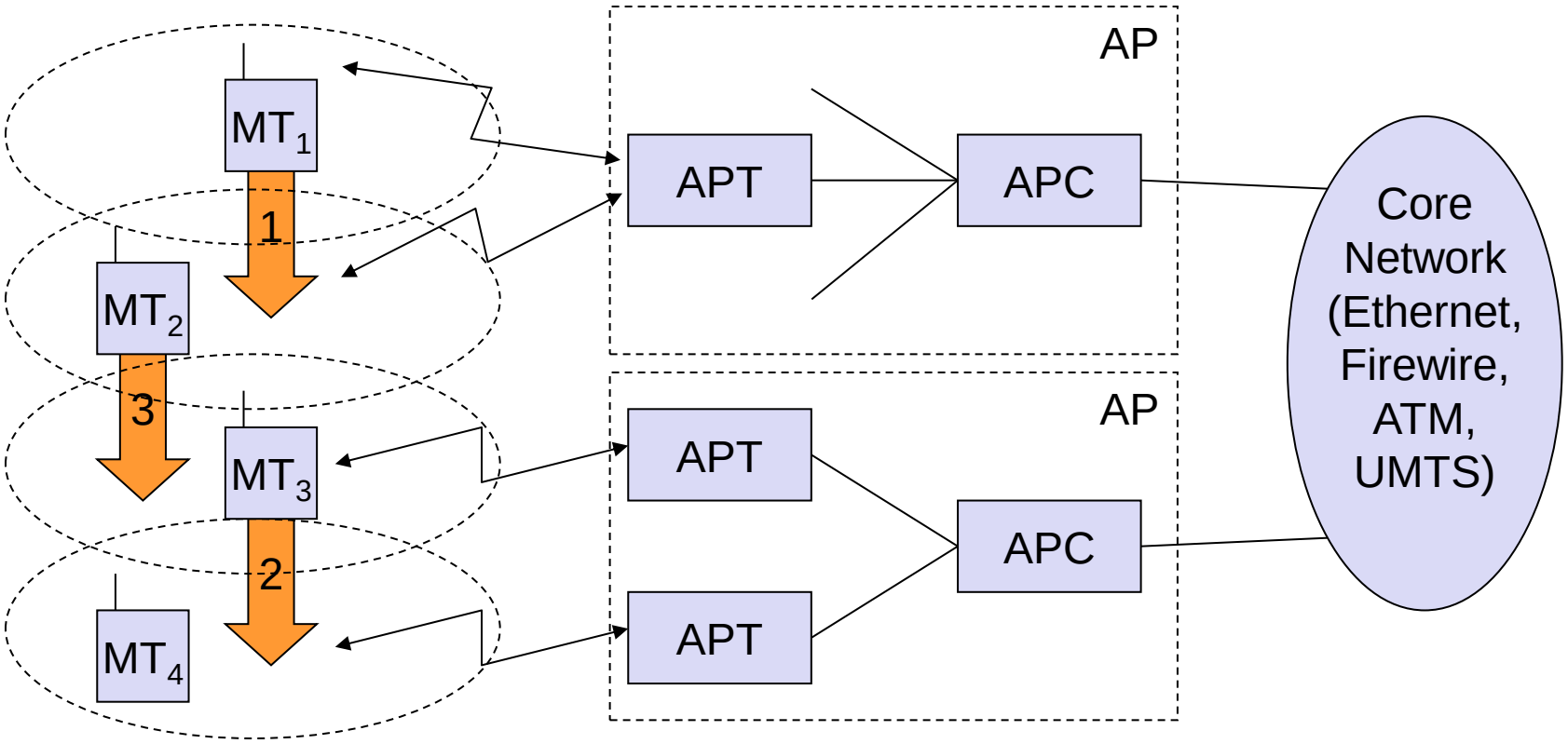



**Figure 14: HiperLAN2 basic structure and handover scenarios**

# Architecture of an infrastructure-based HiperLAN2 (2)

- The system automatically assigns the APT/AP with the best transmission quality.
- No frequency planning is necessary
  - as the APs automatically select the appropriate frequency via dynamic frequency selection.

# Handover Scenarios (1)

Three handover situations may occur

- *Sector handover* (Inter sector):
  - If sector antennas are used for an AP, the AP shall support handover.
  - This type of handover is handled inside the DLC layer so is not visible outside the AP
- *Radio handover* (Inter-APT/Intra-AP):
  - This handover type is handled within the AP, no external interaction is needed.
  - In Figure 14, the terminal $MT_3$, moves from one APT to another of the same AP.
  - All context data for the connections are already in the AP (encryption keys, authentication and connection parameters) and does not have to be renegotiated.

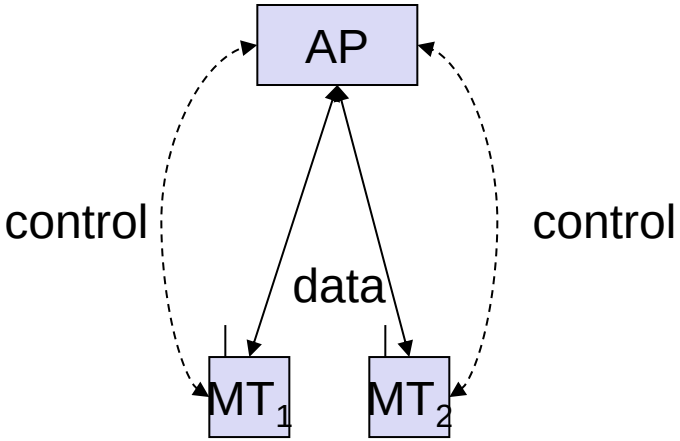
# Handover Scenarios (2)

- *Network handover* (Inter-AP/Intra-network):
  - This is the most complex situation: $MT_2$ moves from one AP to another.
  - In this case, the core network and higher layers are also involved.
  - This handover might be supported by the core network.

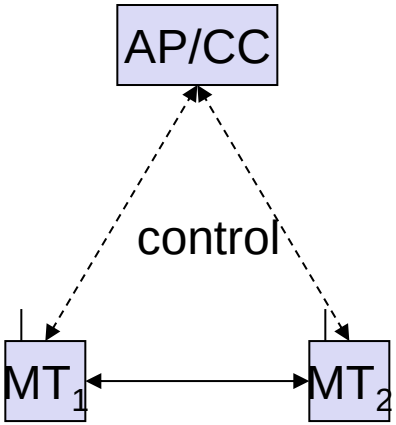
# Modes of Operation (1)

HiperLAN2 networks can operate in two different modes which may be used simultaneously in same network

- *Centralized mode (CM)*:
  - This infrastructure-based mode is shown in a more abstract way in Figure 15 (left).
  - All APs are connected to a core network and MTs are associated with APs.
  - Even if two MTs share the same cell, all data is transferred via the AP.
  - In this mandatory mode the AP takes complete control of everything.




**Centralized**




**Direct**

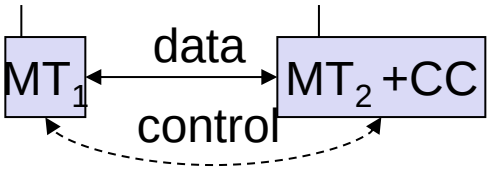



**Figure 15: HiperLAN2 centralized vs. direct mode**

# Modes of Operation (2)

- *Direct mode (DM)*:
  - This optional ad-hoc mode of HiperLAN2 is illustrated in Figure 15 (right).
  - Data is directly exchanged between MTs if they can receive each other, but the network still has to be controlled.
  - This can be done via an AP that contains the central controller (CC) or via an MT that contains the CC functionality.

# HiperLAN2 protocol stack (1)

- Figure 16 shows the HiperLAN2 protocol stack as used in access points.
- The physical layer handles all functions related to modulation, forward error correction, signal detection, synchronization etc.
- The data link control (DLC) layer contains the MAC functions, the radio link control (RLC) sublayer and error control functions.
  - If an AP comprises several APTs then each APT requires an own MAC instance.
- Above the MAC, DLC is divided into a control and a user part.
  - The user part contains error control mechanisms

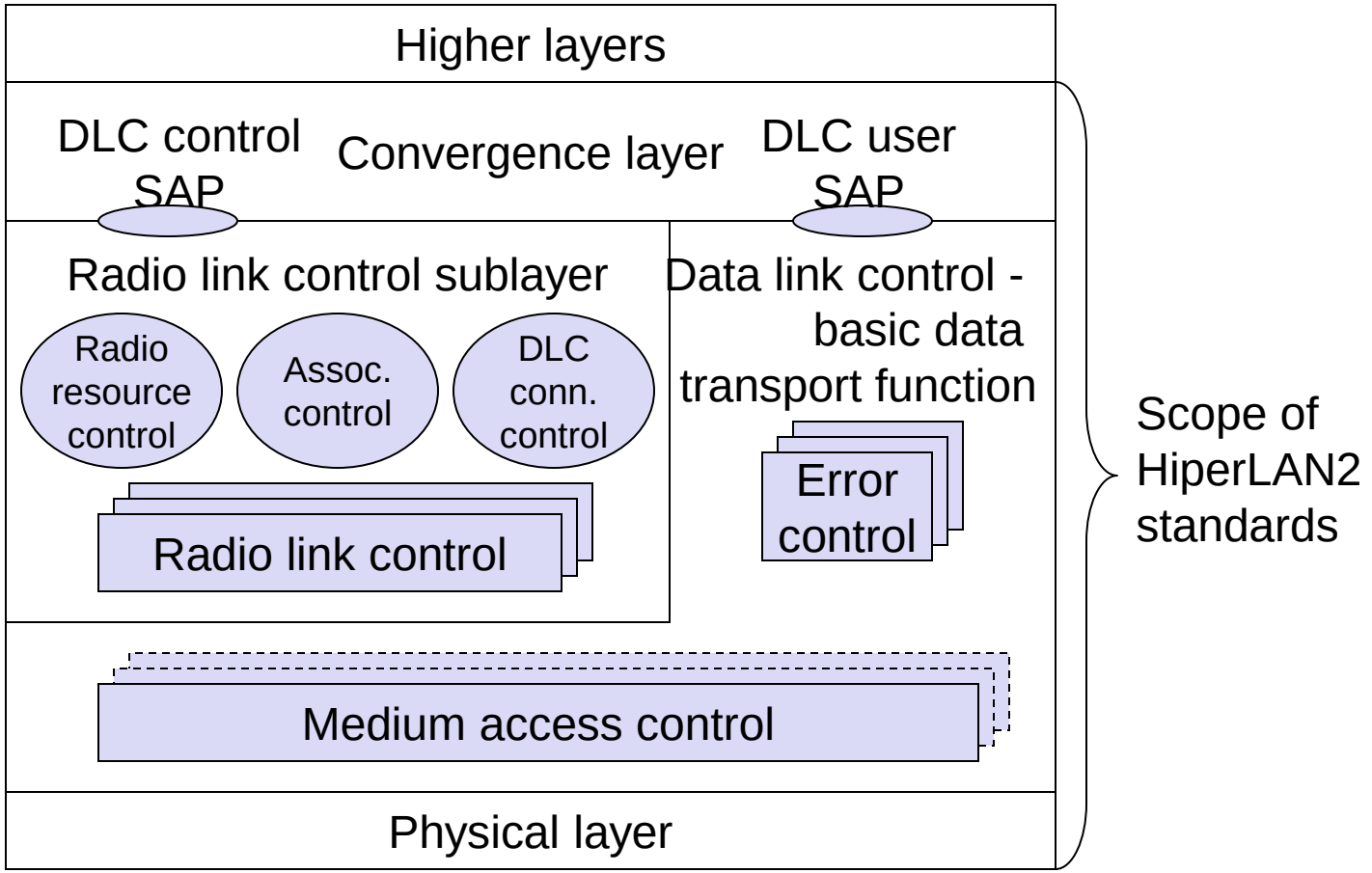



**Figure 16: HiperLAN2 protocol stack**

# HiperLAN2 protocol stack (2)

- The radio link control (RLC) sublayer comprises most control functions in the DLC layer.
  - The association control function (ACF) controls association and authentication of new MTs
  - The DLC user connection control (DDC or DUCC) service controls connection setup, modification, and release.
  - The radio resource control (RRC) handles handover between APs and within an MP. These functions control the dynamic frequency selection and power save mechanisms of the MTs.
- The convergence layer may comprise segmentation and reassembly functions and adaptations to fixed LANs, 3G networks, etc.