WIRELESS LOCAL AREA NETWORKS

MODULE 4

Introduction

- wireless local area network (WLAN) technologies constitute a fast-growing market introducing the flexibility of wireless access into office, home, or production environments.
- These are operated by individuals, not by large-scale network providers.
- The global goal of WLANs is to replace office cabling, to enable tetherless(wireless) access to the internet and, to introduce a higher flexibility for ad-hoc communication in group meetings.
- The two basic variants of WLAN, infrastructure-based and ad-hoc, do not always come in their pure form. There are networks that rely on access points and infrastructure for basic services (e.g., authentication of access, control of medium access for data with associated quality of service, management functions), but that also allow for direct communication between the wireless nodes.
- IEEE 802.11 and HiperLAN2 are typically infrastructure-based networks, which additionally support ad-hoc networking. The third WLAN, Bluetooth, is a typical wireless ad-hoc network

Advantages of WLANs

1.Flexibility: Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (non-visible to each other)

2.Planning: Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans.

3.Design: Wireless networks allow for the design of independent, small devices which can be put into a pocket. Cables not only restrict users but also designers of small notepads, PDAs, etc

4.Robustness: Wireless networks can handle disasters, e.g., earthquakes, flood etc. whereas, networks requiring a wired infrastructure will usually break down completely in disasters

5.Cost: The cost of installing and maintaining a wireless LAN is on average lower than the cost of installing and maintaining a traditional wired LAN, for two reasons.

- First, after providing wireless access to the wireless network via an access point for the first user, adding additional users to a network will not increase the cost.
- And second, wireless LAN eliminates the direct costs of cabling and the labor associated with installing and repairing it.

6.Ease of Use: Wireless LAN is easy to use and the users need very little new information to take advantage of WLANs.

Disadvantages of WLANs

1.Quality of Services: Quality of wireless LAN is typically lower than wired networks. The main reason for this is the lower bandwidth due to limitations is radio transmission, higher error rates due to interference and higher delay/delay variation due to extensive error correction and detection mechanisms.

2.Proprietary Solutions: Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardization functionality plus many enhanced features. Most components today adhere to the basic standards IEEE 802.11a or 802.11b.

3.Restrictions: Several govt. and non-govt. institutions world-wide regulate the operation and restrict frequencies to minimize interference.

Design goals for WLANs

1.Global operation: Wireless LAN products are sold in all countries so, national and international frequency regulations have to be considered.

2.Low Power: Devices communicating via a wireless LAN are typically power consuming, also wireless devices running on battery power. Whereas the LAN design should take this into account and implement special power saving modes and power management functions.

3.License free operation: LAN operators don't want to apply for a special license to be able to use the product. The equipment must operate in a license free band, such as the 2.4 GHz ISM band.

4.Robust transmission technology: If wireless LAN uses radio transmission, many other electrical devices can interfere with them (such as vacuum cleaner, train engines, hair dryers, etc.).Wireless LAN transceivers cannot be adjusted for perfect transmission in a standard office or production environment

5.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.

6.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

7.Protection of investment: A lot of money has already been invested into wired LANs. The new WLANs should protect this investment by being interoperable with the existing networks. This means that simple bridging between the different LANs should be enough to interoperate, i.e., the wireless LANs should support the same data types and services that standard LANs support.

8.Safety and security: Wireless LANs should be safe to operate, especially regarding low radiation if used, e.g., in hospitals. Users cannot keep safety distances to antennas. The equipment has to be safe for pacemakers, too.

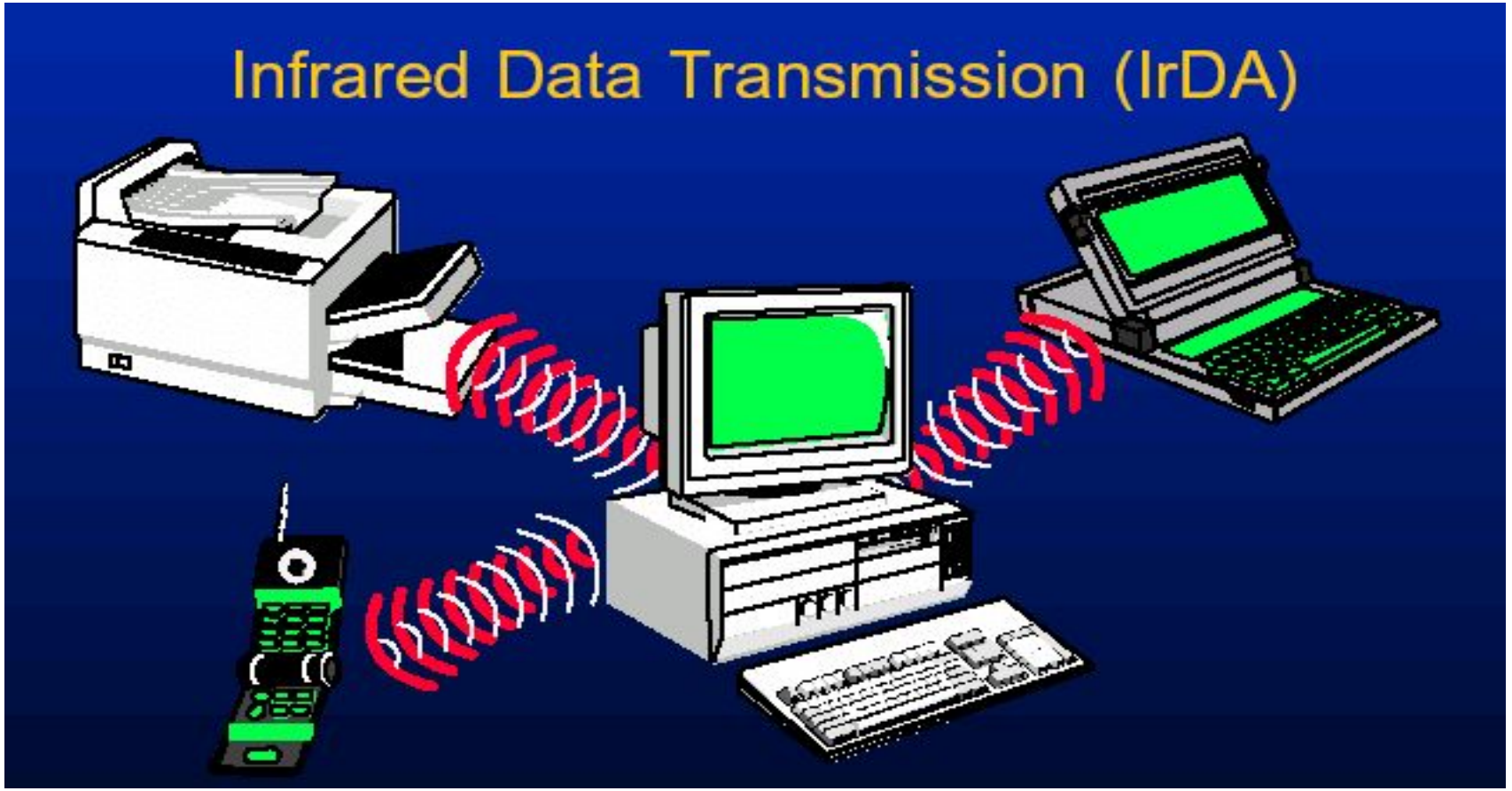
- Users should not be able to read personal data during transmission, i.e., encryption mechanisms should be integrated. The networks should also take into account user privacy, i.e., it should not be possible to collect roaming profiles for tracking persons if they do not agree.

9.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

Infrared vs Radio Transmission

Infrared Transmission



- Infrared technology uses diffuse light reflected at walls, furniture etc. or a directed light if a line of sight (LOS) exists between sender and receiver.
- Infrared light is the part of the electromagnetic spectrum, and is an electromagnetic form of radiation. It comes from the heat and thermal radiation, and it is not visible to the naked eyes.
- In infrared transmission, senders can be simple light emitting diodes (LEDs) or laser diodes. Photodiodes act as receivers.
- Infrared is used in wireless technology devices or systems that convey data through infrared radiation. Infrared is electromagnetic energy at a wave length or wave lengths somewhat longer than those of red light.

- Infrared wireless is used for medium and short range communications and control. Infrared technology is used in instruction detectors; robot control system, medium range line of sight laser communication, cordless microphone, headsets, modems, and other peripheral devices.
- Infrared radiation is used in scientific, industrial, and medical application. Night vision devices using active near infrared illumination allow people and animals to be observed without the observer being detected.
- Infrared transmission technology refers to energy in the region of the electromagnetic radiation spectrum at wavelength longer than those of visible light but shorter than those of radio waves.
- Infrared technology allows computing devices to communicate via short range wireless signals. With infrared transmission, computers can transfer files and other digital data bidirectional.

Advantages of infrared

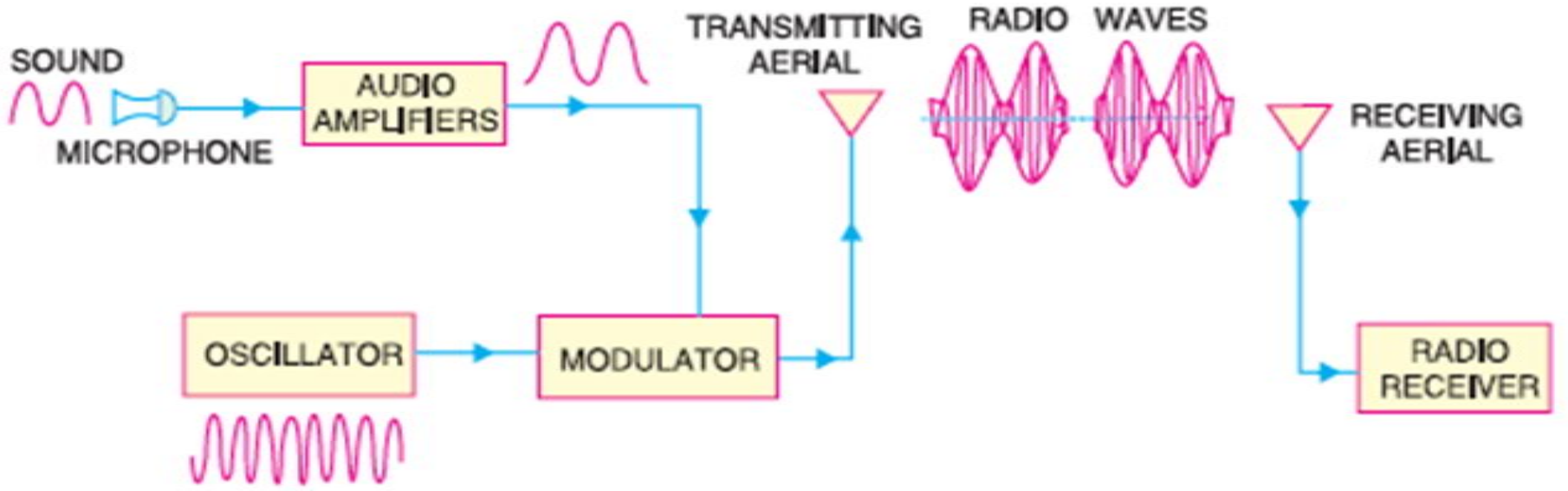
1. The main advantage of infrared technology is its simple and extremely cheap senders and receivers which are integrated into nearly all mobile devices available today.
2. No licenses are required for infrared and shielding is very simple.
3. PDAs, laptops, notebooks, mobile phones etc. have an infrared data association (IrDA) interface.
4. Electrical devices cannot interfere with infrared transmission.

Disadvantages of Infrared

1. Disadvantages of infrared transmission are its low bandwidth compared to other LAN technologies.
2. Limited transfer rates to 115 Kbit/s and we know that even 4 Mbit/s is not a particular high data rate.
3. Their main disadvantage is that infrared is quite easily shielded.
4. Infrared transmission cannot penetrate walls or other obstacles.
5. Typically, for good transmission quality and high data rates a LOS (Line of site), i.e. direct connection is needed.

Radio Transmission

- Almost all networks use radio waves for data transmission, e.g., GSM at 900, 1800, and 1900 MHz, DECT at 1880 MHz etc. Radio transmission technologies can be used to set up ad-hoc connections for work groups, to connect, e.g., a desktop with a printer without a wire, or to support mobility within a small area.



- The two main types of radio transmission are AM (Amplitude Modulation) and (FM) Frequency Modulation.
- FM minimizes noise and provides greater reliability. Both AM and FM process sounds in patterns that are always varying of electrical signals.
- In an AM transmission the carrier wave has a constant frequency, but the strength of the wave varies. The FM transmission is just the opposite; the wave has constant amplitude but a varying frequency.
- Usually the radio transmission is used in the transmission of sounds and pictures. Such as, voice, music and television.
- The images and sounds are converted into electrical signals by a microphone or video camera. The signals are amplified, and transmitted. If the carrier is amplified it can be applied to an antenna.
- The antenna converts the electrical signals into electromagnetic waves and sends them out or they can be received. The antenna consists commonly of a wire or set of wires.

Advantages of Radio Transmission

1. radio transmissions are used for wide area networks (e.g. microwave links) and mobile cellular phones.
2. Radio transmission can cover larger areas and can penetrate (thinner) walls, plants, furniture etc.
3. Additional coverage is gained by reflection.
4. Radio typically does not need a LOS (Line of Site) if the frequencies are not too high.
5. Higher transmission rates (e.g. 54 Mbit/s) than infrared.

Disadvantages of Radio Transmission

1. Radio transmission can be interfered with other senders, or electrical devices can destroy data transmitted via radio.
2. Bluetooth is simple and more basic than infrared.
3. Radio is only permitted in certain frequency bands.
4. Shielding is not so simple.
5. Very limited ranges of license free bands are available worldwide and those that are available are not the same in all countries.

Infrastructure networks

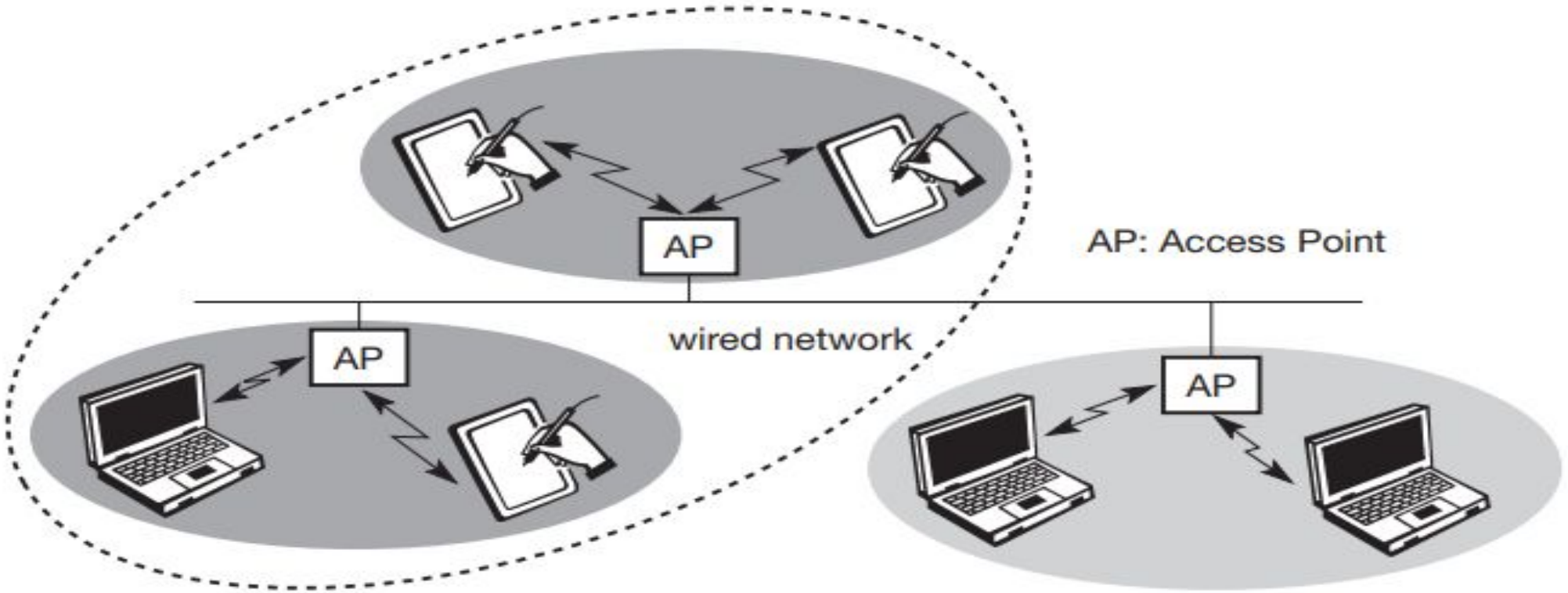


Fig.1:Infrastructure-based wireless networks

- Infrastructure networks not only provide access to other networks, but also include forwarding functions, medium access control etc
- In these infrastructure-based wireless networks, communication typically takes place only between the wireless nodes and the access point, 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.
- Several wireless networks may form one logical wireless network, so the access points together with the fixed network in between can connect several wireless networks to form a larger network beyond actual radio coverage.

- Typically, the design of infrastructure-based wireless networks is simpler because most of the network functionality lies within the access point, whereas the wireless clients can remain quite simple.
- This structure is similar to switched Ethernet or other star-based networks, where a central element (e.g., a switch) controls network flow.
- This type of network can use different access schemes with or without collision. Collisions may occur if medium access of the wireless nodes and the access point is not coordinated.
- However, if only the access point controls medium access, no collisions are possible. This setting may be useful for quality of service guarantees such as minimum bandwidth for certain nodes. The access point may poll the single wireless nodes to ensure the data rate.
- 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.

Advantages of Infrastructure LAN

1. An access point allows to easily expand a wired network with wireless capability
2. Wired and wirelessly networked computers can communicate with each other
3. If there are multiple access points to the network, as in an office or large home, users can *roam* between interlocking access point cells, without ever losing a connection to the network
4. If access point is with a built-in router and firewall, the router allows to share Internet access between all computers, and the firewall hides the network
5. The design of infrastructure-based wireless networks is simpler because most of the network functionality lies within the access point, whereas the wireless clients can remain quite simple

Ad-hoc wireless networks

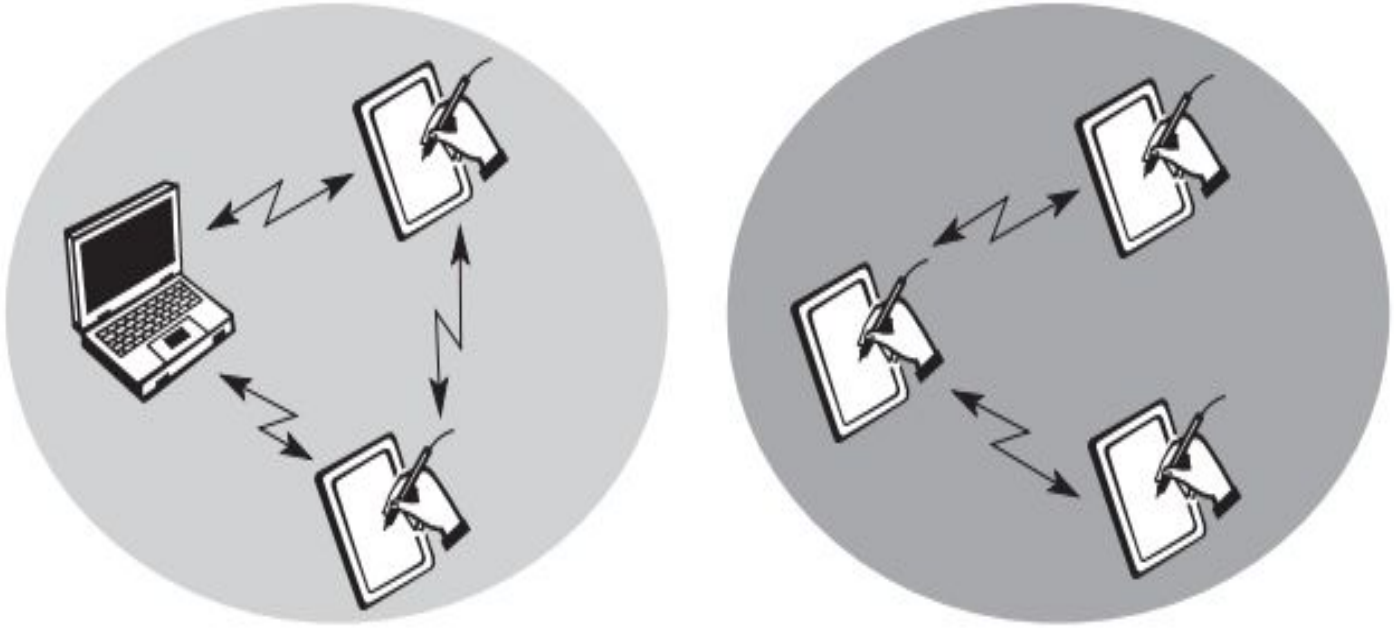


Fig.2:Two ad-hoc wireless networks

- Ad-hoc wireless networks, do not need any infrastructure to work. Each node can communicate directly with other nodes, so no access point controlling medium access is necessary.
- Figure2 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 or if other nodes can forward the message.
- Nodes from the two networks cannot communicate with each other if they are not within the same radio range.
- In ad-hoc networks, the complexity of each node is higher because every node has to implement medium access mechanisms, mechanisms to handle hidden or exposed terminal problems, and perhaps priority mechanisms, to provide a certain quality of service.
- This type of wireless network exhibits the greatest possible flexibility needed for unexpected meetings, quick replacements of infrastructure or communication scenarios far away from any infrastructure.

Advantages of ADHOC LAN

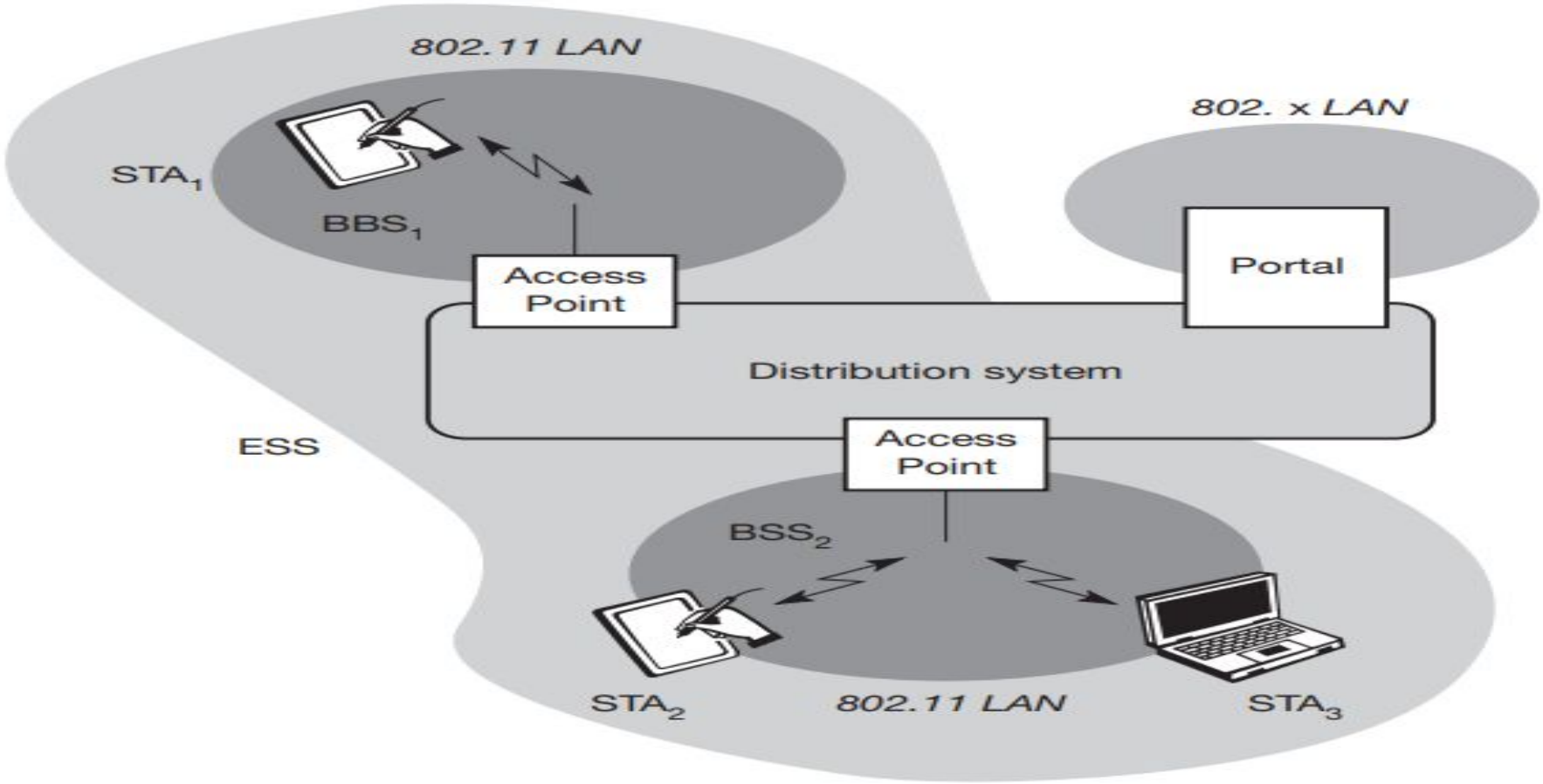
1. Ad-hoc networks are simple to set up
2. Ad-hoc networks are inexpensive as the cost of purchasing an access point is reduced
3. Ad-hoc networks are fast. Throughput rates between two wireless network adapters are twice as fast as when an access point is used.
4. Adhoc mode is suitable for quick wireless connection setup in office rooms, hotels or in places where wired infrastructure is not available

Infrastructure Network	Infrastructure-less Network (Ad hoc)
This network is faster than Ad hoc network.	This network is slower than infrastructure network.
This network provides more security options.	This network provides fewer security options.
In this network access point handles all wireless nodes which are present in range.	There is no need for access point in Ad hoc networks.
Applications are IEEE 802.11 and HIPERLAN2.	Bluetooth is a type of Ad hoc network.
This network used frequently in hotel lobbies, airport lounges, train stations, etc.	This networks are frequently used in the military, local networks are used for communication among a fixed group of people, etc.
For the set up of a permanent network, an infrastructure network is used.	For the set up of a temporary network, an Ad hoc network is used.

IEEE 802.11

- **IEEE 802.11** is part of the IEEE 802 set of local area network (LAN) technical standards, and specifies the set of medium access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) computer communication.
- The standard and amendments provide the basis for wireless network products using the Wi-Fi brand and are the world's most widely used wireless computer networking standards.
- IEEE 802.11 is used in most home and office networks to allow laptops, printers, smartphones, and other devices to communicate with each other and access the Internet without connecting wires.

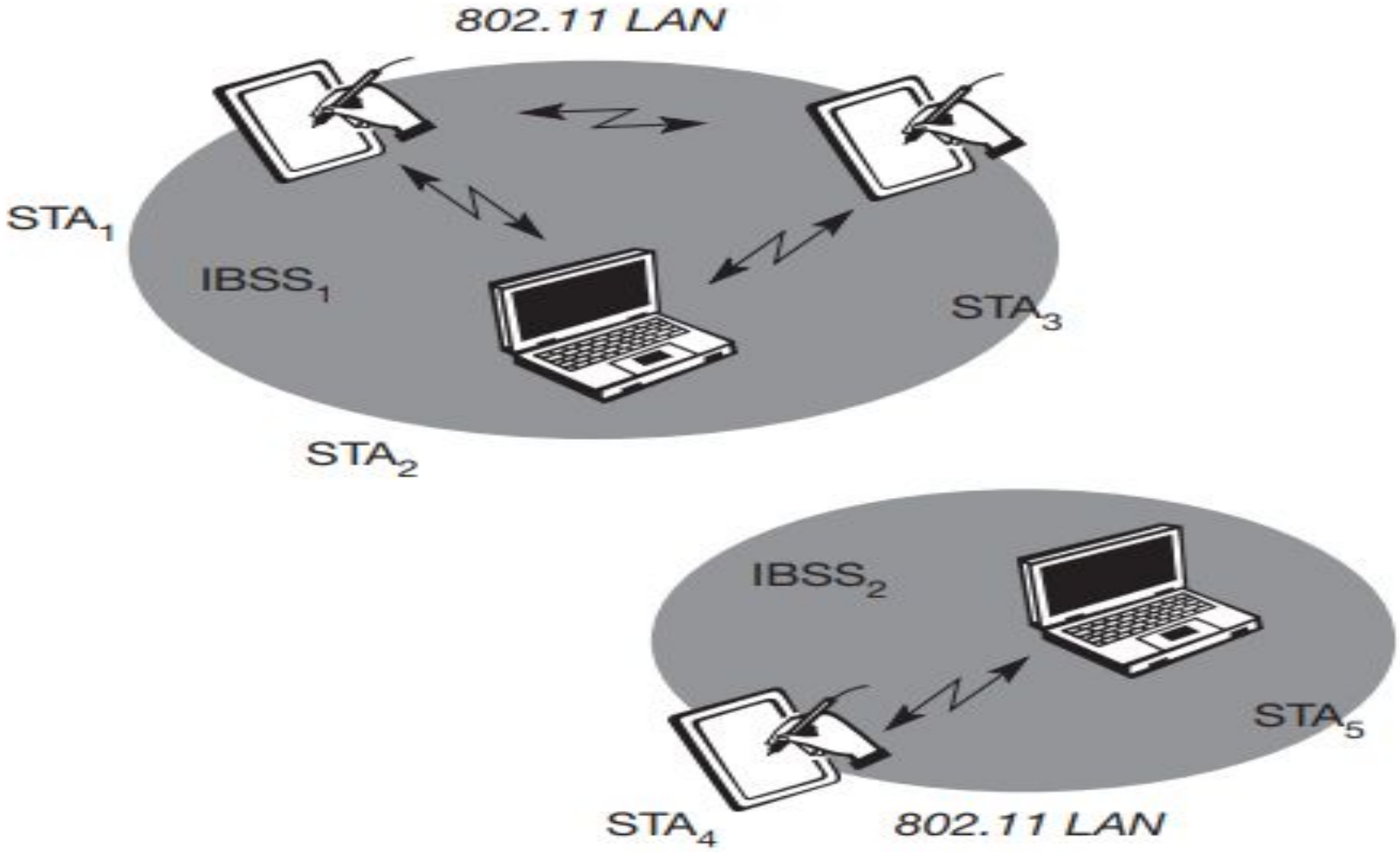
System architecture



Architecture of an infrastructure-based IEEE 802.11

- Several nodes, called stations (STAi), 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 (BSSi). The example shows two BSSs – BSS1 and BSS2 – which are connected via a distribution system.
- A distribution system connects several BSSs via the AP to form a single network and thereby extends the wireless coverage area. This network is now called an extended service set (ESS) and has its own identifier, the ESSID.
- The ESSID is the ‘name’ of a network and is used to separate different networks. Without knowing the ESSID, it should not be possible to participate in the WLAN.

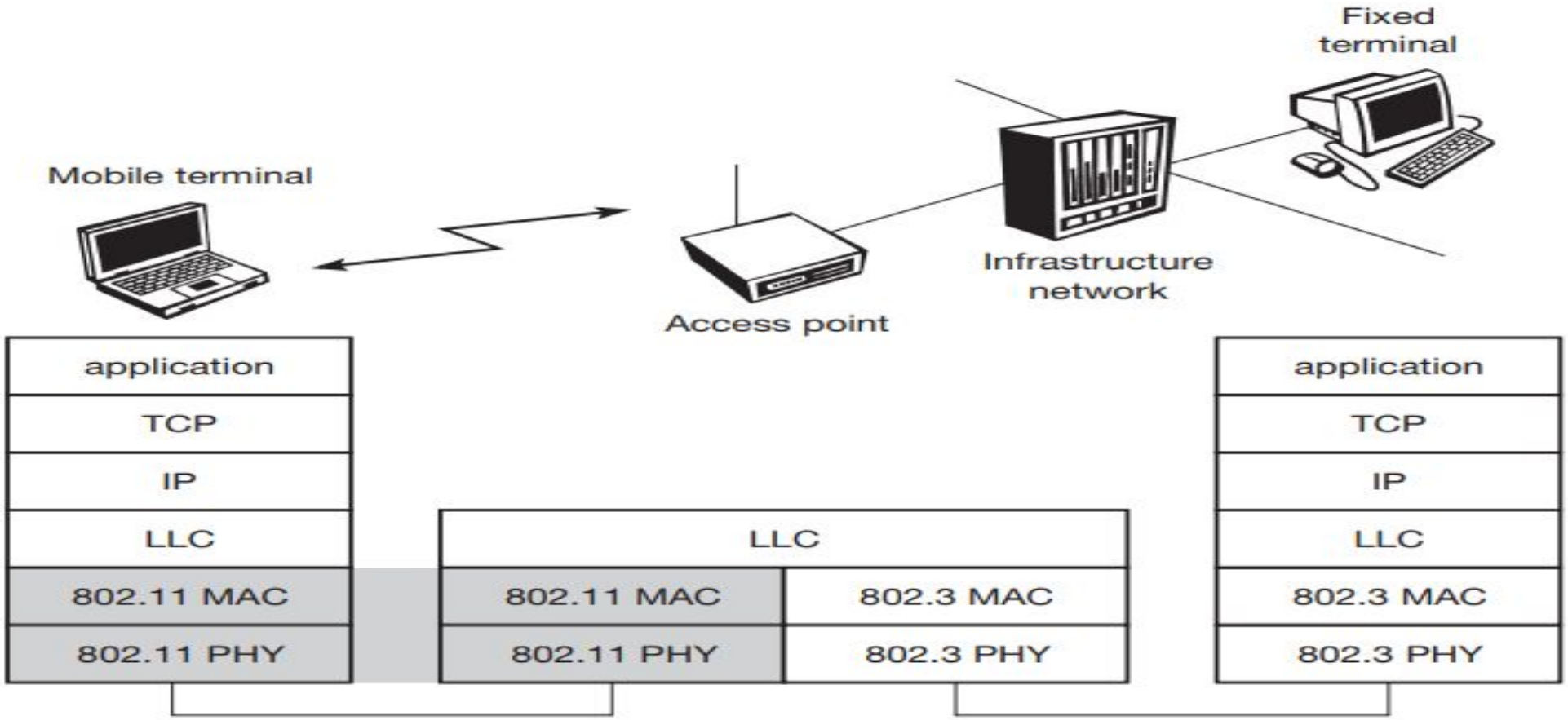
- The distribution system connects the wireless networks via the APs with a portal, which forms the interworking unit to other LANs.
- Stations can select an AP and associate with it. The APs support roaming (i.e., changing access points), the distribution system handles data transfer between the different APs.
- APs provide synchronization within a BSS, support power management, and can control medium access to support time-bounded service.



Architecture of IEEE 802.11 ad-hoc wireless LANs

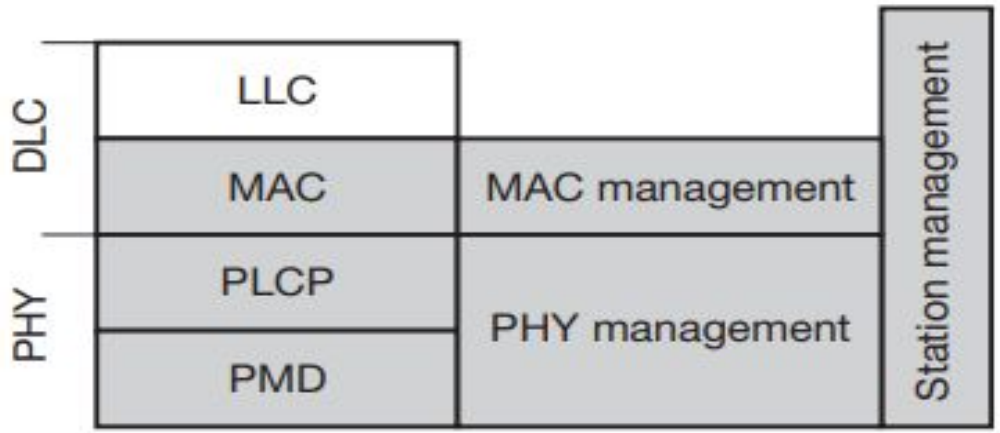
- In IEEE 802.11 ad-hoc wireless LANs, an IBSS comprises a group of stations using the same radio frequency.
- Stations STA1, STA2, and STA3 are in IBSS1, STA4 and STA5 in IBSS2. This means for example that STA3 can communicate directly with STA2 but not with STA5.
- Several IBSSs can either be formed via the distance between the IBSSs or by using different carrier frequencies (then the IBSSs could overlap physically).
- IEEE 802.11 does not specify any special nodes that support routing, forwarding of data or exchange of topology information as, e.g., HIPERLAN 1 or Bluetooth.

Protocol architecture



IEEE 802.11 protocol architecture and bridging

- IEEE 802.11 wireless LAN 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 WLAN behaves like a slow wired LAN. Consequently, the higher layers (application, TCP, IP) look the same for wireless nodes as for wired nodes.
- The IEEE 802.11 standard only covers the physical layer PHY and medium access layer MAC like the other 802.x LANs do.
- The physical layer is subdivided into the physical layer convergence protocol (PLCP) and the physical medium dependent sublayer PMD.
- The basic tasks of the MAC layer comprise medium access, fragmentation of user data, and encryption.



IEEE 802.11 protocol architecture and management

- The PLCP sublayer provides a carrier sense signal, called clear channel assessment (CCA), and provides a common PHY service access point (SAP) independent of the transmission technology.
- Finally, the PMD sublayer handles modulation and encoding/decoding of signals.
- Apart from the protocol sublayers, the standard specifies management layers and the 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, synchronization of a station with regard to an access point, and power management to save battery power
- MAC management also maintains the MAC management information base (MIB).
- The main tasks of the PHY management include channel tuning and PHY MIB maintenance.
- Finally, 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).

IEEE802.11 Physical layer

- IEEE 802.11 supports three different physical layers:

1. one layer based on infra red and
2. two layers based on radio transmission

(primarily in the ISM band at 2.4 GHz, which is available worldwide).

- 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.

a) Frequency hopping spread spectrum physical layer

- Frequency hopping spread spectrum (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.
- The original standard defines 79 hopping channels for North America and Europe, and 23 hopping channels for Japan (each with a bandwidth of 1 MHz in the 2.4 GHz ISM band).
- The selection of a particular channel is achieved by using a pseudo-random hopping pattern.
- National restrictions also determine further parameters, e.g., maximum transmit power is 1 W in the US, 100 mW EIRP (equivalent isotropic radiated power) in Europe and 10 mW/MHz in Japan.

- The frame consists of two basic parts,

1.the PLCP part (preamble and header) and

2.the payload part.

- While the PLCP part is always transmitted at 1 Mbit/s, and payload (MAC data) can use 1 or 2 Mbit/s.
- Additionally, MAC data is scrambled using the polynomial

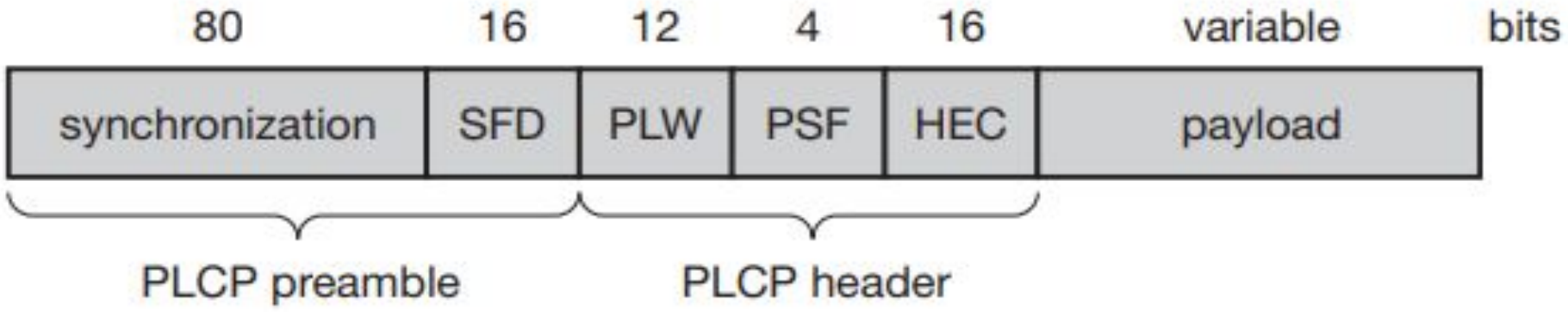
$$s(z) = z^7 + z^4 + 1$$

1.for DC blocking

(process of filtering the DC component of the signal) and

2. For whitening of the spectrum

(process of making the magnitude spectrum uniform).



Format of an IEEE 802.11 PHY layer frame using FHSS

- The fields of the frame fulfill the following functions:
- **Synchronization:** The PLCP preamble starts with 80 bit synchronization, which is a **010101**... bit pattern. This pattern is used for synchronization of potential receivers and signal detection by the CCA.
- **Start frame delimiter (SFD):** The following 16 bits indicate the start of the frame and provide frame synchronization.
- The SFD pattern is **0000 1100 1011 1101**.

- **PLCP_PDU length word (PLW):** This first field of the PLCP header indicates the length of the payload in bytes including the 32 bit CRC at the end of the payload. PLW can range between 0 and 4,095.
- **PLCP signaling field (PSF):** This 4 bit field indicates the data rate of the payload following. All bits set to zero (0000) indicates the lowest data rate of 1 Mbit/s. The granularity is 500 kbit/s, thus 2 Mbit/s is indicated by 0010 and the maximum is 8.5 Mbit/s (1111). This system obviously does not accommodate today's higher data rates.
- **Header error check (HEC)**: Finally, the PLCP header is protected by a 16 bit checksum with the standard ITU-T generator polynomial

$$G(x) = x^{16} + x^{12} + x^5 + 1$$

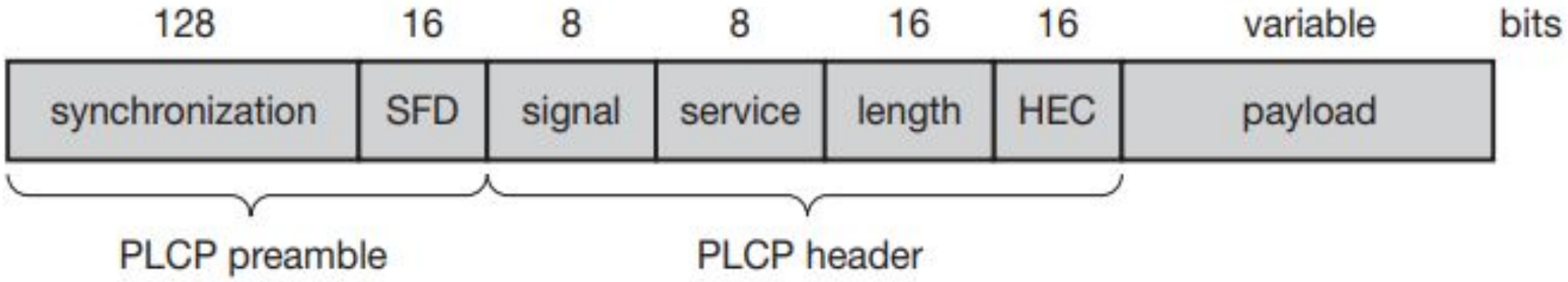
b) Direct sequence spread spectrum physical layer

- Direct sequence spread spectrum (DSSS) is the alternative spread spectrum method separating by code and not by frequency. In the case of IEEE 802.11 DSSS, spreading is achieved using the 11-chip Barker sequence

$$(+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1).$$

- The key characteristics of this method are its robustness against interference and its insensitivity to multipath propagation (time delay spread).
- However, the implementation is more complex compared to FHSS. IEEE 802.11 DSSS PHY also uses the 2.4 GHz ISM band and offers both 1 and 2 Mbit/s data rates.

- The system uses differential binary phase shift keying (DBPSK) for 1 Mbit/s transmission and differential quadrature phase shift keying (DQPSK) for 2 Mbit/s as modulation schemes.
- Again, the maximum transmit power is 1 W in the US, 100 mW EIRP in Europe and 10 mW/MHz in Japan.
- The symbol rate is 1 MHz, resulting in a chipping rate of 11 MHz. All bits transmitted by the DSSS PHY are scrambled with the polynomial $s(z) = z7 + z4 + 1$ for DC blocking and whitening of the spectrum.
- Many of today's products offering 11 Mbit/s according to 802.11b are still backward compatible to these lower data rates
- The frame consists of two basic parts, the PLCP part (preamble and header) and the payload part. While the PLCP part is always transmitted at 1 Mbit/s, payload, i.e., MAC data, can use 1 or 2 Mbit/s.



PHY layer frame using DSSS

- **Synchronization:** The first 128 bits are not only used for synchronization, but also gain setting, energy detection (for the CCA), and frequency offset compensation. The synchronization field only consists of scrambled 1 bits.
- **Start frame delimiter (SFD)**: This 16 bit field is used for synchronization at the beginning of a frame and consists of the pattern

1111 0011 1010 0000.

- **Signal**: Originally, only two values have been defined for this field to indicate the data rate of the payload. The value 0x0A indicates 1 Mbit/s (and thus DBPSK), 0x14 indicates 2 Mbit/s (and thus DQPSK). Other values have been reserved for future use, i.e., higher bit rates.

- **Service:** This field is reserved for future use; however, 0x00 indicates an IEEE 802.11 compliant frame.

- **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.

c) Infra red physical layer

- The PHY layer, which is based on infra red (IR) transmission, uses near visible light at 850–950 nm. Infra red light is not regulated apart from safety restrictions (using lasers instead of LEDs).
- The standard does not require a line-of-sight between sender and receiver, but should also work with diffuse light. This allows for point-to-multipoint communication.
- The maximum range is about 10 m if no sunlight or heat sources interfere with the transmission. Typically, such a network will only work in buildings, e.g., classrooms, meeting rooms etc.
- Frequency reuse is very simple – a wall is more than enough to shield one IR based IEEE 802.11 network from another.
- Today, no products are available that offer infra red communication based on 802.11. Proprietary products offer, e.g., up to 4 Mbit/s using diffuse infra red light. Alternatively, directed infra red communication based on IrDA can be used

Medium access control layer

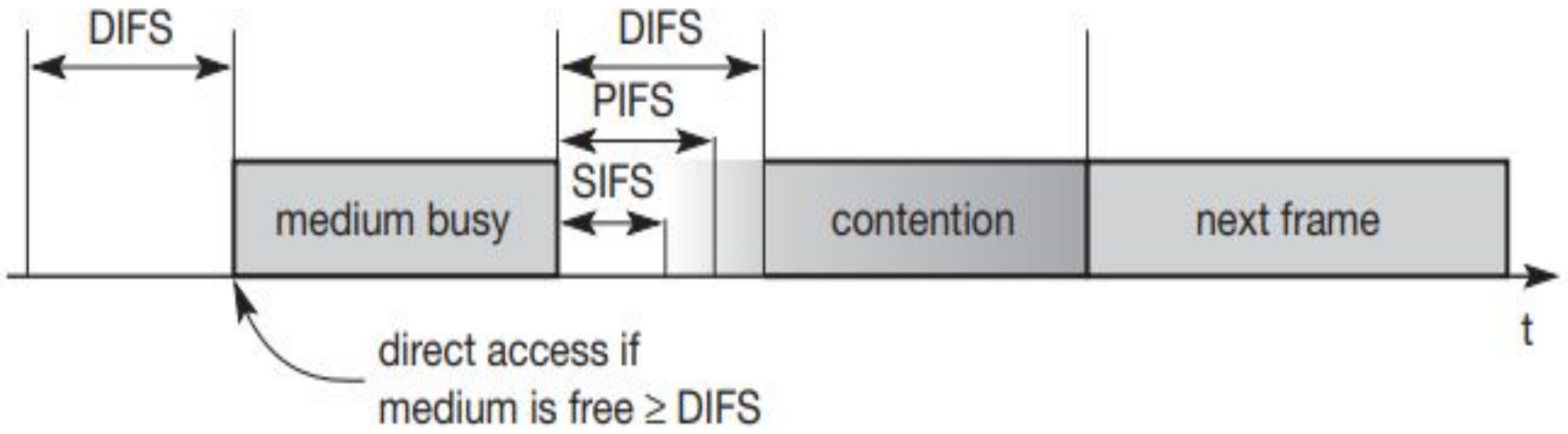
- The MAC layer has to fulfill several tasks. First of all, it has to control medium access, but it can also offer support for roaming, authentication, and power conservation.
- The basic services provided by the MAC layer are the mandatory asynchronous data service and an optional time-bounded service.
- While 802.11 only offers the asynchronous service in ad-hoc network mode, both service types can be offered using an infrastructure-based network together with the access point coordinating medium access.
- The asynchronous service supports broadcast and multi-cast packets, and packet exchange is based on a ‘best effort’ model, i.e., no delay bounds can be given for transmission

- The following three basic access mechanisms have been defined for IEEE 802.11:

1. the mandatory basic method based on a version of CSMA/CA,
2. an optional method avoiding the hidden terminal problem,
3. a contention-free polling method for time-bounded service.

- The first two methods are also summarized as distributed coordination function (DCF),
- The third method is called point coordination function (PCF).
- DCF only offers asynchronous service, while PCF offers both asynchronous and time-bounded service but needs an access point to control medium access and to avoid contention.

- The MAC mechanisms are also called distributed foundation wireless medium access control (DFWMAC).
- For all access methods, several parameters for controlling the waiting time before medium access are important.

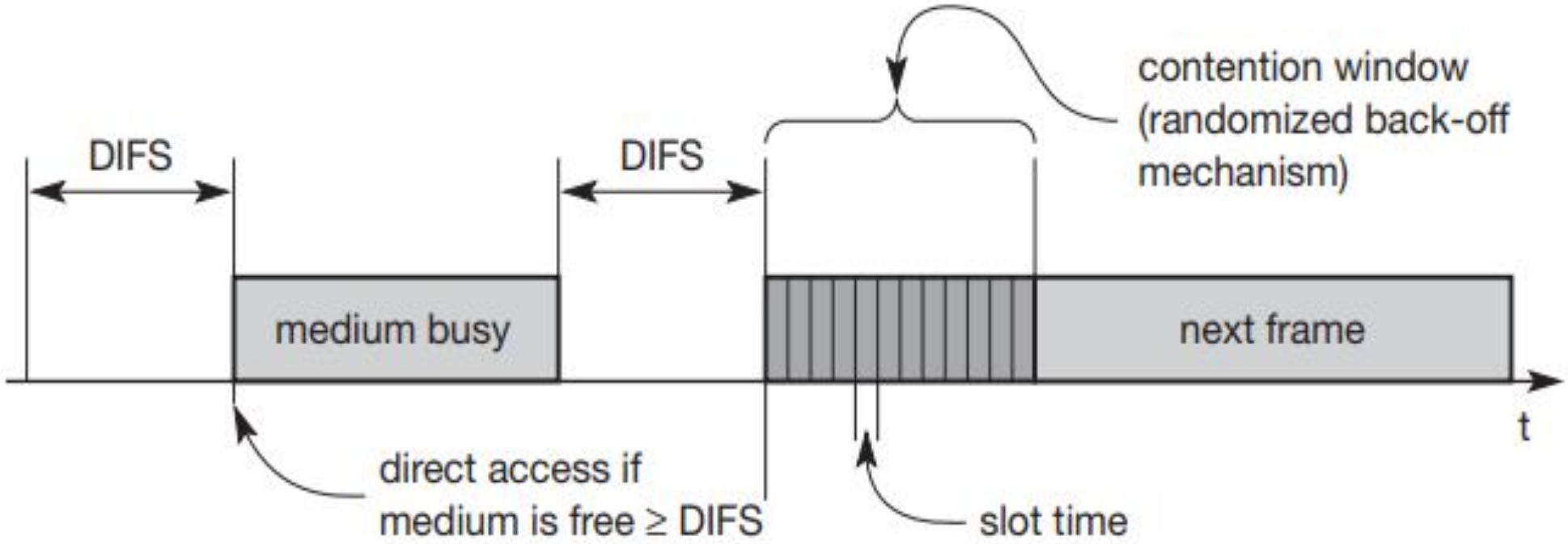


Medium access and inter-frame spacing

- Figure shows the three different parameters that define the priorities of medium access.
- The values of the parameters depend on the PHY and are defined in relation to a slot time.
- Slot time is derived from the medium propagation delay, transmitter delay, and other PHY dependent parameters.
- Slot time is 50 µs for FHSS and 20 µs for DSSS. The medium, as shown, can be busy or idle (which is detected by the CCA).
- If the medium is busy this can be due to data frames or other control frames. During a contention phase several nodes try to access the medium

- Short inter-frame spacing (SIFS): The shortest waiting time for medium access (so the highest priority) is defined for short control messages, such as acknowledgements of data packets or polling responses. For DSSS SIFS is 10 µs and for FHSS it is 28 µs.
- PCF inter-frame spacing (PIFS): A waiting time between DIFS and SIFS (and thus a medium priority) is used for a time-bounded service. An access point polling other nodes only has to wait PIFS for medium access. PIFS is defined as SIFS plus one slot time.
- DCF inter-frame spacing (DIFS): This parameter denotes the longest waiting time and has the lowest priority for medium access. This waiting time is used for asynchronous data service within a contention period .DIFS is defined as SIFS plus two slot times

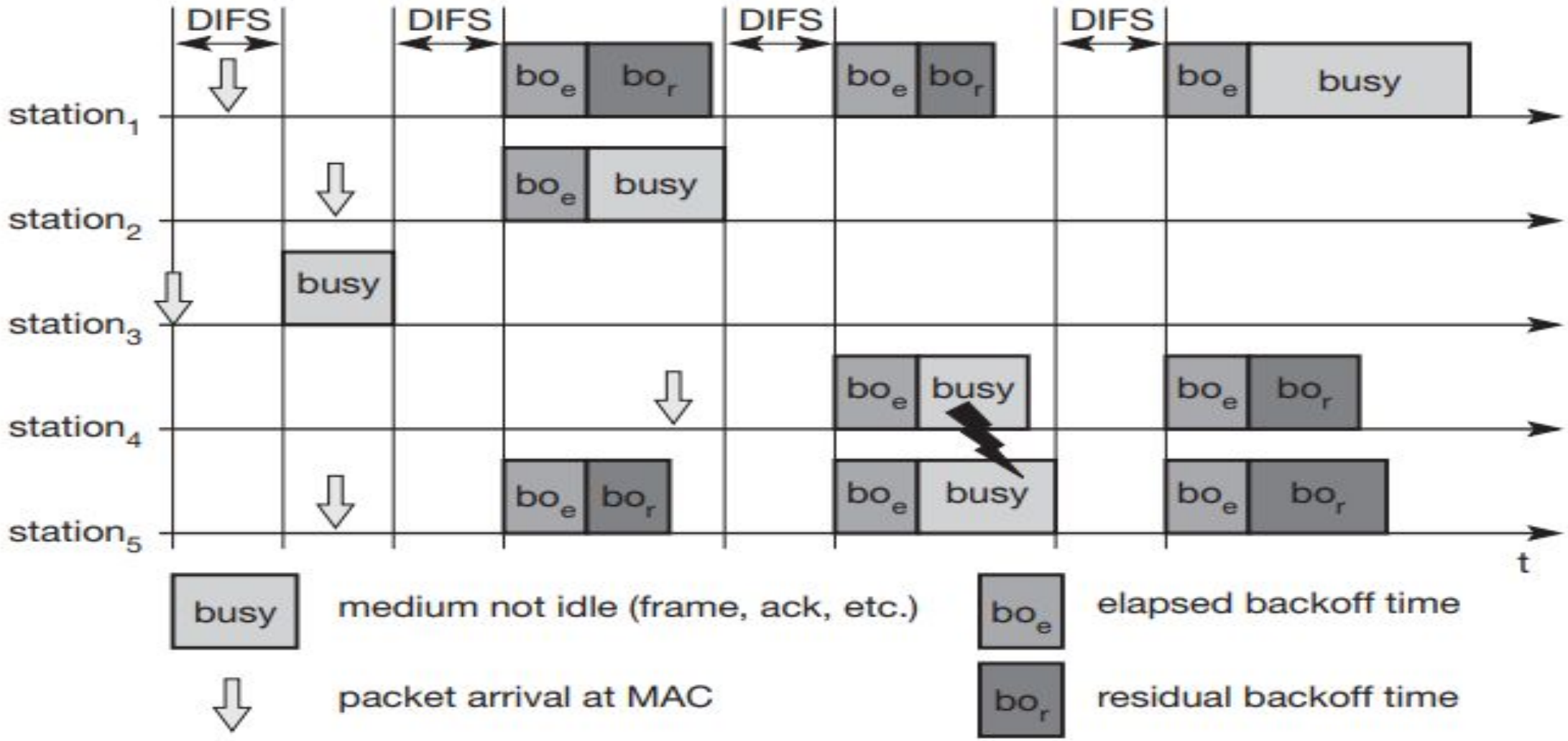
Basic DFWMAC-DCF using CSMA/CA



Contention window and waiting time

- The mandatory access mechanism of IEEE 802.11 is based on carrier sense multiple access with collision avoidance (CSMA/CA), which is a random access scheme with carrier sense and collision avoidance through random backoff.
- If the medium is idle for at least the duration of DIFS (with the help of the CCA signal of the physical layer), a node can access the medium at once. This allows for short access delay under light load. But as more and more nodes try to access the medium, additional mechanisms are needed.
- If the medium is busy, nodes have to wait for the duration of DIFS, entering a contention phase afterwards. Each node now chooses a random backoff time within a contention window and delays medium access for this random amount of time.
- This additional randomly distributed delay helps to avoid collisions – otherwise all stations would try to transmit data after waiting for the medium becoming idle again plus DIFS.

- If the randomized additional waiting time for a node is over and the medium is still idle, the node can access the medium immediately (i.e., no other node has a shorter waiting time).
- If the node continues to sense the medium. As soon as a node senses the channel is busy, it has lost this cycle and has to wait for the next chance, i.e., until the medium is idle again for at least DIFS.
- This means that deferred stations do not choose a randomized backoff time again, but continue to count down. As soon as the counter expires, the node accesses the medium.
- Stations that have waited longer have the advantage over stations that have just entered, in that they only have to wait for the remainder of their backoff timer from the previous cycle(s).



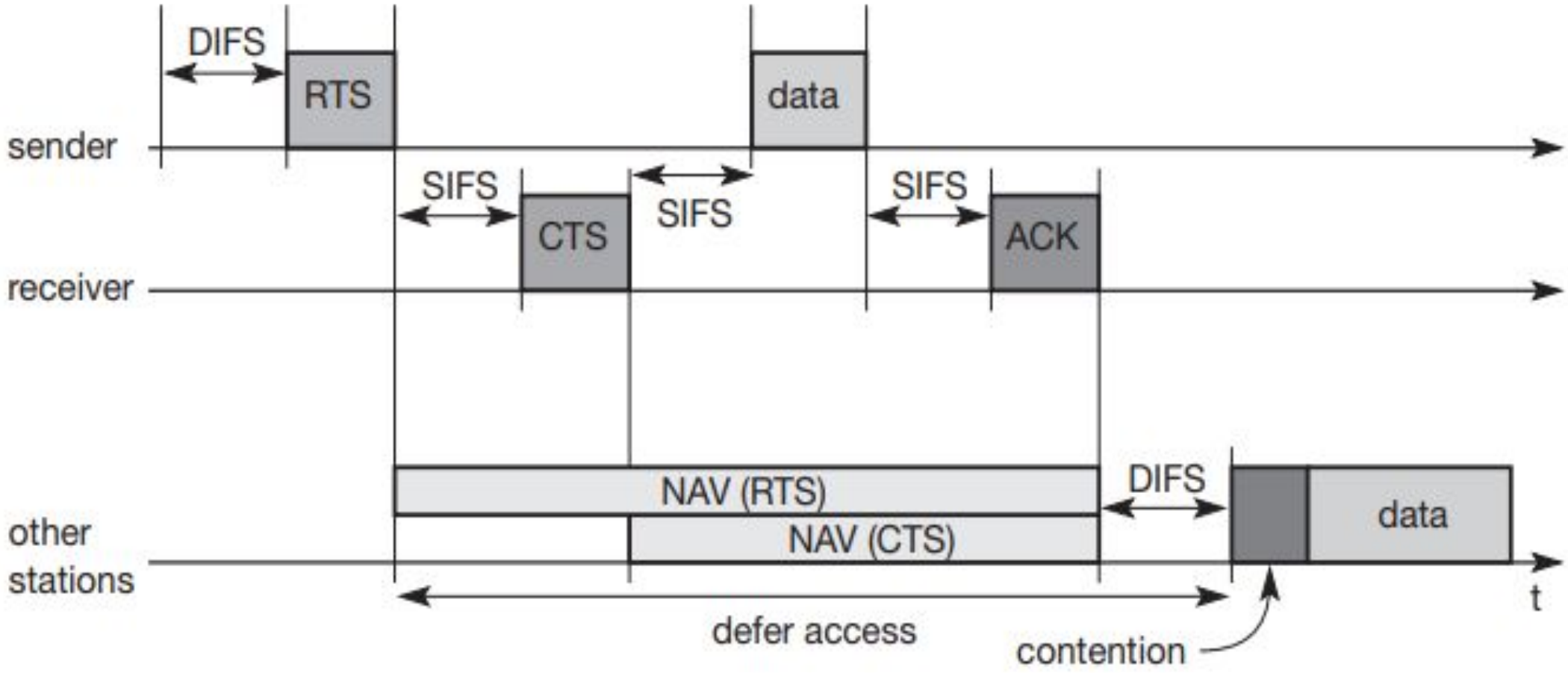
Basic DFWMAC–DCF with several competing senders

- Figure explains the basic access mechanism of IEEE 802.11 for five stations trying to send a packet at the marked points in time.
- Station3 has the first request from a higher layer to send a packet (packet arrival at the MAC SAP). The station senses the medium, waits for DIFS and accesses the medium, i.e., sends the packet.
- Station1, station2, and station5 have to wait at least until the medium is idle for DIFS again after station3 has stopped sending. Now all three stations choose a backoff time within the contention window and start counting down their backoff timers.
- The random backoff time of station1 as sum of boe (the elapsed backoff time) and bor (the residual backoff time). The same is shown for station5.

- Station2 has a total backoff time of only boe and gets access to the medium first. No residual backoff time for station2 is shown.
- The backoff timers of station1 and station5 stop, and the stations store their residual backoff times.
- While a new station has to choose its backoff time from the whole contention window, the two old stations have statistically smaller backoff values. The older values are on average lower than the new ones.
- Now station4 wants to send a packet as well, so after DIFS waiting time, three stations try to get access. It can now happen, as shown in the figure, that two stations accidentally have the same backoff time, no matter whether remaining or newly chosen. This results in a collision on the medium as shown, i.e., the transmitted frames are destroyed.

- Station1 stores its residual backoff time again. In the last cycle shown station1 finally gets access to the medium, while station4 and station5 have to wait.
- A collision triggers a retransmission with a new random selection of the backoff time. Retransmissions are not privileged.
- Still, the access scheme has problems under heavy or light load. Depending on the size of the contention window (CW), the random values can either be too close together (causing too many collisions) or the values are too high (causing unnecessary delay). The system tries to adapt to the current number of stations trying to send.

DFWMAC-DCF with RTS/CTS extension

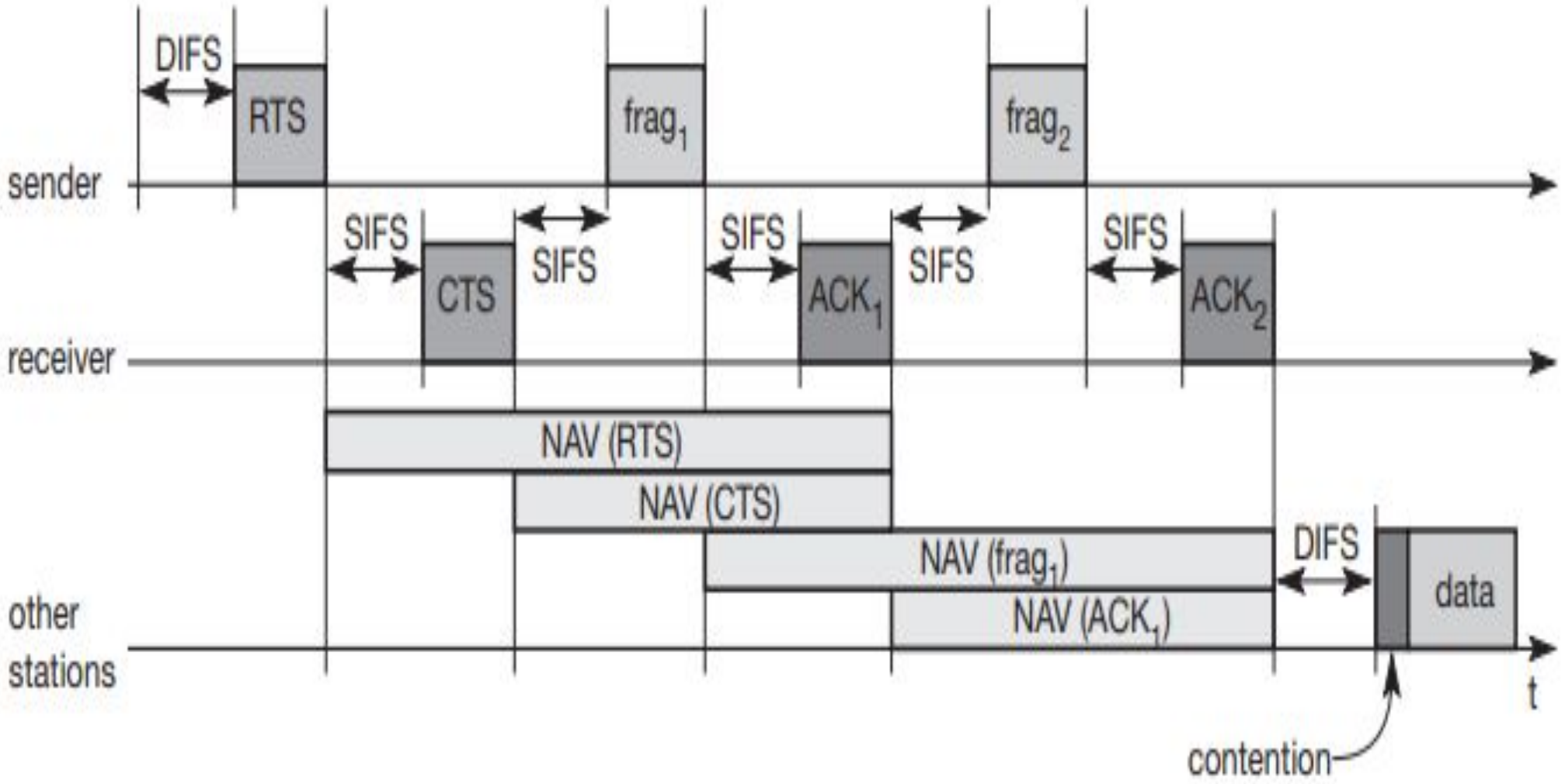


IEEE 802.11 hidden node provisions for contention-free access

- Figure illustrates the use of RTS and CTS. After waiting for DIFS (plus a random backoff time if the medium was busy), the sender can issue a request to send (RTS) control packet.
- The RTS packet thus is not given any higher priority compared to other data packets. The RTS packet includes the receiver of the data transmission to come and the duration of the whole data transmission. This duration specifies the time interval necessary to transmit the whole data frame and the acknowledgement related to it.
- Every node receiving this RTS now has to set its net allocation vector (NAV) in accordance with the duration field. The NAV then specifies the earliest point at which the station can try to access the medium again.
- If the receiver of the data transmission receives the RTS, it answers with a clear to send (CTS) message after waiting for SIFS.

- This CTS packet contains the duration field again and all stations receiving this packet from the receiver of the intended data transmission have to adjust their NAV.
- The latter set of receivers need not be the same as the first set receiving the RTS packet. Now all nodes within receiving distance around sender and receiver are informed that they have to wait more time before accessing the medium.
- Basically, this mechanism reserves the medium for one sender exclusively (this is why it is sometimes called a virtual reservation scheme).
- Finally, the sender can send the data after SIFS. The receiver waits for SIFS after receiving the data packet and then acknowledges whether the transfer was correct. The transmission has now been completed, the NAV in each node marks the medium as free and the standard cycle can start again.

- Within this scenario (i.e., using RTS and CTS to avoid the hidden terminal problem), collisions can only occur at the beginning while the RTS is sent. Two or more stations may start sending at the same time (RTS or other data packets).
- Using RTS/CTS can result in a non-negligible overhead causing a waste of bandwidth and higher delay.
- An RTS threshold can determine when to use the additional mechanism (basically at larger frame sizes) and when to disable it (short frames).

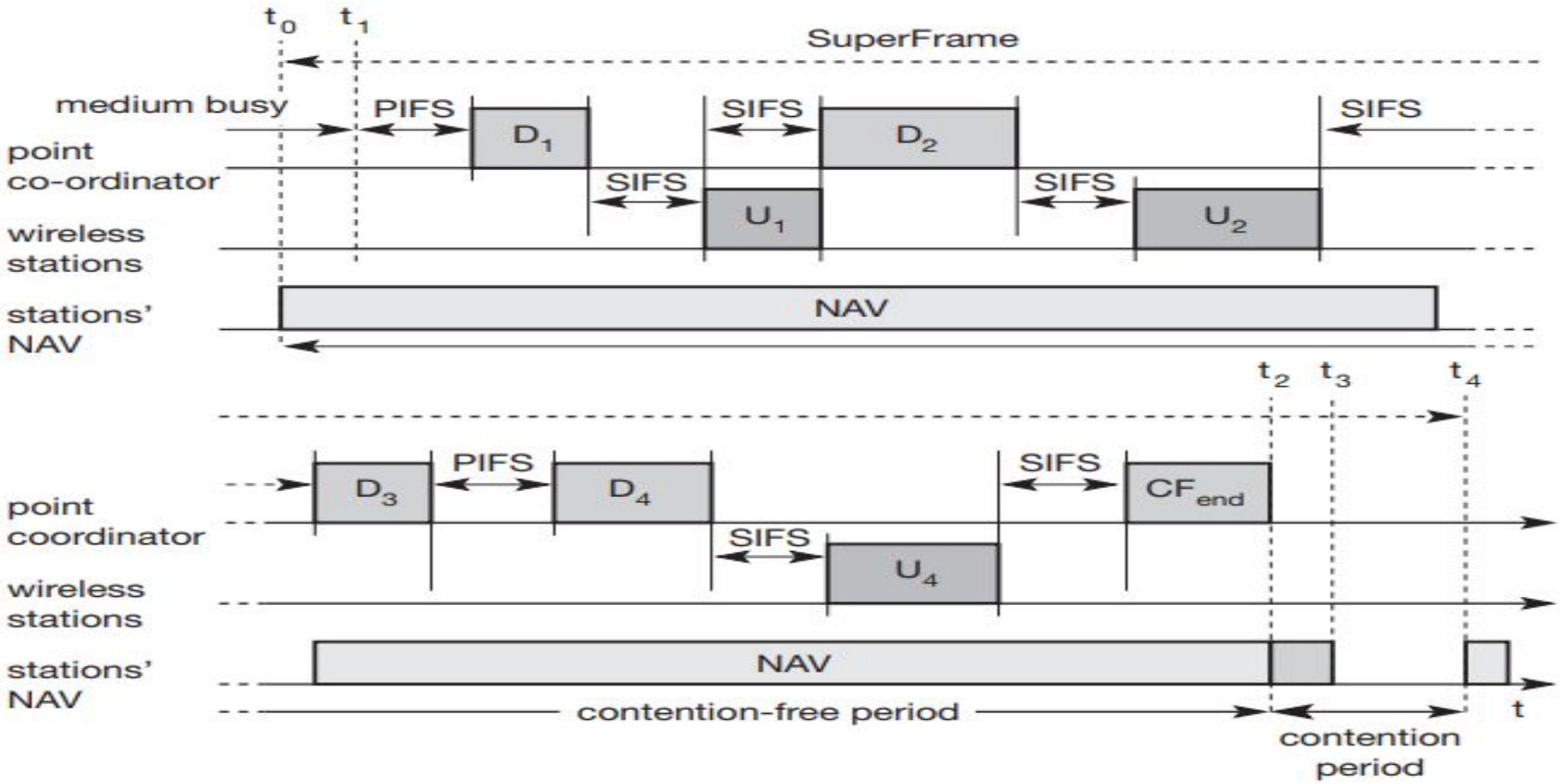


IEEE 802.11 fragmentation of user data

- The probability of an erroneous frame is much higher for wireless links assuming the same frame length. One way to decrease the error probability of frames is to use shorter frames. In this case, the bit error rate is the same, but now only short frames are destroyed and, the frame error rate decreases.
- However, the mechanism of fragmenting a user data packet into several smaller parts should be transparent for a user. The MAC layer should have the possibility of adjusting the transmission frame size to the current error rate on the medium.
- The IEEE 802.11 standard specifies a fragmentation mode .Again, a sender can send an RTS control packet to reserve the medium after a waiting time of DIFS. This RTS packet now includes the duration for the transmission of the first fragment and the corresponding acknowledgement.
- A certain set of nodes may receive this RTS and set their NAV according to the duration field. The receiver answers with a CTS, again including the duration of the transmission up to the acknowledgement. A (possibly different) set of receivers gets this CTS message and sets the NAV.

- The two access mechanisms presented so far cannot guarantee a maximum access delay or minimum transmission bandwidth. To provide a time-bounded service, the standard specifies a point coordination function (PCF) on top of the standard DCF mechanisms.
- The point co-ordinator in the access point splits the access time into super frame periods as shown in Figure. A super frame comprises a contention free period and a contention period.
- The contention period can be used for the two access mechanisms presented above. The figure also shows several wireless stations (all on the same line) and the stations' NAV (again on one line)

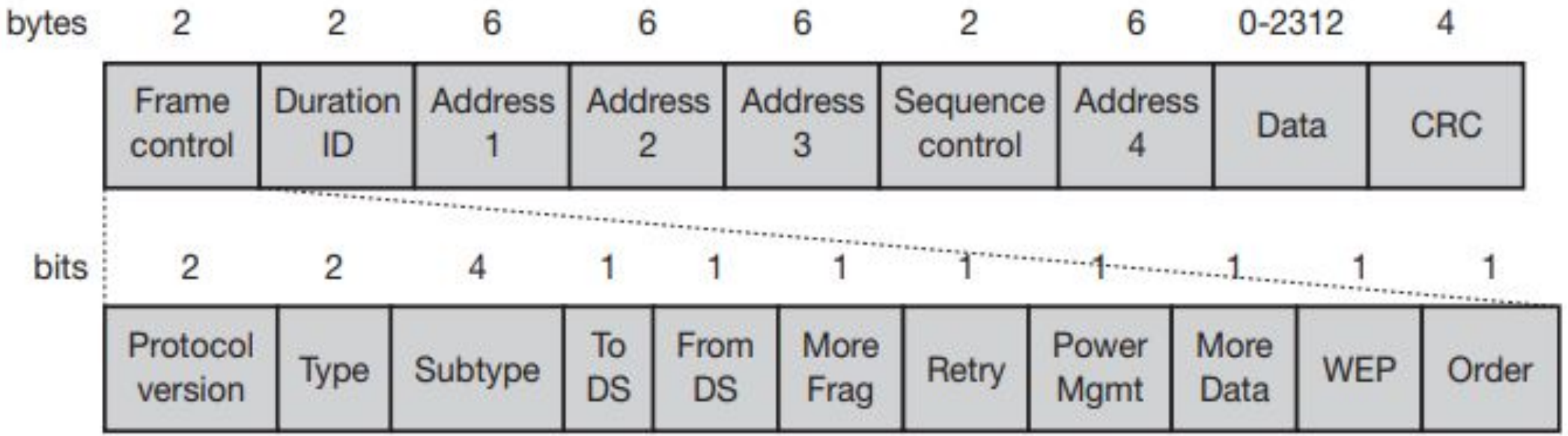
DFWMAC-PCF with polling



- At time t0 the contention-free period of the super frame should theoretically start, but another station is still transmitting data (i.e., the medium is busy).
- This means that PCF also defers to DCF, and the start of the super frame may be postponed. The only possibility of avoiding variations is not to have any contention period at all.
- After the medium has been idle until t1, the point coordinator has to wait for PIFS before accessing the medium. As PIFS is smaller than DIFS, no other station can start sending earlier.
- The point coordinator now sends data D1 downstream to the first wireless station. This station can answer at once after SIFS.After waiting for SIFS again, the point coordinator can poll the second station by sending D2.
- This station may answer upstream to the coordinator with data U2. Polling continues with the third node. This time the node has nothing to answer and the point coordinator will not receive a packet after SIFS.

- After waiting for PIFS, the coordinator can resume polling the stations. Finally, the point coordinator can issue an end marker (CFend), indicating that the contention period may start again.
- Using PCF automatically sets the NAV, preventing other stations from sending. In the example, the contention-free period planned initially would have been from t0 to t3.
- However, the point coordinator finished polling earlier, shifting the end of the contention-free period to t2. At t4, the cycle starts again with the next super frame.

MAC frames



- Figure shows the basic structure of an IEEE 802.11 MAC data frame together with the content of the frame control field. The fields in the figure refer to the following:

- Frame control: The first 2 bytes serve several purposes. They contain several sub-fields as explained after the MAC frame.

- Duration/ID: If the field value is less than 32,768, the duration field contains the value indicating the period of time in which the medium is occupied (in µs). This field is used for setting the NAV for the virtual reservation mechanism using RTS/CTS and during fragmentation. Certain values above 32,768 are reserved for identifiers.

- Address 1 to 4: The four address fields contain standard IEEE 802 MAC addresses (48 bit each), as they are known from other 802.x LANs. The meaning of each address depends on the DS bits in the frame control field

- Sequence control: Due to the acknowledgement mechanism frames may be duplicated. Therefore a sequence number is used to filter duplicates.

- Data: The MAC frame may contain arbitrary data (max. 2,312 byte), which is transferred transparently from a sender to the receiver(s).

- Checksum (CRC): Finally, a 32 bit checksum is used to protect the frame as it is common practice in all 802.x networks.

The frame control field contains the following fields:

- Protocol version: This 2 bit field indicates the current protocol version and is fixed to 0 by now. If major revisions to the standard make it incompatible with the current version, this value will be increased.
- Type: The type field determines the function of a frame:

00: management
01:control
10:data
11 : reserved.
Each type has several subtypes as indicated in the following field.

- Subtype: Example subtypes for management frames are:

0000 for association request,
1000 for beacon.
RTS is a control frame with subtype 1011,
CTS is coded as 1100.
User data is transmitted as data frame with subtype 0000.

- To DS/From DS : MAC frames can be transmitted between mobile stations; between mobile stations and an access point and between access points over a DS.
- Two bits within the Frame Control field, ‘to DS’ and ‘from DS’, differentiate these cases and control the meaning of the four addresses used. Table gives an overview of the four possible bit values of the DS bits and the associated interpretation of the four address field.

to DS	from DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	–
0	1	DA	BSSID	SA	–
1	0	BSSID	SA	DA	–
1	1	RA	TA	DA	SA

- More fragments: This field is set to 1 in all data or management frames that have another fragment of the current MSDU to follow.
- Retry: If the current frame is a retransmission of an earlier frame, this bit is set to 1. With the help of this bit it may be simpler for receivers to eliminate duplicate frames.
- Power management: This field indicates the mode of a station after successful transmission of a frame. Set to 1 the field indicates that the station goes into power-save mode. If the field is set to 0, the station stays active.
- More data: In general, this field is used to indicate a receiver that a sender has more data to send than the current frame. This can be used by an access point to indicate to a station in power-save mode that more packets are buffered.

Or it can be used by a station to indicate to an access point after being polled that more polling is necessary as the station has more data ready to transmit.

- Wired equivalent privacy (WEP): This field indicates that the standard security mechanism of 802.11 is applied. However, due to many weaknesses found in the WEP algorithm higher layer security should be used to secure an 802.11 network.
- Order: If this bit is set to 1 the received frames must be processed in strict order

For addressing, the following four scenarios are possible

1. Ad-hoc network:

If both DS bits are zero, the MAC frame constitutes a packet which is exchanged between two wireless nodes without a distribution system. DA indicates the destination address, SA the source address of the frame, which are identical to the physical receiver and sender addresses respectively. The third address identifies the basic service set (BSSID) , the fourth address is unused.

2. Infrastructure network, from AP:

If only the 'from DS' bit is set, the frame physically originates from an access point. DA is the logical and physical receiver, the second address identifies the BSS, the third address specifies the logical sender, the source address of the MAC frame. This case is an example for a packet sent to the receiver via the access point.

3. Infrastructure network, to AP:

If a station sends a packet to another station via the access point, only the ‘to DS’ bit is set. Now the first address represents the physical receiver of the frame, the access point, via the BSS identifier. The second address is the logical and physical sender of the frame, while the third address indicates the logical receiver.

4.Infrastructure network, within DS:

For packets transmitted between two access points over the distribution system, both bits are set. The first receiver address (RA), represents the MAC address of the receiving access point. Similarly, the second address transmitter address (TA), identifies the sending access point within the distribution system. Now two more addresses are needed to identify the original destination DA of the frame and the original source of the frame SA. Without these additional addresses, some encapsulation mechanism would be necessary to transmit MAC frames over the distribution system transparently

MAC management

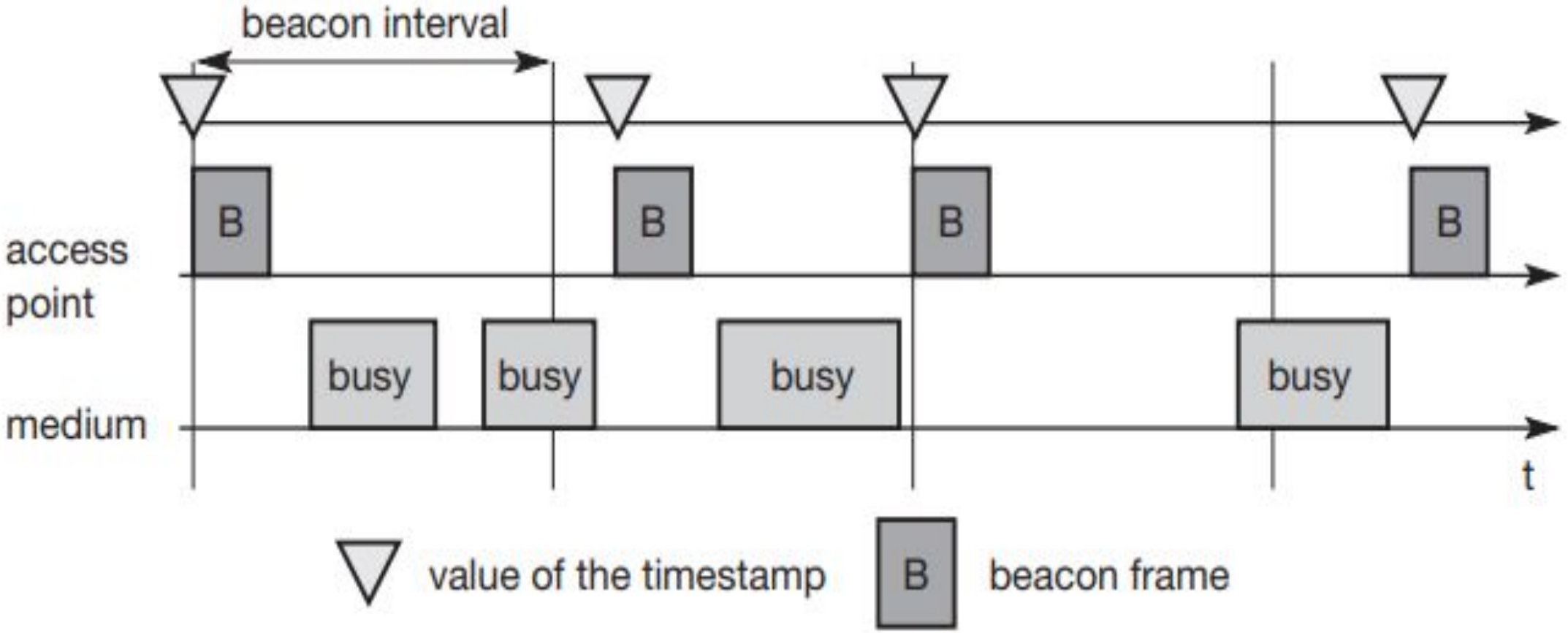
- MAC management plays a central role in an IEEE 802.11 station as it more or less controls all functions related to system integration, i.e., integration of a wireless station into a BSS, formation of an ESS, synchronization of stations etc.

1. Synchronization: Functions to support finding a wireless LAN, synchronization of internal clocks, generation of beacon signals.
2. Power management: Functions to control transmitter activity for power conservation, e.g., periodic sleep, buffering, without missing a frame.
3. Roaming: Functions for joining a network (association), changing access points, scanning for access points.
4. Management information base (MIB): All parameters representing the current state of a wireless station and an access point are stored within a MIB for internal and external access. A MIB can be accessed via standardized protocols such as the simple network management protocol (SNMP)

1) Synchronization

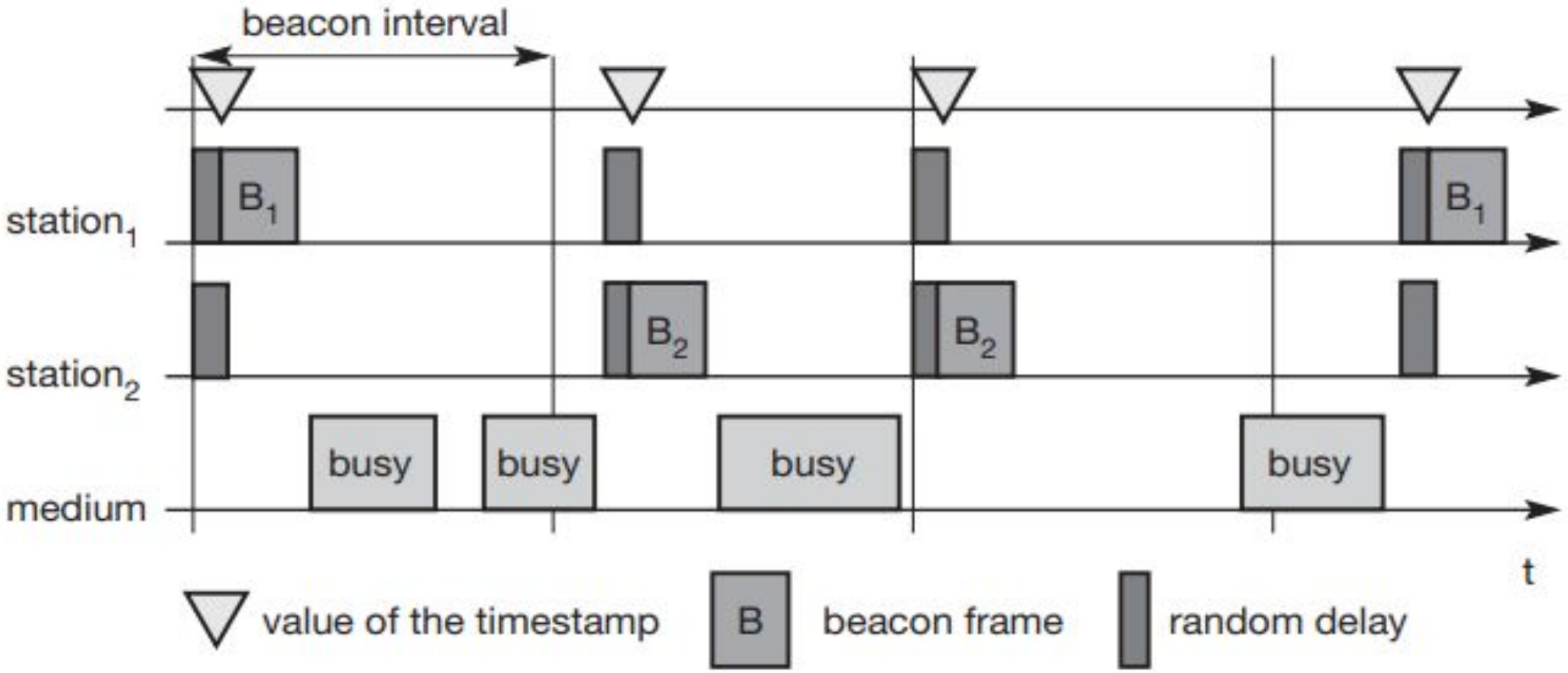
- Each node of an 802.11 network maintains an internal clock. To synchronize the clocks of all nodes, IEEE 802.11 specifies a timing synchronization function (TSF).
- Synchronized clocks are needed for power management, but also for coordination of the PCF and for synchronization of the hopping sequence in an FHSS system.
- Using PCF, the local timer of a node can predict the start of a super frame, i.e., the contention free and contention period.
- FHSS physical layers need the same hopping sequences so that all nodes can communicate within a BSS.

- Within a BSS, timing is conveyed by the (quasi)periodic transmissions of a beacon frame. A beacon contains a timestamp and other management information used for power management and roaming (e.g., identification of the BSS).
- The timestamp is used by a node to adjust its local clock. The node is not required to hear every beacon to stay synchronized; however, from time to time internal clocks should be adjusted.
- The transmission of a beacon frame is not always periodic because the beacon frame is also deferred if the medium is busy.



Beacon transmission in a busy 802.11 infrastructure network

- Within infrastructure-based networks, the access point performs synchronization by transmitting the (quasi)periodic beacon signal, whereas all other wireless nodes adjust their local timer to the time stamp.
- The access point is not always able to send its beacon B periodically if the medium is busy. However, the access point always tries to schedule transmissions according to the expected beacon interval (target beacon transmission time), i.e., beacon intervals are not shifted if one beacon is delayed.
- The timestamp of a beacon always reflects the real transmit time, not the scheduled time.



Beacon transmission in a busy 802.11 ad-hoc network

- For ad-hoc networks, the situation is slightly more complicated as they do not have an access point for beacon transmission. In this case, each node maintains its own synchronization timer and starts the transmission of a beacon frame after the beacon interval.
- However, the standard random back off algorithm is also applied to the beacon frames so only one beacon wins. All other stations now adjust their internal clocks according to the received beacon and suppress their beacons for this cycle.
- If collision occurs, the beacon is lost. In this scenario, the beacon intervals can be shifted slightly because all clocks may vary as the start of a beacon interval from a node's point of view.
- However, after successful synchronization all nodes again have the same consistent view.

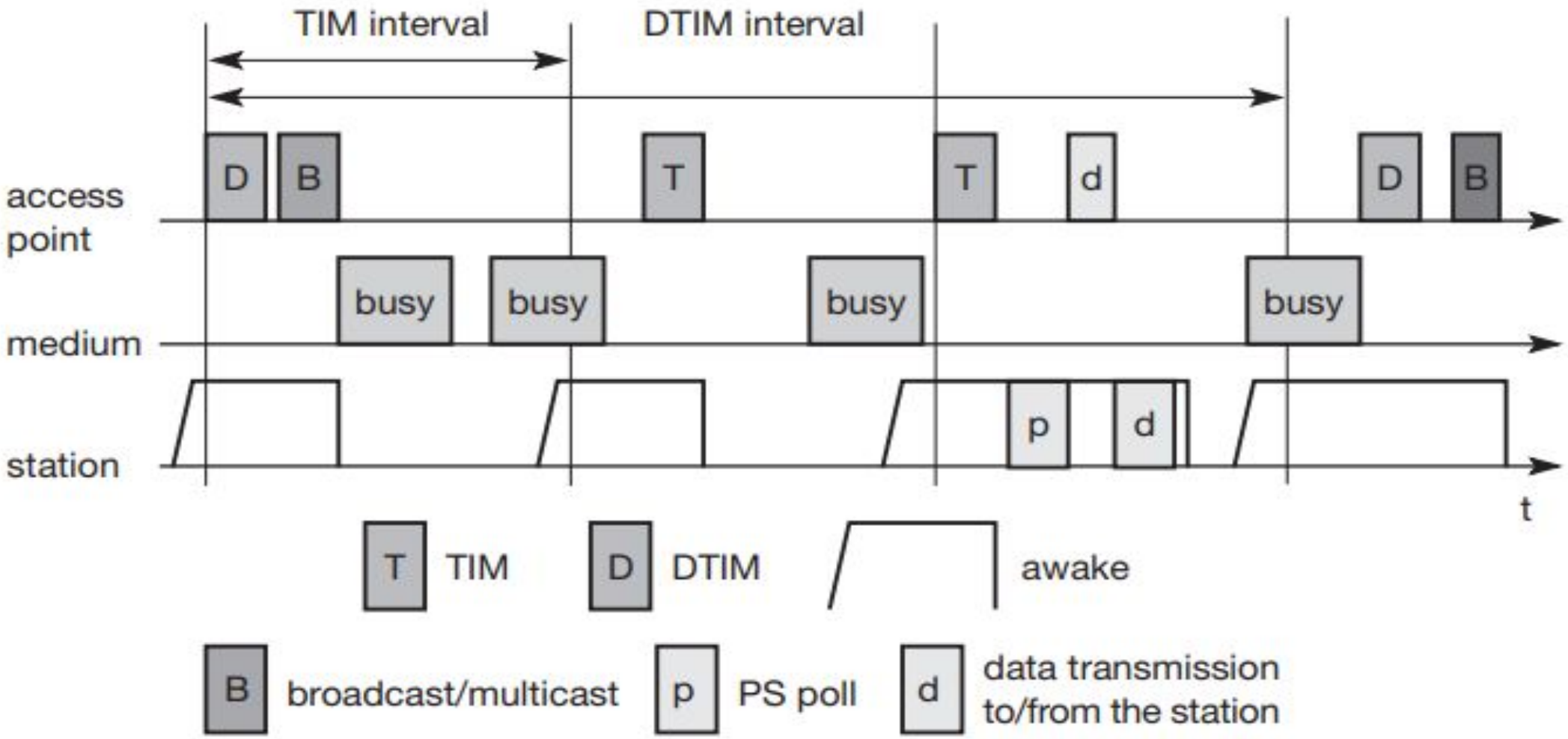
2) Power management

- Wireless devices are battery powered (unless a solar panel is used). Therefore, power-saving mechanisms are crucial for the commercial success of such devices
- The basic idea of IEEE 802.11 power management is to switch off the transceiver whenever it is not needed.
- For the sending device this is simple to achieve as the transfer is triggered by the device itself.
- However, since the power management of a receiver cannot know in advance when the transceiver has to be active for a specific packet, it has to ‘wake up’ the transceiver periodically
- The basic idea of power saving includes two states for a station: sleep and awake, and buffering of data in senders.

- If a sender intends to communicate with a power-saving station it has to buffer data if the station is asleep.
- The sleeping station on the other hand has to wake up periodically and stay awake for a certain time. During this time, all senders can announce the destinations of their buffered data frames.
- If a station detects that it is a destination of a buffered packet it has to stay awake until the transmission takes place. Waking up at the right moment requires the timing synchronization function (TSF)

Power management in infrastructure-based networks:

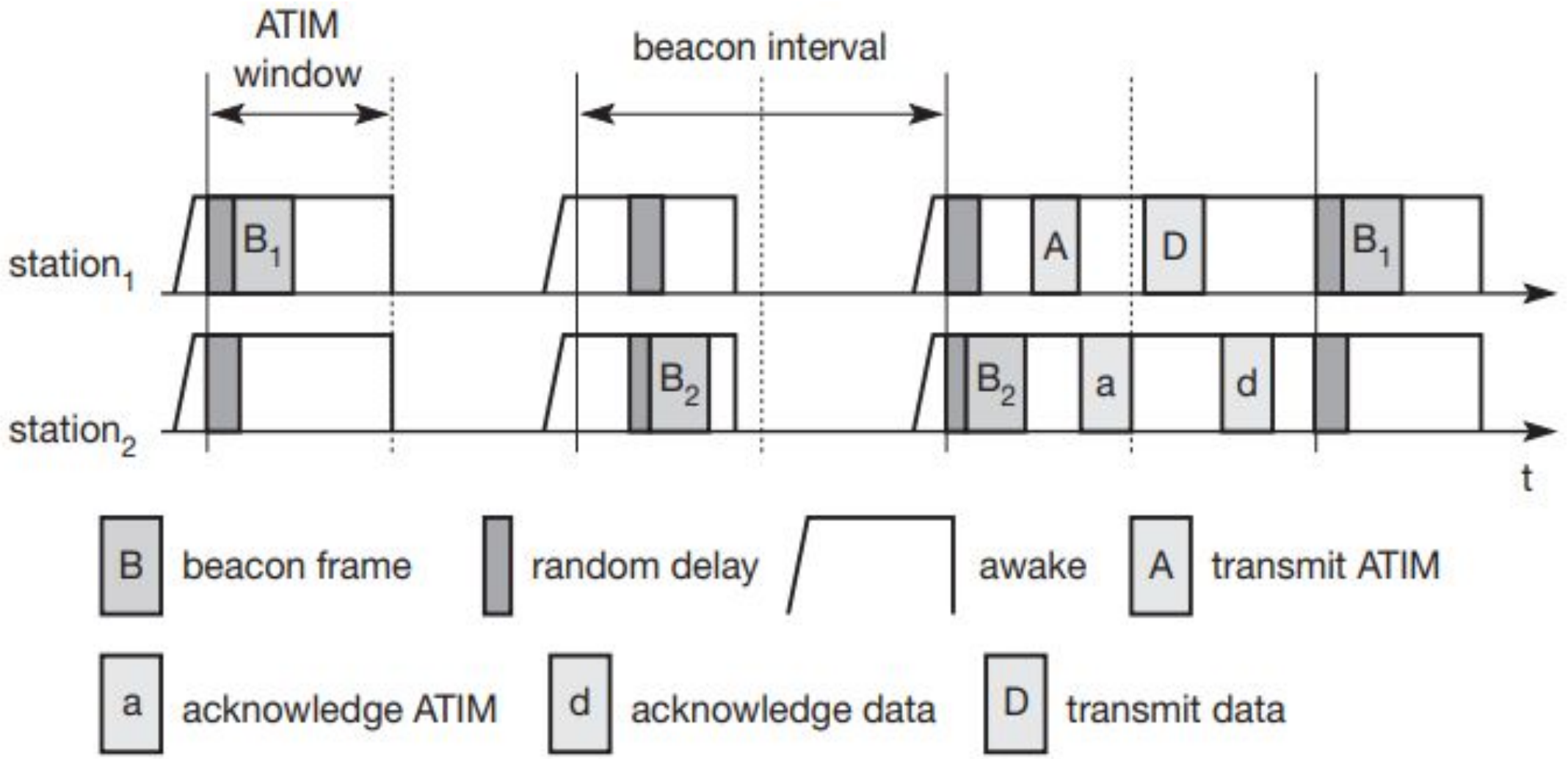
- The access point buffers all frames destined for stations operating in power-save mode. With every beacon sent by the access point, a traffic indication map (TIM) is transmitted. The TIM contains a list of stations for which unicast data frames are buffered in the access point
- The TSF assures that the sleeping stations will wake up periodically and listen to the beacon and TIM.
- If the TIM indicates a unicast frame buffered for the station, the station stays awake for transmission. For multi-cast/broadcast transmission, stations will always stay awake. Another reason for waking up is a frame which has to be transmitted from the station to the access point.



Power management in IEEE 802.11 infrastructure networks

- Figure shows an example with an access point and one station along with the state of the medium.
- The access point transmits a beacon frame each beacon interval. This interval is now the same as the TIM interval. Additionally, the access point maintains a delivery traffic indication map (DTIM) interval for sending broadcast/multicast frames.
- The DTIM interval is always a multiple of the TIM interval. All stations wake up prior to an expected TIM or DTIM.
- In the first case, the access point has to transmit a broadcast frame and the station stays awake to receive it. After receiving the broadcast frame, the station returns to sleeping mode.
- The station wakes up again just before the next TIM transmission. This time the TIM is delayed due to a busy medium so, the station stays awake. The access point has nothing to send and the station goes back to sleep.

- At the next TIM interval, the access point indicates that the station is the destination for a buffered frame. The station answers with a PS (power saving) poll and stays awake to receive data.
- The access point then transmits the data for the station, the station acknowledges the receipt and may also send some data .This is acknowledged by the access point .Afterwards, the station switches to sleep mode again.
- Finally, the access point has more broadcast data to send at the next DTIM interval, which is again deferred by a busy medium. Depending on internal thresholds, a station may stay awake if the sleeping period would be too short.
- This mechanism clearly shows the trade-off between short delays in station access and saving battery power. The shorter the TIM interval, the shorter the delay, but the lower the power-saving effect.



Power management in IEEE 802.11 ad-hoc networks

- There is no access point to buffer data in one location but each station needs the ability to buffer data if it wants to communicate with a power-saving station.
- All stations now announce a list of buffered frames during a period when they are all awake. Destinations are announced using ad-hoc traffic indication map (ATIMs) – the announcement period is called the ATIM window.
- Figure shows a simple ad-hoc network with two stations. Again, the beacon interval is determined by a distributed function (different stations may send the beacon).
- However, due to this synchronization, all stations within the ad-hoc network wake up at the same time. All stations stay awake for the ATIM interval as shown in the first two steps and go to sleep again if no frame is buffered for them.
- In the third step, station1 has data buffered for station2. This is indicated in an ATIM transmitted by station1.

- After the ATIM window, station1 can transmit the data frame, and station2 acknowledges its receipt. In this case, the stations stay awake for the next beacon.
- One problem with this approach is that of scale. If many stations within an ad-hoc network operate in power-save mode, they may also want to transmit their ATIM within the ATIM window.
- More ATIM transmissions take place, more collisions happen and more stations are deferred.
- The access delay of large networks is difficult to predict. QoS guarantees can not be given under heavy load.

3) Roaming

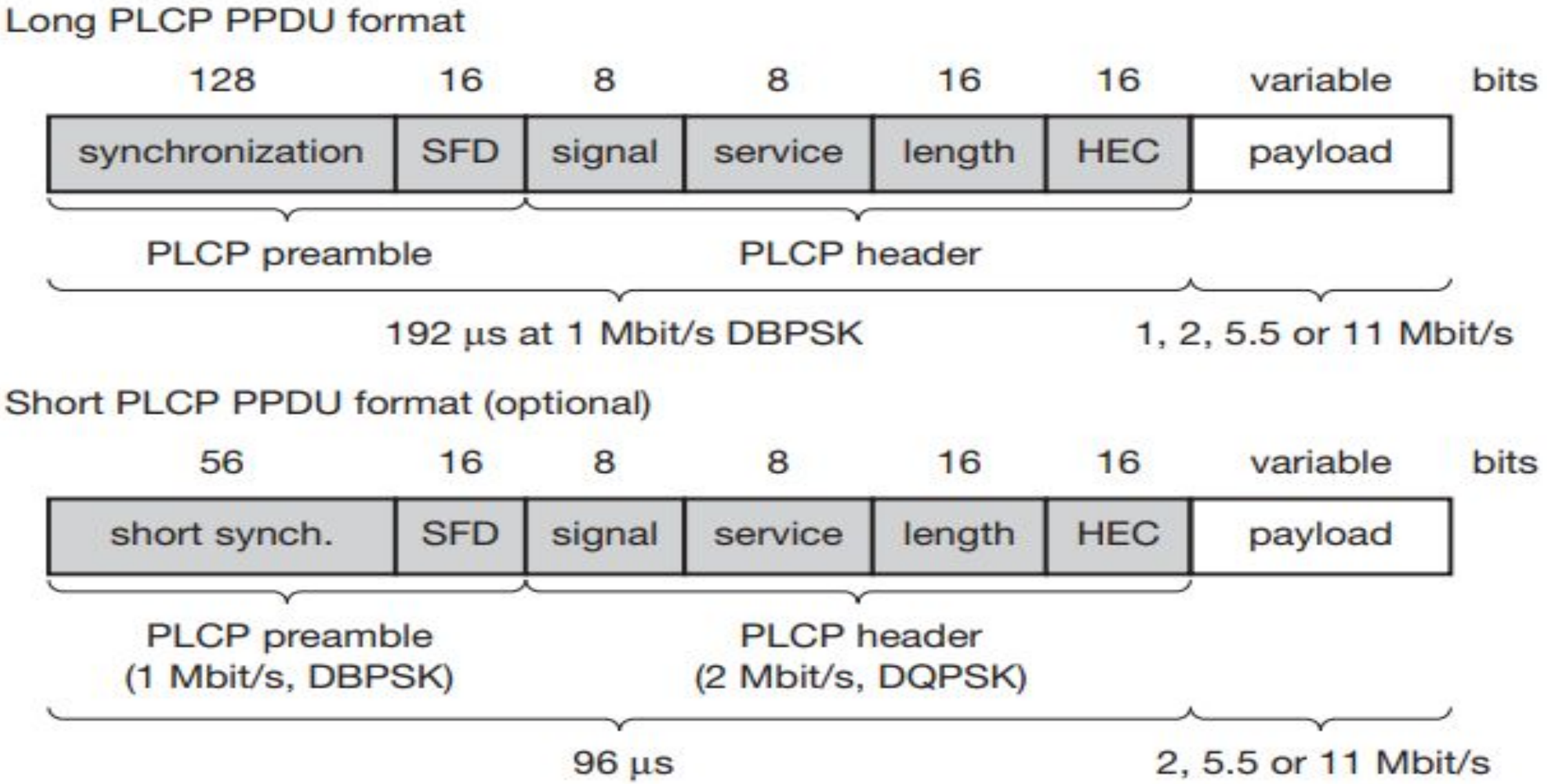
- If a user walks around with a wireless station, the station has to move from one access point to another to provide uninterrupted service. *Moving between access points is called roaming.*
- The steps for roaming between access points are:
- A station decides that the current link quality to its access point AP1 is too poor. The station then starts scanning for another access point
- Scanning involves the active search for another BSS and can also be used for setting up a new BSS in case of ad-hoc networks. IEEE 802.11 specifies scanning on single or multiple channels (if available at the physical layer) and differentiates between passive scanning and active scanning.

- Passive scanning simply means listening into the medium to find other networks, i.e., receiving the beacon of another network issued by the synchronization function within an access point.
- Active scanning comprises sending a probe on each channel and waiting for a response. Beacon and probe responses contain the information necessary to join the new BSS.
- The station then selects the best access point for roaming based on, e.g., signal strength, and sends an association request to the selected access point AP2.
- The new access point AP2 answers with an association response. If the response is successful, the station has roamed to the new access point AP2. Otherwise, the station has to continue scanning for new access points

- The access point accepting an association request indicates the new station in its BSS to the distribution system (DS).
- The DS then updates its database, which contains the current location of the wireless stations.
- This database is needed for forwarding frames between different BSSs, i.e. between the different access points controlling the BSSs, which combine to form an ESS.
- Additionally, the DS can inform the old access point AP1 that the station is no longer within its BSS.

802.11b

- Depending on the current interference and the distance between sender and receiver 802.11b systems offer 11, 5.5, 2, or 1 Mbit/s.
- Maximum user data rate is approx 6 Mbit/s.
- The lower data rates 1 and 2 Mbit/s use the 11-chip Barker sequence and DBPSK or DQPSK, respectively.
- The new data rates, 5.5 and 11 Mbit/s, use 8-chip complementary code keying (CCK).
- The standards operates on certain frequencies in the 2.4 GHz ISM band, depending on national regulations.
- Altogether 14 channels have been defined and for each channel the center frequency is given.
- Depending on national restrictions 11 (US/Canada), 13 (Europe with some exceptions) or 14 channels (Japan) can be used.

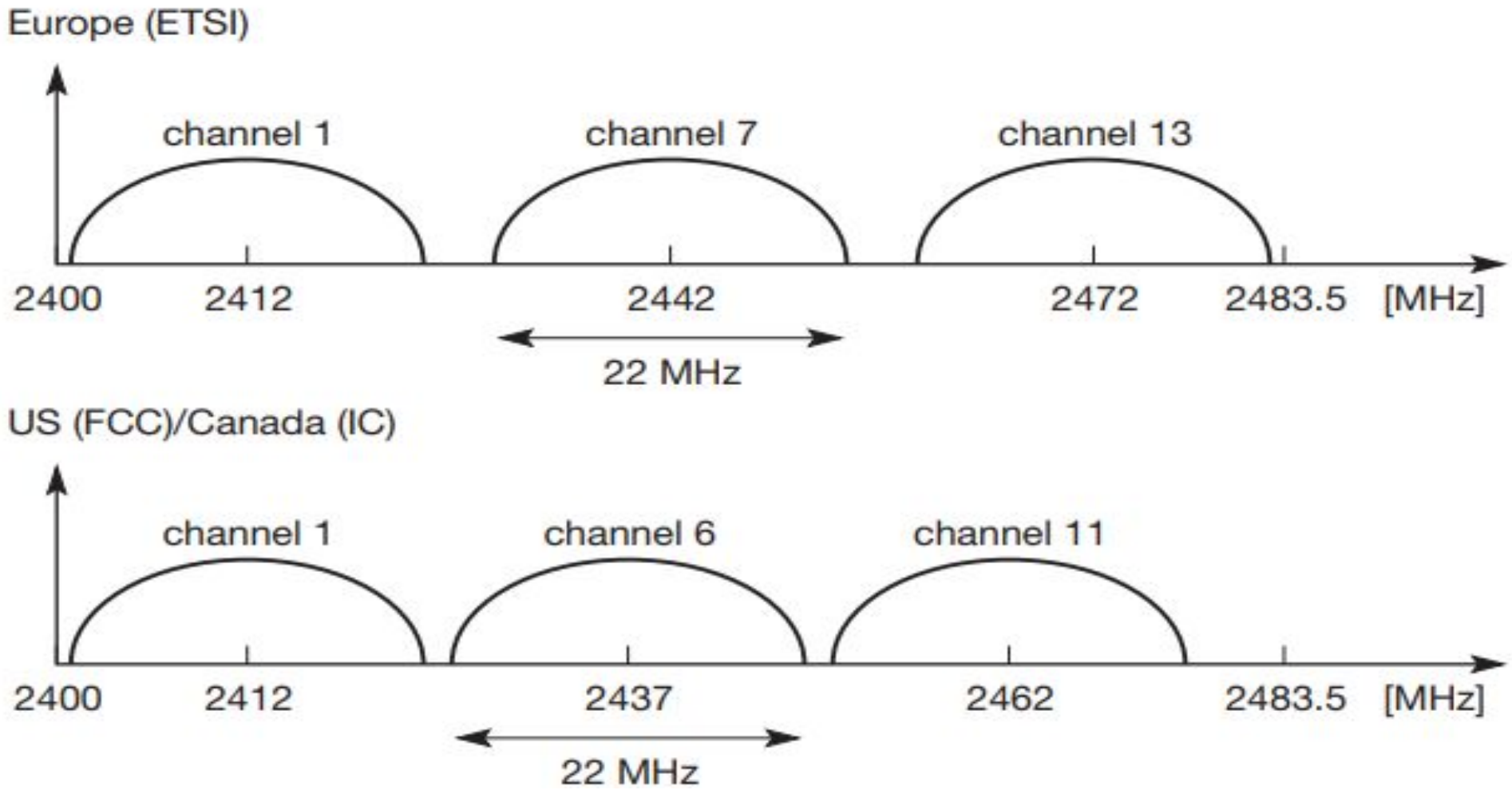


IEEE 802.11b PHY packet formats

- Figure shows two packet formats standardized for 802.11b. The mandatory format is called long PLCP PPDU. One difference is the rate encoded in the signal field this is encoded in multiples of 100 kbit/s. Thus, 0x0A represents 1 Mbit/s, 0x14 is used for 2 Mbit/s, 0x37 for 5.5 Mbit/s and 0x6E for 11 Mbit/s.
- Note that the preamble and the header are transmitted at 1 Mbit/s using DBPSK.
- The optional short PLCP PPDU format differs in several ways. The short synchronization field consists of 56 scrambled zeros instead of scrambled ones.
- The short start frame delimiter SFD consists of a mirrored bit pattern compared to the SFD of the long format:
- 0000 0101 1100 1111 is used for the short PLCP PDU instead of

  1111 0011 1010 0000 for the long PLCP PPDU.

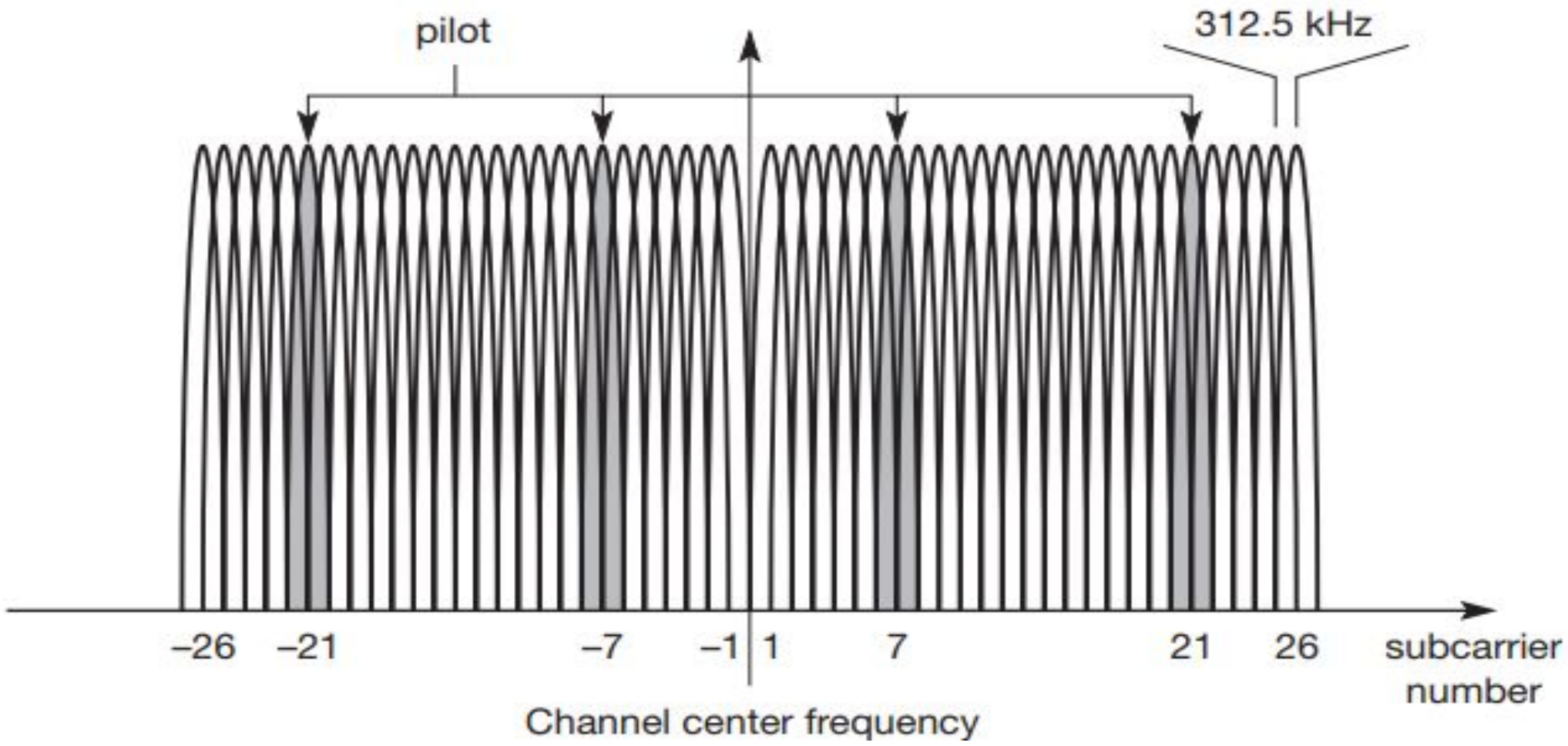
- Receivers that are unable to receive the short format will not detect the start of a frame (but will sense the medium is busy).
- Only the preamble is transmitted at 1 Mbit/s, DBPSK.
- The following header is already transmitted at 2 Mbit/s, DQPSK, which is also the lowest available data rate.
- As Figure shows, the length of the overhead is only half for the short frames (96 µs instead of 192 µs). This is useful for, e.g., short, but time-critical, data transmissions.



IEEE 802.11b non-overlapping channel selection

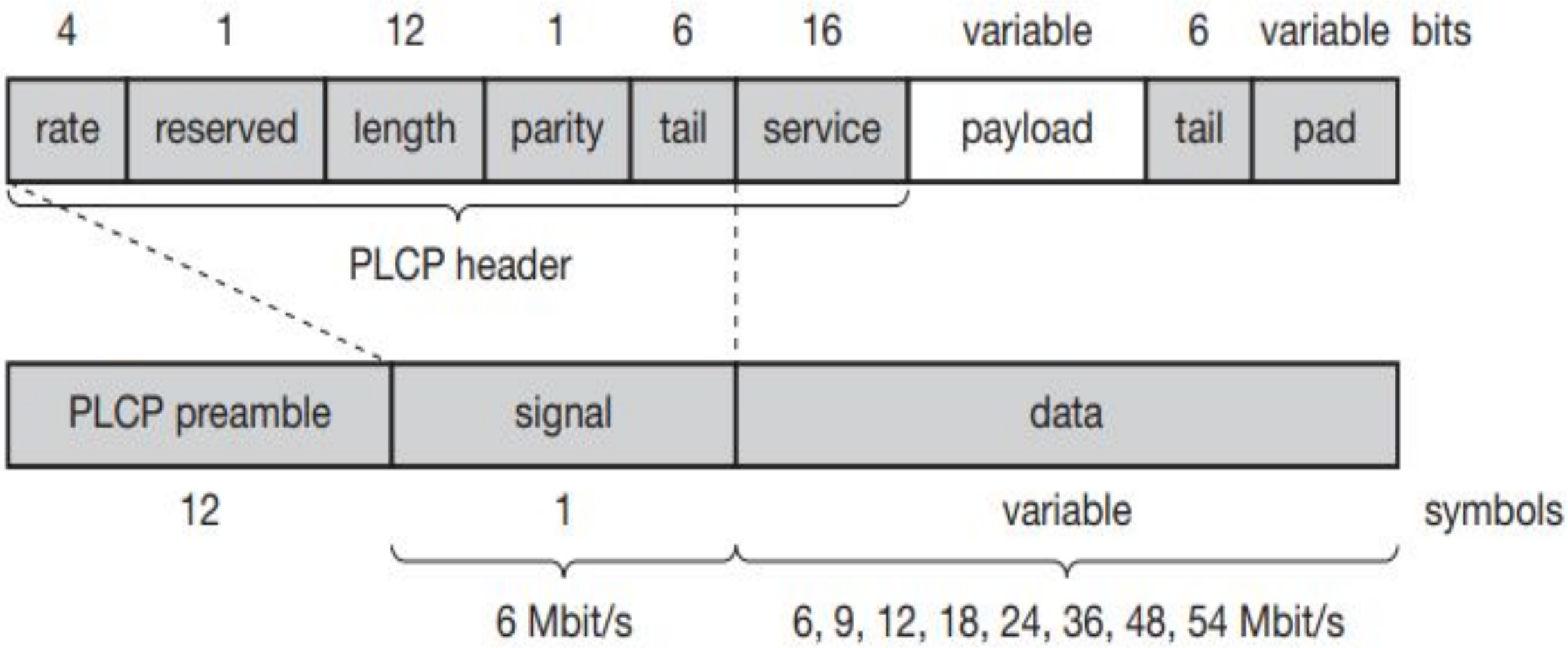
- Figure illustrates the non-overlapping usage of channels for an IEEE 802.11b installation with minimal interference in the US/Canada and Europe.
- The spacing between the center frequencies should be at least 25 MHz (the occupied bandwidth of the main lobe of the signal is 22 MHz). This results in the channels 1, 6, and 11 for the US/Canada or 1, 7, 13 for Europe, respectively.
- It may be the case that, e.g., travellers from the US cannot use the additional channels (12 and 13) in Europe as their hardware is limited to 11 channels. Some European installations use channel 13 to minimize interference.
- Users can install overlapping cells for WLANs using the three non-overlapping channels to provide seamless coverage.

802.11a



Usage of OFDM in IEEE 802.11a

- the US 5 GHz U-NII (Unlicensed National Information Infrastructure) bands IEEE 802.11a offers up to 54 Mbit/s using OFDM
- Figure shows the usage of OFDM in IEEE 802.11a, the basic idea of OFDM (or MCM in general) was the reduction of the symbol rate by distributing bits over numerous subcarriers.
- IEEE 802.11a uses a fixed symbol rate of 250,000 symbols per second independent of the data rate (0.8 µs guard interval for ISI mitigation plus 3.2 µs used for data results in a symbol duration of 4 µs).
- As Figure shows, 52 subcarriers are equally spaced around a center frequency. The spacing between the subcarriers is 312.5 kHz.
- 26 subcarriers are to the left of the center frequency and 26 are to the right. The center frequency itself is not used as subcarrier.
- Subcarriers with the numbers –21, –7, 7, and 21 are used for pilot signals to make the signal detection robust against frequency offsets.



IEEE 802.11a physical layer PDU

- The PLCP preamble consists of 12 symbols and is used for frequency acquisition, channel estimation, and synchronization. The duration of the preamble is 16 µs.
- The following OFDM symbol, called signal, is BPSK-modulated.
- The 4 bit rate field determines the data rate and the modulation of the rest of the packet (examples are 0x3 for 54 Mbit/s, 0x9 for 24 Mbit/s, or 0xF for 9 Mbit/s).
- The length field indicates the number of bytes in the payload field.
- The parity bit shall be an even parity for the first 16 bits of the signal field (rate, length and the reserved bit).
- Finally, the six tail bits are set to zero.

- The data field is sent with the rate determined in the rate field and contains a service field which is used to synchronize the descrambler of the receiver (the data stream is scrambled using the polynomial x7 + x4 + 1) and which contains bits for future use.
- The payload contains the MAC PDU (1-4095 byte).
- The tail bits are used to reset the encoder.
- Finally, the pad field ensures that the number of bits in the PDU maps to an integer number of OFDM symbols

The following are the advantages of the IEEE 802.11a standard compared to 802.11b:

1. 802.11a uses 5GHz frequency band which is less crowded and hence has relatively smaller interference problem.
2. 802.11a supports up to 54Mbps of bandwidth, which is much faster than the 11Mbps bandwidth provided by 802.11b standard devices.
3. 802.11a offers as many as 12 non-overlapping channels. With more channels, larger number of users can be accommodated with no performance degradation.

Some of the disadvantages of using the 802.11a standard are:

1. Not many client devices such as note book computers, PDAs support 802.11a standard. Most of these support either 802.11b or Bluetooth standards.
2. It is more expensive compared to other contemporary technologies like 802.11b and Bluetooth.
3. 802.11a standards are not compatible with 802.11b. Hence, devices manufactured complying with 802.11a and 802.11b respectively, are not interoperable.
4. The distance covered will be slightly less compared to 802.11b due to higher operating frequency (5 GHz). Note that, higher the radio frequency, lower the propagation distance for a given output power.

	IEEE 802.11a	IEEE 802.11b
Standard Ratified	Sep. 99	Sep 99
Raw Data Rates	54 Mbps	11 Mbps
Average Actual Throughput	4-5 Mbps	27 Mbps
Frequency	5 GHz	2.4 GHz
Available Spectrum	300 MHz	83.5 MHz
Modulation Encoding	OFDM	DSSS/CCK
# Channels/ non-overlapping	12/8	11/3

Comparison of IEEE 802.11 standards

Standard	Frequency Band	Bandwidth	Modulation Scheme	Channel Arch.	Maximum Data Rate	Range
802.11	2.4 GHz	20 MHz	BPSK to 256-QAM	DSSS, FHSS	2 Mbps	20 m
b	2.4 GHz	21 MHz	BPSK to 256-QAM	CCK, DSSS	11 Mbps	35 m
a	5 GHz	22 MHz	BPSK to 256-QAM	OFDM	54 Mbps	35 m
g	2.4 GHz	23 MHz	BPSK to 256-QAM	DSSS, OFDM	54 Mbps	70 m
n	2.4 GHz, 5 GHz	24 MHz and 40 MHz	BPSK to 256-QAM	OFDM	600 Mbps	70 m
ah	900 MHz	1, 2, 4, 8, and 16 MHz	BPSK to 256-QAM	SC, OFDM	40 Mbps	1 km

WIFI Security Standards

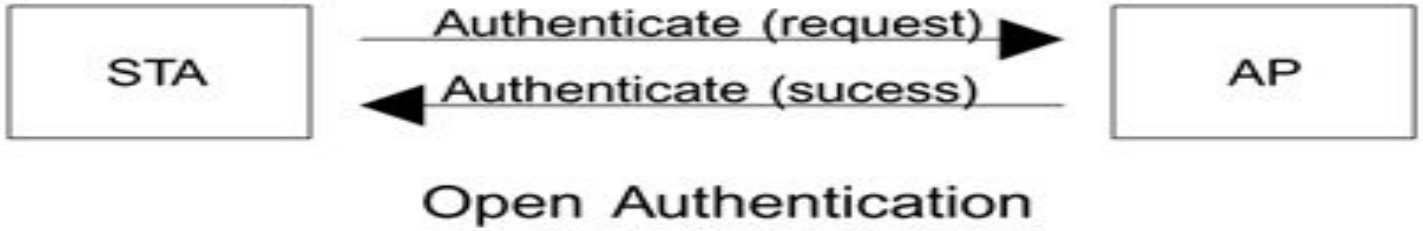
- Wireless networks and security in today's world have become a major necessity for human education, entertainment, and survival.
- Authorization and authentication are major factors that need to be ensured to maintain privacy.
- Wireless networks have Wireless security encryption to secure the authentication.
- This security is ensured by establishing a secure connection for authenticated and authorized users by providing the connection with a strong password or security key.
- Wireless security encryption finds its importance in protecting any malicious activity carried on information that may result in breaching the privacy of individuals or organizations.

- The encryption types are supported based on the specification of networking devices such as routers. The default encryption key may be provided by the router manufacturer and displayed at the bottom of the router.
- Wireless security encryption plays the role of providing safety, ensuring privacy, and allowing only authorized and authenticated access to networks.
- Wireless security encryption is mainly divided into four main types:

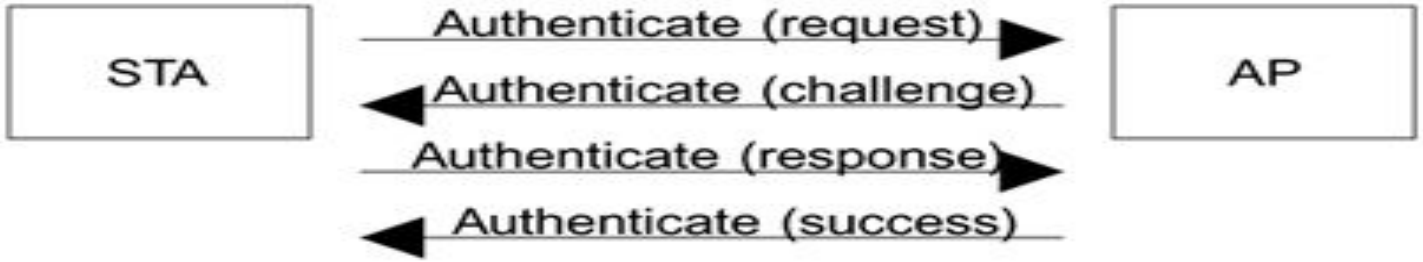
1. Wired Equivalent Privacy Protocol (WEP)
2. Wi-Fi Protected Access Protocol (WPA)
3. Wi-Fi Protected Access 2 Protocol (WPA2)
4. Wi-Fi Protected Access 3 Protocol (WPA3)

Wired Equivalent Privacy (WEP)

- WEP can be referred to as a security algorithm introduced to provide data privacy (or confidently) for wireless networks.
- WEP (or Wired
- One of the most essential features of Wired Equivalent Privacy is its 10 or 26 hexadecimal digits key, or we can also say 40 or 104 bits.
- There are two parts to WEP security. The first is the authentication phase and the second is the encryption phase.
- Equivalent Privacy) was introduced as part of the 802.11 standards. **WEP** employs a shared key authentication mechanism and the RC4 encryption algorithm to encrypt data.
- However, this protocol — introduced in 1997 — is outdated and considered insecure because it is easily hackable



Open Authentication



WEP Authentication

Authentication Sequences in the Original IEEE 802.11 Standard

Algorithm Num	Transaction Seq.	Status Code	Challenge Text

Authentication Message Format

- There are two parts to WEP security. The first is the authentication phase and the second is the encryption phase.
- The IEEE 802.11 uses three types of message: control, management, and data. The authentication phase uses management frames.
- For the open authentication, the mobile device sends one message requesting authentication and the access point replies with a success message.
- For WEP-based authentication, an exchange of four messages occurs. First the mobile device requests authentication, and then the access point sends a challenge message.
- The mobile device responds to the challenge to prove that it knows a secret key and, if the proof is accepted, the access point sends the success message.

- However, in practice many systems provide proprietary screening methods, the most popular being MAC address lists. The access point has a list of the MAC addresses that it will allow to join the network.
- The authentication is refused unless the mobile device's MAC address is found in the list.
- If someone were to mistakenly enter the wrong key value, or fail to update his keys, the access point would reject the authentication and the user would be notified of the failure.
- Without the authentication phase, the mobile device is accepted, but every frame it sends is discarded by the access point due to decryption failure.
- From the mobile side, it is hard to distinguish this failure from failure due to interference or being out of range.

- The fields for authentication messages general format,
- Algorithm Number indicates the type of authentication being used:

0 : Open system

1 : Shared key (WEP)

- The Transaction Sequence indicates where we are in the authentication sequence.
- The Status Code is sent in the final message to indicate success or failure of the authentication request.
- The Challenge Text field is used in the shared key (WEP) authentication.
- When the mobile device requests authentication, the access point sends a random number called challenge text. This is an arbitrary 128-bit number (preferably random). The mobile device then encrypts this number with the secret key using WEP and sends it back to the access point.
- Because the access point remembers the random number previously sent, it can check whether the result sent back was encrypted with the correct key; the mobile device must know the key in order to encrypt the random value successfully.

Wifi Protected Access(WPA)

- Wi-Fi Protected Access was introduced in 2003, this protocol was the Wi-Fi Alliance's replacement for WEP.
- It shared similarities with WEP but offered improvements in how it handled security keys and the way users are authorized.
- While WEP provides each authorized system with the same key, WPA uses the temporal key integrity protocol (TKIP), which dynamically changes the key that systems use.
- This prevents intruders from creating their own encryption key to match the one used by the secure network. The TKIP encryption standard was later superseded by the Advanced Encryption Standard (AES).
- In addition, WPA included message integrity checks to determine if an attacker had captured or altered data packets. The keys used by WPA were 256-bit, a significant increase over the 64 bit and 128-bit keys used in the WEP system.

WPA2

- WPA2 was introduced in 2004 and was an upgraded version of WPA. WPA2 is based on the robust security network (RSN) mechanism and operates on two modes:
- **Personal mode or Pre-shared Key (WPA2-PSK)** – which relies on a shared passcode for access and is usually used in home environments.
- **Enterprise mode (WPA2-EAP)** – as the name suggests, this is more suited to organizational or business use.
- Both modes use the CCMP – which stands for Counter Mode Cipher Block Chaining Message Authentication Code Protocol. The CCMP protocol is based on the Advanced Encryption Standard (AES) algorithm, which provides message authenticity and integrity verification.
- CCMP is stronger and more reliable than WPA's original Temporal Key Integrity Protocol (TKIP), making it more difficult for attackers to spot patterns.

WPA2 drawback

- WPA2 is vulnerable to key reinstallation attacks (KRACK). KRACK exploits a weakness in WPA2, which allows attackers to pose as a clone network and force the victim to connect to a malicious network instead.
- This enables the hacker to decrypt a small piece of data that may be aggregated to crack the encryption key.
- However, devices can be patched, and WPA2 is still considered more secure than WEP or WPA.

WPA3

- WPA3 is the third iteration of the Wi-Fi Protected Access protocol, introduced WPA3 in 2018.
- WPA3 introduced new features for both personal and enterprise use, Including:
- **Individualized data encryption**: When logging on to a public network, WPA3 signs up a new device using a Wi-Fi Device Provisioning Protocol (DPP) system that allows users to use Near Field Communication (NFC) tags or QR codes to allow devices on the network.
- In addition, WPA3 security uses GCMP-256 encryption rather than the previously used 128-bit encryption. ding:

- **Simultaneous Authentication of Equals protocol**: This is used to create a secure handshake, where a network device will connect to a wireless access point, and both devices communicate to verify authentication and connection.
- Even if a user's password is weak, WPA3 provides a more secure handshake using Wi-Fi DPP.
- **Stronger brute force attack protection**: WPA3 protects against offline password guesses by allowing a user only one guess, forcing the user to interact with the Wi-Fi device directly, meaning they would have to be physically present every time they want to guess the password. WPA2 lacks built-in encryption and privacy in public open networks, making brute force attacks a significant threat.

Wireless Security Protocols

	WEP	WPA	WPA 2	WPA 3
Stands For	Wired Equivalent Privacy	Wi-Fi Protected Access	Wi-Fi Protected Access 2	Wi-Fi Protected Access 3
Developed	1997	2003	2004	2018
Security Level	Very Low	Low	High	Very High
Encryption	RC4	TKIP with RC4	AES-CCMP	AES-CCMP AES-GCMP
Key Size	64 bit 128 bit	128 bit	128 bit	128 bit 256 bit
Authentication	Open System & Shared Key	Pre Shared Key & 802.1x with EAP	Pre Shared Key & 802.1x with EAP	AES-CCMP AES-GCMP
Integrity	CRC-32	64 Bit MIC	CCMP with AES	SHA-2

Wireless LAN Threats

- The risk of attacks occurring on wireless LANs is high.There are a number of reasons for this great increase in attacks, but the main one is that the nature of a wireless network is to provide easy access to end users, but this ease of access creates a more open attack surface
- The 7 most common wireless network threats are:

1. Configuration Problems:

- Simple configuration problems are often the cause of many vulnerabilities because many consumer/SOHO-grade access points ship with no security configuration at all.
- Other potential issues with configuration include weak passphrases, feeble security deployments, and default SSID usage.

2.Denial of Service:

- Anybody familiar with network security is aware of the concept of denial of service (DoS), also referred to as a “spoiler.” It is one of the simplest network attacks to perpetrate because it only requires limiting access to services.
- This can be done by placing viruses or worm programs on your network, or by simply sending a large amount of traffic at a specific target with the intent of causing a slowdown or shutdown of wireless services.
- This allows attackers to hijack resources, view unauthorized information disclosures, and introduce backdoors into the system.

3. Passive Capturing

- Passive capturing (or eavesdropping) is performed simply by getting within range of a target wireless LAN, then ‘listening to’ and capturing data which can be used for breaking existing security settings and analyzing non-secured traffic.
- Such information that can be “heard” include SSIDs, packet exchanges, and files .

4.Rogue (or Unauthorized/Ad-Hoc) Access Points:

- One method often used by attackers involves setting up a rogue access point within the range of an existing wireless LAN.
- The idea is to ‘fool’ some of the authorized devices in the area to associate with the false access point, rather than the legitimate one.

5. Evil Twin Attacks

- An attacker can gather enough information about a wireless access point to impersonate it with their own, stronger broadcast signal.
- This fools unsuspecting users into connecting with the evil twin signal and allows data to be read or sent over the internet.

6. Hacking of Lost or Stolen Wireless Devices

- if an employee loses a smartphone, laptop, etc., that is authorized to be connected to your network, it's very easy for the finder or thief to gain full access. All that’s necessary is to get past the password, which is quite simple to do.
- Make it a policy and practice to have employees immediately report a misplaced or stolen device so that it can be remotely locked, given a password change, or wiped clean.

7.Freeloading

- Sometimes unauthorized users will piggyback on your wireless network to gain free access.
- Additionally, employees sharing files with unrecognized networks, or giving permission for a friend or family member to use their login credentials for computer access, both seriously disrupt security measures.

What can you do to minimize the risks to your wireless network?

- **Change default passwords.**
- Most network devices, including wireless access points, are pre-configured with default administrator passwords to simplify setup.
- These default passwords are easily available to obtain online, and so provide only marginal protection.
- Changing default passwords makes it harder for attackers to access a device.
- Use and periodic changing of complex passwords is your first line of defense in protecting your device.

- **Restrict access.**
- Only allow authorized users to access your network. Each piece of hardware connected to a network has a media access control (MAC) address.
- You can restrict access to your network by filtering these MAC addresses.
- Consult your user documentation for specific information about enabling these features. You can also utilize the “guest” account, which is a widely used feature on many wireless routers.
- This feature allows you to grant wireless access to guests on a separate wireless channel with a separate password, while maintaining the privacy of your primary credentials.

- **Encrypt the data on your network.**
- Encrypting your wireless data prevents anyone who might be able to access your network from viewing it.
- There are several encryption protocols available to provide this protection. Wi-Fi Protected Access (WPA), WPA2, and WPA3 encrypt information being transmitted between wireless routers and wireless devices.
- WPA3 is currently the strongest encryption. WPA and WPA2 are still available; however, it is advisable to use equipment that specifically supports WPA3, as using the other protocols could leave your network open to exploitation.

- **Protect your Service Set Identifier (SSID).**
- To prevent outsiders from easily accessing your network, avoid publicizing your SSID.
- All Wi-Fi routers allow users to protect their device's SSID, which makes it more difficult for attackers to find a network. At the very least, change your SSID to something unique.
- Leaving it as the manufacturer's default could allow a potential attacker to identify the type of router and possibly exploit any known vulnerabilities.
- **Install a firewall.**
- Consider installing a firewall directly on your wireless devices (a host-based firewall), as well as on your home network (a router- or modem-based firewall).
- Attackers who can directly tap into your wireless network may be able to circumvent your network firewall—a host-based firewall will add a layer of protection to the data on your computer

- **Maintain antivirus software.**
- Install antivirus software and keep your virus definitions up to date.
- Many antivirus programs also have additional features that detect or protect against spyware and adware.
- **Use file sharing with caution.**
- File sharing between devices should be disabled when not needed.
- You should always choose to only allow file sharing over home or work networks, never on public networks.
- You may want to consider creating a dedicated directory for file sharing and restrict access to all other directories.
- In addition, you should password protect anything you share.

- **Keep your access point software patched and up to date.**
- The manufacturer of your wireless access point will periodically release updates to and patches for a device's software and firmware.
- Be sure to check the manufacturer's website regularly for any updates or patches for your device.
- **Check your internet provider's or router manufacturer's wireless security options.**
- Your internet service provider and router manufacturer may provide information or resources to assist in securing your wireless network.
- Check the customer support area of their websites for specific suggestions or instructions.

Bluetooth

- Bluetooth technology are ad-hoc piconets, which are local area networks with a very limited coverage and without the need for an infrastructure.
- A piconet is a collection of Bluetooth devices which are synchronized to the same hopping sequence.
- This network is needed to connect different small devices in close proximity (about 10 m) without expensive wiring or the need for a wireless infrastructure

Networking key features

1. Bluetooth operates on 79 channels in the 2.4 GHz band with 1 MHz carrier spacing.
2. Each device performs frequency hopping with 1,600 hops/s in a pseudo random fashion.
3. Bluetooth applies FHSS for interference mitigation (and FH-CDMA for separation of networks).

IEEE 802.11 criteria for wireless personal area networks (WPAN)

1. Market potential: How many applications, devices, vendors, customers are available for a certain technology?
2. Compatibility: Compatibility with IEEE 802.
3. Distinct identity: Originally, the study group did not want to establish a second 802.11 standard. However, topics such as, low cost, low power, or small form factor are not addressed in the 802.11 standard.
4. Technical feasibility: Prototypes are necessary for further discussion, so the study group would not rely on paper work.
5. Economic feasibility: Everything developed within this group should be cheaper than other solutions and allow for high-volume production

User scenarios

- Many different user scenarios can be imagined for wireless piconets or WPANs:

1. Connection of peripheral devices:

- Today, most devices are connected to a desktop computer via wires (e.g., keyboard, mouse, joystick, headset, speakers). This type of connection has several disadvantages: each device has its own type of cable, different plugs are needed, wires block office space.
- In a wireless network, no wires are needed for data transmission. However, batteries now have to replace the power supply, as the wires not only transfer data but also supply the peripheral devices with power.

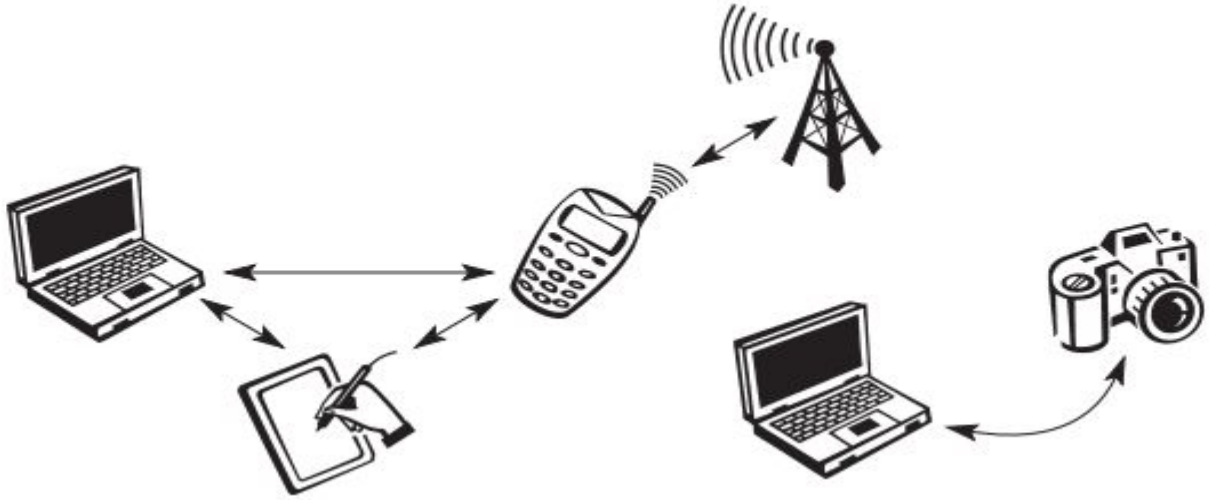
.

2. 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; small devices might not have WLAN adapters following the IEEE 802.11 standard, but cheaper Bluetooth chips built in.

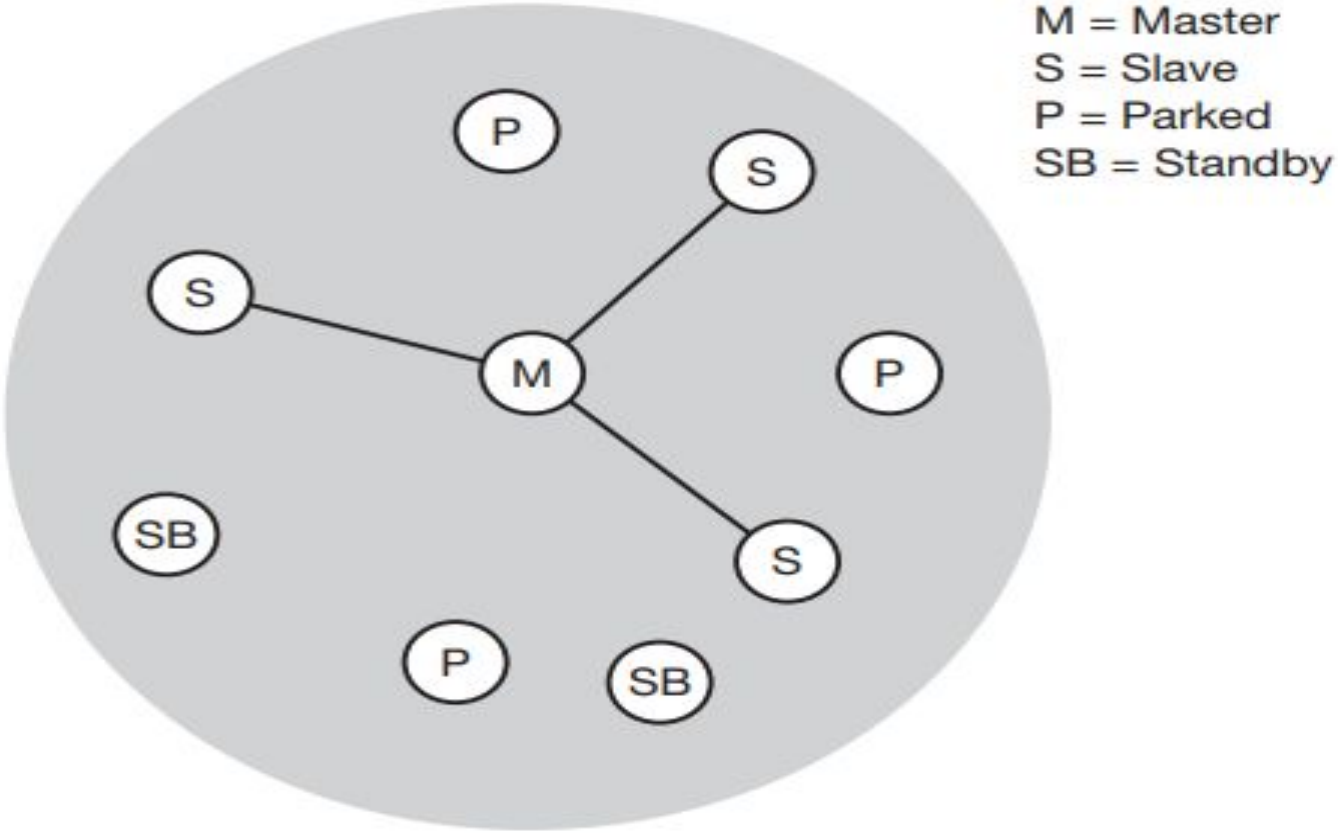
3. Bridging of networks:

- 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 then act as a bridge between the local piconet and, e.g., the global GSM network as shown in fig.
- 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.

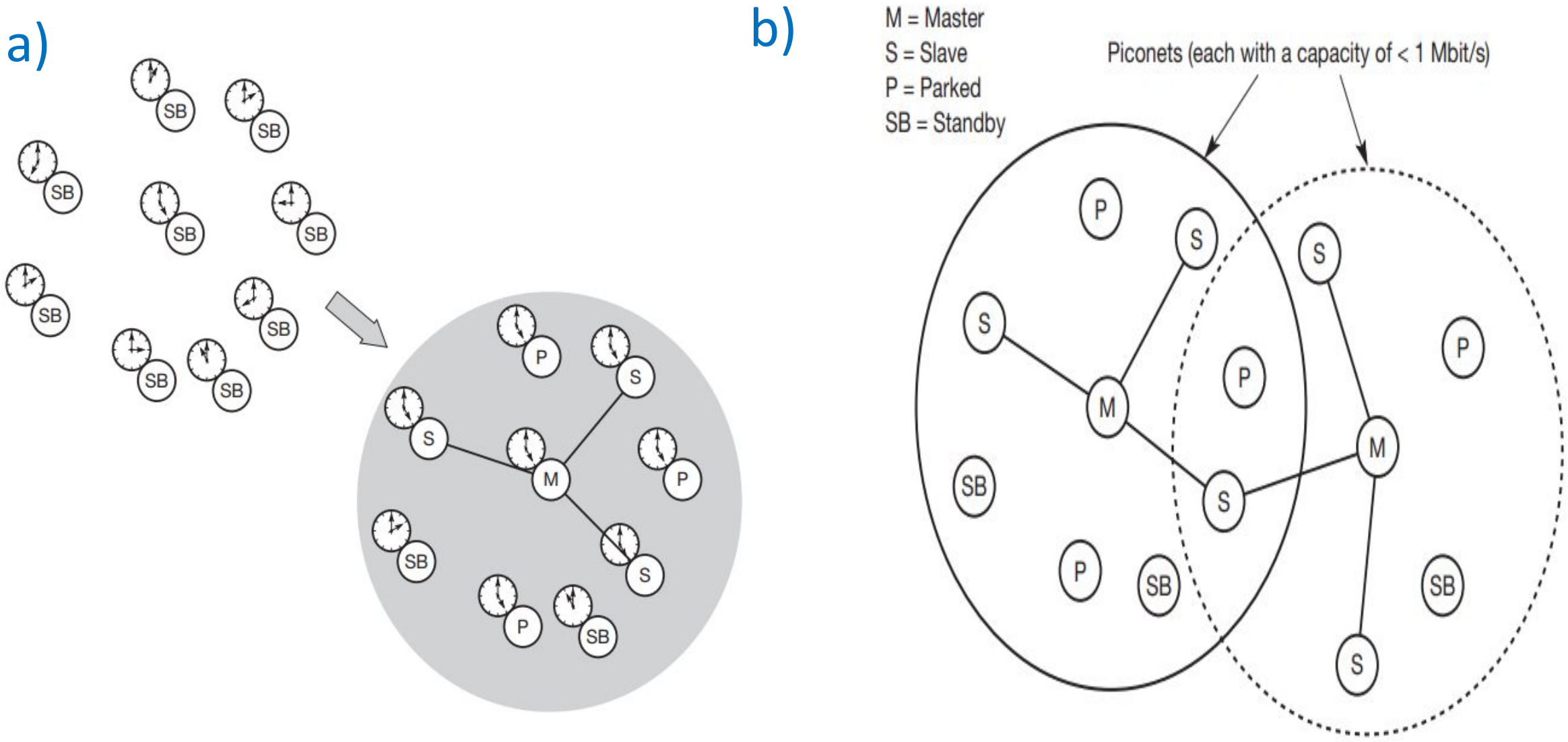
Bluetooth Architecture



Simple Bluetooth piconet

- Figure shows a collection of devices with different roles. One device in the piconet can act as master (M), all other devices connected to the master must act as slaves (S).
- The master determines the hopping pattern in the piconet and the slaves have to synchronize to this pattern.
- Each piconet has a unique hopping pattern. If a device wants to participate it has to synchronize to this.
- Two additional types of devices are shown- parked devices (P) and Devices in stand-by (SB) .

- Parked devices (P) can not actively participate in the piconet (i.e., they do not have a connection), but are known and can be reactivated within some milliseconds Devices in stand-by (SB) do not participate in the piconet.
- Each piconet has exactly one master and up to seven simultaneous slaves. More than 200 devices can be parked.
- The reason for the upper limit of eight active devices, is the 3-bit address used in Bluetooth.
- If a parked device wants to communicate and there are already seven active slaves, one slave has to switch to park mode to allow the parked device to switch to active mode.



Forming a) Bluetooth piconet and b) scatternet

Formation of a piconet and scatternet

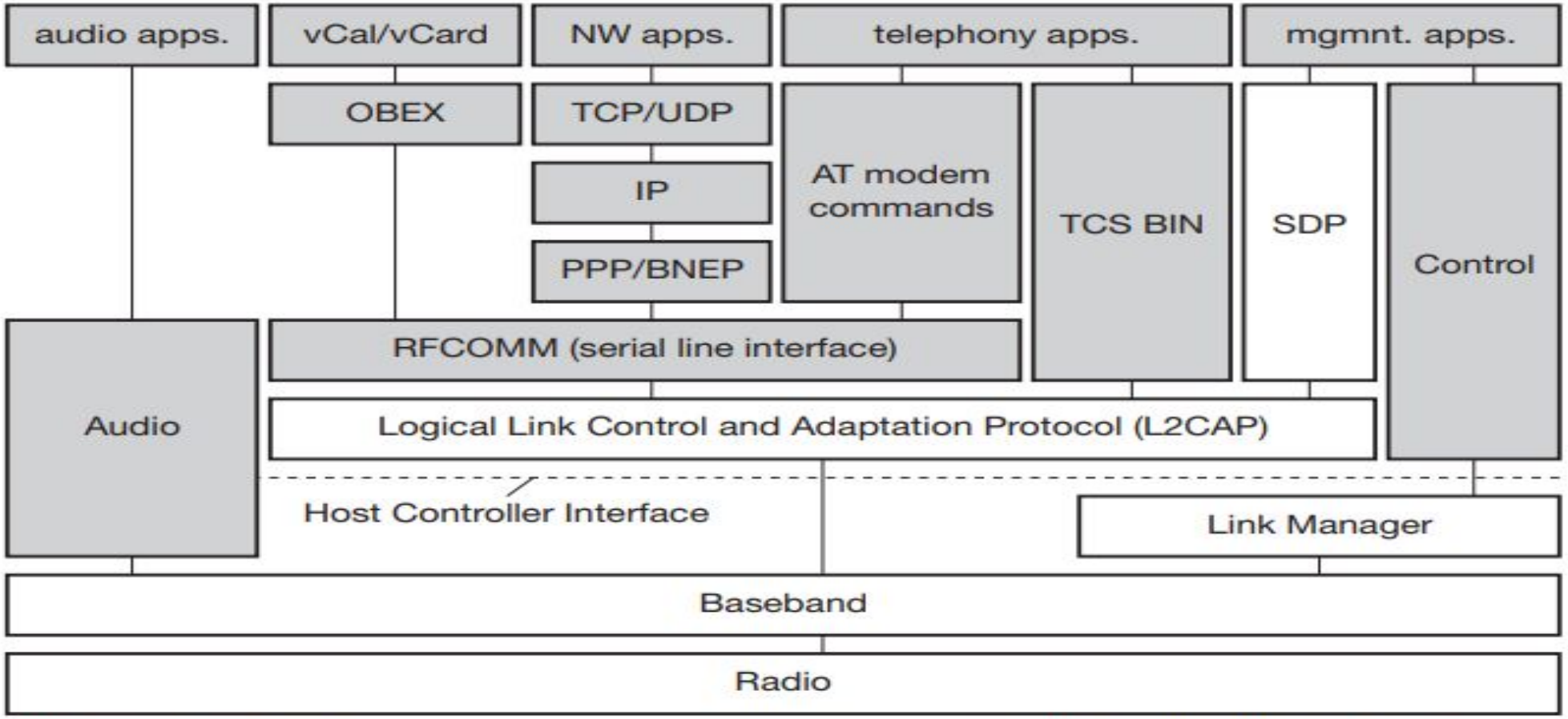
- In piconet(fig. a) all active devices have to use the same hopping sequence they must be synchronized. The first step involves a master sending its clock and device ID.
- All Bluetooth devices have the same networking capabilities, i.e., they can be master or slave. There is no distinction between terminals and base stations, any two or more devices can form a piconet.
- The unit establishing the piconet automatically becomes the master, all other devices will be slaves.
- The hopping pattern is determined by the device ID, a 48-bit worldwide unique identifier.
- The phase in the hopping pattern is determined by the master's clock. After adjusting the internal clock according to the master a device may participate in the piconet.

- 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 do not need an address.
- All users within one piconet have the same hopping sequence and share the same 1 MHz channel. As more users join the piconet, the throughput per user drops quickly. This led to the idea of forming groups of piconets called scatternet (fig. b)
- Only those units that really must exchange data share the same piconet, so that many piconets with overlapping coverage can exist simultaneously.
- In fig. the scatternet consists of two piconets, in which one device participates in two different piconets. Both piconets use a different hopping sequence, always determined by the master of the piconet.

- Bluetooth applies FH-CDMA for separation of piconets. In an average sense, all piconets can share the total of 80 MHz bandwidth available.
- Adding more piconets leads to a graceful performance degradation of a single piconet because more and more collisions may occur.
- A collision occurs if two or more piconets use the same carrier frequency at the same time. This will probably happen as the hopping sequences are not coordinated.
- If a device wants to participate in more than one piconet, it has to synchronize to the hopping sequence of the piconet it wants to take part in.
- If a device acts as slave in one piconet, it simply starts to synchronize with the hopping sequence of the piconet it wants to join. After synchronization, it acts as a slave in this piconet and no longer participates in its former piconet

- To enable synchronization, a slave has to know the identity of the master that determines the hopping sequence of a piconet.
- Before leaving one piconet, a slave informs the current master that it will be unavailable for a certain amount of time. The remaining devices in the piconet continue to communicate as usual.
- A master can also leave its piconet and act as a slave in another piconet. It is clearly not possible for a master of one piconet to act as the master of another piconet as this would lead to identical behavior.
- As soon as a master leaves a piconet, all traffic within this piconet is suspended until the master returns.
- If this is done periodically, for instance, isochronous data streams can be forwarded from one piconet to another. However, scatternets are not yet supported by all devices.
- Communication between different piconets takes place by devices jumping back and forth between theses nets.

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.

- The Bluetooth protocol stack can be divided into a core specification, which describes the protocols from physical layer to the data link control together with management functions, and profile specifications.
- The latter 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.
- 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

- RFCOMM : On top of L2CAP is the cable replacement protocol RFCOMM that emulates a serial line interface following the EIA-232 (formerly RS-232) standards.
- This allows for a simple replacement of serial line cables and enables many legacy applications and protocols to run over Bluetooth. RFCOMM supports multiple serial ports over a single physical channel.
- TCS BIN : 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
- Many protocols have been adopted in the Bluetooth standard. Classical Internet applications can still use the standard TCP/IP stack running over PPP or use the more efficient Bluetooth network encapsulation protocol (BNEP).

- Telephony applications can use the AT modem commands as if they were 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 protocol stacks is the support of audio. Audio applications may directly use the baseband layer after encoding the audio signals.