MOBILE COMPUTING (CS417)

UNIT-4: Wireless LAN

Wireless LAN (WLAN): - A wireless LAN (WLAN), also known as Wi-Fi, is a computer network that uses radio waves to link two or more devices without the need for physical cables. WLANs are commonly used in homes, offices, and other public places to provide internet access and file sharing capabilities.

How WLANs Work: -

WLANs operate by using radio waves to transmit data between devices. A WLAN network typically consists of two main components:

- **Access point (AP):** An AP is a device that acts as a central hub for the WLAN. It broadcasts a radio signal that allows other devices to connect to the network.

- **Wireless network adapter:** A wireless network adapter is a device that is installed in a computer or other device to allow it to connect to a WLAN. The adapter receives and transmits radio waves from the AP.

When a device with a wireless network adapter wants to connect to a WLAN, it sends out a request to the AP. The AP responds by sending back a list of available networks. The device can then select the network it wants to connect to and enter the network's password (if required).

Once connected, the device can communicate with other devices on the network and access the internet.

Advantages of WLANs are:

- **Flexibility:** Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.). Sometimes wiring is difficult if firewalls separate buildings (real firewalls made out of, e.g., bricks, not routers set up as a firewall). Penetration of a firewall is only permitted at certain points to prevent fire from spreading too fast.
- **Planning:** Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans. As long as devices follow the same standard, they can communicate. For wired networks, additional cabling with the right plugs and probably interworking units (such as switches) have to be provided.
- **Design:** Wireless networks allow for the design of small, independent devices which can for example be put into a pocket. Cables not only restrict users but also designers of small PDAs, notepads etc. Wireless senders and receivers can be hidden in historic buildings, i.e., current networking technology can be introduced without being visible.

- **Robustness:** Wireless networks can survive disasters, e.g., earthquakes or users pulling a plug. If the wireless devices survive, people can still communicate. Networks requiring a wired infrastructure will usually break down completely.
- **Cost:** After providing wireless access to the infrastructure via an access point for the first user, adding additional users to a wireless network will not increase the cost. This is, important for e.g., lecture halls, hotel lobbies or gate areas in airports where the numbers using the network may vary significantly. Using a fixed network, each seat in a lecture hall should have a plug for the network although many of them might not be used permanently. Constant plugging and unplugging will sooner or later destroy the plugs. Wireless connections do not wear out.

Disadvantages of WLANs are:

- **Quality of service:** WLANs typically offer lower quality than their wired counterparts. The main reasons for this are the lower bandwidth due to limitations in radio transmission (e.g., only 1–10 Mbit/s user data rate instead of 100–1,000 Mbit/s), higher error rates due to interference (e.g., 10–4 instead of 10–12 for fiber optics), and higher delay/delay variation due to extensive error correction and detection mechanisms.
- **Proprietary solutions:** Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardized functionality plus many enhanced features (typically a higher bit rate using a patented coding technology or special inter-access point protocols). However, these additional features only work in a homogeneous environment, i.e., when adapters from the same vendors are used for all wireless nodes.
- **Restrictions:** All wireless products have to comply with national regulations. Several government and non-government institutions worldwide regulate the operation and restrict frequencies to minimize interference. Consequently, it takes a very long time to establish global solutions like, e.g., IMT-2000, which comprises many individual standards. WLANs are limited to low-power senders and certain license-free frequency bands, which are not the same worldwide.
- **Safety and security:** Using radio waves for data transmission might interfere with other high-tech equipment in, e.g., hospitals. Senders and receivers are operated by laymen and, radiation has to be low. Special precautions have to be taken to prevent safety hazards. The open radio interface makes eavesdropping much easier in WLANs than, e.g., in the case of fiber optics. All standards must offer (automatic) encryption, privacy mechanisms, support for anonymity etc. Otherwise more and more wireless networks will be hacked into as is the case already (aka war driving: driving around looking for unsecured wireless networks.

Design Goals of WLAN: -

● **Global operation:** WLAN products should sell in all countries so, national and international frequency regulations have to be considered. In contrast to the infrastructure of wireless WANs, LAN equipment may be carried from one country into another – the operation should still be legal in this case.

● **Low power:** Devices communicating via a WLAN are typically also wireless devices running on battery power. The LAN design should take this into account and implement special power-saving modes and power management functions.

● **License-free operation:** LAN operators do not want to apply for a special license to be able to use the product. The equipment must operate in a license-free band, such as the 2.4 GHz ISM band.

● **Robust transmission technology:** Compared to their wired counterparts, WLANs operate under difficult conditions. If they use radio transmission, many other electrical devices can interfere with them (vacuum cleaners, hairdryers, train engines etc.). WLAN transceivers cannot be adjusted for perfect transmission in a standard office or production environment. Antennas are typically omnidirectional, not directed. Senders and receivers may move.

● **Simplified spontaneous cooperation:** To be useful in practice, WLANs should not require complicated setup routines but should operate spontaneously after power-up. These LANs would not be useful for supporting, e.g., ad-hoc meetings.

● **Easy to use:** In contrast to huge and complex wireless WANs, wireless LANs are made for simple use. They should not require complex management, but rather work on a plug-and-play basis.

● **Protection of investment:** 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.

● **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.

● **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 Transmission: -

- 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.
- No licenses are required for infrared and shielding is very simple.
- PDAs, laptops, notebooks, mobile phones etc. have an infrared data association (IrDA) interface.
- Electrical devices cannot interfere with infrared transmission.

Disadvantages of Infrared Transmission: -

- Disadvantages of infrared transmission are its low bandwidth compared to other LAN technologies.
- Limited transfer rates to 115 Kbit/s and we know that even 4 Mbit/s is not a particular high data rate.
- Their main disadvantage is that infrared is quite easily shielded.
- Infrared transmission cannot penetrate walls or other obstacles.
- 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: -

- Advantages of radio transmission include the long-term experiences made with radio transmission for wide area networks (e.g. microwave links) and mobile cellular phones.
- Radio transmission can cover larger areas and can penetrate (thinner) walls, plants, furniture etc.
- Additional coverage is gained by reflection.
- Radio typically does not need a LOS (Line of Site) if the frequencies are not too high.
- Higher transmission rates (e.g. 54 Mbit/s) than infrared (directed laser links, which offer data rates well above 100 Mbit/s).

Disadvantages of Radio Transmission: -

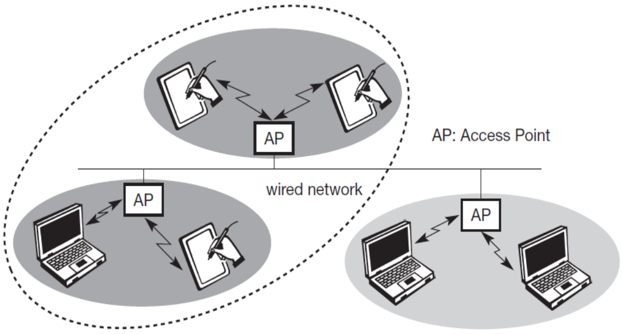
- Radio transmission can be interfered with other senders, or electrical devices can destroy data transmitted via radio.
- Bluetooth is simple than infrared.
- Radio is only permitted in certain frequency bands.
- Shielding is not so simple.
- Very limited ranges of license free bands are available worldwide and those that are available are not the same in all countries.
- A lot harmonization is going on due to market pressure.

Infrastructure and Adhoc Networks: -

Infrastructure Networks: - Many WLANs of today need an **infrastructure** network. 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 as shown in Fig, 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 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.

Figure 7.1
Example of three infrastructure-based wireless networks



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 reminiscent of 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.

Ad-hoc Networks: - Ad-hoc wireless networks, however, do not need any infrastructure to work. Each node can communicate directly with other nodes, so no access point controlling medium access is necessary. Figure 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 shown in Figure cannot, therefore, 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 as it is, for example, needed for unexpected meetings, quick replacements of infrastructure or communication scenarios far away from any infrastructure.

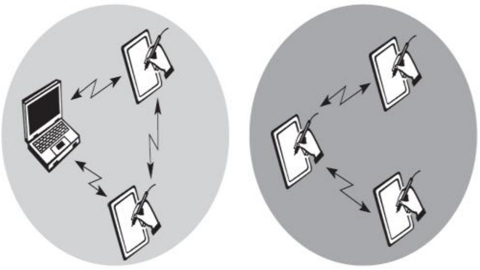


Figure 7.2
Example of two ad-hoc wireless networks

However, ad-hoc networks might only have selected nodes with the capabilities of forwarding data. Most of the nodes must connect to such a special node first to transmit data if the receiver is out of their range.

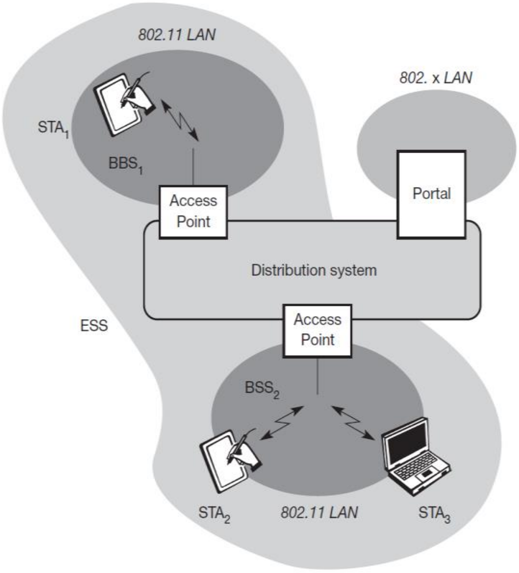
IEEE 802.11: - The IEEE standard 802.11 (IEEE, 1999) specifies the most famous family of WLANs in which many products are available. As the standard's number indicates, this standard belongs to the group of 802.x LAN standards, e.g., 802.3 Ethernet or 802.5 Token Ring. This means that the standard specifies the physical and medium access layer adapted to the special requirements of wireless LANs, but offers the same interface as the others to higher layers to maintain interoperability.

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

Additional features of the WLAN should include the support of power management to save battery power, the handling of hidden nodes, and the ability to operate worldwide. The 2.4 GHz ISM band, which is available in most countries around the world, was chosen for the original standard. Data rates envisaged for the standard were 1 Mbit/s mandatory and 2 Mbit/s optional.

System Architecture: - Figure shows the components of an infrastructure and a wireless part as specified for IEEE 802.11. Several nodes, called **stations (STA_i)**, are connected to **access points (AP)**. Stations are terminals with access mechanisms to the wireless medium and radio contact to the AP. The stations and the AP which are within the same radio coverage form a **basic service set (BSS_i)**. The example shows two BSSs – BSS_1 and BSS_2 – 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.
The distribution system connects the wireless networks via the APs with a **portal**, which forms the interworking unit to other LANs.
The architecture of the distribution system is not specified further in IEEE 802.11. It could consist of bridged IEEE LANs, wireless links, or any other networks. However, **distribution system services** are defined in the standard (although, many products today cannot interoperate and needs the additional standard IEEE 802.11f to specify an inter access point protocol).

Figure 7.3
Architecture of an
nfrastructure-based
IEEE 802.11



IEEE 802.11 allows the building of ad-hoc networks between stations, thus forming one or more independent BSSs (IBSS) as shown in Figure. In this case, an IBSS comprises a group of stations using the same radio frequency. Stations STA_1, STA_2, and STA_3 are in $IBSS_1$, STA_4 and STA_5 in $IBSS_2$. This means for example that STA_3 can communicate directly with STA_2 but not with STA_5. Several IBSSs can either be formed via the distance between the IBSSs as shown in Fig 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.

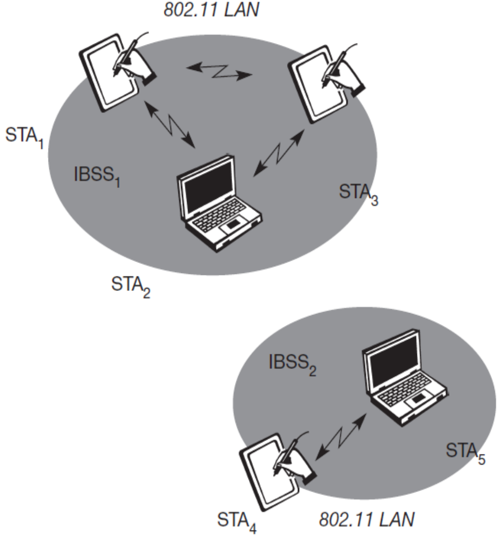
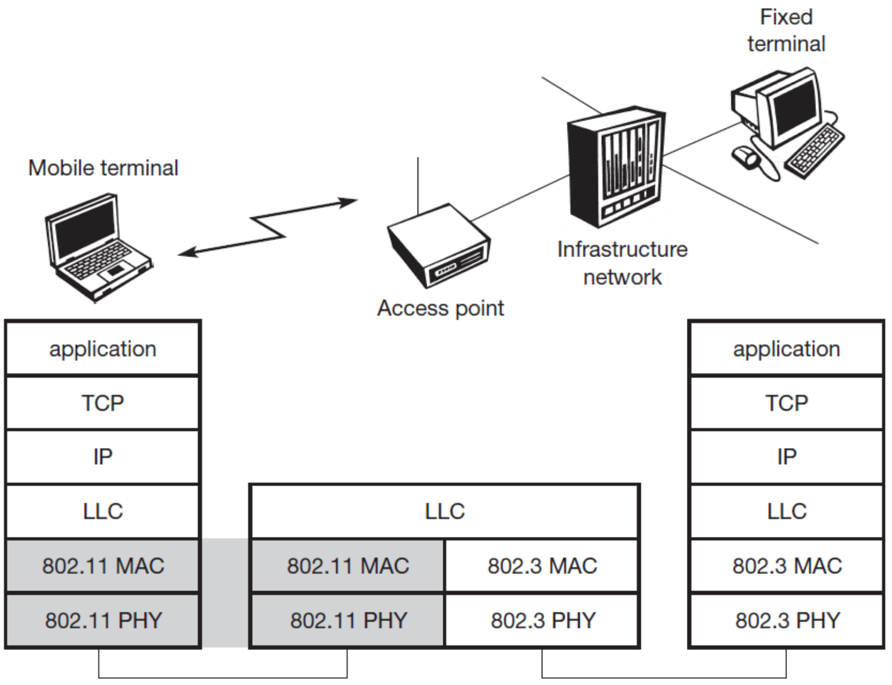


Figure 7.4
Architecture of
IEEE 802.11 ad-hoc
wireless LANs

Protocol Architecture: - Figure shows the most common scenario: an IEEE 802.11 wireless LAN connected to a switched IEEE 802.3 Ethernet via a bridge. 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 upper part of the data link control layer, the logical link control (LLC), covers the differences of the medium access control layers needed for the different media.

The IEEE 802.11 standard only covers the physical layer **PHY** and 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.

Figure 7.5
IEEE 802.11
protocol architecture
and bridging



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. 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 about 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).

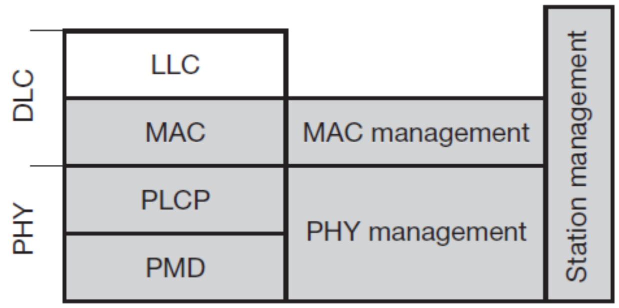


Figure 7.6
Detailed IEEE 802.11
protocol architecture
and management

Physical Layer: - IEEE 802.11 supports three different physical layers: one layer based on infra-red and 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.

Frequency hopping spread spectrum: -

Figure shows a frame of the physical layer used with FHSS. 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. Additionally, MAC data is scrambled using the polynomial $s(z) = z^7 + z^4 + 1$ for DC blocking and whitening of the spectrum. The fields of the frame fulfill the following functions:

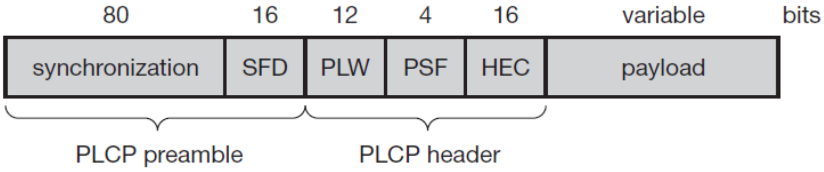


Figure 7.7 Format of an IEEE 802.11 PHY frame using FHSS

- **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 0000110010111101.
- **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 signalling 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 $G(x) = x^{16} + x^{12} + x^5 + 1$.

Direct sequence spread spectrum: -

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.

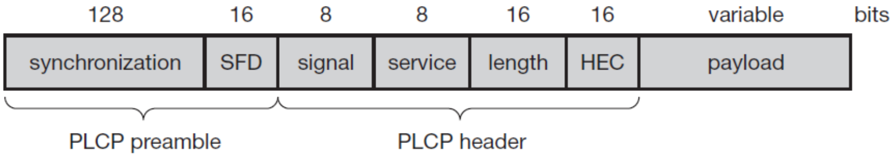


Figure 7.8 Format of an IEEE 802.11 PHY frame using DSSS

Figure shows a frame of the physical layer using DSSS. 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. The fields of the frame have the following functions:

● **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-bit.
● **Start frame delimiter (SFD):** This 16-bit field is used for synchronization at the beginning of a frame and consists of the pattern 1111001110100000.
● **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.

Infrared: - 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.

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: the mandatory basic method based on a version of CSMA/CA, an optional method avoiding the hidden terminal problem, and finally 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)**.
Below 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.

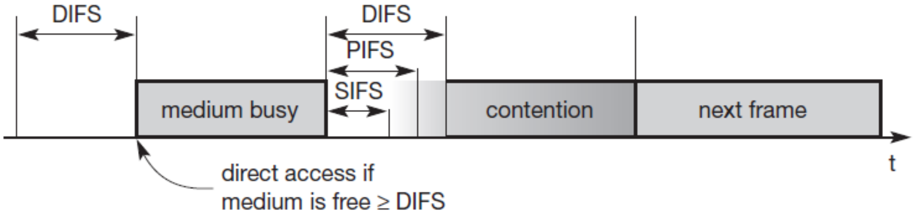


Figure 7.9
Medium access and inter-frame spacing

● **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.

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 shown in below Figure 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: management (=00), control (=01), or data (=10). The value 11 is 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. All details can be found in IEEE, 1999.

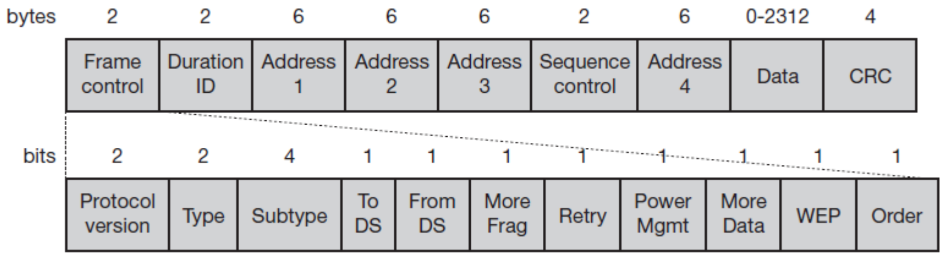


Figure 7.16
IEEE 802.11 MAC packet structure

- **To DS/From DS:** Explained in the following in more detail.
- **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 (Borisov, 2001).
- **Order:** If this bit is set to 1 the received frames must be processed in strict order.

MAC Management: - MAC management plays a central role in an IEEE 802.11 station as it 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.
The following functional groups have been identified and will be discussed in more detail in the following sections:

- **Synchronization:** Functions to support finding a wireless LAN, synchronization of internal clocks, generation of beacon signals.
- **Power management:** Functions to control transmitter activity for power conservation, e.g., periodic sleep, buffering, without missing a frame.
- **Roaming:** Functions for joining a network (association), changing access points, scanning for access points.
- **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).

802.11b: - 802.11b is a standard for wireless networking technology. It was one of the earliest Wi-Fi standards introduced and operates in the 2.4 GHz frequency range. This standard was ratified by the Institute of Electrical and Electronics Engineers (IEEE) in 1999 as part of the IEEE 802.11 family of standards.
Key features and details of 802.11b include:

- **Speed**: It supports a maximum data rate of up to 11 Mbps (megabits per second). While this speed was decent at the time of its introduction, it's significantly slower compared to more modern Wi-Fi standards.

- **Compatibility**: 802.11b devices are compatible with other standards within the 802.11 family, such as 802.11a, 802.11g, and 802.11n. However, when devices of different standards operate in the same network, they usually default to the speed of the slowest device, which in this case would be 802.11b.
- **Range**: Its range is typically limited compared to more recent standards like 802.11n or 802.11ac, which operate on both the 2.4 GHz and 5 GHz frequency bands. The 2.4 GHz frequency used by 802.11b can be more prone to interference from other devices like cordless phones or microwave ovens.
- **Obsolescence**: Due to its relatively slow speed and limited capabilities compared to newer standards like 802.11n and 802.11ac, 802.11b has become largely obsolete in modern networking setups. Most devices and networks have since moved on to faster and more advanced Wi-Fi standards.

Advantages of 802.11b

- Relatively low cost
- Easy to install and configure
- Widely supported by devices
- Backward compatibility with original 802.11 devices

Disadvantages of 802.11b

- Susceptible to interference from other devices in the 2.4 GHz band
- Relatively low data rate compared to newer standards
- Not suitable for real-time applications or high-bandwidth activities

Applications of 802.11b

- Home and office networking
- Internet access in public places
- Connecting mobile devices to the internet
- File sharing and printing
- Wireless gaming

802.11b has been largely superseded by newer standards, such as 802.11g and 802.11n, which offer higher data rates and greater range. However, 802.11b is still widely used due to its low cost and compatibility with many devices.

802.11a: - 802.11a is another wireless networking standard, ratified by the IEEE in 1999 alongside 802.11b. It operates in the 5 GHz frequency band and was developed around the same time as 802.11b but using a different frequency.

Key features of 802.11a include:

- **Speed**: 802.11a offers a higher maximum data rate compared to 802.11b, providing speeds of up to 54 Mbps. This was a significant improvement in data transfer rates compared to its predecessor.
- **Frequency Band**: Unlike 802.11b, which operates in the 2.4 GHz frequency range, 802.11a uses the less congested 5 GHz frequency band. This frequency band typically experiences less interference from other devices operating in the 2.4 GHz range, resulting in potentially better performance in environments with many wireless devices.
- **Channels**: 802.11a provides more available channels than 802.11b. It offers a total of 12 non-overlapping channels in the 5 GHz band compared to the three non-overlapping channels in the 2.4 GHz band of 802.11b. This allows for more simultaneous connections without interference.
- **Compatibility**: 802.11a is not backward compatible with 802.11b. Devices using these different standards cannot communicate directly with each other. However, dual-band devices that support both 802.11a and 802.11b/g can connect to networks using either standard.
- **Range and Obsolescence**: While 802.11a offered higher speeds and better performance in many aspects compared to 802.11b, it had shorter range and poorer penetration through walls and obstacles due to its use of the higher frequency 5 GHz band. As newer Wi-Fi standards emerged, such as 802.11n and subsequent iterations like 802.11ac and 802.11ax, these standards combined the advantages of both 2.4 GHz and 5 GHz bands, surpassing the limitations of 802.11a.

Advantages of 802.11a

- Higher data rate than 802.11b
- Less susceptible to interference from other devices in the 2.4 GHz band
- Suitable for real-time applications and high-bandwidth activities

Disadvantages of 802.11a

- More expensive than 802.11b
- Not as widely supported by devices
- Signal does not penetrate walls and other obstacles as well as 802.11b

Applications of 802.11a

- Home and office networking
- Internet access in public places
- Connecting mobile devices to the internet
- File sharing and printing

- Wireless gaming

802.11a has been largely superseded by newer standards, such as 802.11n and 802.11ac, which offer even higher data rates and greater range. However, 802.11a is still used in some niche applications, such as wireless bridges and backhaul links.

Bluetooth: - Bluetooth is an open wireless technology standard for exchanging data over short distances (using short wavelength radio transmission) from fixed and mobile devices, creating personal area networks (PANs) with high levels of security. It was formed by 5 companies in 1998. They are Ericsson, Intel, IBM, NOKIA and Toshiba. The Bluetooth specifications are developed and licensed by the Bluetooth Special Interest Group (SIG). Bluetooth SIG worked together to develop an integrated voice/data image. Bluetooth is named after King Harold Gormsen who was born in 10th century in United Denmark and Norway.

Features of Bluetooth: -

- Robustness
- Low complexity
- Low power
- Low cost

Characteristics of Bluetooth: -

- Bluetooth operates in unlicensed ISM band at 2.4 GHz (2400-2483.5 MHz).
- The range of bluetooth device is power class dependent: 1 meter, 10 meter, 100 meter.
- Devices connected using bluetooth frequency link forms a piconet.

Classes of Bluetooth: -

Class	**Maximum permitted power mW(dBm)**	**Range (Approximate)**
Class 1	100 mW(20 dBm)	~100 m
Class 2	2.5 mW(4 dBm)	~10 m
Class 3	1 mW(0 dBm)	~1 m

Applications of Bluetooth: -

- Wireless control and communication between a mobile phone and a hands-free headset.
- Wireless communication between PC's input and output devices. For example mouse, keyboard and printer.
- Transfer of files between devices with OBEX.
- Replacement of traditional wired serial communication in the test equipment, GPS receivers, medical equipment, barcode scanner and traffic control devices.
- Dial-up internet access on personal computers or PDA's using a data capable mobile phone as a modem.
- Wireless bridge between two industrial ethernet networks.
- Allowing a DECT phone to ring and answer calls on behalf of a nearby cellphone.
- For low bandwidth applications where higher USB bandwidth is not required and cable-free connection desired.

Advantages of Bluetooth: -

- Bluetooth does not require a clear line of sight between the synced devices.
- This means that the devices need not be facing each other, and it is also possible to carry out transfers when both the devices are in separate rooms.

- The fact that this technology requires no cables and wires is something that has made it so popular.
- The maximum range that it offers is 100 meters, but this range is not the same for all similar connections.
- It depends on the nature of the devices and the version that they operate upon.
- The processing power and battery power that it requires in order to operate is very low.
- This makes it an ideal tool for so many electronic devices, as the technology can be implemented pretty much anywhere.
- One major advantage is its simplicity of use. Anyone can figure out how to set up a connection and sync two devices with ease.
- Moreover, the technology is completely free to use and requires no charges to be paid to any service provider.

Disadvantages of Bluetooth: -

- Though the transfer speeds are impressive at around 1 Mbps, certain other technologies like infrared can offer speeds upto 4 Mbps.
- Even though the security is good, it is even better on infrared.
- This is because of the larger range of bluetooth and the lack of a line of sight.
- Someone who knows how to hack such networks can do so eventually.
- The battery usage duríng a single transfer is negligible, but there are some people who leave the device switched on in their devices.

Bluetooth Architecture: - The architecture of a bluetooth device is described by the two terminologies: piconet and scatternet.

Piconet: -

a) A piconet is a collection of bluetooth devices connected in an adhoc fashion.
b) One device in the piconet act as master (M) and all other devices connected to the master act as slaves (S).
c) Each piconet has exactly one master and upto seven simultaneous slaves, i.e., a master bluetooth device can communicate with upto seven devices.
d) The master determines the hopping pattern in the piconet and the slaves has to synchronize to this pattern.

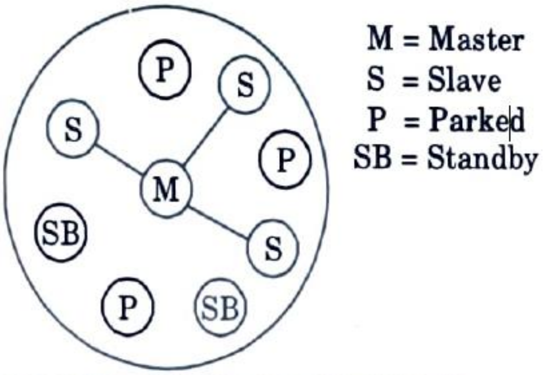


Fig. 2.15.1. Simple bluetooth piconet.

e) Each piconet has a unique hopping pattern.
f) At any given time, data can be transferred between the master and one other device, however, the device can switch roles and the slave can become the master at any time.
g) The master switches rapidly from one device to another in a round robin fashion.

Scatternet: -

a) Group of piconets form a scatternet.

b) Scatternet consists of two piconets in which one device participates in two different piconets.
c) Both piconets use a different hopping sequence and it is always determined by the master of the piconet.
d) Collisicn occurs if two or more piconets use the same carrier frequency at the same time.
e) 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.
f) If a device acts as a slave in one piconet, it simply starts to synchronize with the hopping sequence of the piconet it wants to join.
g) After synchronization, it acts as a slave in the new piconet and no longer participates in the former piconet.
h) Before leaving one piconet, a slave informs the current master that it will be unavailable for a certain amount of time.

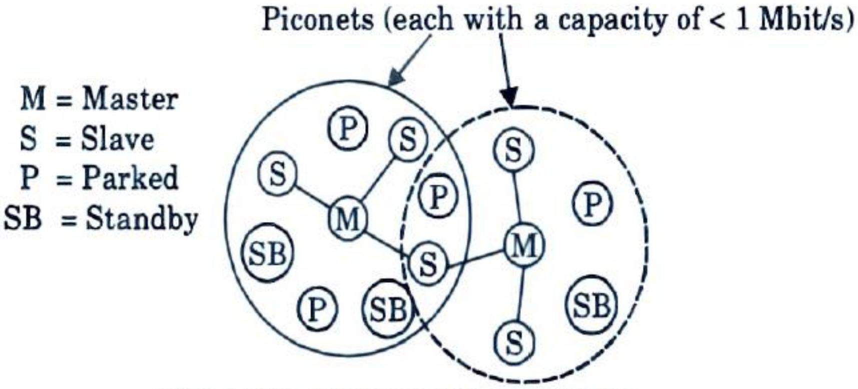


Fig. 2.15.2. Bluetooth scatternet.

Bluetooth Protocol Stack: -

- Bluetooth is defined as a layered protocol architecture consisting of core protocols, cable replacement protocols, telephony control protocols and adapted protocols.
- A simple bluetooth protocols stack is shown in Fig.

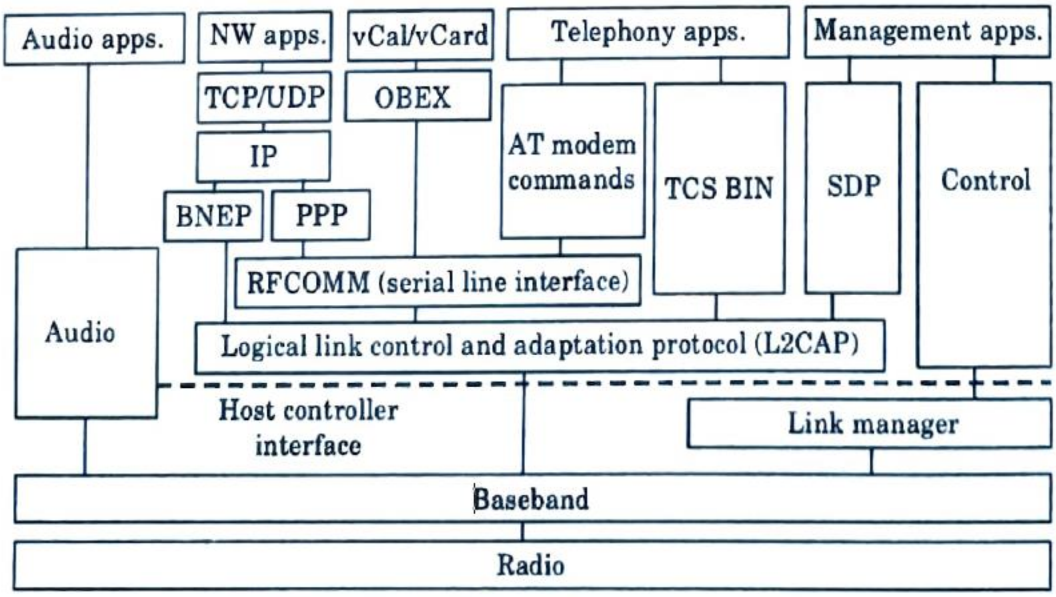


Fig. 2.16.1. Bluetooth protocol stack.

- Here,
  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 Communication

- 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.

Core specifications of bluetooth comprise of the following layers:

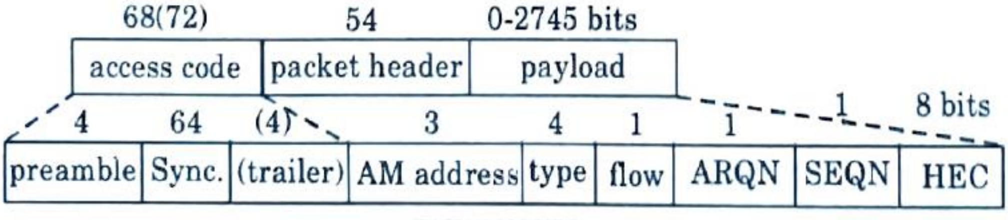
1. **Radio layer (Physical layer):** This layer includes specification of air interface, i.e., frequencies, modulation and transmit power.

Design issues:

- The radio layer operates in the unlicensed ISM band at 2.4 GHz.
- Power consumption is very low due to battery operated devices.
- Frequency band (2400-2483.5 MHz), 83.5 MHz bandwidth.
- Bluetooth uses frequency hopping/TDD scheme at a rate of 1600 hops/sec to avoid narrow band interference.
- Within a piconet, all devices use the same hopping sequence.
- Transmitting power is upto 100 mW and minimum is 1 mW.
- Range is between 10 m - 100 m.

2. **Baseband Layer (MAC Layer):**

- It includes description of basic connection establishment, packet formats, timing and basic QoS parameters.
- The functions of baseband layer are quite complex as it not only performs frequency hopping for interference mitigation and medium access, but also defines physical links and many packet formats.
- It enables the physical radio frequency link between the Bluetooth devices to form a piconet.
- Bluetooth also defines 1 slot, 3 slot and 5 slot packets for higher data rates.



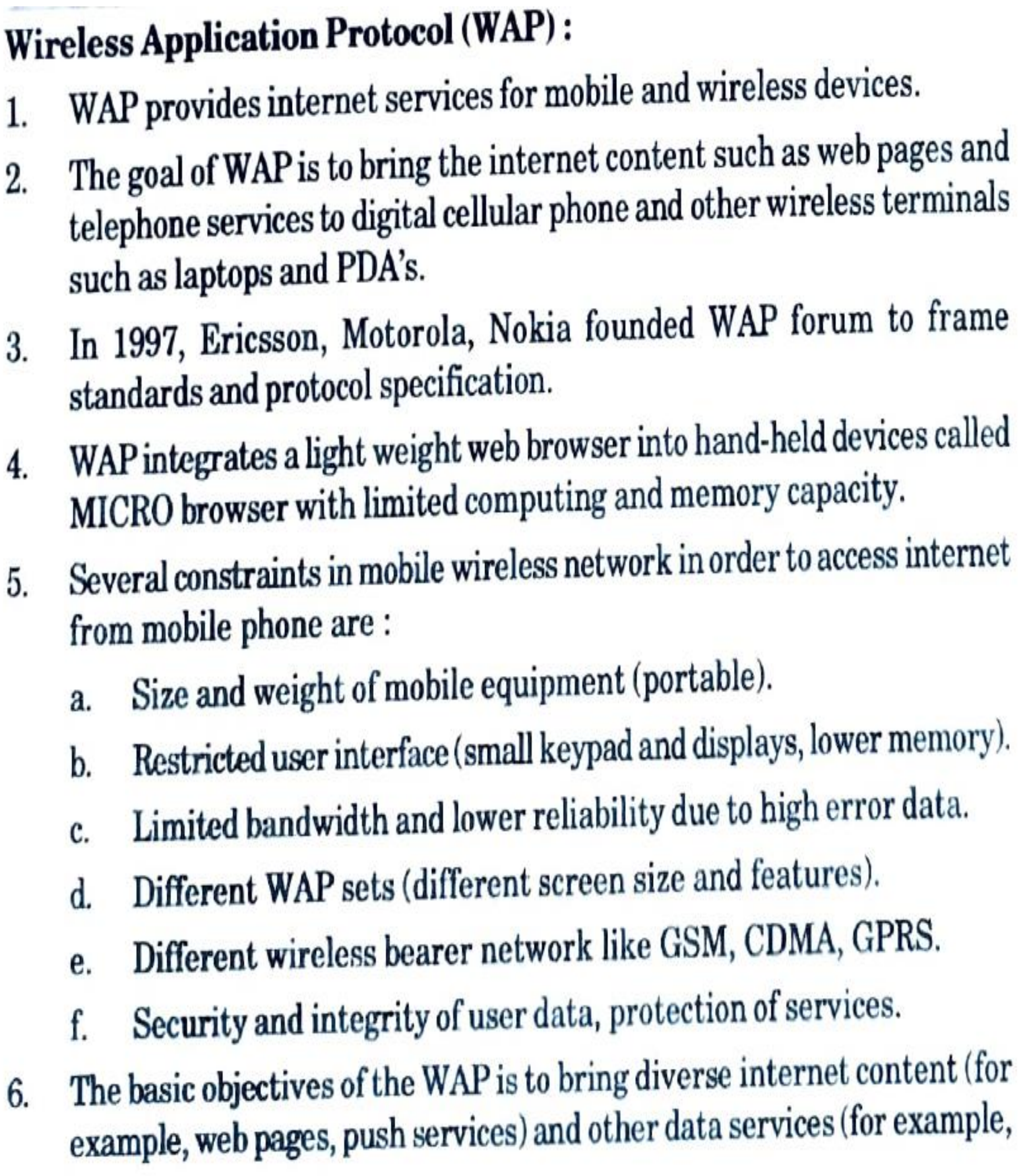
- A bluetooth packet (1 slot) baseband layer consists three fields: access code, packet header, payload.
- Baseband layer offers two different types of links, a synchronous connection-oriented link and an asynchronous connectionless link.

3. **The Link Manager Protocol (LMP):** It provides link set-up and management between devices including security functions and parameters negotiation. LMP performs the following functions:
    - Authentication, Pairing and Encryption
    - Synchronization
    - Capability negotiation
    - Power Control
    - Link Supervision

- State and transmission mode change

4. **Service Discovery Protocol (SDP):** SDP is used to allow devices to discover what services each other support, and what parameters to use services and the characteristics of the services can be queried and after that, a connection between two or more bluetooth devices may be established.
5. **Logical Link Control and Adaptation Protocol Layer (L2CAP):**
   - The bluetooth L2CAP layer provides connectionless and connection-oriented data services to upper layer protocol.
   - It also supports reassembly of packets, and Quality of Service (QoS) communication.
   - This layer does not provide any reliability and uses the baseband to ensure reliability.
   - L2CAP transmits and receives L2CAP data packets upto 64 kbit in length.

Introduction to WAP Architecture and Protocol Stack: -



Wireless Application Protocol (WAP) :

1. WAP provides internet services for mobile and wireless devices.
2. The goal of WAP is to bring the internet content such as web pages and telephone services to digital cellular phone and other wireless terminals such as laptops and PDA's.
3. In 1997, Ericsson, Motorola, Nokia founded WAP forum to frame standards and protocol specification.
4. WAP integrates a light weight web browser into hand-held devices called MICRO browser with limited computing and memory capacity.
5. Several constraints in mobile wireless network in order to access internet from mobile phone are :
   a. Size and weight of mobile equipment (portable).
   b. Restricted user interface (small keypad and displays, lower memory).
   c. Limited bandwidth and lower reliability due to high error data.
   d. Different WAP sets (different screen size and features).
   e. Different wireless bearer network like GSM, CDMA, GPRS.
   f. Security and integrity of user data, protection of services.
6. The basic objectives of the WAP is to bring diverse internet content (for example, web pages, push services) and other data services (for example,

stock quotes) to digital cellular phones and other wireless, mobile terminals (for example, PDAs, laptops).

7. Moreover, a protocol suit should enable global wireless communication across different wireless network technologies, for example, GSM, CDPD, UMTS etc.
8. The forum is embracing and extending existing standards and technologies of the internet wherever possible and is creating a framework for the development of contents and applications that scale across a very wide range of wireless bearer networks and wireless device types.

WAP applications :

1. Handling information of all types.
2. Access to e-mail and chat.
3. Weather information.
4. Information about currency rates.
5. Online music support of WAP multimedia etc.

Que 2.29. **Discuss WAP model.**

Answer

1. The WAP programming model as shown in Fig 2.29.1 is similar to the WWW programming model.
2. This provides several benefits to the application developer community, including a familiar programming model, a proven architecture, and the ability to leverage existing tools (for example web servers, XML tools, etc.).
3. Optimizations and extensions have been made in order to match the characteristics of the wireless environment.
4. Wherever possible, existing standards have been adopted or have been used as the starting point for the WAP technology.

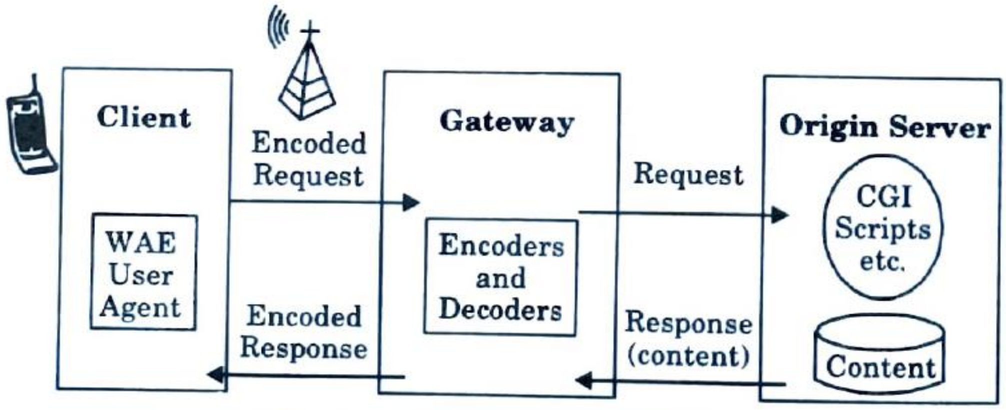


Fig. 2.29.1. WAP programming model.

5. WAP defines a set of standard components that enable communication between mobile terminals and network servers, including :

   a. **Standard naming model :** WWW-standard URLs are used to identify WAP content on origin servers.WWW -standard URIs are used to identify local resources in a device, for example, call control functions.

   b. **Content typing :** All WAP content is given a specific type consistent with WWW typing. This allows WAP user agents to correctly process the content based on its type.

   c. **Standard content formats :** WAP content formats are based on WWW technology and include display markup, calendar information, electronic business card objects, images and scripting language.

   d. **Standard communication protocols :** WAP communication protocols enable the communication of browser requests from the mobile terminal to the network web server.

Architecture / Protocol stack of WAP :

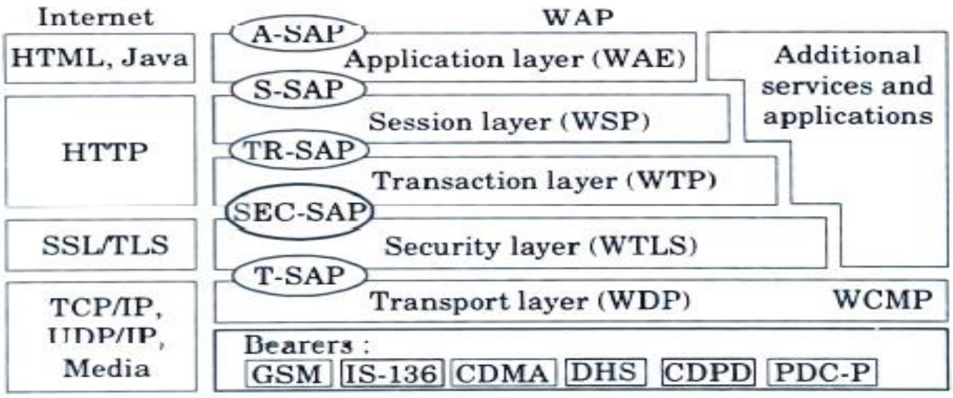


Fig. 2.31.1. WAP layered Architecture and protocol stack.

Wireless application environment (WAE) :

1. WAE is a general-purpose application environment based on a combination of World Wide Web (WWW) and mobile telephony technologies.

2. The primary objective of the WAE effort is to establish an interoperable environment that will allow operators and service providers to build applications and services that can reach a wide variety of different wireless platforms in an efficient and useful manner.

3. WAE includes a micro-browser environment containing the following functionality :

a. **Wireless markup language (WML) :** A lightweight markup language, similar to HTML, but optimized for use in hand-held mobile terminals.

b. **WML script :** A lightweight scripting language, similar to JavaScript.

c. **Wireless telephony application (WTA, WTAI) :** Telephony services and programming interfaces.

d. **Content formats :** A set of well-defined data formats, including images, phonebook records and calendar information.

Wireless session protocol (WSP) :

1. The wireless session protocol (WSP) provides the application layer of WAP with a consistent interface for two session services.
2. The first is a connection-oriented service that operates above the transaction layer protocol WTP.
3. The second is a connectionless service that operates above a secure or non-secure datagram service (WDP).
4. The wireless session protocols currently consist of services suited for browsing applications (WSP/B).
5. WSP/B provides the following functionality :
   a. HTTP/1.1 functionality and semantics in a compact over-the-air encoding.
   b. Long-lived session state.
   c. Session suspend and resume with session migration.
   d. A common facility for reliable and unreliable data push.
   e. Protocol feature negotiation.

Wireless transaction protocol (WTP) :

1. WTP runs on top of a datagram service and provides as a light-weight transaction-oriented protocol that is suitable for implementation in "thin" clients (mobile stations).
2. WTP operates efficiently over secure or non-secure wireless datagram networks and provides the following features :
   a. Three classes of transaction service.
   b. Unreliable one-way requests.
   c. Reliable one-way requests.
   d. Reliable two-way request-reply transactions.

Wireless transport layer security (WTLS) :

1. WTLS is a security protocol based upon the industry-standard transport layer security (TLS) protocol, formerly known as secure sockets layer (SSL).
2. WTLS is intended for use with the WAP transport protocols and has been optimized for use over narrow-band communication channels.
3. WTLS provides the following features :

   a. **Data integrity :** WTLS contains facilities to ensure that data sent between the terminal and an application server is unchanged and uncorrupted.

   c. **Authentication :** WTLS contains facilities to establish the authenticity of the terminal and application server.

   c. **Denial-of-service protection :** WTLS makes many typical denial-of-service attacks harder to accomplish and protects the upper protocol layers.
4. WTLS may also be used for secure communication between terminals, for example, for authentication of electronic business card exchange.

Wireless datagram protocol (WDP) :

1. The transport layer protocol in the WAP architecture is referred to as the wireless datagram protocol (WDP).
2. The WDP layer operates above the data capable bearer services supported by the various network types.
3. As a general transport service, WDP offers a consistent service to the upper layer protocols of WAP and communicate transparently over one of the available bearer services.
4. Since, the WDP protocols provide a common interface to the upper layer protocols the security, session and application layers are able to function independently of the underlying wireless network.

Bearers :

1. The WAP protocols are designed to operate over a variety of different bearer services, including short message, circuit-switched data, and packet data.
2. The bearers offer differing levels of quality of service with respect to throughput, error rate, and delays.
3. The WAP protocols are designed to compensate for or tolerate these varying levels of service.
4. The list of supported bearers will change over time with new bearers being added as the wireless market evolves.

Other services and applications :

1. The WAP layered architecture enables other services and applications to utilize the features of the WAP stack through a set of well-defined interfaces.
2. External applications may access the session, transaction, security and transport layers directly.
3. This allows the WAP stack to be used for applications and services not currently specified by WAP, but deemed to be valuable for the wireless market.
4. For example, applications, such as electronic mail, calendar, phone book, notepad, and electronic commerce, or services, such as white and yellow pages, may be developed to use the WAP protocols.