Unit –V
Wireless LAN

- Introduction
- Infra red v/s Radio Transmission
- Infrastructure and ad-hoc networks
- IEEE 802.11
- HIPERLAN
- Bluetooth

Introduction

- It is a local area network without wires. Also known as WLAN.
- Mobile users can access information and network resources through wireless LAN.
- It is not the replacement for the wired infrastructure. Implemented as an extension to a wired LAN within a building or campus.
- Constitutes a fast-growing market introducing the flexibility of wireless access across into office, home.
- WLANs are operated by individuals, not by large-scale network providers.

Introduction

- The goal of WLANs is to replace office cabling, to enable tetherless access to the internet and to introduce a higher flexibility for ad-hoc communication in.

Several Advantages of WLANs

- Flexibility – nodes can communicate without further restriction, within radio coverage. Radio waves can penetrate walls, senders and receivers can be placed anywhere.
- Planning – only wireless ad-hoc networks allow for communication without previous planning any wired network needs wiring plans. Devices following the same standard, can communicate.

Several Advantages of WLANs

- Design – wireless networks allow for the design of small, independent devices which can for example be put into a pocket. Cables restrict users and also designers of small PDAs, notepads etc.
- Robustness – wireless networks can survive disasters. If the wireless devices survive, people can still communicate.
- Cost – after providing wireless access to the infrastructure via an access point for the first user, adding additional users to wireless network will not increase the cost.

Several Disadvantages of WLANs

- Quality of Service – WLANS offer lower quality than their wired counterparts. Main reasons for this are the lower bandwidth due to limitations in radio transmission, higher error rates due to interference and higher delay/delay variation due to extensive error correction and detection mechanisms.
- Proprietary solutions – due to slow standardization procedures, many companies have proprietary solutions offering standardized functionality plus many enhanced features. These features only work in a homogeneous environment.

Several Disadvantages of WLANs

- Restrictions – wireless products have to comply with national regulations. Several government and non-government institutions worldwide regulate the operation and restrict frequencies to minimize interference. WLANs are limited to low-power senders and certain license free frequency bands which are not same worldwide.

Several Disadvantages of WLANs

- Safety and security – use of radio waves for data transmission might interfere with other high-tech equipment in. Senders and receivers are operated by laymen and radiation has to be low. Special precautions to be taken to prevent safety hazards. All standards must offer encryption, privacy mechanisms, support for anonymity etc.

Design goals for WLANs

- Many different and sometimes competing, design goals have to be taken into account for WLANs to ensure their commercial success.
  - Global operation
  - Low power
  - License free operation
  - Robust transmission technology
  - Simplified spontaneous cooperation
  - Easy to use
  - Protection of investment
  - Safety and security
  - Transparency for applications

Design goals for WLANs

- Global operation – all 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.

Design goals for WLANs

- Low power – devices communicating via a WLAN are 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.

Design goals for WLANs

- Robust transmission technology – if WLANs use radio transmission, many other electrical devices can interfere with them. WLAN transceivers cannot be adjusted for perfect transmission in a standard office or production environment. Antennas are omnidirectional, not directed. Senders and receivers may move.
- Simplified spontaneous cooperation – WLANs should not require complicated setup routines but should operate spontaneously after power-up.

Design goals for WLANs

- Easy to use – wireless LANs are made for simple use and not require complex management, but rather work on plug-and-play basis.
- Protection of investment – the new WLANs should protect a lot of money which has been already invested into wired LANs by being interoperable with the existing networks. 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.

Design goals for WLANs

- Safety and security – WLANs should be safe to operate, regarding low radiation if used. Users cannot keep safety distances to antennas. Users should not be able to read personal data during transmission., so encryption mechanisms should be integrated. The networks should also consider user privacy, i.e. it should not be possible to collect roaming profiles for tracking persons if they do not agree.

Design goals for WLANs

- Transparency for applications – already running applications should continue to run over WLANs, the only difference being higher delay and lower band width. The fact of wireless access and mobility should be hidden if it is not relevant, but the network should also support location aware applications.

Infra red vs radio transmission

- Two different basic transmission technologies can be used to set up WLANs.
- One is based on the transmission of infra red light e.g. at 900 nm wavelength.
- Other one is much more popular, uses radio transmission in the GHz range e.g. 2.4 GHz in the license free ISM band.
- Both of these technologies can be used to set up ad-hoc connections for work groups, to connect or to support mobility within a small area.

Infra red vs radio transmission

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

Infra red vs radio transmission

- Infra red technology - Advantages
  - Its simple and extremely cheap senders and receivers which are integrated into nearly all mobile devices available today.
  - PDAs, laptops, notebooks, mobile phone and many other devices have an infra red data association (IrDA) interface.
  - No licenses are needed for intra red technology and shielding is very simple.
  - Electrical devices do not interfere with infra red transmission.

Infra red vs radio transmission

- Infra red technology – Disadvantages
  - Its low bandwidth compared to other LAN technologies.
  - Main disadvantage is that infra red is quite easily shielded.
  - Infra red transmission cannot penetrate walls or other obstacles.

Infra red vs radio transmission

- Radio transmission
  - Almost all networks e.g. GSM at 900, 1800 an d1900 MHz, DECT at 1880 MHz etc. use radio waves for data transmission.

Infra red vs radio transmission

- Radio transmission – Advantages
  - Include the long-term experiences made with radio transmission for wide area networks and mobile cellular phones.
  - Can cover larger areas and can penetrate (thinner) walls, furniture, plants etc. Additional coverage is gained by reflection.
  - Radio typically does not need a LOS if the frequencies are not too high.
  - Current radio-based products offer much higher transmission rates than infra red.

Infra red vs radio transmission

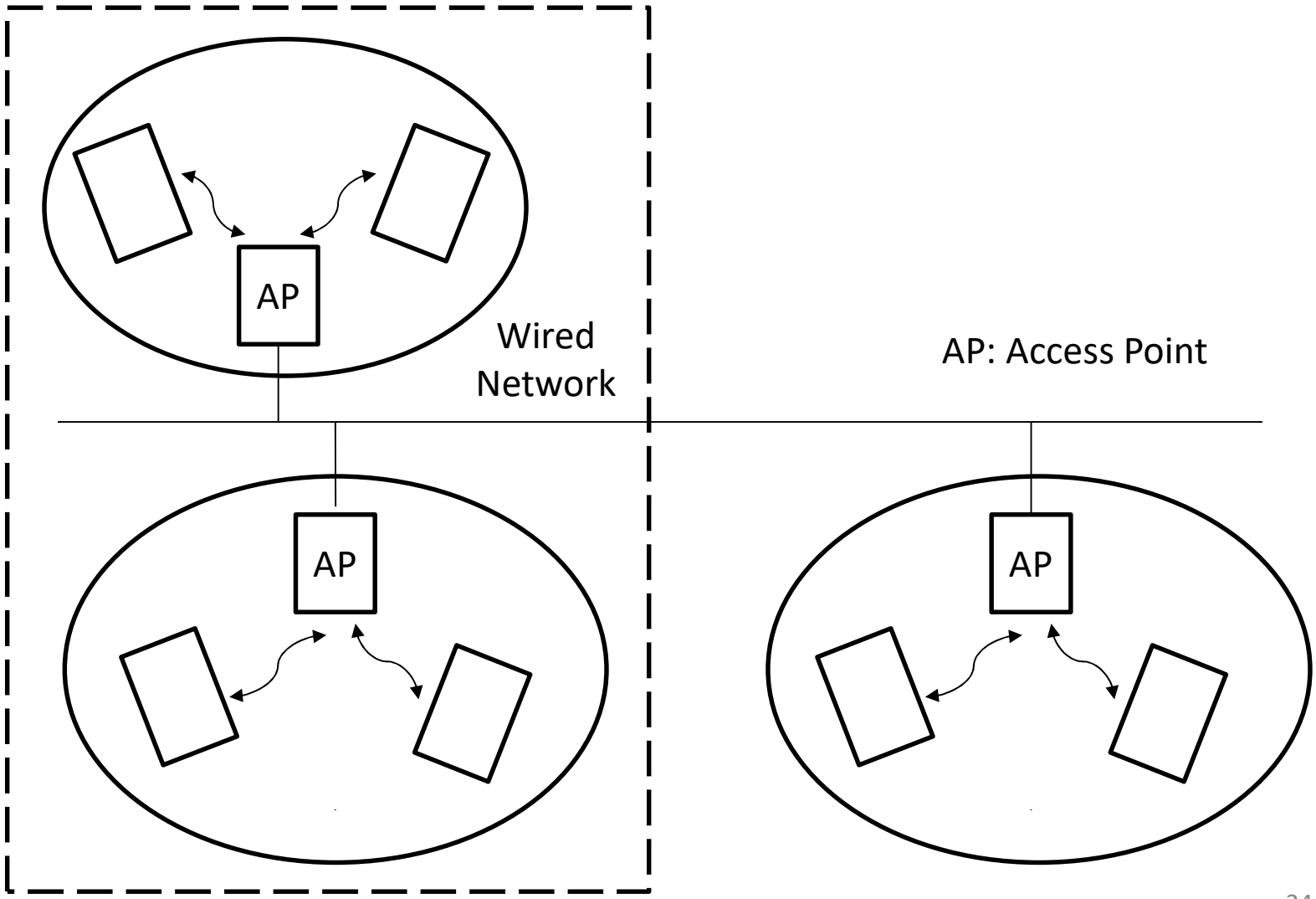
- Radio transmission – disadvantages
  - Shielding is not simple.
  - Radio transmission can interfere with other senders, or electrical devices can destroy data transmitted via radio.
  - Radio transmission is only permitted in certain frequency bands.
  - Limited ranges of license-free bands are available worldwide and those that are available are not the same in all countries.

Infrastructure and ad-hoc networks

- Many WLANs need an infrastructure networks which 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 control medium access, but also acts as a bridge to other wireless or wired networks.

Infrastructure and ad-hoc networks

- Infrastructure based wireless networks



Infrastructure and ad-hoc networks

- Infrastructure based wireless networks
  - Diagram contains three access points with their three wireless networks and a wired network.
  - Many 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.
  - The design is simpler because most of the network functionality lies within access point, whereas the wireless clients can remain quite simple.

Infrastructure and ad-hoc networks

- Infrastructure based wireless networks
  - 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.
  - If only the access point controls medium access, no collisions are possible.
  - 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 and ad-hoc networks

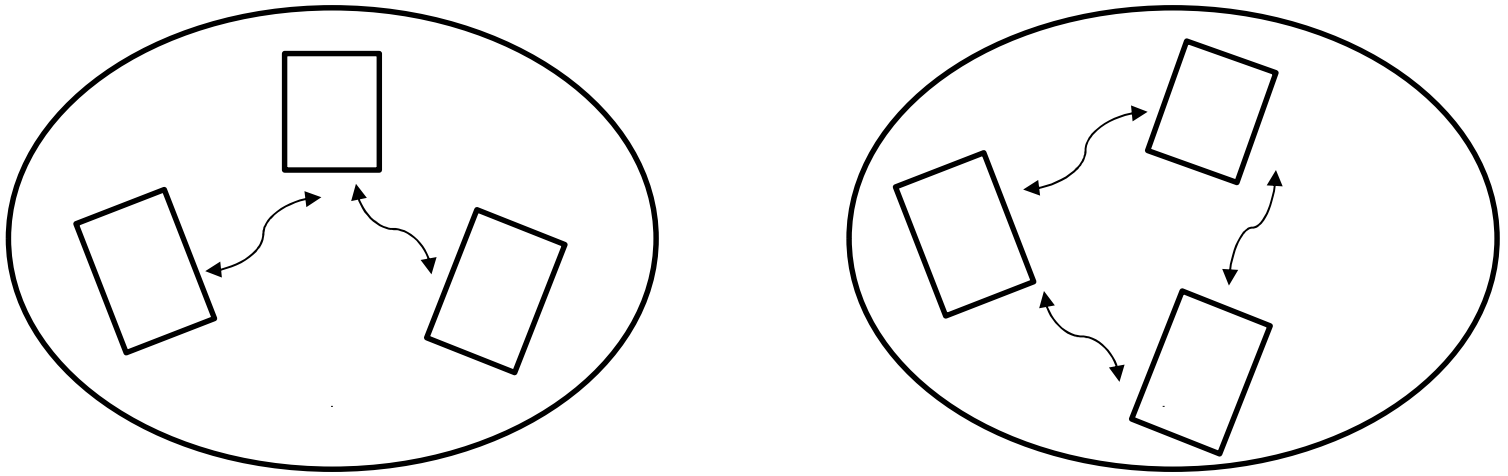
- Infrastructure based wireless networks
  - Infrastructure based networks lose some of the flexibility wireless networks can offer.
  - Cellular phone networks are infrastructure-based networks for wide area. Also satellite-based cellular phones have an infrastructure- the satellite.
  - Infrastructure does not necessary imply a wired fixed network.

Infrastructure and ad-hoc networks

- Ad-hoc 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.

Infrastructure and ad-hoc networks

- Ad-hoc networks



Infrastructure and ad-hoc networks

- Ad-hoc networks
  - Diagram represents two ad-hoc networks with three nodes each.
  - Nodes 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, therefore, communicate with each other if they are not within the same radio range.
  - Exhibits the greatest possible flexibility as it is.

Infrastructure and ad-hoc networks

- Ad-hoc networks
  - The complexity of each node is higher because every node has to implement medium access mechanisms to handle hidden or exposed terminal problems and priority mechanisms to provide a certain quality of service.

Infrastructure and ad-hoc networks

- Many networks that rely on access points and infrastructure for basic services, but that also allow for direct communication between the wireless nodes.
- Ad-hoc networks might have selected nodes with the capabilities of forwarding data.
- Most of the nodes have to connect to such a special node first to transmit data if the receiver is out of their range.

Infrastructure and ad-hoc networks

- Out of three WLANs, IEEE802.11 and HiperLAN2 are infrastructure-based networks, which additionally support ad-hoc networking. Many implementations offer the basic infrastructure-based version.
- Bluetooth is a wireless ad-hoc network, which focuses precisely on spontaneous ad-hoc meetings or on the simple connection of two or more devices without requiring the setup of an infrastructure.

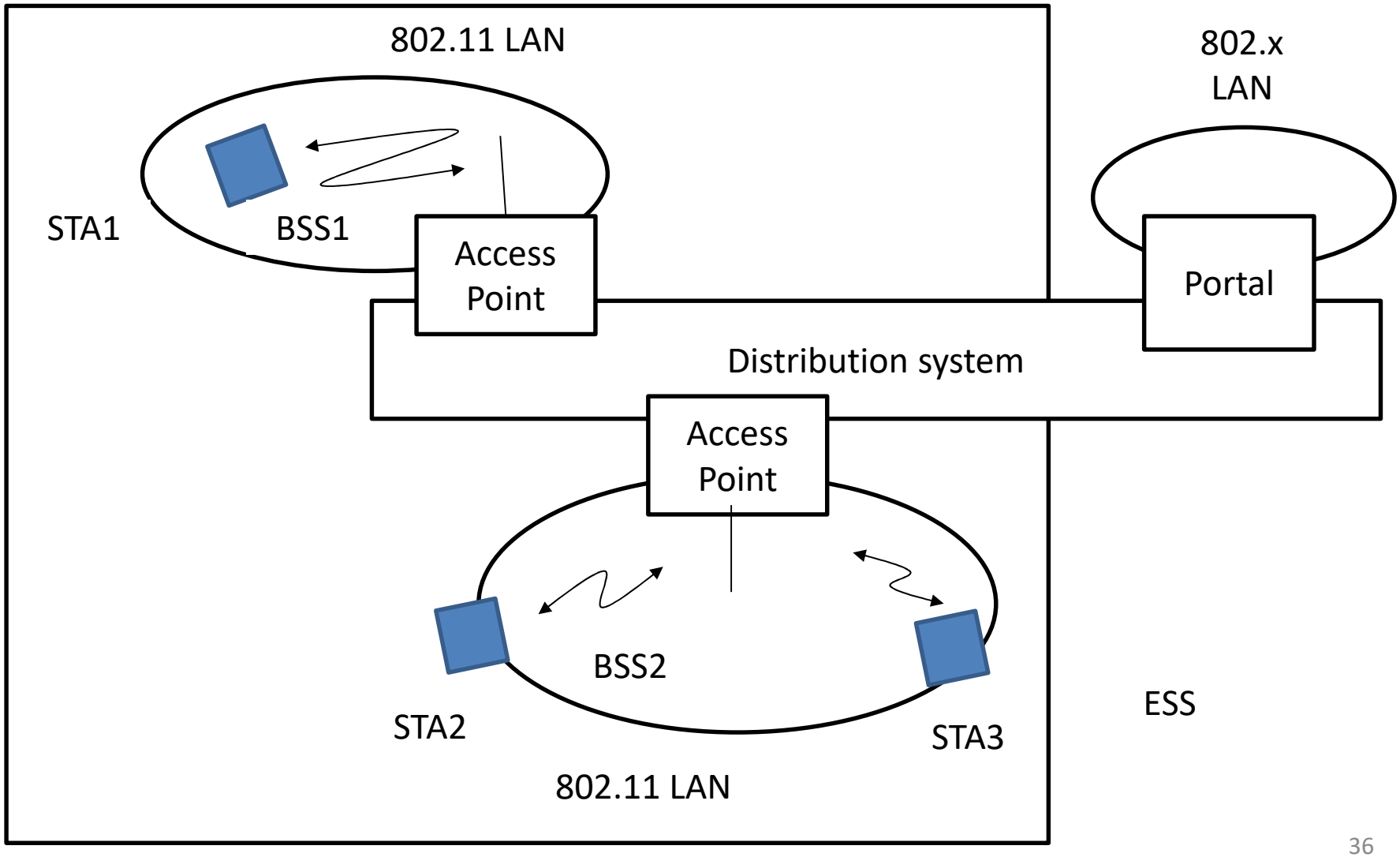
IEEE 802.11

- This IEEE standard 802.11 specifies the most famous family of WLANs.
- The standard's number indicate that standard belongs to the group of 802.x LAN standards like 802.3 Ethernet or 802.5 token ring.
- Means that the standard specifies the physical and medium access layer adapted to the special requirements of wireless LANs but offers same interface as the others to higher layers to maintain interoperability.

IEEE 802.11

- The primary goal was the specification of a simple and robust WLAN which offer time-bounded and asynchronous services.
- The MAC layer should be able to operate with multiple physical layers exhibiting a different medium sense and transmission characteristic.
- Infra red and spread spectrum radio transmission techniques were for physical layers.
- 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 was chosen for the original standard.

IEEE 802.11 – System Architecture an infrastructure-based



IEEE 802.11 – System Architecture an infrastructure-based

- Exhibit two different basic system architectures: infrastructure-based or ad-hoc.
- Figure gives the components of an infrastructure and a wireless part for IEEE802.11.
- Several nodes called stations (STA_i) are connected to access point.
- These stations are terminals with access mechanisms to the wireless medium and radio contact to the AP.

IEEE 802.11 – System Architecture an infrastructure-based

- The stations and the AP within the same radio coverage form a basic service set (BSS_i)
- According to the diagram, two BSSs 1,2 are connected via a distribution system which connects several BSSs via the AP to form a single network and thereby extends the wireless coverage area.
- Network is now called as extended service set (ESS) and has its own identifier, the ESSID.

IEEE 802.11 – System Architecture an infrastructure-based

- 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.

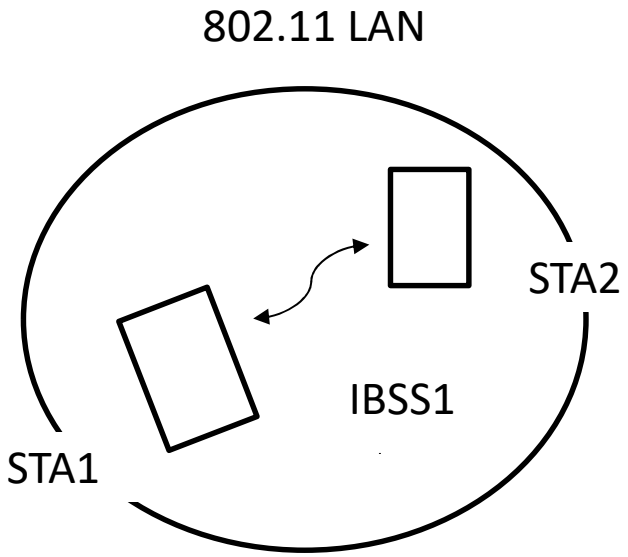
IEEE 802.11 – System Architecture an infrastructure-based

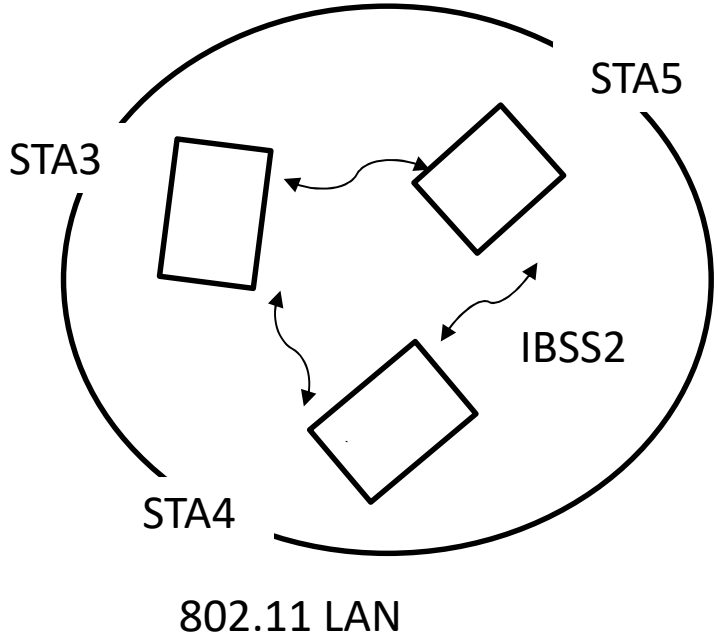
- Architecture of the distribution system is not specified further in IEEE802.11.
- It could consist of bridged IEEE LANs, wireless links, or any other networks.
- However, distribution system services are defined in the standard.

IEEE 802.11 – System Architecture an infrastructure-based

- Stations can select an AP and associate with it. APs support changing access points i.e. roaming, 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.

IEEE 802.11 – System Architecture ad-hoc





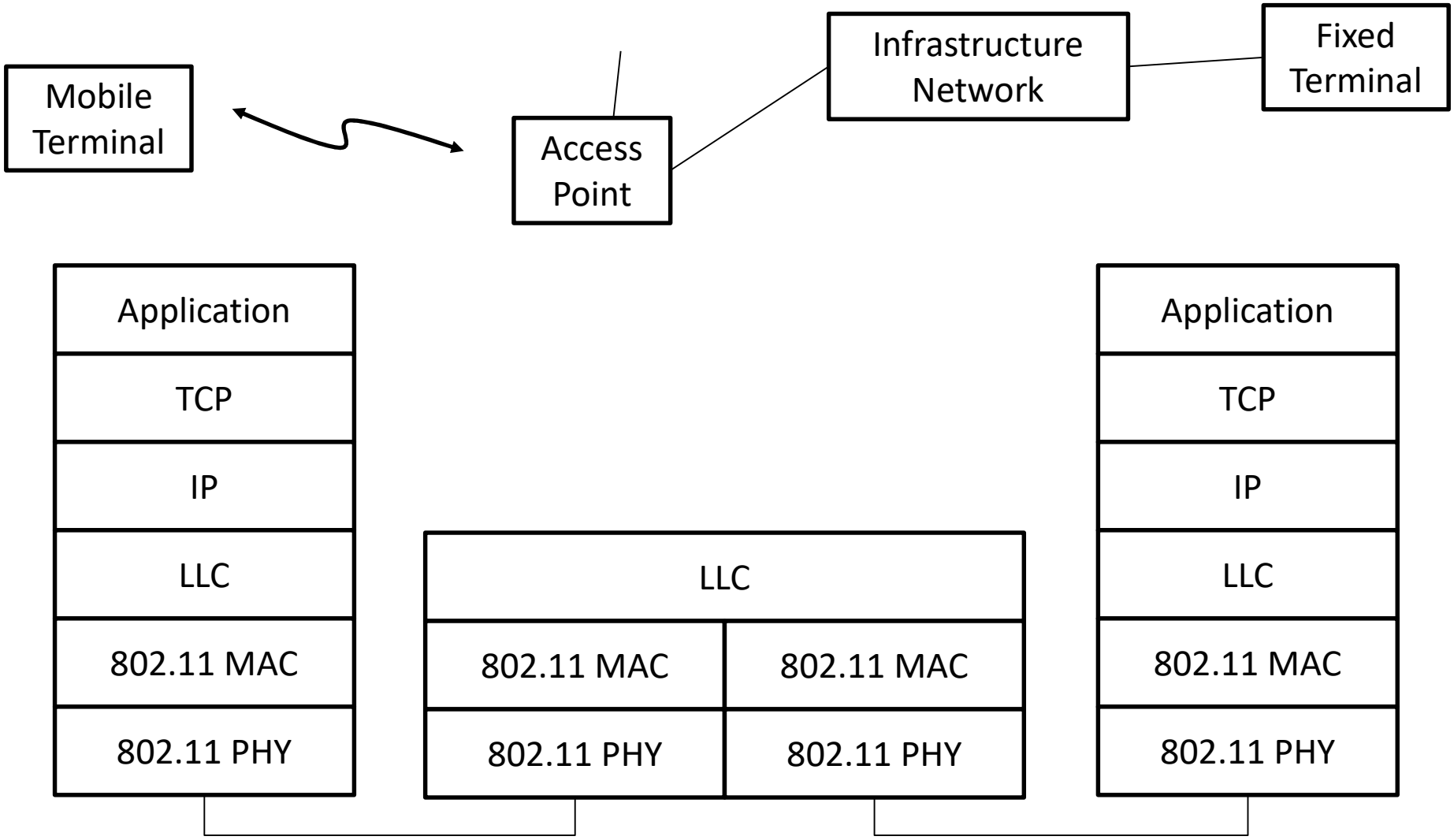
IEEE 802.11 – System Architecture ad-hoc

- IEEE 802.11 also allows building of ad-hoc networks between stations in addition to infrastructure-based networks.
- Thus forming one or more independent BSSs (IBSS)
- An IBSS consists of a group of stations using the same radio frequency.
- Stations STA1 and STA2 are in IBSS1, STA3, STA4 and STA5 are in IBSS2.
- Here, STA3 can communicate with STA4 but not with STA1.

IEEE 802.11 – System Architecture ad-hoc

- Several IBSSs can either be formed via the distance between the IBSSs or by using different carrier frequencies.
- IEEE802.11 does not specify any special nodes that support routing, forwarding of data or exchange of topology information like HIPERLAN1 or Bluetooth.

IEEE 802.11 – Protocol Architecture



IEEE 802.11 – Protocol Architecture

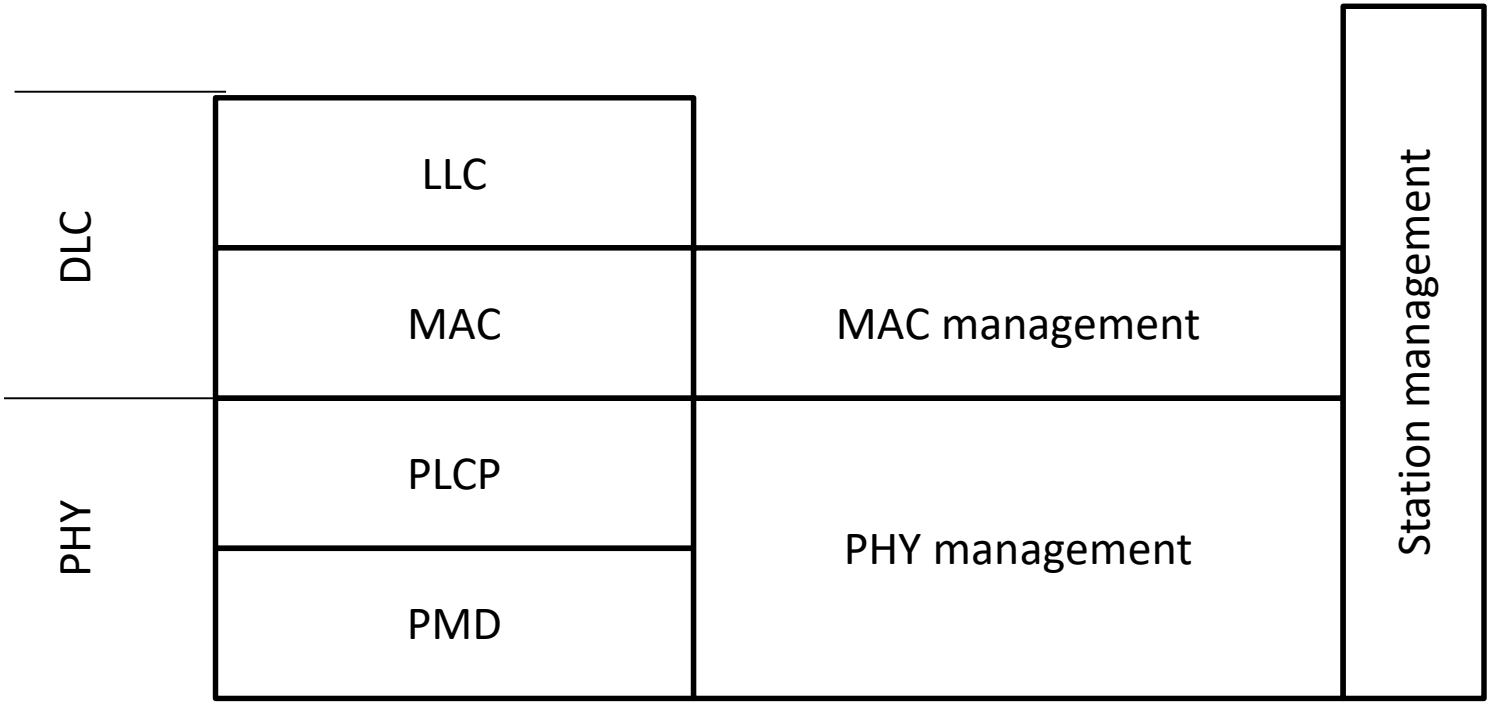
- IEEE802.11 fits seamlessly into the other 802.x standards for wired LANs.
- As shown in diagram, an IEEE 802.11 wireless LAN connected to a switched IEEE 802.3 Ethernet via a bridge.
- Applications should not notice any difference apart from the lower bandwidth and higher access time from the wireless LAN. The WLAN behaves like a slow wired LAN.
- The application, TCP and IP layers look the same for wireless nodes as for wired nodes.

IEEE 802.11 – Protocol Architecture

- The upper part of data link control layer, the logical link control covers the differences of the medium access control layers needed for the different media.
- No explicit LLC layer is visible in many of today's network.
- The IEEE 802.11 standard covers only the PHY and medium access layer MAC like other 802.x LANs.

IEEE 802.11 – Protocol Architecture

- The physical layer is subdivided into the physical layer convergence protocol (PLCP) and the physical medium dependent sublayer (PMD).



IEEE 802.11 – Protocol Architecture

- The task of the MAC layer consists of medium access, fragmentation of user data and encryption.
- 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.
- Modulation and encoding/decoding is handled by the PMD sublayer.
- Apart from the protocol sublayers, there exist management layers and the station management.

IEEE 802.11 – Protocol Architecture

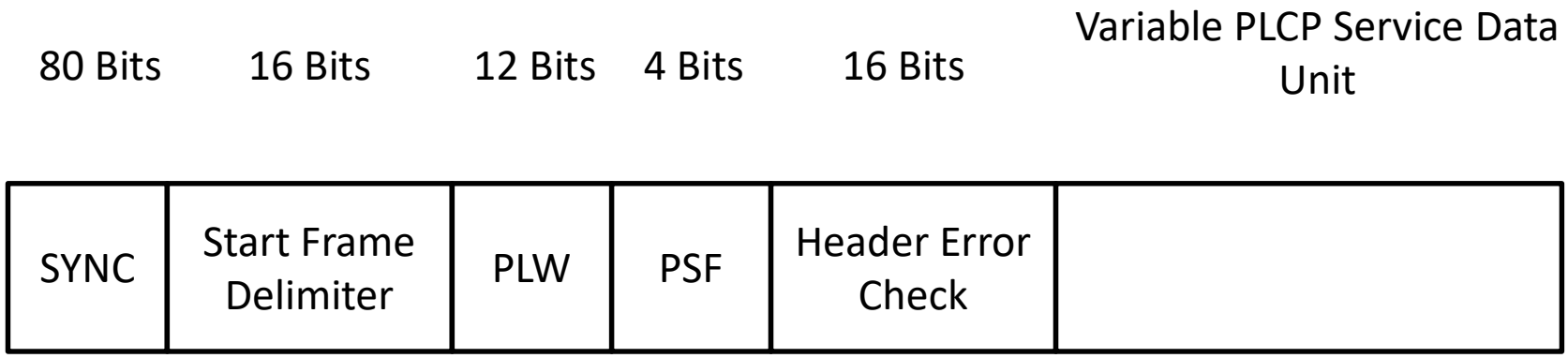
- The MAC management supports the association and re-association of a station to an access point, and power management to save battery power. Also maintains the MAC management information base (MIB).
- The PHY management handles channel tuning and PHY MIB maintenance.
- The station management interacts with both PHY and MAC management. Performs additional higher layer functions like control bridging and interaction with the distribution system in case of an AP.

IEEE 802.11 – Physical Layer

- IEEE 802.11 supports three physical layers – one based on infra red and two layers base on radio transmission- FHSS and DSSS.
- All PHY variants include the provision of the clear channel assessment signal (CCA) and is needed for the MAC mechanisms controlling medium access and indicates if the medium is currently idle.
- The transmission technology focuses on how this signal is obtained.
- A service access point (SAP) with 1 or 2 Mbit/s transfer rate to the MAC layer is offered by the PHY layer.

IEEE 802.11 – Physical Layer

- FHSS – Frequency Hopping Spread Spectrum
  - In this mode, physical layer carries the clocking information to synchronize the receiver clock with the clock of the transmitted packet.
  - Figure given below depicts the FHSS PPDU packet.



IEEE 802.11 – Physical Layer

- FHSS – Frequency Hopping Spread Spectrum
  - The fields in the FHSS PLCP are
    - SYNC – made up of alternate zeroes and ones. This bit pattern is to synchronize the clock of the receiver.
    - Start Frame Delimiter – indicates the beginning of the frame and the content of this field is fixed and is always 0000110010111101.
    - PSDU length word (PLW) – specifies the length of the PSDU in octets.

IEEE 802.11 – Physical Layer

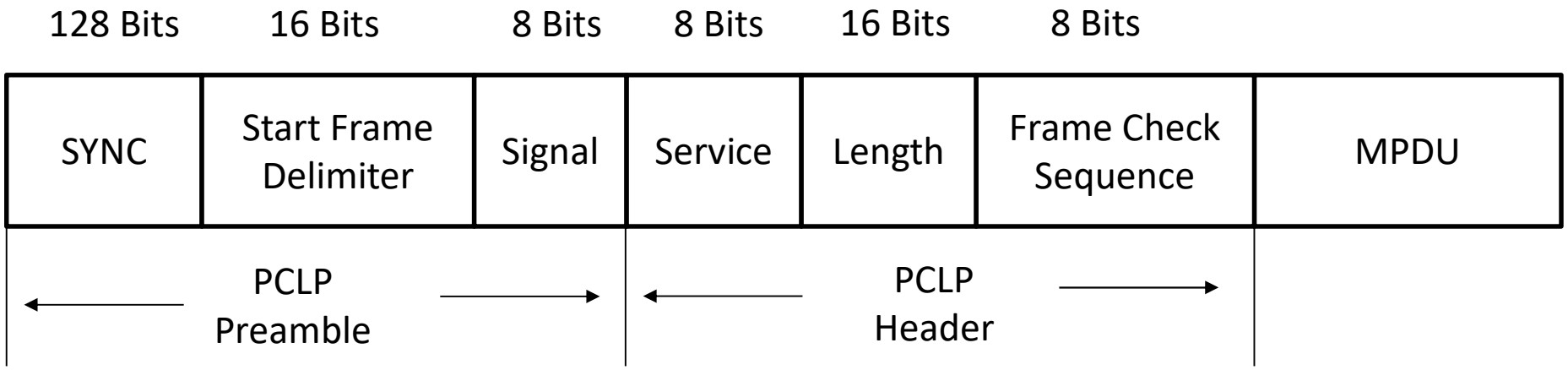
- FHSS – Frequency Hopping Spread Spectrum
  - The fields in the FHSS PLCP are
    - PLCP Signaling (PSF) – contains information about the data rate of the fields from whitened PSDU. The PLCP preamble is always transmitted at 1Mbps irrespective of the data rate of the wireless LAN. Also contains information about the speed of the link.
    - Header Error Check – contains the CRC according to CCITT CRC-16 algorithm.

IEEE 802.11 – Physical Layer

- FHSS – Frequency Hopping Spread Spectrum
  - FHSS PMD is responsible for converting the binary bit sequence into analog signal and transmit the PPDU frame into the air. FHSS PMD performs this using the frequency hopping.
  - The FHSS PMD transmits PPDU by hopping from channel to channel according to a particular pseudo-random hopping sequence.
  - Once the hopping sequence is set in the access point, stations automatically synchronize to the correct hopping sequence.

IEEE 802.11 – Physical Layer

- Direct Sequence Spread Spectrum (DSSS) Physical Layer
  - DSSS PLCP is responsible for synchronizing and receiving the data bits correctly.
  - Figure below depicts the DSSS PPDU packet.



IEEE 802.11 – Physical Layer

- Direct Sequence Spread Spectrum (DSSS) Physical Layer
  - Fields of DSSS PLCP are as follows:
    - SYNC – field is made up of alternate zeroes and ones. Bit pattern is to synchronize the clock of the receiver with the received frame.
    - Start frame delimiter – indicates the beginning of the frame and the content of the field is fixed and is always 1111001110100000.

IEEE 802.11 – Physical Layer

- Direct Sequence Spread Spectrum (DSSS) Physical Layer
  - Fields of DSSS PLCP are as follows:
    - Signal – defines the type of modulation the receiver must use to demodulate the signal. The PLCP preamble and the header are always transmitted at 1 Mbps. The bandwidth defined by this field applies to MPDU field.
    - Service – field is not used and is usually 0.
    - Length – field contains an unsigned 16-bit integer indicating the length of the frame. Unlike the FHSS, this is not in octets. It is rather in microseconds. The receiver will use this to synchronize with the clock to determine the end of frame.

IEEE 802.11 – Physical Layer

- Direct Sequence Spread Spectrum (DSSS) Physical Layer
  - Fields of DSSS PLCP are as follows:
    - Frame Check Sequence – 16-bit checksum based on CCITT CRC-16 algorithms.

IEEE 802.11 – Physical Layer

- Direct Sequence Spread Spectrum (DSSS) Physical Layer
  - DSSS PMD translates the binary digital sequence into analog radio signals and transmits the PPDU frame into the air.
  - The DSSS physical layer operates within the ISM band.

IEEE 802.11 – Physical Layer

- Infra red
  - The PHY layer which is based on infra red transmission, uses near visible light 850-950 nm.
  - Infra red light is not regulated apart from safety restrictions.
  - The standard does not require a line-of-sight between sender and receiver but should also work with diffuse light.
  - Allows for point-to-multipoint communication. The maximum range is about 10 m if no sunlight or heat sources interfere with the transmission.
  - Such a network will only work in buildings. Frequency reuse is very simple.

IEEE 802.11 – MAC Layer

- The MAC layer defines two different access methods
  - The Distributed Coordination Function
  - The Point Coordination Function

IEEE 802.11 – MAC Layer

- Basic Access Method – CSMA/CA
  - Distributed coordination function (DCF) uses Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA) as the access method.
  - Wireless LANs cannot implement CSMA/CD for three reasons:
    - For collision detection a station must be able to send data and receive collision signals at the same time. This can mean costly stations and increased bandwidth requirements.
    - Collision may not be detected because of the hidden station problem.
    - The distance between stations can be great. Signal fading could prevent a station at one end from hearing a collision at the other end.

IEEE 802.11 – MAC Layer

- Basic Access Method – CSMA/CA
  - In case of wireless LANs, a Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol is used, as it is not possible to detect a collision of data packets in mid air.

IEEE 802.11 – MAC Layer

- Basic Access Method – CSMA/CA - Mechanism
  - When a wireless station wants to communicate, it first listens to its media – radio spectrum to check if it can sense radio waves from any other wireless station.
  - If the medium is free for specified time, then the station is allowed to transmit. This time interval is called Distributed Inter Frame Space (DIFS).
  - If the current device senses carrier signal of another wireless device on the same frequency, as it wants to transmit on, it back off (does not transmit) and initiate a random timeout.

IEEE 802.11 – MAC Layer

- Basic Access Method – CSMA/CA - Mechanism
  - After the timeout has expired, the wireless station again listens to the radio spectrum and if it still senses another wireless station transmitting, it continues to initiate random timeouts until it does not detect or sense another wireless station transmitting on the same frequency.
  - When it does not sense another wireless station transmitting, the current wireless station starts transmitting its own carrier signal to communicate with the other wireless station and once synchronized, transmits data.

IEEE 802.11 – MAC Layer

- Basic Access Method – CSMA/CA - Mechanism
  - The receiving station checks the CRC of the received packet and sends an acknowledgement packet (ACK). Receipt of the acknowledgement indicates to the transmitter that no collision occurred. If the sender does not receive the acknowledgement, then it retransmits the fragment until it receives acknowledgement or is abandoned after a given number of retransmission.

IEEE 802.11 – MAC Layer

- Basic Access Method – CSMA/CA
  - It can be observed that the more times a wireless station has to back off or go into a random timeout, the less opportunity it has to transmit its data.
  - Reduced opportunity for data transmission leads to less effective access to wireless bandwidth.
  - Reduces the speed of operation.
  - In worse case scenario, after several retries, completely timeout and the wireless connection would be lost.

IEEE 802.11 – MAC Layer

- Virtual Carrier Sense
  - To reduce the probability of two stations colliding because they cannot sense each other's presence, the standard defines a Virtual Carrier Sense Mechanism.
  - In this, a station wanting to transmit a packet first transmits a short control packet called RTS, which includes the source, destination and the duration of the following transaction (the data packet and the respective ACK).
  - The destination station after receiving request packet responds with a response control packet called CTS, which includes the same duration information.

IEEE 802.11 – MAC Layer

- Virtual Carrier Sense
  - All stations that receives either the RTS and / or the CTS, set their Virtual Carrier Sense indicator called Network Allocation Vector (NAV), for the given duration and use this information together with the Physical Carrier Sense when sensing the medium.
  - Mechanism reduces the probability of a collision on the receiver side by a station that is hidden from the transmitter to the short duration of the RTS transmission because the station senses the CTS and reserves the medium as busy until the end of the transaction.

IEEE 802.11 – MAC Layer

- Virtual Carrier Sense
  - The duration information on the RTS also protects the transmitter area from collision during the ACK.
  - Due to the fact that the RTS and CTS are short frames, the mechanism also reduces the overhead of collisions, since these are recognized faster than if the whole packet was to be transmitted.

IEEE 802.11 – MAC Layer

- Fragmentation and Reassembly
  - Several reasons why it is preferable to use smaller packets in a Wireless LAN environments:
    - Due to the higher Bit Error Rate of a radio link, the probability of a packet getting corrupted increases with the packet size.
    - In case of packet corruption due to collision or noise, the smaller the packet, the less overhead it causes to retransmit it.
    - On a Frequency Hopping system, the medium is interrupted periodically for hopping, so, the smaller the packet, smaller the chance that the transmission will be postponed after dwell time.

IEEE 802.11 – MAC Layer

- Fragmentation and Reassembly
  - The wireless LAN uses standard Ethernet LAN as the backbone in majority of cases.
  - It is required that wireless LAN is able to handle Ethernet packets of 1518 bytes long and any change in the protocol for wireless LAN may cause a major change in the protocol of the higher layers.
  - Because of this, IEEE decided to solve the problem by adding a simple fragmentation / reassembly mechanism at MAC layer of the wireless LAN.

IEEE 802.11 – MAC Layer

- Fragmentation and Reassembly
  - Uses simple Send-and-Wait algorithm, where the transmitting station is not allowed to transmit a new fragment until one of the following conditions occur:
    - Receives an ACK for the said fragment or
    - Decides that the fragment was retransmitted too many times and drops the whole frame.
  - The standard does allow the station to transmit to a different address between retransmission of a given fragment.
  - Useful when an AP has several outstanding packets to different destinations and one of them does not respond.

IEEE 802.11 – MAC Layer

- Inter Frame Spaces
  - The standard defines four types of spacing intervals, are called Inter Frame Spaces (IFS).
  - IFSs are used to defer a station's access to the medium and provide various levels of priorities:
    - SIFS (Short Inter Frame Space) – shortest IFS with the highest priority. RTS, CTS uses SIFS intervals. SIFS value is a fixed value per PHY and is calculated in such a way that the transmitting station will be able to switch back to receive mode and be capable of decoding the incoming packet.
    - PIFS (Point Coordination IFS) – used by the AP (or point coordinator), to gain access to the medium before any other station. Value of PIFS is SIFS plus a Slot Time, i.e. 78 microseconds.

IEEE 802.11 – MAC Layer

- Inter Frame Spaces
  - IFSs are used to defer a station's access to the medium and provide various levels of priorities:
    - DIFS (Distributed IFS) – the Inter Frame Space used for a station willing to start a new transmission, which is calculated as PIFS plus one slot time, i.e. 128 microseconds.
    - EIFS (Extended IFS) – a longer IFS used by a station that has received a packet that it could not understand. It is required to prevent the station from colliding with a future packet belonging to the current dialog.

IEEE 802.11 – MAC Layer

- Maintaining Synchronized Stations
  - Synchronization of stations is necessary to keep hopping and other functions like power saving synchronized.
  - In BSS infrastructure, synchronization is achieved by all the stations updating their clocks according to the AP's clock.
  - The AP periodically transmits frames called Beacon frames which contain the value of the AP's clock at the moment of transmission.
  - This is the time when physical transmission actually happens, and not when the packet was put in the queue for transmission.

IEEE 802.11 – MAC Layer

- Maintaining Synchronized Stations
  - The receiving stations check the value of their clocks the moment the signal is received and correct it to be synchronized with the AP's clock which prevents clock drifting which could cause loss of synchronization after a few hours of operation.

IEEE 802.11 – MAC Layer

- Power saving
  - Enables stations to go into sleep mode without losing information.
  - The AP maintains a continually updated record of all stations currently in power saving mode.
  - AP buffers the packets addressed to these stations until either the stations specifically request the packets by sending a polling request, or until the stations change their operation mode.
  - As part of Beacon frames, the AP periodically transmits information about which power saving stations have frames buffered at the AP.
  - If there is an indication that there is a frame stored at the AP waiting for delivery, then the station stays awake and sends a polling message to the AP to receive these frames.

IEEE 802.11 – MAC Layer

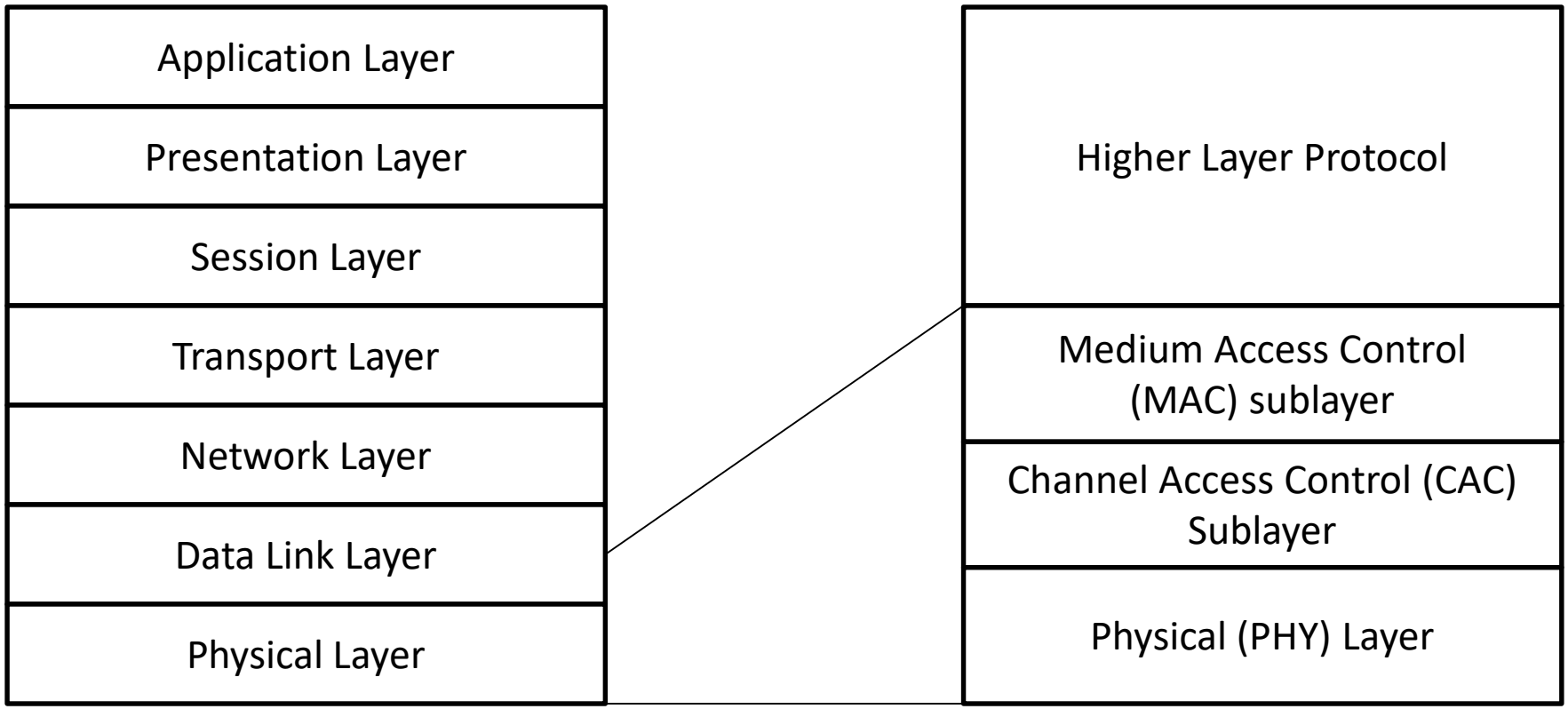
- Point coordination function (PCF)
  - An optional access method that can be implemented in an infrastructure network and not in an ad hoc network.
  - Implemented on top of the DCF and is used mostly for time sensitive transmission.
  - PCF has a centralized, contention-free polling access method.
  - The AP performs polling for stations that are capable of being polled. The stations are polled one after another, sending any data they have to the AP.

HIPERLAN

- HiperLAN is a European counterpart for the wireless local area network – stands for High PErformance Radio Local Area Network.
- HiperLAN is a family of standards developed in Europe by BRAN project of ETSI.
- Defines interoperability standards which specify a common air interface MAC and physical layers in OSI model.
- Figure shows the stack relationship of HiperLAN with OSI layers which is equivalent to wireless LAN defined by IEEE 802.11 standards.

HIPERLAN

- OSI and HiperLAN Reference Models



HIPERLAN

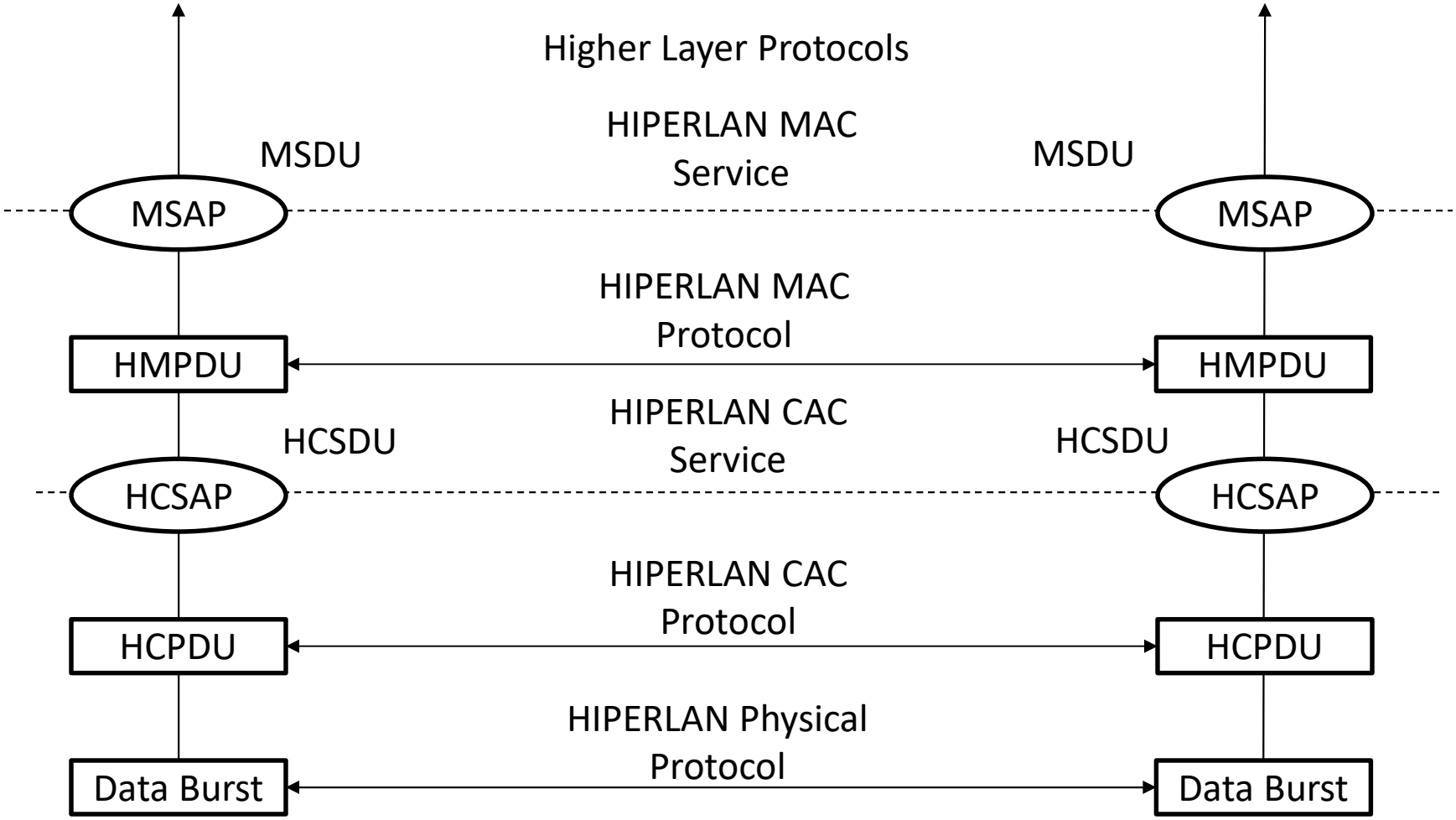
- The physical layer and the media access control part of the HiperLAN Data link layer are like 802.11 standards.
- A new sublayer called channel access and control (CAC) sublayer which deals with the access requests to the channels.
- The request is served depending upon the usage of the channel and the priority of the request.
- CAC layer provisions hierarchical independence with Elimination-Yield Non-Preemptive Multiple Access Mechanism (EY-NPMA).

HIPERLAN

- EY-NPMA codes priority choices and other functions into one variable length radio plus preceding the packet data.
- EY-NPMA helps network to function with lesser collisions even when there are a large number of users.
- Because of EY_NPMA priority mechanism, multimedia applications work better in HiperLAN.

HIPERLAN

- Communication Model



HIPERLAN

- Communication Model
  - The HiperLAN MAC service is compatible with the ISO MAC service definition
    - Defines the communication service over a single HiperLAN
    - Allows the timing requirements of the MAC Service Data Unit (MSDU) transfer to be specified
    - Allows the exploration of available HiperLANs for dynamic HiperLAN access.

HIPERLAN

- Communication Model
  - The HiperLAN CAC service defines the communication service over a single shared communication channel
    - Allows the channel access priority requirements of the HiperLAN CAC service Data Unit (HCSDU) transfer to be specified.
    - Frees the HCS-user from the concerns of the characteristics peculiar to any particular communication channel.

HIPERLAN

- Communication Model
  - The HiperLAN MAC Protocol
    - Provides the HiperLAN MAC service
    - Specifies the behavior of a HM-entity in a given HiperLAN.
    - Is compatible with the ISO MAC bridges specification.
    - Uses the HiperLAN CAC service.

HIPERLAN

- Communication Model
  - The HiperLAN CAC protocol provides the HiperLAN CAC service
    - Specifies for a particular set of one or more shared radio channels, the appropriate hierarchically independent channel access mechanism used by a HiperLAN CAC entity in a given HiperLAN
    - Uses the transmission and reception facilities specified by the HiperLAN physical layer.

HIPERLAN

- Communication Model
  - The HiperLAN physical layer protocol provides the transmission and reception facilities to the HiperLAN CAC sublayer; and specifies, for a particular set of one or more shared radio channels, the techniques of transmission, reception and channel assessment in a given channel.

HIPERLAN

- Versions
  - HiperLAN/1 and HiperLAN/2
  - HiperLAN1 started in 1991, was approved in 1996.
  - HiperLAN/2 specifications, completed in early 2000, were designed as a fast wireless connection for many kinds of networks like UMTS, ATM and IP networks.
  - HiperLAN/2 operates in the 5 GHz band and offers upto 54 Mbit/s data transfer rate.
  - The media access control (MAC protocol) in HiperLAN/2, is dynamic TDMA.
  - HiperLAN/2 offers better security measures than HiperLAN/1 as the data is secured with DES or Triple DES algorithms.

Bluetooth

- The concept behind Bluetooth wireless technology was unifying the telecom and computing industries.
- Allows users to make ad hoc wireless connections between devices like mobile phones, desktop or notebook computers without any cable.
- Devices carrying Bluetooth-enabled chips that easily transfer data at a speed of about 1 Mbps in basic mode within a 50 m (150 feet) range or beyond through walls, clothing and even luggage bags.

Bluetooth - Protocol

- The Bluetooth radio is built into small microchip and operates in a globally available frequency band ensuring interoperability worldwide.
- Uses the unlicensed 2.4 GHz ISM (Industrial Scientific and Medical) frequency band.
- There are 79 available Bluetooth channels spaced 1 MHz apart from 2.402 GHz to 2.480 GHz.
- Standard is managed and maintained by Bluetooth Special Interest Group.
- IEEE has also adapted Bluetooth as the 802.15.1a standard.

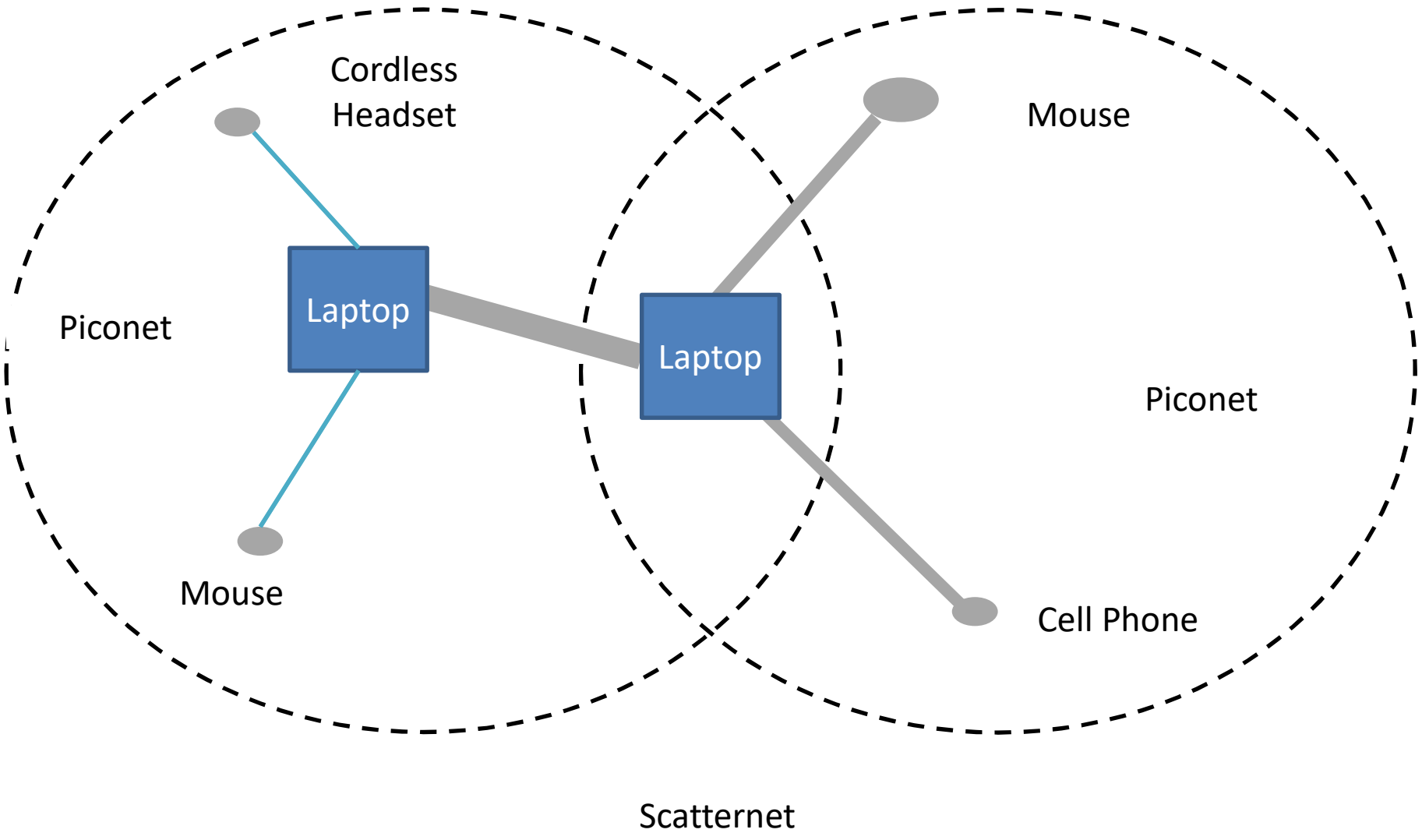
Bluetooth - Protocol

- Bluetooth allows power levels starting from 1mW covering 10 cm to 100mW covering upto 100 meters.
- Supports both unicast – point-to-point and multicast – point-to-multipoint connections.
- Uses the concept of master and slave. Together form a piconet.
- In master-slave protocol a device cannot talk as and when they desire. They need to wait till the time the master allows them to talk.

Bluetooth - Protocol

- Up to seven slave devices can be set to communicate with a master.
- Several of these piconets can be linked together to form a larger network in an ad hoc manner.
- The topology can be thought as a flexible, multiple piconet structure and network of piconets is called scatternet.
- A scatternet is formed when a device from one piconet also acts as member of another piconet.
- A device being master in one piconet can simultaneously be a slave in the other one.

Bluetooth - Protocol



Bluetooth - Protocol

- Bluetooth protocol is a combination of different protocols.
- The Bluetooth core protocol plus the Bluetooth radio protocols are required by most of the Bluetooth devices, while rest of the protocols are used by different applications as needed.
- At the physical layer Bluetooth uses spread spectrum technologies – both direct sequence and frequency hopping.
- Bluetooth uses connectionless (ACL-Asynchronous Connectionless link) and connection-oriented (SCO-synchronous connection-oriented Link) links.

Bluetooth - Protocol

- The cable replacement layer, the telephony control layer and the adopted protocol layer form application-oriented protocols that enable applications to run over the Bluetooth Core protocols.

Bluetooth – Protocol Stack

- Bluetooth protocol stack can be thought of as a combination of multiple application specific stacks.
- Different applications run over one or more vertical slices from this protocol stack.
- These are:
  - Radio Frequency COMMunication (RFCOMM)
  - Telephony Control Specification (TCS Binary)
  - Service Discovery Protocol (SDP)
- Each applications environment uses a common data link and physical layer.

Bluetooth – Protocol Stack

- RFCOMM and the TCS Binary protocols are based on the ETSI TS 07.10 and the ITU-T recommendation Q.931 respectively.
- Some applications have some relationships with other protocols to control link manager.
- Bluetooth protocol stack can be divided into four basic layers according to their functions. These are:
  - Bluetooth core protocols
  - Cable replacement protocol
  - Telephony control protocol
  - Adopted protocols

Bluetooth – Protocol Stack

- Bluetooth Core Protocols
  - Comprises Baseband, Link Manager Protocol (LMP), Logical Link Control and Adaptation Protocol (L2CAP), and Service Discovery Protocol (SDP).

Bluetooth – Protocol Stack

- Bluetooth Core Protocols – Baseband
  - The baseband and Link Control layer enables the physical RF link between Bluetooth units forming a piconet.
  - Layer uses inquiry and paging procedures to synchronize the transmission with different Bluetooth devices.
  - Using SCO and ACL link different packets can be multiplexed over the same RF link.
  - ACL packets are used for data, while the SCO packet can contain audio or combination of both audio and data.
  - All audio and data packets can be provided with different levels of CRC or FEC for error detection and correction.

Bluetooth – Protocol Stack

- Bluetooth Core Protocols – Link Management protocol (LMP)
  - When two Bluetooth devices come within each other's radio range, link managers of either device discover each other.
  - LMP engages itself in peer-to-peer message exchange which perform various security functions starting from authentication to encryption.
  - LMP layer performs the link setup and negotiation of baseband packet size.
  - LMP also controls the power modes, connection state and duty cycles of Bluetooth devices in a piconet.

Bluetooth – Protocol Stack

- Bluetooth Core Protocols – Logical Link Control and Adaptation Protocol (L2CAP)
  - Responsible for segmentation of large packets and the reassembly of fragmented packets. L2CAP is also responsible for multiplexing of Bluetooth packets from different applications.

Bluetooth – Protocol Stack

- Bluetooth Core Protocols – Service Discovery Protocol
  - Enables a Bluetooth device to join a piconet. Using SDP a device inquires what services are available in a piconet and how to access them.
  - SDP uses client-server model where the server has a list of services defined through service records. One service record in a server describes the characteristics of one service.
  - In a Bluetooth device there can be only one SDP server. If devices provides multiple service, one SDP server acts on behalf of all of them.
  - Multiple applications in a device may use a single SDP client to query servers for service records.

Bluetooth – Protocol Stack

- Bluetooth Core Protocols – Service Discovery Protocol
  - A Bluetooth device in an inquiry mode broadcasts ID packets on 32 frequency channels of the Inquiry Hopping sequence.
  - It sends two IDs packets every 625 µs and listens for responses the following 625 µs.
  - At this stage the unique identity of the devices called Bluetooth globalID is exchanged.
  - A globalID indicates a device's profile along with capability functions.

Bluetooth – Protocol Stack

- Bluetooth Core Protocols – Service Discovery Protocol
  - Upon matching of the device profile a connection is set up and devices exchange data.
  - When connection is setup, the paging device becomes the master and the paged device becomes the slave.
  - A Bluetooth device may operate both as a server and as a client at the same time forming a scatternet. They can also switch from master to slave and vice versa.

Bluetooth – Protocol Stack

- Cable replacement protocol
  - Protocol has only one member, Radio Frequency Communication (RFCOMM)

Bluetooth – Protocol Stack

- Cable replacement protocol - RFCOMM
  - It is a serial line communication protocol and is based on ETSI 07.10 specification.
  - The cable replacement protocol emulates RS-232 control and data signals over Bluetooth baseband protocol.

Bluetooth – Protocol Stack

- Telephony Control Protocol
  - Comprises two protocol stacks – Telephony Control Specification Binary (TCS BIN) and the AT-Commands.

Bluetooth – Protocol Stack

- Telephony Control Protocol – Telephony Control Protocol Binary
  - TCS Binary or TCS BIN is a bit-oriented protocol. Defines the call control signaling protocol for set up of speech and data calls between Bluetooth devices.
  - Also defines mobility management procedures for handling groups of Bluetooth TCS devices.
  - TCS binary is based on the ITU-T Recommendation Q.931.

Bluetooth – Protocol Stack

- Telephony Control Protocol – AT-Commands
  - Protocol defines a set of AT-Commands by which a mobile phone can be used and controlled as a mode, for FAX and data transfers.
  - AT – short form of attention commands are used for from a computer or DTE – data terminal equipment to control a modem or DCE.
  - AT-commands in Bluetooth are based on ITU-T recommendation V.250 and GSM 07.07.

Bluetooth – Protocol Stack

- Adopted Protocols
  - Has many protocol stacks like point-to-point protocol, TCP/IP protocol, OBEX (Object Exchange Protocol), Wireless application protocol (WAP), vCard, vCalendar, Infrared Mobile Communication (IrMC) etc.

Bluetooth – Protocol Stack

- Adopted Protocols – PPP Bluetooth
  - Offers PPP over RFCOMM to accomplish point-to-point connections.
  - Point-to-Point protocol is the means of taking IP packets to/from the PPP layer and placing them onto the LAN.

Bluetooth – Protocol Stack

- Adopted Protocols – TCP/IP
  - Protocol is used for communication across the Internet.
  - TCP/IP stacks are used in various devices including printers, handheld computers and mobile handsets.
  - Access to these protocols is operating system independent, although traditionally realized using a socket programming interface model.
  - TCP/IP/PPP is used for the all Internet Bridge usage scenarios.
  - UDP/IP/PPP is also available as transport for WAP.

Bluetooth – Protocol Stack

- Adopted Protocols – OBEX Protocol
  - It is a session protocol developed by the Infrared Data Association (IrDA) to exchange objects.
  - Provides the functionality of HTTP in a much lighter fashion.
  - Protocol defines a folderlisting object, which can be used to browse the contents of folders on remote devices.

Bluetooth – Protocol Stack

- Adopted Protocols – Content Formats
  - vCard and vCalendar specifications define the format of an electronic business card and personal calendar entries developed by the Versit consortium, these are now maintained by the Internet Mail Consortium.
  - Other content formats supported by OBEX are vMessage and vNote which are used to exchange messages and notes. They are defined in the IrMC (IrDA Mobile Communication) specification.
  - IrMC also defines a format for synchronization of data between devices.

Bluetooth Security

- In wireless environment security concerns are high.
- Bluetooth offers security infrastructure starting from authentication, key exchange, to encryption.
- In addition to encryption, a frequency hopping scheme with 1600 hops/se is employed.
- At the lowest levels of the protocol stack, Bluetooth uses the publicly available cipher algorithm known as SAFER+ to authenticate device's identity.
- In addition to this, different application verticals use their own security infrastructure at the application layer.

Bluetooth Application Models

- File transfer – in this usage model offers the ability to transfer data objects from one device to another. Object type includes files, audio, image files, folders or directories or streaming media formats. Model also offers a possibility to browse the contents of the folders on a remote device.
- Internet Bridge – in this usage model, a mobile phone or cordless modem acts as modem to the PC, providing dial-up networking and fax capabilities without need for physical connection to the PC.

Bluetooth Application Models

- Lan Access – in this usage model multiple data terminals use a LAN access point (LAP) as a wireless connection to an Ethernet LAN. Once connected, the terminals operate as if they were connected directly to the LAN.
- Synchronization – this model provides a device-to-device synchronization of data.
- Headset – the headset can be wirelessly connected for the purpose of acting as a remote device's audio input and output interface. Very convenient for hands-free cellular phone usage in automobiles.

References

- Jochen Schiller, Mobile Communications (Second Edition), Pearson Education
- Asoke K. Talukder, Hasan Ahmed, Roopa R. Yavagal, Mobile Computing Technology, Applications and Service Creation, Second Edition, McGraw Hill Education (India) Private Limited
- Behrouz A. Forouzan, Data communications and networking (Fourth Edition), Tata McGraw-Hill Publishing Company Limited.