HOME ASSIGNMENT:

1(a) Explain the advantages and Disadvantages of Wireless LAN's?

Advantages:

1. Flexibility: Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere.

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

3. Design: Wireless networks allow for 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 etc.

4. Robustness: Wireless networks can survive disasters eg: earthquakes or users pulling a plug. If the wireless devices survive, people can still communicate.

5. Cost: After providing wireless access to the infrastructure via an access point for the first user, adding additional users to a wireless network could not increase the cost.

Disadvantages:

1. Quality of service: WLAN's typically offer lower quality than their wired counterparts. The main reasons for this

are the lower bandwidth due to limitations in radio transmission, higher error rates due to interference et

2. Proprietary solutions: due to slow standardization proced many companies have come up with proprietary solutio offering standardized functionality plus many enhanc features.

3. Restrictions: All wireless products have to comply w national regulations. several government and non-governmen institutions worldwide regulate the operation and restrict frequencies to minimize interference.

4. Global operation: WLAN products should sell in all countries so, national and international frequency regulations have to considered.

5. 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.

1(b) compare Infrared and Radio transmissions used for IEEE 802.11

Infrared	Radio transmission.
1. users IR (infrared) diodes, diffuse light, multiple reflections (wall, furniture etc)	1. Typically using the license free ISM (industrial scientific, medical) band at 2.4 GHz

2. Advantages:

→ simple, cheap, available in many mobile devices.
→ no license needed
→ simple shielding possible.

3. Disadvantages:

→ interference by sunlight, heat sources etc
→ many things shield or absorb IR light
→ low bandwidth.

4. Example:

IrDA (Infrared Data Association) interface available everywhere

2. Advantages:

→ Experience from wireless LAN and mobile phones can be used.
→ coverage of larger area possible (radio can penetrate walls, furniture)

3. Disadvantages:

→ limited license free frequency bands
→ shielding more difficult, interference with other electrical devices.

4. Example:

WaveLAN (Lucent), HIPERLAN, Bluetooth.

2 (a) Draw the IEEE 802.11 MAC packet structure and explain each field?

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 32769, the duration field contains the value indicating the period of time in which the medium is occupied.

Address 1 to 4: The 4 addresses field contain standard IEEE 802. MAC addresses as they are known from other 802.x LANs.

Sequence control: Due to retransmission mechanism, frames may be duplicated. Therefore a sequence number is used to filter duplicates.

Data: The MAC frame may contain arbitrary data, which is transferred transparently from a sender to the receiver.

Checksum: Finally, a 32 bit checksum is used to protect the frame. It is common practice in all 802.x networks.

The frame control field is shown below contains the following fields for receivers to eliminate duplicate frames.

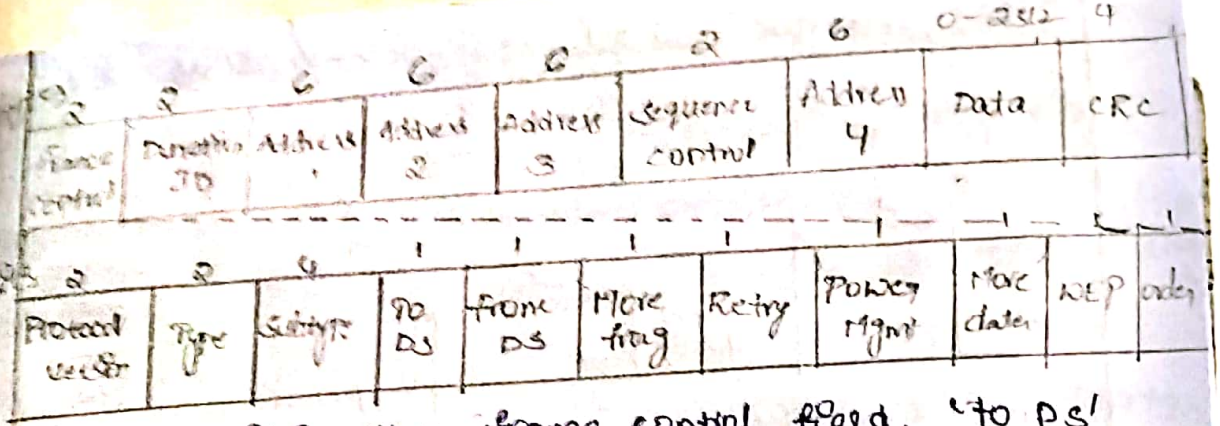
Power management: This field indicates the mode of a station after successful transmission of a frame set to 1 the field indicates that the station goes into power save mode. If the field is set to 0, the station stays active.

More data: In general, this field is used to indicate a receiver that a sender has more data to send than the current frame.

Wired Equivalent Privacy (WEP): This field indicates that the standard security mechanism of 802.11 is applied.

Order: If this bit is set to 1 the received frames must be processed in strict order.

→ MAC frames can be transmitted between mobile stations and an access point and between access point over a DS.



Two bits within the frame control field, 'to DS' and 'from DS' differentiate these cases and control the meaning of four addresses used.

→ Every station, access point or wireless node, filters on address 1

→ The second address address 2, represents the physical transmitter of a frame.

→ The remaining two addresses, address 3 address 4 are mainly necessary for the logical assignment of frames.

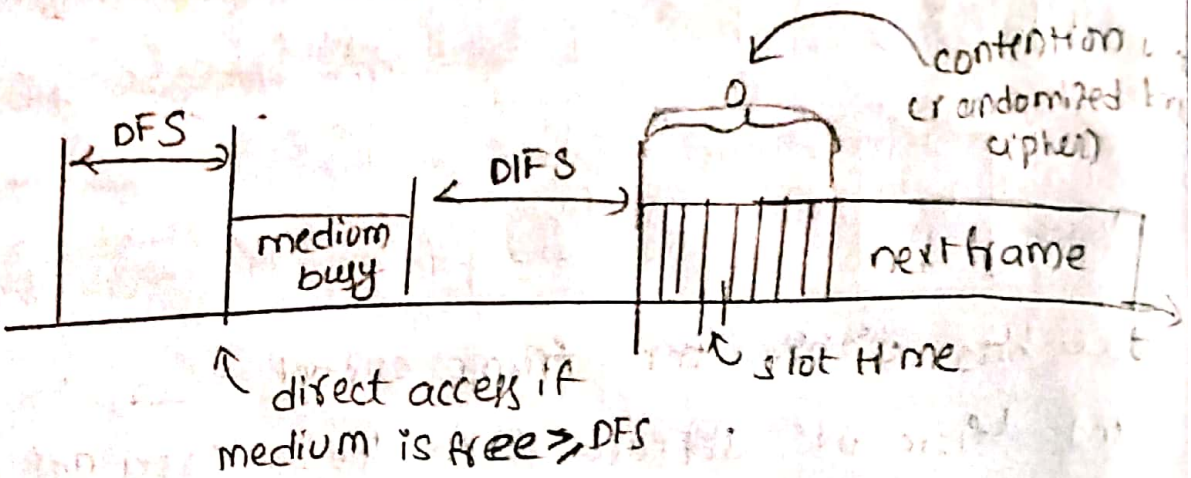
2(b) Explain DFWMAC-DCF Scheme of IEEE 802.11 with neat sketches?

Basic DFWMAC-DCF using CSMA/CA:

- The mandatory access mechanism of IEEE 802.11 is based on carrier sense multiple access with collision avoidance (CSMA/CA), which is random access scheme with carrier sense & collision avoidance through random backoff.

→ If the medium is idle for atleast the duration of DIFS, a node can access the medium at once.

- This allows for short access delay under light load.



contention window & waiting time:

→ If the medium is busy, nodes have to wait for the duration of DIFS, entering a contention window afterwards.

→ Each node now chooses a random backoff time within a contention window and delays medium access for this random amount of time.

→ The node continues to sense the medium.

→ As soon as a node senses the channel is busy, it has lost cycle and has to wait for the next chance i.e until the medium is idle again, for atleast DIFS.

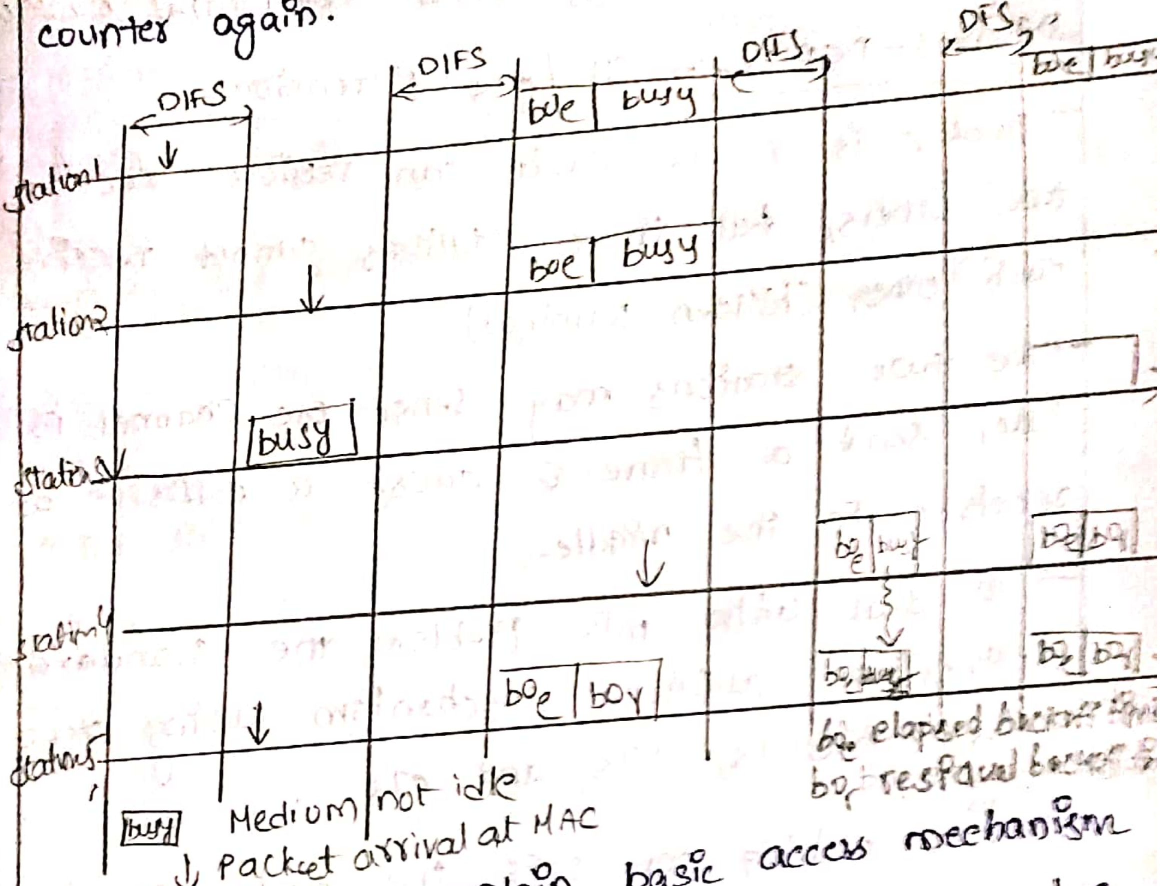
→ obviously, the basic CSMA/CA mechanism is not fair.

→ Independent of overall time a node has already waited for transmission, each node has the same chances for transmitting data in the next cycle.

→ To provide fairness, IEEE 802.11 adds a backoff timer.

→ Again, each node selects a random waiting time within range of contention window.

→ If certain station does not get access to medium in 1st cycle, it stops its backoff timer, wait for channel to be idle again for DIFS & starts counter again.



→ Above diagram explain basic access mechanism of IEEE 802.11 for 5 stations trying to send a packet at market points in time.

→ Station 3 has the 1st request from a higher layer to send a packet.

→ Station 1,2,5 have to wait atleast until the medium is idle for DIFS again after station 3 has stopped sending.

→ The contention window starts with a size of eg;

$CW_{min} = 7$

Each time a collision occur, indicating a higher load on medium, the CW doubles up to a Maximum

→ The larger the contention window is, the greater is the resolution power of randomsized scheme.

• This algorithm is also called exponential backoff.

DFWMAC-DCF with RTS/CTS Extension:

→ Problem is if one station can ~~retrieve~~ receive two others, but those stations cannot receive each other (hidden terminal)

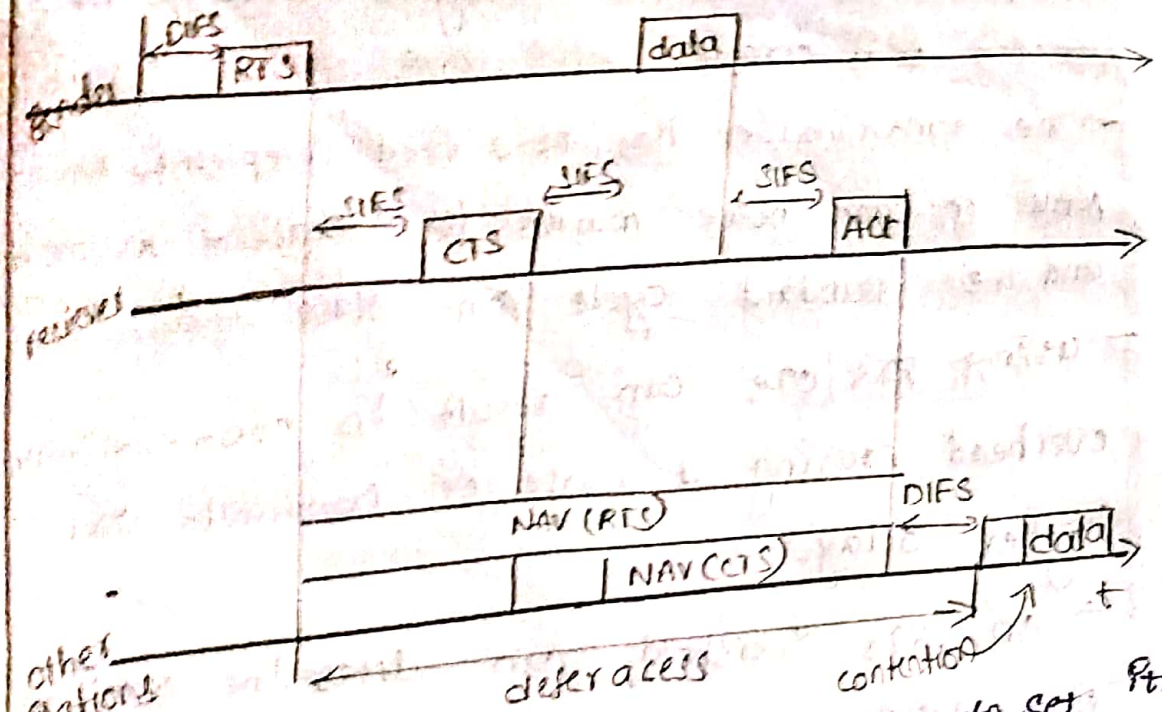
→ The two stations may sense the channel is idle, send a frame & cause a collision at receiver in the middle.

→ To deal with this problem, the standard defines an additional mechanism using two control packets, RTS and CTS.

→ After waiting for DIFS, the sender can issue a request to send (RTS) control packet.

→ The RTS packet thus is not given any higher priority compared to other data packets.

→ The RTS packet includes the receiver of data transmission to come & the duration of whole data transmission.



→ Every node receiving this RTS now has to set its net allocation vector (NAV) in accordance with duration field.

→ The NAV then specifies the earliest point at which the station can try to access the medium again.

→ If the receiver of the data transmission receives the RTS, it answers with a clear to send (CTS) message after waiting for SIFS.

→ The CTS packet contains the duration field again and all stations receiving this packet from receiver of intended data transmission have to adjust their NAV.

→ Basically this mechanism reserves the medium for one sender exclusively.

→ Finally the sender can send the data after SIFS. The receiver waits for SIFS after receiving the

data packet & then acknowledges whether the transfer was correct.

→ The transmission has now been completed, the NAV in each node marks the medium as free and the standard cycle can start again.

→ using RTS/CTS can result in non-negligible overhead causing a waste of bandwidth and higher delay.

→ An RTS threshold can determine when to use the additional mechanism & when to disable it.

→ Wireless LANs have bit error rates in transmission that are typically several orders of magnitude higher than eg fiber optics.

→ one way to reduce the error probability of frames is to use shorter frames.

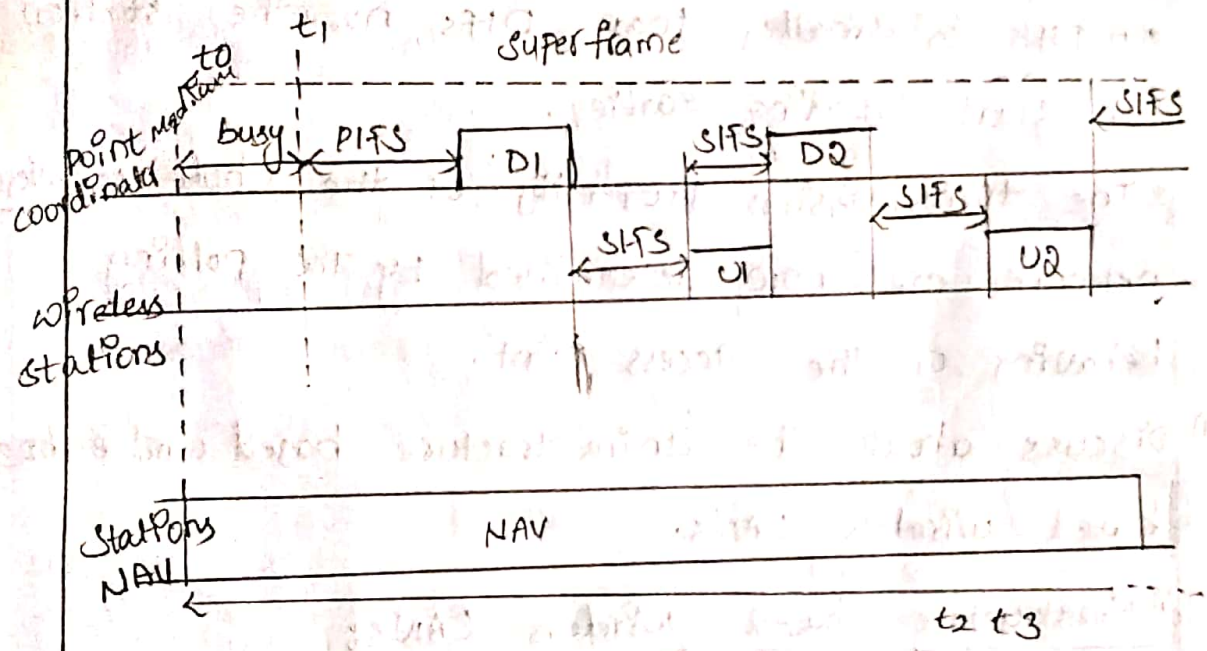
→ The IEEE 802.11 standard specifies a fragmentation mode.

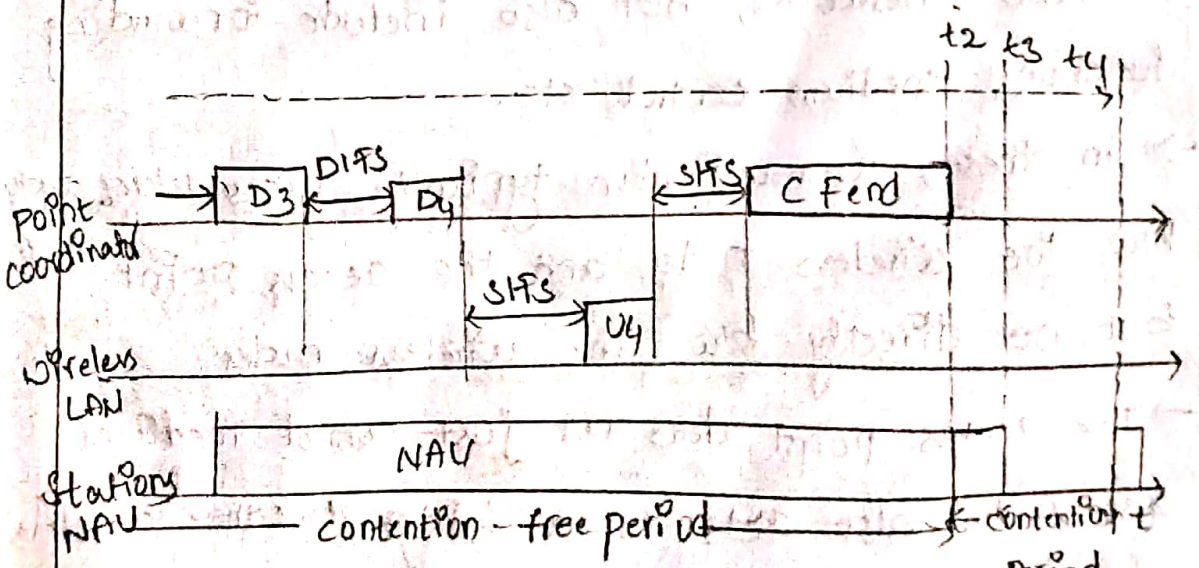
Dynamic-pcf with polling:

• The two access mechanisms presented so far cannot guarantee a maximum access delay or minimum transmission bandwidth.

• To provide a time-bounded service, the standard specifies a point coordination function (PCF) on top of the Dcf mechanisms.

- using PCF requires an access point that controls medium access and poll the single nodes.
- The point coordinator in the access point splits the access time into super frame periods.
- A super frame comprises a contention free period and a contention period.
- The contention period can be used for two access mechanisms presented above.





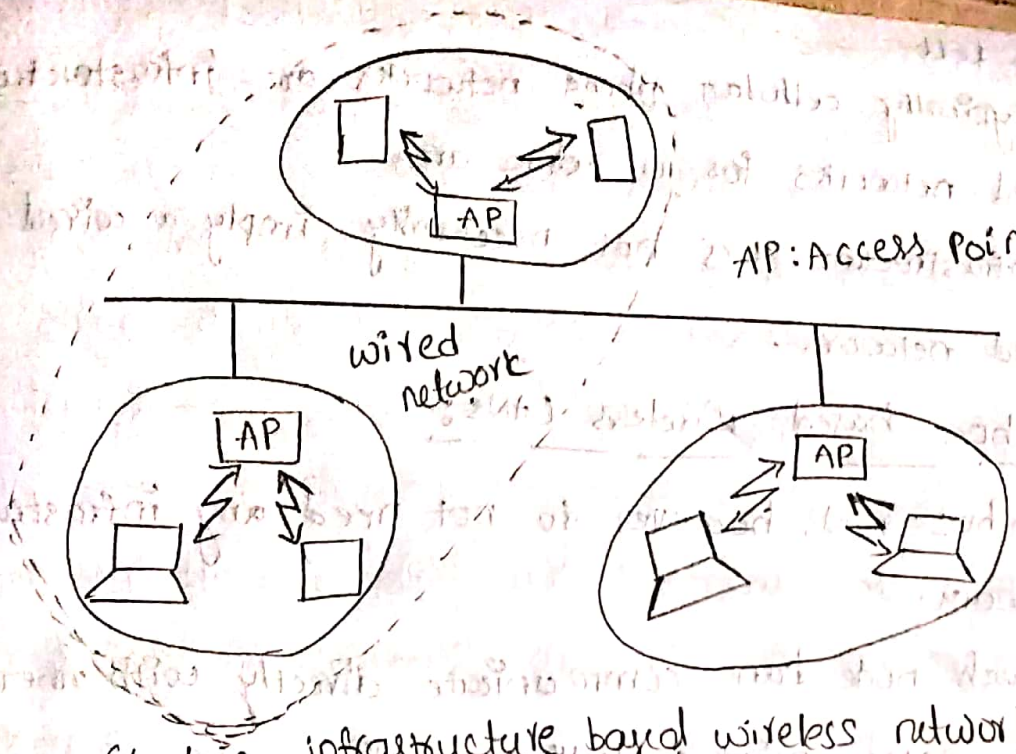
contention-free access using polling mechanisms (PCF)

• At time to the contention-free period of super frame should theoritically start, but another station is still transmitting data.
• This means that PCF also defers to DCF and the start of super frame may be postponed.
• After the medium has been idle until the point coordinator has to wait for PIFS before accessing medium.
• A PIFS is smaller than DIFS, no other station can start sending earlier.
• The transmission properties of the whole wireless network are now determined by the polling behavior of the access point.

3(a) Discuss about the Infrastructure based and Ad-hoc based wireless LANs.

Infrastructure based Wireless LANs:

→ Infrastructure networks not only provide access to other networks, but also include forwarding functions medium control etc.
→ In these, communication typically takes place only blw the wireless nodes and the access point but not directly blw the wireless nodes.
→ The access point does not just control medium access, but also acts as a bridge to other wireless or wired networks.



Ex of 3 infrastructure based wireless networks

→ Typically, the design of infrastructure based wireless networks is simpler because most of the network functionality lies within the access point, whereas the wireless client can remain quite simple.

→ The structure is reminiscent of switched Ethernet or other star based networks, where a central-element controls network flow.

→ The type of network can use different access schemes with or without collision.

→ collisions may occur if medium access of wireless nodes & the access point is not coordinated.

→ However if only the access point controls medium access, no collisions are possible.

→ Infrastructure-based networks lose some of flexibility wireless networks can offer, e.g they cannot be used for disaster relief incases where no infrastructure

is left.

→ Typically cellular phone networks are infrastructure based networks for a wide area.

→ Infrastructure does not necessarily imply a wired fixed network.

Ad-hoc based Wireless LANs:

→ Ad-hoc WN, 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

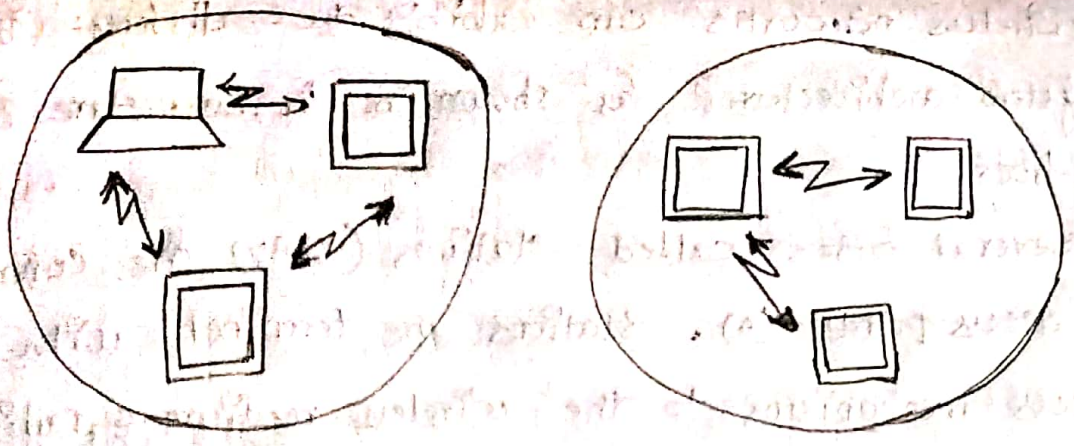
→ Nodes within and ad-hoc network can only communicate if they can reach other physically i.e if they are within each other's radio range or if other nodes can forward the message.

→ 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 terminals problem.

→ This type of WN exhibits the greatest possible flexibility for ex: needed for unexpected meetings

→ clearly the two basic variants of WN infrastructure & ad-hoc, do not always come in their pure form

→ Ad-hoc networks might only have selected nodes with capability of forwading data.

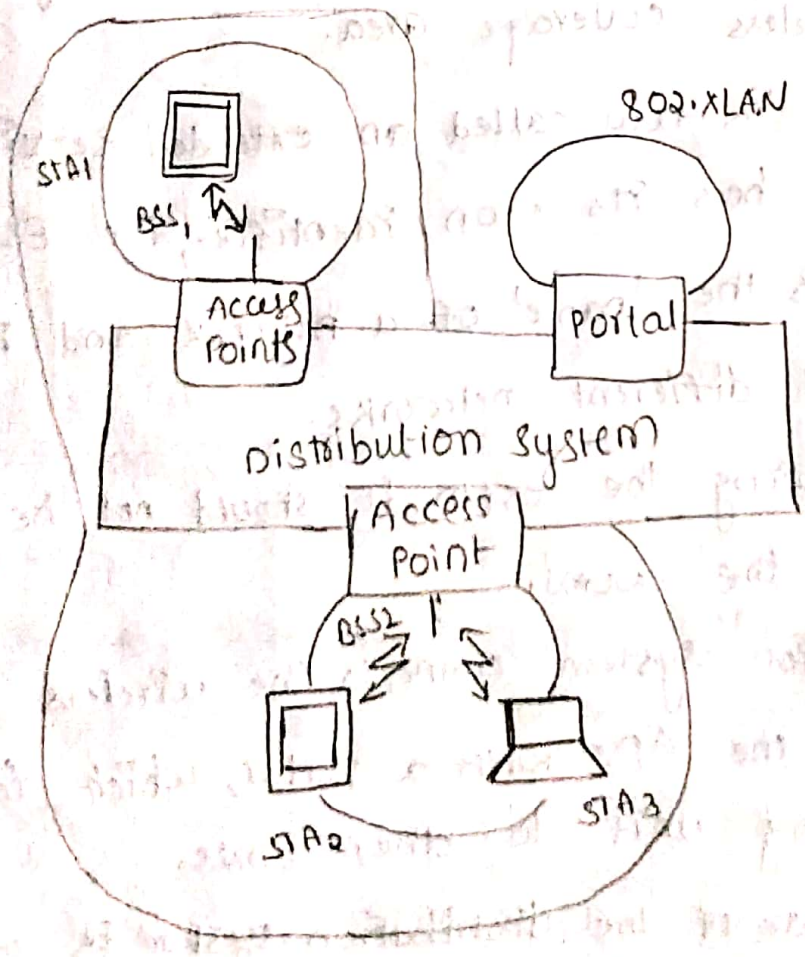


Examples of two & hoc-wireless networks.

→ Most of the nodes have to connect to such a special node first to transmit data if the receiver is out of their range.

→ Bluetooth is typical wireless adhoc network.

3(b) Discuss about the architecture of infrastructure based and adhoc IEEE 802.11 wireless LANs.



Architecture of an infrastructure-based IEEE802.11

→ Wireless networks can exhibit two different basic system architectures as shown in: infrastructure or ad-hoc.

→ several nodes, called stations (STAs) are connected to access points (A). Stations are terminals with access mechanisms to the wireless medium & radio contact to AP.

→ The stations and the AP which are within the same radio coverage from a basic service set (BSSP)

→ The example shows two BSS_1 – BSS, and BSS_2 – Ohs are connected via a distribution system.

→ A distribution system connects several BSSs via the AD 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 seperate different networks.

→ Without knowing the ESSID it should not be participate in the WLAN.

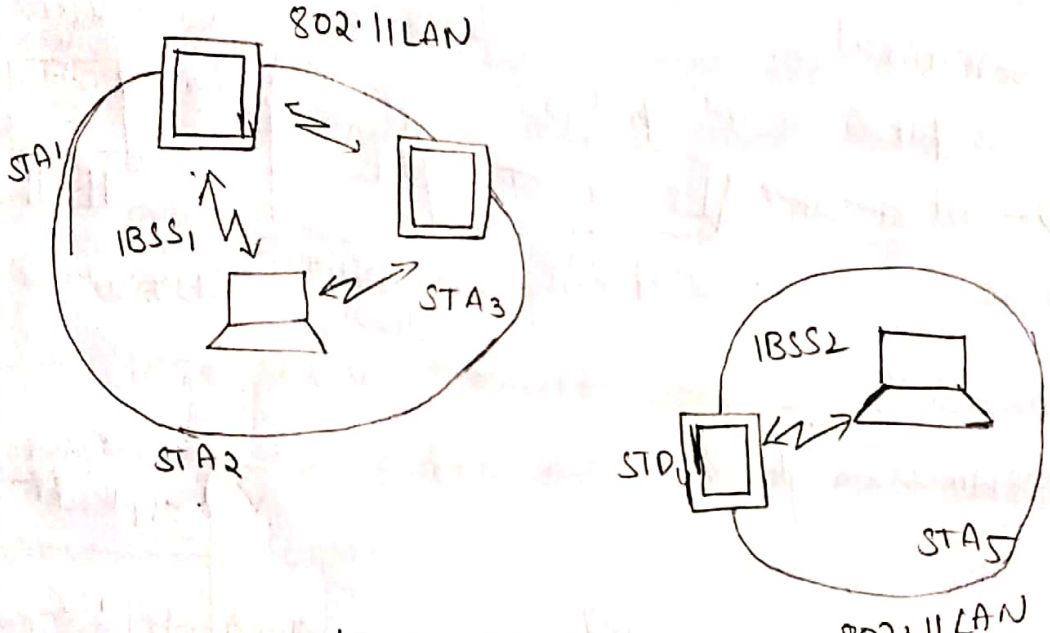
→ The distribution system connects the wireless networks via the APs with a portal, which forms the interworking unit to other LANs.

→ The architecture of the distribution system is not specified further in IEEE 802.11

→ However distribution system services are defined in the standard IEEE 802.11 f to specify an inter access point protocol.

→ Stations can select an AP and associate with it. The APs support roaming the distribution system handles data transfer blw the different APs.

→ APs provide synchronization within a BSS, support power management, & can control medium access to support time-bounded service.



Architecture of IEEE 802.11 ad-hoc wireless LANs

→ In addition to infrastructure-based networks, IEEE 802.11 allows the building of ad-hoc networks between stations, thus forming one or more independent BSSs as shown in above figure.

→ In this case, an IBSS comprises a group of stations using the same radio frequency.

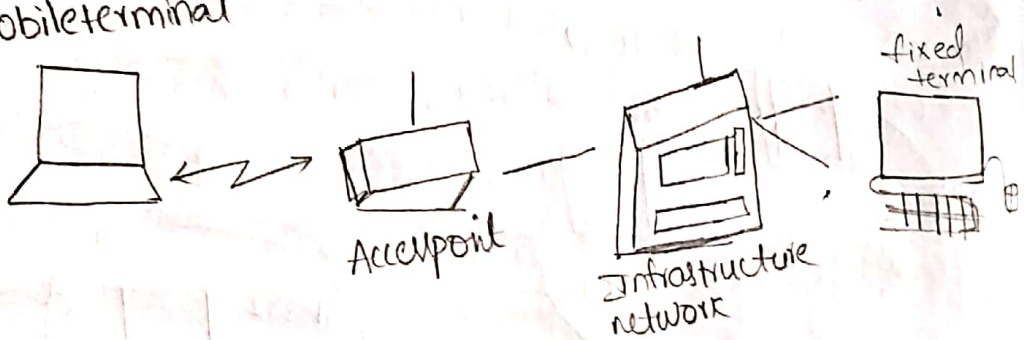
→ Stations STA1, STA2 and STA3 are in IBSS1, STA4 and STA5 in IBBS2.

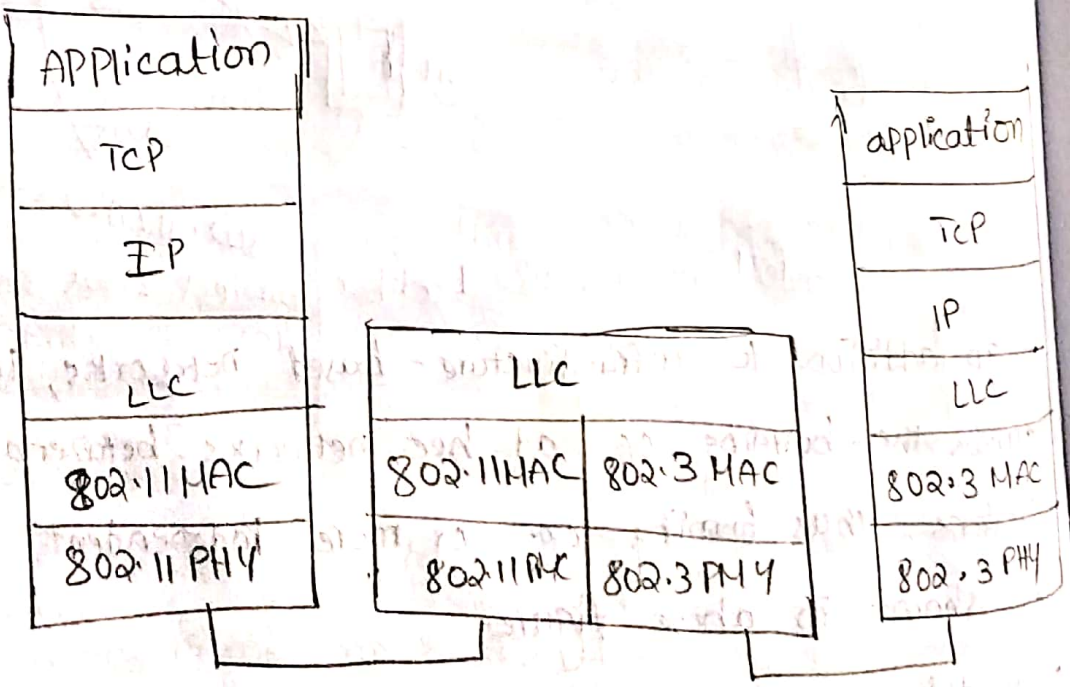
→ This means for example that STA_3 can communicate directly with STA_1 but not with STA_5.

→ Several IBSSs can either be formed via the distance b/w the IBSSs or by using different carrier frequencies.

→ IEEE 802.11 does not specify any special nodes that support routing, forwarding of data or exchange of topology information as e.g.; HiperLAN1, Bluetooth.

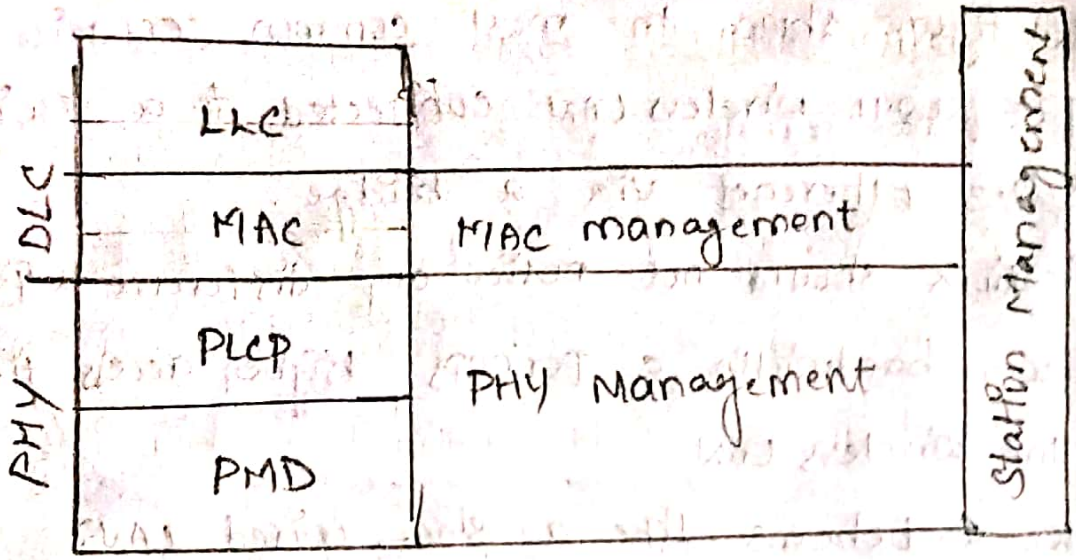
4. Discuss about IEEE 802.11 protocol architecture?





→ As indicated by the standard number, IEEE 802.11 fits seamlessly into other 802.x standards for wired LANs.

→ Above figure shows the most common scenario:
- 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 lower bandwidth & perhaps higher access time from the wireless LAN.
→ The WLAN behaves like a slow wired LAN.
- consequently, the higher layer (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 MAC layers needed for the different media.
→ In many of today's network, no explicit LLC layer is visible.
- 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 PHY is sub divided into physical layer convergence protocol (PLCP) and the physical medium dependent sublayer PMD.
- The basic tasks of MAC layer comprise medium access, fragmentation of user data & 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 transmission technology.



→ Apart from the protocol sublayers the standard specifies management layers & station management.

→ The MAC management supports the association & Re-association of a station to an access point & roaming blw different access points.

→ It also controls authentication mechanisms, encryption, power management to save battery power.

→ MAC management also maintains the MAC management information base (MIB)

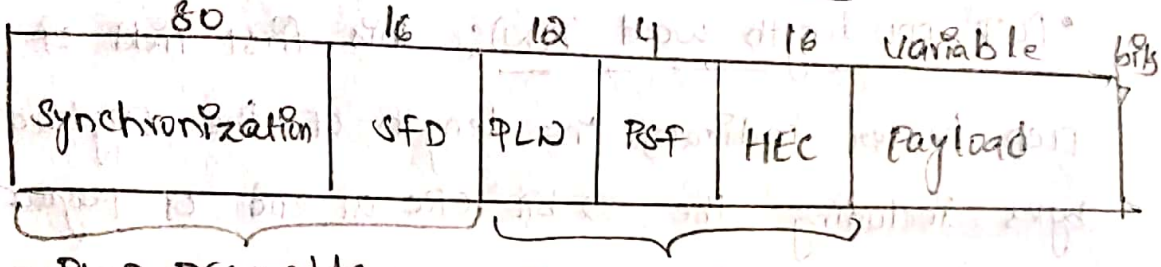
→ The main tasks of PHY management include channel tuning & PHY MIB maintainance.

→ Finally, station management interacts with both management layers & is responsible for additional higher layer functions.

5. Discuss about IEEE 802.11 physical layer fHss frame and Dsss frame.

- IEEE 802.11 supports three different physical layers: one layer based on infrared and two layers based on radio transmission.
- All PHY variants include the provision of the clear channel assessment signal(CCA)

frequency hopping spread spectrum (fHss):



format of IEEE 802.11 PHY frame using fHss.

→ fHss is a spread spectrum technique which allows for the coexistence of multiple networks in the same area by seperating different networks using different hopping sequences.

- The original standard defines 79 hopping channels for North America and Europe, and 23 hopping channels for Japan.

→ The selection of particular channel is achieved by using a pseudo-random hopping pattern.

- The standard specifies Gaussian shaped FSK, GFSK, as modulation for the fHss PHY.

Synchronization: the PLCP preamble starts with 30 bit synchronization which is a 010101... bit pattern.

- This pattern is used for synchronization of potential receivers & signal detection by CCA.

Start-frame delimiter (SFD): The following 16 bits indicate the start of 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 end of payload.

- PLW can range b/w 0 and 4095.

- PLCP signalling field (PSF): The 4 bit field indicates the data rate of the payload following.

- All bits set to zero (0000) indicates the lowest data rate of 1Mbit/s.

- The granularity of PS 500 k bits/s, thus 2Mbits/s is indicated by 0010 & the maximum PS 8.5 M bits/s (1111).

- This system obviously does not accomodate today's higher data rates.

Header error check (HEC): finally, the PLCP header is protected by a 16 bit checksum with standard CRC generator polynomial $G(x) = x^{16} + x^{12} + x^5 + 1$.

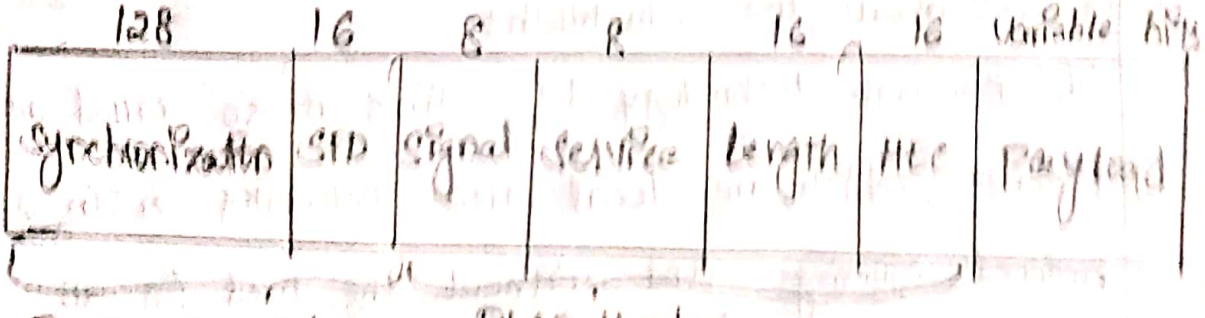
Direct sequence spread spectrum (DSSS):

→ DSSS is alternate spread spectrum method separating by code & not by frequency.

→ In the case of IEEE 802.11 DSSS, spreading is achieved using the 11-bit 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 & its insensitivity to multipath propagation.

- IEEE 802.11 DSSS PHY also uses the 2.4 GHz ISM band & offers both 1 and 2 Mbit/s data rates.
- The symbol rate is 1MHz, resulting in a chipping rate of 11MHz.
- All bits transmitted by the DSSS PHY are scrambled with the polynomial $S(z) = z^7 + z^4 + 1$ for DC blocking & whitening of spectrum.



format of IEEE 802.11 PHY frame using DSSS

Synchronization: The first 128 bits are not only used for synchronization, but also gain setting, energy detection & frequency offset compensation.

- It only consists of 1 scrambled 1 bits.

Start Frame Delimiter (SFD): This 16 bit field is used for synchronization at the beginning of frame and consist of pattern 1111001110100000.

Signal: originally, only 2 values have been defined for this field to indicate data rate of the payload.

- value 0x0A indicates 1M bit/s (DBPSK)
  value 0x14 indicates 2M bit/s (DQPSK)

Service: This field is reserved for future use; however 0x 00 indicates an IEEE 802.11 complaint frame.

Length: 16 bits are used in this case for length indication of the payload in microseconds.

Header error Check (HEC): signal, service & length fields are protected by this checksum using the ITU-T CRC-16 standard polynomial.

6. Discuss about the Bluetooth?

- The Bluetooth technology here aims at so called ad-hoc Piconets, which are local area networks with a very limited coverage and without the need for an infrastructure.

→ this is a different type of network is needed to different small devices in close proximity (about 10m) without expensive wiring.

- IEEE 802.11 discussed wireless personal area networks

(WPAN) under the following five criteria:

1. Market potential
2. compatibility
3. District Identity
4. Technical feasibility
5. Economic feasibility.

Characteristics

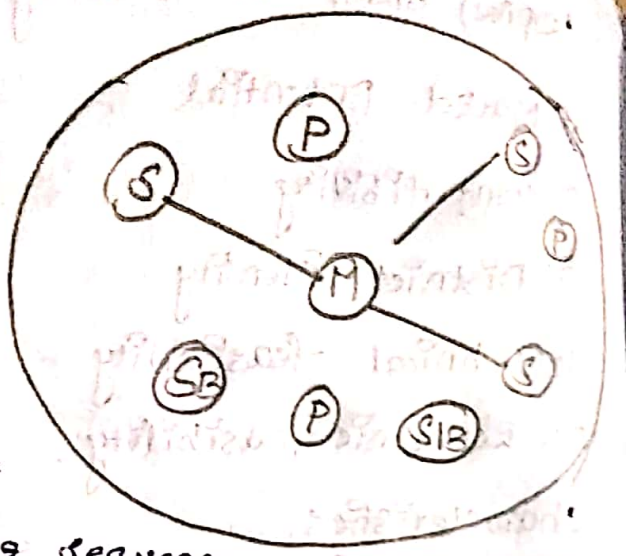
→ 2.4 GHz ISM band, 79 (23) RF channels 1MHz carrier spacing.

- channel 0: 2402 MHz ... Channel 78: 2480 MHz
- G-fsk modulation, 1-100 MW transmit power.

→ FHSS and TDD

- frequency hopping with 1600 hops/s
- Hopping sequence in a pseduo random fashion determined by a master.
- Time division duplex for send/receive seperation
- voice link - SCO (synchronous connection oriented)
- FEC (Forward error correction), no retransmission, 64 Kbit/s duplex, point-to-point circuit switched.
- Data link - ACL (Asynchronous connection less)
  - Asynchronous, task acknowledge, point-to-multipoint upto 433.9 Kbit/s symmetric or 723.2/57.6 Kbit/s asymmetric, pocket switched.
- Topology
  - overlapping piconets (star) forming a scatternet.

Piconet:



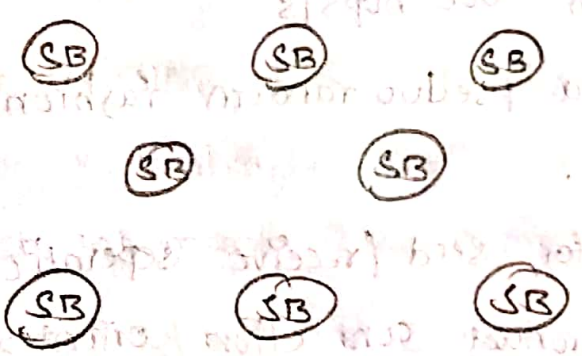
- collection of devices in an ad-hoc fashion.
- Each piconet has a unique hopping pattern.
- participation in a piconet = synchronization to hopping sequence.

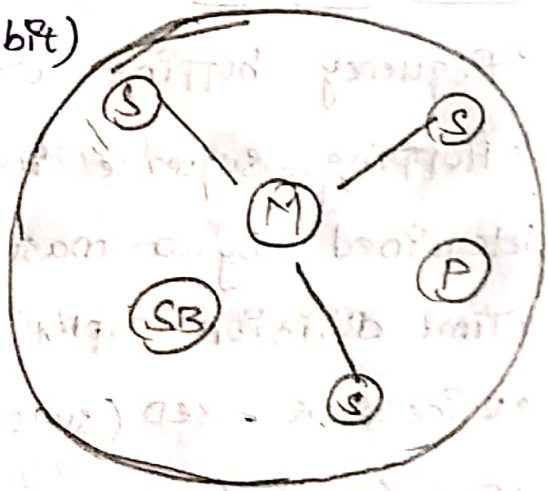
forming a piconet:

- All devices in a piconet hop together

Addressing

- Active member Address (3 bit)
- Parked member Address (8 bit)





Bluetooth Protocol Stacks

AT: Attention sequence

OBEX — object exchange

TCS BIN — Telephony control protocol specification

BNEP — Bluetooth network encapsulation protocol.

SDP — service discovery protocol.

RFCOMM — radio frequency COMM.

Radio: specification of air interface, frequencies modulation

Based band: Description of basic connection establishment, packet formats, timing.

Linker manager protocol: Link set-up & management between devices including security functions & parameter negotiation.

Logical link control & adaptation protocol (LQCAP):

- Adaptation of higher layers to the baseband
- service discovery protocol.
- Discovery in close proximity plus querying of service characterstic.

TCS BIN

- Call control signalling for the establishment of voice and data.
- calendar & business exchange protocol card objects (vcalendar/vcard) can be exchanged using the object using the object exchange protocol (OBEX) as common with IrDA interfaces.

The following group of functions are covered by the LMP (Linker Manager protocol)

1. Authentication, pairing & encryption.
2. Synchronization
3. capability negotiation
4. Quality of service negotiation.

5. Power control

6. Link supervision

7. State & transmission mode change.

Data rate:

- Synchronous : 64 Kbit/s
- Asynchronous : 433.9 Kbit/s symmetric
  (connectionless) 732.2/57.6 Kbit/s asymmetric

Transmission range:

- PAS (personal operating space) upto 10cm
- with special transceivers up to 100m.

Frequency

- free 2.4 GHz ISM-band.

Security

- challenge/response (SAFER+), hopping sequence

Availability

- Integrated into many products, several vendors.

Connection setup time:

- Depends on power-mode
- Max 2.56s, avg 0.40s

Quality of service

- Guarantees, ARQ/FEC

Manageability

- Public/private keys needed, key management not specified, simple system integration.

Special advantage/ Disadvantage:

Advantage:

- Already integrated into several products, available worldwide, free ISM-band, several vendors, simple system, simple ad-hoc networking, peer-to-peer, scatternets.

Disadvantage:

- Interference on ISM-band, limited range, max 8 devices/ network master, high set-up latency.

Bluetooth protocol Stack: