UNIT III

6

Wireless LAN

- Wireless Local Area Network is fast growing technology
- Goal of WLANs is to replace office cabling, to enable tetherless access to internet and to introduce a higher flexibility for adhoc communication.

Advantages of WLAN

1) Flexibility
   - within radio coverage, nodes can communicate without restrictions
   - Radio waves can penetrate walls so that senders & receivers can be placed anywhere

2) Planning
   - wireless adhoc n/w does not need previous planning. (No additional wiring)

3) Design
   - wireless n/w's allow for the design of small, independent devices
   - Senders & receivers can be hidden.

4) Robustness
- wireless n/w's can survive disasters
  Eg. earthquakes
- people can still communicate.

5) Cost
- once infrastructure is setup for wireless access no additional cost is required for additional users.

Disadvantages of WLAN

1) Quality of service
- WLAN offer low quality than wired.
- Reasons
  - lower bandwidth due to limitations in radio transmission
  - higher error rates due to interference.
  - higher delay variation due to extensive error correction & detection

2) proprietary solutions.
- Due to slow standardization procedures many companies have come up with proprietary solutions offering standardized functionality plus enhanced features.

3) Restrictions
- All wireless products have to comply with national regulations.

4) Safety and Security:
- Senders and receivers are operated by laymen. Special precaution have to be taken to prevent safety hazards.

5)
- All standards must offer encryption, privacy mechanisms, support for anonymity otherwise more and more wireless n/ws will be hacked.

Design goals of WLAN.

1) Global operation
- WLAN products should sell in all countries, so national and international frequency regulations have to be considered.

2) low power
- Devices Communicate via WLAN work on battery power. LAN design should implement power saving modes and power management functions.

3) License free operation.

- Equipment must operate in license free
- LAN operators need not apply for special license.

4) Robust transmission technology

- WLANs should operate under diff conditions
- If they use radio transmission, many devices can interfere with them.
- Senders & receives move.
- Antennas are omni directional.

5) Simplified spontaneous cooperation.

- WLANs to be useful in practice, WLANs should not require complicated setup routines but should operate spontaneously after power up.

6) Easy to use

- WLANs are made for simple use.
- They should not require complex management but rather work on plug & play basis.

7) Protection of investment

- lot of investment has already invested for WLAN.
- New WLANS should protect must investment by being interoperable with existing n/w.

8) Safety and security

- WLANs should be safe to operate.
- users should not able to read personal data during transmission i.e encryption should be integrated.
- N/ws should provide account user privacy.

9) Transparency for applications

- Existing applications should continue to run over WLANS.

Infrared vs radio transmission

- Infrared technology uses diffuse light reflected at walls, furniture etc & directed light if line-of-sight (LOS) exists b/t sender & receiver.
- Senders can be
  - simple light emitting diodes (LEDs)
  - laser diodes.
- Receivers are photo diodes.
- 2 basic transmission technologies can be used to set up WLANs.
  1) Infrared light
  2) radio transmission.

Advantages of Infrared transmission.

- simple
- cheap sender and receiver
- integrated into all mobile devices.
- No licenses are needed for infrared technology
- Shielding is very simple.
- Electrical devices do not interfere with infrared transmission.

Disadvantages of infra red transmission.

- Low bandwidth.
- easily shielded.
- Cannot penetrate walls & other obstacles.
- For good transmission quality and high data rates, LOS is needed.

Advantages of radio transmission.

- long term experience with radio transmission for WAN.
- Cover larger areas.
- Can penetrate walls, furniture, plants
- more coverage can be gained by deflection.
- Does not need LOS if frequencies are too high.
- offer higher transmission rates

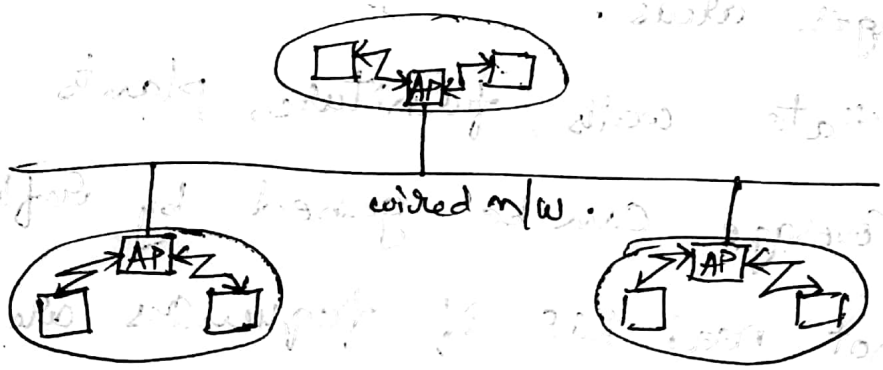
Disadvantages of radio transmission.

- Shielding is not simple.
- Can interfere with other devices & destroy data transmitted.
- radio transmission is permitted in certain frequency.

Infrastructure and ad-hoc n/w's.

Infrastructure n/w's

- Provide access to other n/w's
- include forwarding functions, medium access control
- Communication takeplace b/t wireless nodes and access point. (not directly b/t wireless nodes)
- access point control medium access, act as bridge to other wire & wireless n/w.
- 3 access points with 3 wireless n/w & a wired n/w.



- Design of infrastructure based n/w is simple.
- This type of n/w can use diff access schemes with & without collision.
- Cellular phone n/w's & Satellite based cellular phones are infrastructure based n/w's.

Adhoc n/w's

- Does not need any infrastructure to work.
- Each node can communicate directly with other nodes. So no need of access point.
- 2 adhoc n/w with 3 nodes.

- Nodes within adhoc n/w can only communicate if they can reach each other.
  Cannot communicate with each other if they are not within same radio range.
- Complexity of each node is higher.
- This type of n/w exhibits greatest possible flexibility.

Examples.

- IEEE 802.11 & HiperLAN 2 is infrastructure base n/w.
- Bluetooth is wireless ad-hoc n/w.

IEEE 802.11

- Simple and robust WLAN which offers time bounded & asynchronous services.

✱ System architecture

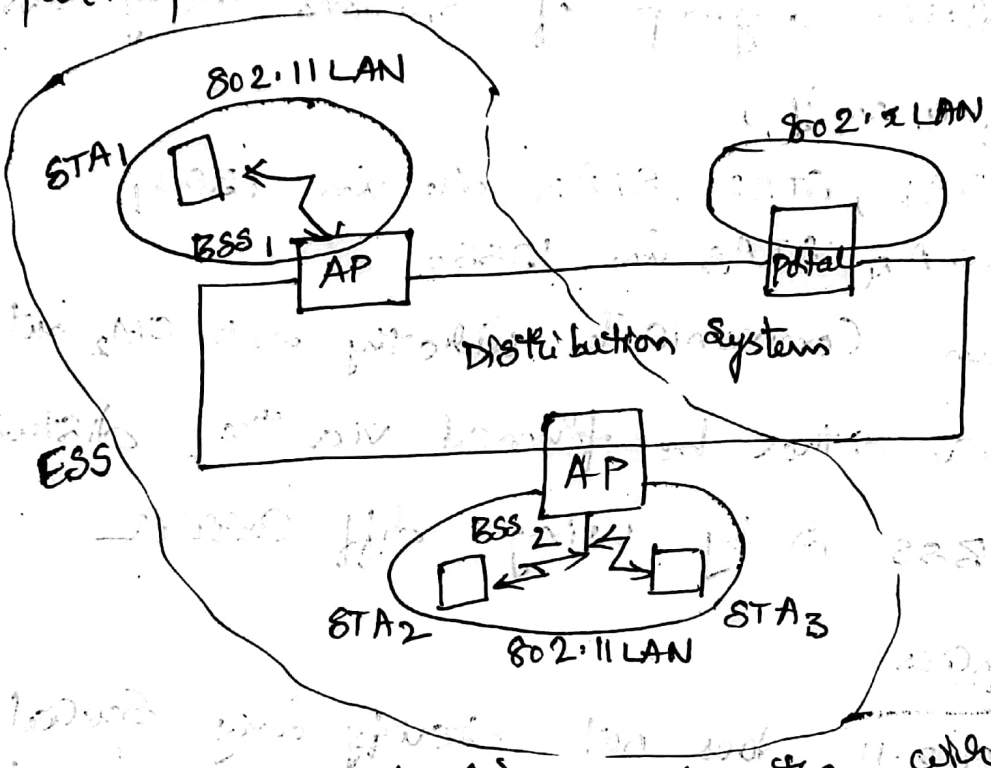
Wireless n/w exhibit 2 diff basic sys architectures

1) Infrastructure based
2) adhoc.

1) Infrastructure based IEEE 802.11

- Several nodes, called stations (STA$_i$) are connected to access points (AP).
- Stations are terminals with access mechanisms to wireless medium and radio contact to AP.
- AP & stations are within same coverage. form Basic service set (BSS$_i$)
- BSS$_1$ and BSS$_2$ are connected via distributed systems
- Distributed system connects several BSS via AP to form single n/w & extends the wireless coverage area.
- This n/w is Extended Service set (ESS) and has its own identifier, ESSID.

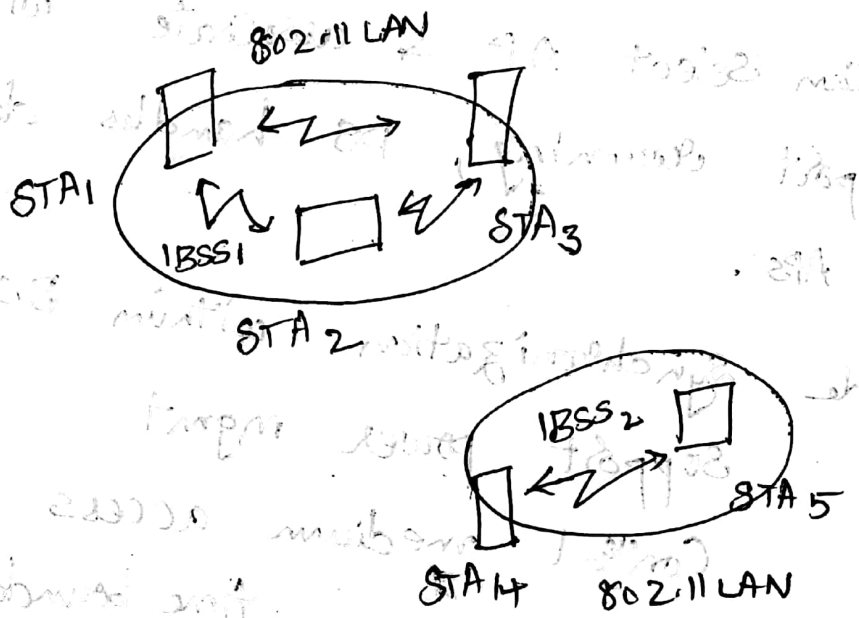
- ESSID is name of n/w & used to separate different n/ws.
without knowing ESSID it is not possible to participate in WLAN.



- Distribution System(DS) Connects the wireless n/ws via APs with a portal, which forms interworking Unit to other LANs.
- Stations can select AP & associate with it.
APs support roaming, DS handles data transfer b/t diff APs.
- AP provide synchronization within BSS,
support power mgmt
Control medium access to support time bounded service.

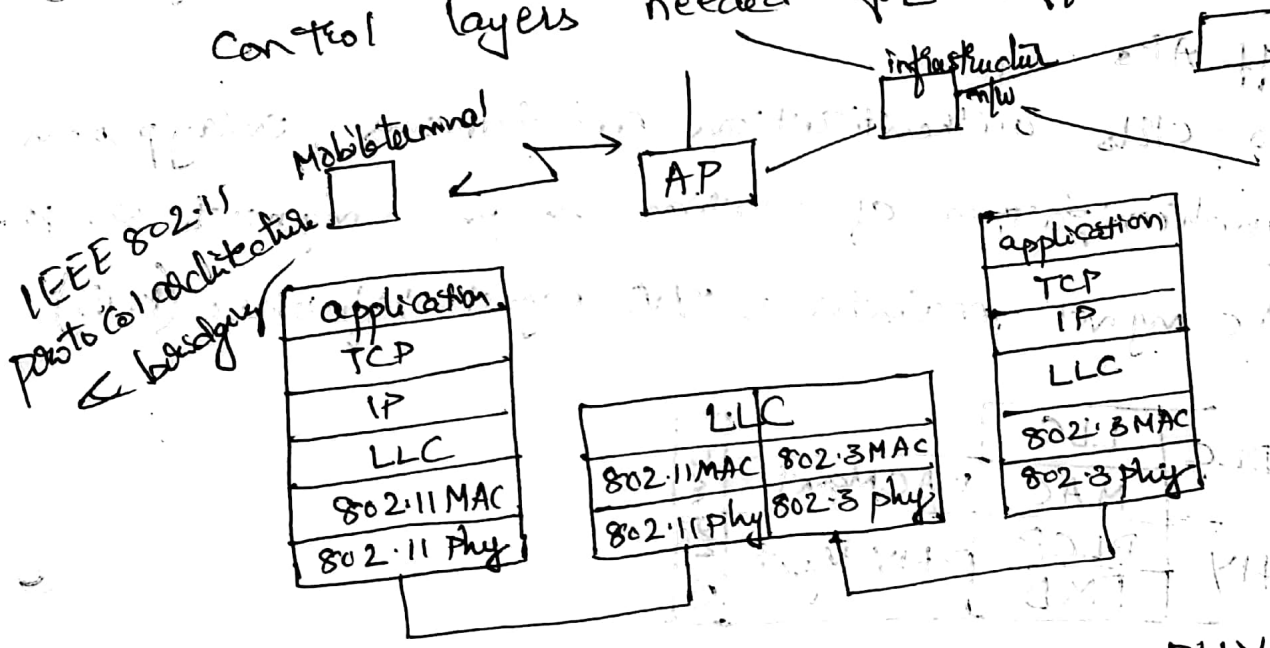
2) Adhoc wireless LAN's IEEE 802.11

- IEEE 802.11 allows the building of adhoc n/w b/t stations thus forming one or more independent BSSs (IBSS)
- IBSS comprises a group of stations using same radio frequency,
- Stations STA_1, STA_2, STA_3 are in $IBSS_1$, STA_4, STA_5 in $IBSS_2$
- STA_3 can communicate directly with STA_2 but not STA_1
- IBSSs can either be formed via the distance b/t IBSS & by using diff carrier frequencies
- IEEE 802.11 does not specify any special nodes that support routing, forwarding of data & exchange of topology information.



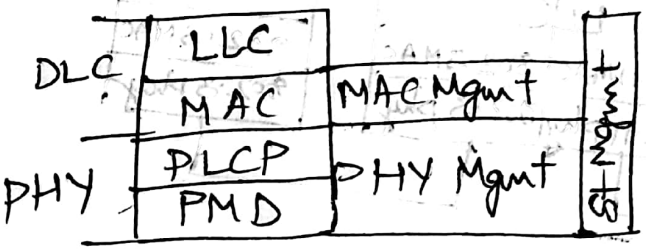
Protocol architecture

- IEEE 802.11 wireless LAN connect to IEEE 802.3 via a bridge
  WLAN behaves like slow wired LAN.
- Higher layers TCP, IP, application are same for wireless as for wired.
- Upper part of data link control layer, logical link control (LLC) covers the diff of medium access control layers needed for diff media.



- IEEE 802.11 only covers physical lay PHY and medium access layer MAC like other LAN.
- Physical layer is subdivided into
  physical layer Convergence protocol (PLCP)
  Physical medium dependent sublayer (PMD)
- Basic tasks of MAC layer comprise medium access, fragmentation of user data & encryption.

- PLCP Sublayer provides carrier sense signal called clear channel assessment CCA & provides common PHY service access point SAP.
- PMD Sublayer handles modulation & encoding/ decoding of signals.
- Apart from protocol sublayers, standard specifies mgmt layers & station mgmt.
- MAC mgmt supports association & deassociation of station to an access point & roaming b/w diff APs
- also CRIs authentication mechanisms, encryption Synchronization of station & power mgmt to save power
- MAC mgmt maintains MAC mgmt info Base (MIB)



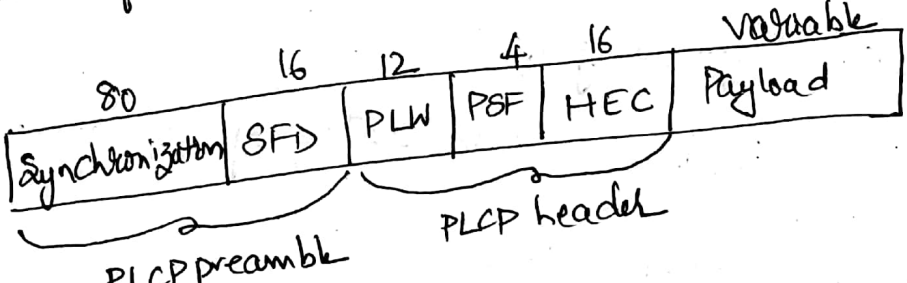
- Main tasks of PHY Mgmt include channel tuning & PHY PMD maintenance.
- Station Mgmt interacts with both Mgmt layers and is responsible for addition layer fns.

Physical layer

- IEEE 802.11 supports 3 different physical layers
  - one based on infra red
  - two based on radio transmission.

1) Frequency hopping Spread Spectrum (FHSS)

- This techniques allows for coexistence of multiple n/ws in same area by separating diff n/ws using diff hopping sequences.
- The selection of particular channel is achieved by using a pseudo random hopping pattern.
- Frame of physical layer used with FHSS.



- Frame consists of 2 parts
  1) PLCP part (preamble, header)
  2) Payload.

- Fields of frame perform following functions

Synchronization :

- PLCP preamble starts with 80 bit Synchronization
- which is 010101 --- bit pattern
- This pattern is used for Synchronization of potential receivers and signal detection by CCA.

Start frame delimiter (SFD)

- 16 bit indicate start of frame and provide frame Synchronization.

SFD pattern is 0000110010111101

PLCP_PDU length word (PLW)

- indicate length of payload in bytes.

PLCP Signalling field (PSF)

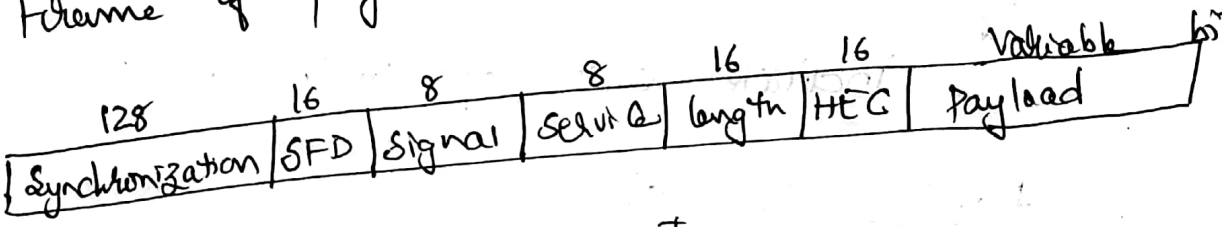
- indicate data rate of payload.

Header error check

- PLCP header is protected by 16 bit checksum.

2) Direction sequence spread Spectrum. (DSSS)

- DSSS is spread spectrum method separating by code and not by frequency.
- characteristics of this method are
  - its robustness against interference
  - its insensitivity to multipath propagation.
- This method is more complex than FHSS.
- Frame of physical layer using DSS.



- Frame consists of 2 parts
  1) PLCP part (preamble & header)
  2) payload part.
- Fields of frame perform following functions.

Synchronization
- used for synchronization
  gain setting
  energy detection
  frequency offset compensation.

Start frame delimiter (SFD)
- used for synchronization at beginning of a frame and consists of pattern 1111001110100000

Signal
- indicate data rate of payload.

Service
- reserve for future use.

length
- indicate length of payload.

Header error check
- Signal, service, length fields are protected by checksum.

8) Infrared
- physical layer based on infrared uses visible light
- Does not require line-of-sight b/t sender and receiver but also work with diffuse light.
- This allows point to multi point communication.

MAC layer

- Tasks of MAC layer
  - Control medium access
  - Offer support for roaming, authentication and power conservation
- Services provided by MAC layer
  - Mandatory asynchronous data service
  - optional time bounded service.
- 802.11 offer
  - only asynchronous service in adhoc based n/w
  - 2 services in infrastructure based n/w.
- 3 access mechanisms have been defined for IEEE 802.11
  1) Mandatory basic method based on CSMA/CA
  2) Optional method avoiding hidden terminal problem
  3) Contention free polling method for time bounded service.
- First 2 methods are summarized as distributed coordination function (DCF)
- Third method is point coordination function (PCF)

- DCF offers asynchronous service
  PCF offers both asynchronous & time-bounded service
- MAC mechanisms are also called distributed foundation wireless medium access control (DFWMAC).
-

Bluetooth

- Bluetooth technology aims at adhoc piconets These are local area n/w's with limited coverage and without need for an infrastructure.
- This n/w is needed to connect small devices in close proximity without expensive wiring & need for wireless infrastructure
- Data rate is 1Mbit/s asynchronous (data) & Synchronous (voice) Schemes are available
- In Spring 1998 5 Companies (Ericsson, Intel, IBM, Nokia, Toshiba) funded Bluetooth with the goal of developing a single-chip, low cost, radio based wireless n/w Technology.
- Bluetooth fulfills the Criteria of wireless personal Area N
  - Market Potential
  - Compatibility
  - Distinct identity
  - Technical feasibility
  - Economic feasibility.

User Scenarios

- Connection of peripheral devices

  Most devices are connected to a desktop Computer via wires.

  disadv: Each device has its own type of cable, different plugs are needed, wires block office space.

  In wireless n/w, no wires are needed for data transmission.

- Support of adhoc networking

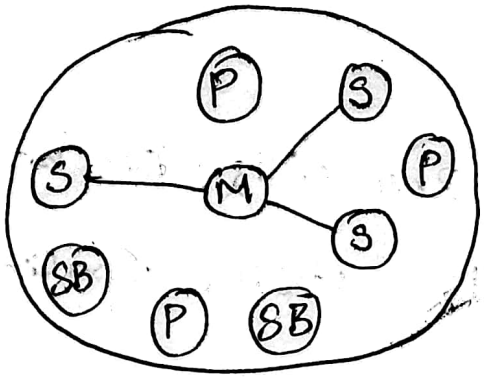
  wireless n/w's can support this type of interaction; Small devices might not have WLAN adapters following IEEE 802.11 standard, but cheaper Bluetooth chips built in.

- Bridging of n/w's

  Using wireless piconets, a mobile phone can be connected to PDA & laptop in simple way.

  Mobile phones will not have full WLAN adapters built in but could have a bluetooth chip.

  Mobile phone can then act as bridge b/t local piconet and GSM N/w.



- Parked devices (P) cannot actively participate in piconet but are known and can be reactivated within some milliseconds.
- Devices in Stand-by (SB) do not participate in piconet.
- Each piconet has one master
  Seven Slaves.
  more than 200 parked devices.
  - If parked device wants to communicate and there already 7 Slaves, one slave has to switch to park mode to allow parked device to be active.

Bluetooth Architecture

- Bluetooth operates in 2.4 GHz ISM band on 79 channels with 1MHz carrier spacing.
- Each device performs frequency hopping with 1,600 hops/s in pseudo random fashion.
- Bluetooth applies FHSS for interference mitigation.
  - A piconet is a collection of bluetooth devices which are synchronized to same hopping sequence.
    one device act as master (M) and all other devices connected to the master must act as slaves (S).
  - Master determines hopping pattern in piconet and slaves have to synchronize to this pattern.
  - Each piconet has unique hopping pattern. If a device wants to participate it has to synchronize to this.

formation of piconet

As all active devices have to use same hopping sequence they must be synchronized.

First step, master sending its clock and device ID.

All bluetooth devices have same networking capabilities

Unit establishing piconet automatically becomes master, all others will be slaves.

- hopping pattern is determined by device ID, a 48-bit unique identifier.
- Phase in hopping pattern is determined by masters clock.

A device should adjust its internal clock according to master & participate in piconet.

- All active devices are assigned a 3-bit active member address (AMA)

- parked devices use 8-bit parked member address (PMA)
  Devices in standby do not need address.
- All users within one piconet have same hopping sequence & share 1 MHz channel.
- As users join piconet, throughput per user drops quickly.

  This forms groups of piconets called scatternet. only those units that really must exchange data share same piconet, so that many piconets with overlapping coverage can exists simultaneously.