3

WLAN

WIRELESS LANs

The increased demands for mobility and flexibility in our daily life are demands that lead the development from wired LANs to wireless LANs (WLANs).

WLANs use electromagnetic radio waves to transport data between computers in a Local Area Network(LAN),without the limitations set by " hard wired network cable or phone wire connection", Whilst simple optical links are commercially available, radio is presently more useful since it is not strictly restricted to line of sight paths.

Radio waves are often called radio carriers when they are used to carry information. The data to be transported is superimposed on the radio carrier by various modulation techniques which allow the data to be faithfully reconstructed at the receiving end.-Once data is superimposed (modulated)onto the radio carrier, this combined "radio signal" now occupies more than a single frequency components or spectra of the modulating data add frequency to the basic carrier (in direct proportion to its information content or bit rate).

The frequency range which is needed to accommodate a radio signal with any given modulation bandwidth is called a channel. Radio receiver techniques can select one radio channel while efficiently rejecting signals on other frequencies. Many radio signals to and from many users can thereby co-exist in the same place and time without interfering with each other if the radio waves are transmitted at minimum necessary power within different radio channels.

3.1 ADVANTAGES OF WLAN OVER WIRED LAN

(1) Flexibility: With in radio coverage nodes can communicate without further restriction.
(2) Planning: Wireless ad hoc network allow communication without planning whereas wired network needs wiring plans.
(3)Design: Wireless Network can survive disaster. If the wireless devices survive people can communicate.
(4) Cost: Adding additional users to a wireless network will be increase the cost. But where as with fixed network addition of an user will lead into unplugging and plugging. Wireless connections do not wear out.

Disadvantages:

(1) QOS:

- Wireless offers lower quality than that of wired .The reasons are:
- The Lower bandwidth due to limitations in radio transmission.
- High error rate due to interference.
- Higher delay due to error correction and detection mechanisms.

(2) Proprietary Solution:

- Many companies have comeup with proprietary solutions offering standardized functionality.
- This is due to slow standardization procedures.

(3) Restriction:

- The wireless products need to comply with national regulations.
- WLAN are limited to low power senders and certain license free frequency hand which are not same world wide.

(4) Safety and security:

The radio waves are used for data transmission. They will interface with other equipment. Precautions have to be taken to prevent safety hazards.

As it is via radio transmission eaves dropping is possible.

Design Goals: TO Ensure Commercial Success

(1) Global Operation:

While the product is being sold in all the countries, national and international frequency regulation should be considered.

(2) Low Power:

Devices communicating via WLAN are also wireless devices. These Devices run on battery power- While designing a WLAN these aspects should also be considered (i.e) Power saving modes and power management functions to be considered

` **(3) License Free Operation:**

The equipment must operate in a license free band such as 2.4 GHz ISM Band.

(4) Robust Transmission Technology:

WLAN operate under difficult conditions. As they are radio transmission many other electrical devices can interfere with them.

(5) Simplified Spontaneous Co-Operation:

WLAN should not require complicated startup routines, but should run spontaneously after power up.

(6) Easy to Use:

WLAN"s are made for simple use. They should be like plug and play.

(7) Production of Investment:

For transition from wired to wireless, simple bridging should be enough to interoperate.

(i.e.) Wireless LAN should support the same data types and services as that of wired LAN.

(8) Safety and security:

WLAN should be safe to operate. When low radiation are used.the network should consider user privacy and security.

(9) Transparency:

Existing applications should continue to run over WLAN with a trade off to higher delay and lower bandwidth.

3.2 Wireless Transmission Technologies

Two basic transmission technologies used are

(1) Infrared,

(2) Radio Transmission.

The two technologies can be used to setup ad hoc connections for work group to connect or support mobility.

1) Infrared:

1. This technology uses diffuse light reflected at walls, etc (or) directed light if line of sight exists between sender and receiver.
2. Sender can be LED or laser diodes.
3. Receivers can be photo diodes.

Advantages:

- Simple and cheap because of LED/ Diodes(crystal rectifier).
- No license needed-uses only infra-red.
- No interferences form/ with electrical devices.

Disadvantages:

- Low bandwidth.
- The infra-red can be easily shielded.
- Infra-red cannot penetrate walls/o.
- LOS is needed.

Infrared is used when

- Good transmission quality is needed.
- High data rates.LOS is needed.

2) Radio transmission:

The radio waves are used data transmissions in wireless network.

Advantages:

- Long term for WAN.
- Coverage is larger.
- Can penetrate walls, furniture"s etc.
- Additional coverage is by reflection.
- Does not need LOS.
- Higher transmission rates above 100 mb/s.

Disadvantages:

- Shielding is not simple.
- Interference is possible.

- Radio transmission is permitted in certain frequency bands only.
- Limited range of license free hands are available world wide and are not available same in all countries.

3.3 Settings For WLAN

They are two settings to establish WLAN
They are
1) Infra-Structure
2) Ad hoc Networks.

1) Infrastructure

- WLAN"s need an infrastructure to build network.
- They provide access to other networks, forwarding, and MAC functions.
- Communication is between wireless node and access point. (refer figure 3.1)
- Two wireless nodes cannot communicate each other.

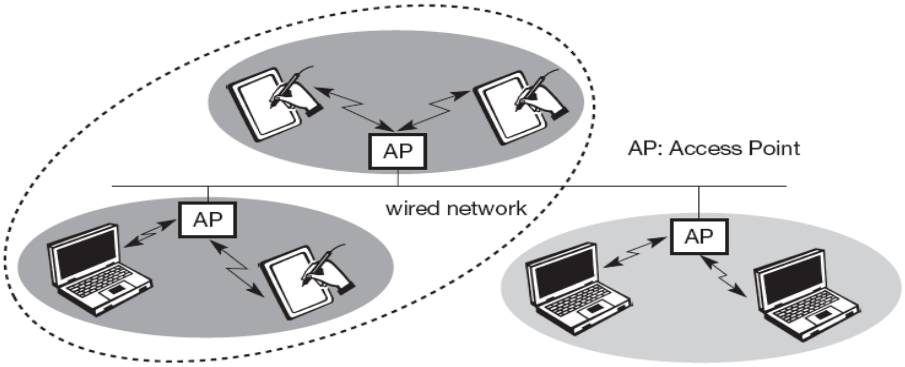


Fig3.1 : Example of the infrastructure-based wireless network

- The above figure shows three access points with in the wireless network.
- Several wireless network form one logical wireless network.
- The access points are fixed network can connect wireless networks to form a larger network.
- The structure is similar to that of star shaped network.

Functions of Access Points:

1. Controls the access to the medium.
2. Acts as a bridge to wired and wireless networks.
3. The network functionality lies within the access point thus making the design of infra structured based wireless network easier.

- The network uses different access schemes to access the medium via access point.
- Collisions occur if the access point and wireless nodes are not co-ordinated.
- If the access point controls the medium the system will be collisions free (eg).Cellular phone network are infra-structure based.

Disadvantage:

1. Loose some flexibility of wireless network because the ap are interconnected via wires.

2) Adhoc Wireless Network:

- They do not need any infra-structure.
- Each node can communicate directly with other nodes which are in the same range.
- No access point to control the medium is needed.

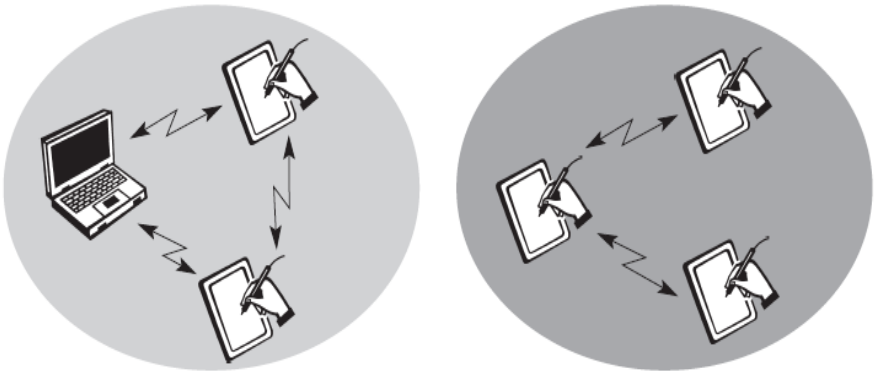


Fig 3.2: Example of two ad-hoc wireless networks

Ad hoc Network:

- Nodes with in an ad hoc network can communicate if they can reach Physically (i.e.) if the two nodes are with in each others radio range. (or) they can forward the message.
- The nodes cannot communicate of they are not within the same radio range.

Advantage and Disadvantage:

- Complexity is higher.
- Highest flexibility

Conclusion:

The two basic types does not always come in their pure form.

3.4 WLAN Technologies

Wireless LAN Standards that are currently being explored in the field of communications technology are:

1. IEEE 802.11.
   a.802.11a b.802.11b c.802.11g

2. BRAN
   A.HiperLAN1/2 b.Hiperaccess c.Hiperman
3. Bluetooth

Wireless LAN Standards: There are several wireless LAN solutions available today, With varying levels of standardization and industry are, HomeRF and Wi-Fi* (IEEE**802.11b).Of these two, 802.11 technologies enjoy wider industry support and are targeted to solve Enterprise,home and even public hot spot. Wireless LAN needs.

3.5 IEEE 802.11

3.5.1 Introduction to IEEE 802.11

The IEEE finalized the initial standard for wireless LANs,IEEE 802.11 in june 1997.This initial standard specifies a 2.4 GHz operating frequency with data rates of 1 and 2 Mbps.With this standard, one could choose to use either frequency hopping or direct sequence(two non compatible forms of spread spectrum modulation).

Because of realatively low data rates (as compared to Ethernet), Products based on the initial standard did not flourish as many had hoped.In late 1999, the IEEE published two supplements to the initial 802.11a and 802.11b(Wi-fi*)

IEEE802.11a

The 802.11a standard (High Speed Physical Layer in the 5 MB/s.The advantages of this standard(compared to 802.11b.Higher speed Physical Extension in the 2.4 GHz Band) include having much higher capacity and less RF(radio frequency) interference with other types of devices (e.g., Bluetooth), and products are just now becoming available throughput 2002.However,802.11a isn"t compatible with 802.11b and 802.11g products.

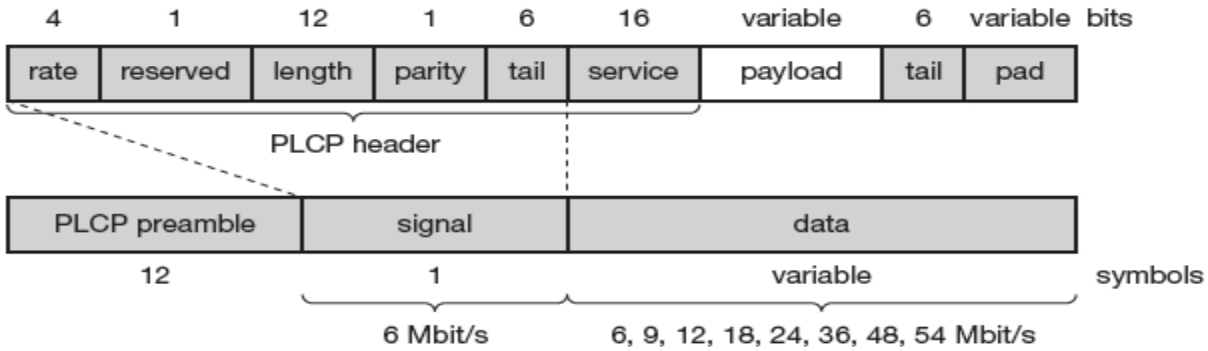


Fig 3.3 IEEE 802.11a physical layer PDU

IEEE802.11b

As with the initial standard,802,11b operates in the 2.4 GHz band,but it includes 5.5 and 11Mb/s in addition to the initial 1 and 2 Mb/s.The 802.11b standard only specifies direct sequence modulation, but it is backward compatible with the initial direct sequence wireless LANs. The IEEE 802.11b standard is what most companies choose today for deploying wireless LANs. The following is Long PLCP PPDU format. The short PLCP PPDU format has short synchronization instead of normal synchronization.

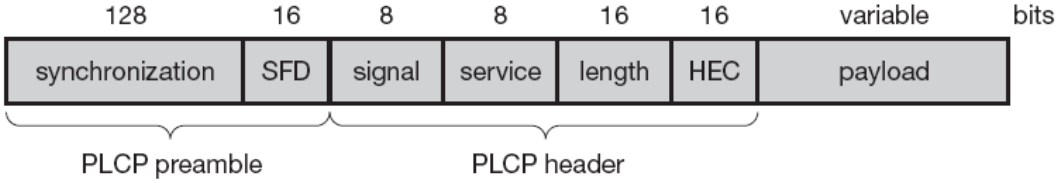


FIG 3.4 IEEE 802.11b PHY packet formats

IEEE802.11g

The 802.11 working group is currently working to extend the data rates in the 2.4 Ghz band to 54Mb/s using OFDM (Orthogonal Frequency Division Multiplexing).

3.5.2 System Architecture

Wireless networks can be of either of 2 basic architectures.

(1) Infra structure based

(2) Ad hoc based.

Infrastructure based IEEE 802.11 WLAN

- Portal is a bridge to other wired network.
- Wireless modes are called as station represented as STA.

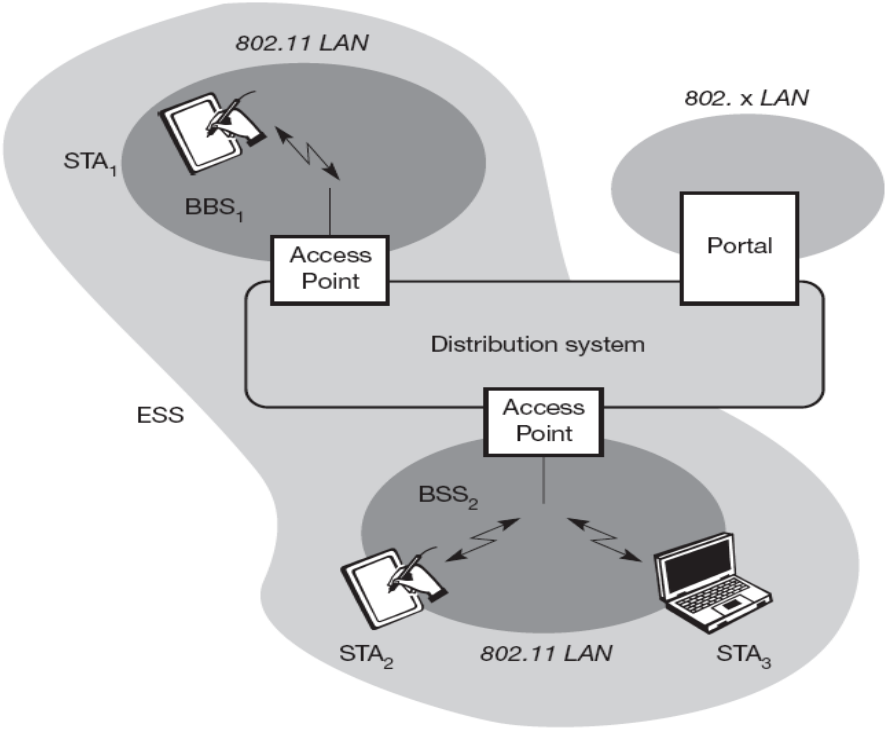


Fig 3.5: Architecture of an infrastructure based IEEE 802.11

- These station are connected to the access point Ap.
- The stations and the Ap which are within the same radio coverage is form Basic Service Set (BSSi).
- The BSS are interconnected via a distribution system.
- The distribution system connects several BSS via Ap to form a single network.
- This network is called Extended Service Set(ESS).
- This ESS has its own identifier ESSID.The ESSID is the name of the network and is used to separate different network.

3.5.3 Distribution System:

- The distribution system connects the wireless network via the AP with a portal,by which other LANs can also be connected.
- The distribution system consists of bridged IEEE LAN,Wireless Lines or any other network.
- Handles data transfer between AP"s.

Function of Access Point:

1. Support roaming
2. Period synchronization with in BSS
3. Support power management.
4. Control medium access.

Architecture of Ad hoc based IEEE 802.11 WLAN

IEEE 802.11 allows the ad hoc network between stations. This ad hoc network is called as independent BSS (IBSSi). The IBSS has the group of stations using the same radio frequency.

In the above diagram S_1,S_2,S_3 can communicated with each other but not with S_4 and S_5.

Protocol Architecture

- The above architecture shows wireless LAN connected to Ethernet via bridge.
- IEEE 802.11 covers the physical layer and medium access layer.
- The physical layer is subdivided into (PCLP) Physical layer convergence protocol and physical medium dependant (PMD) sub layer.

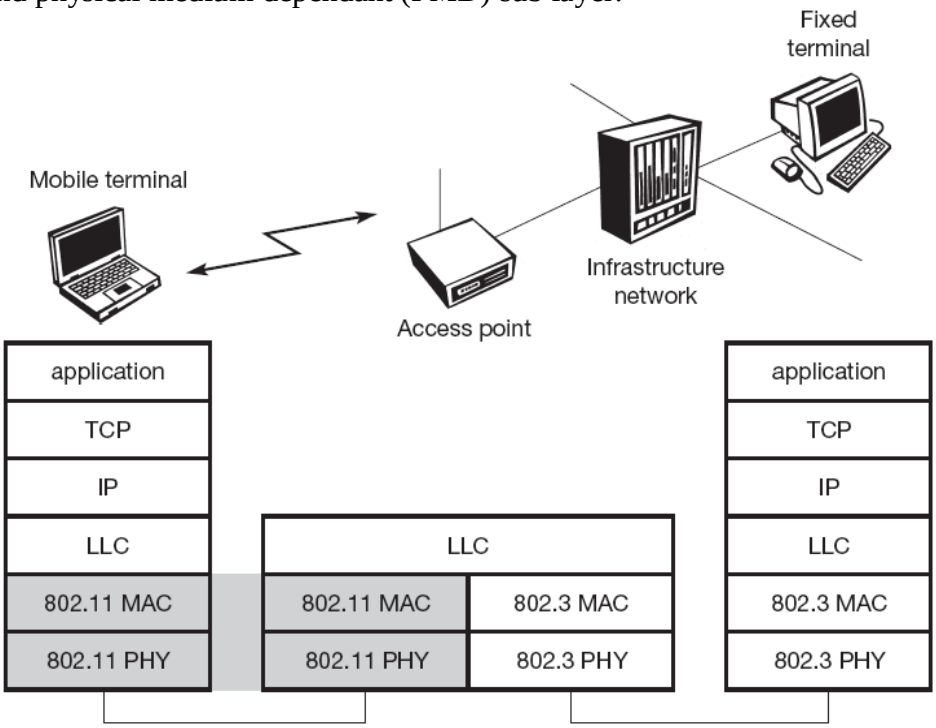


Fig 3.7: IEEE 802.11 Protocol Architecture

Detailed Architecture

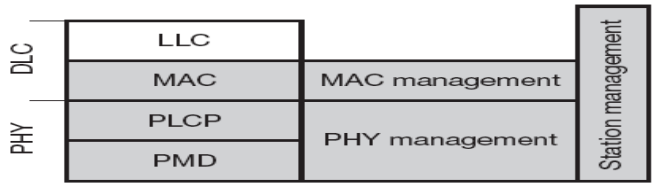


Fig 3.8: Detailed Architecture

Function of MAC

1. Medium access
2. Fragmentation
3. Encryption

Functions of PLCP:

1. Provides a carrier sense signal called clear channel assessment (CCA).
2. Provides PHY service access point (SAP) independent of transmission technology.

Functions of PMD:

1. Handles modulation and encoding/decoding of signals.

Function MAC Management:

1. Supports association and reassociation of station to access point.
2. Supports roaming.
3. Controls authentication, encryption, and synchronization of station with accompoint.
4. Power Management.
5. Maintain management information basic MIB (Management Information Base).

Function of PHY management:

1. Channel Tuning
2. Maintain PHY MIB

Functions of Station Management:

- Interacts with both management layers and is responsible for higher layer functions.

3.5.4 Physical Layer

- IEEE 802.11 supports three different physical layers.
  - One layer based on infrared.
  - Two layers based on radio transmission.
- All the variants have the CCA signal clear channel assessment signal.
- CCA is needed for the MAC to check whether the medium is busy or idle.
- Indicates whether the medium is busy or idle.
- Offers a SAP (Service access point) with 2 MBPS transfer rate.

Three Version of PHY layer:

1. Frequency hopping spread spectrum.
2. Direct sequence spread spectrum.
3. Infra-red.

3.5.4.1 Frequency Hopping Spread Spectrum:

- FHSS is a spread spread spectrum.
- Allows the co-existence of multiple networks in the same area by using different hopping sequence for different network.
- Frame of the physical layer used with FHSS.

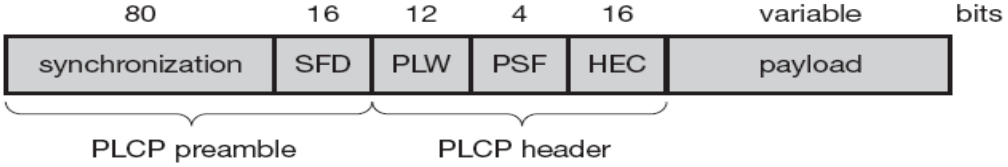


Fig 3.9: Frame Format of FHSS

- The Frame consists of 2 parts.
  1. PLCP part (Physical Layer Convergence Protocol)
  2. Payload part.

PLCP: Consists of Preamble and header.

- PLCP is transmitted @ MBPS.
- Data is scrambled using the polynomial

- $S(Z)=Z^7+Z^4+1$ for DC blocking and widening of spectrum.

Synchronization: S_0 bit synchronization bits which is of the pattern 010101.
This pattern is used for synchronization of receivers and signal detection.

SFD Start Frame Delimiter: The SFD pattern is 0000 1100 1011 1101. It is of length 16 bits which indicate the start of the frame.

PLCP PDU length word PLW: This is the first field of the PCLP header .It indicates the length of the payload. This includes the 32 bit CRC at the end of the payload.PLW can range between 0 and 4095.

PCLP Signaling Field PSF: This is 4 bit field. It indicates the data rate of the payload.

- When PSF is 0000 indicates the rate as 1 MBPS.
- When PSF is 1111 indicates the rate as 8.5 MBPS.

Header Error Check (HEC): The PLCP header is protected by a 16 bit checksum. With a ITU-T generator polynomial $G(X) = x^{16} + X^{12} + X^5 + 1$.

3.5.4.2 Direct Sequences Spread Spectrum: DSSS

This is a spread spectrum method.

- This method uses code.
- For IEEE 802.11 DSSS spreading is achieved by 11 chip Barker sequence (+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1).

Characteristics:

1. Robustness against interference.
2. Insensivity to multipath propagation.
3. Implementation is complex.
4. Uses 204 GHz ISM band and allows both 1 and 2 MBPS data rates.
5. Chipping rate is 11 MHz.
6. All the bits are scrambled by polynomial $s(z) = Z^7+Z^4+1$ and transmitted.
7. System uses differential binary phase shift keying (DBPSK) for MBPS transmission and differential quadrature phase shift keying (DQpsk) for 2 MBPS transmission.

Frame of Physical layer using DSSS

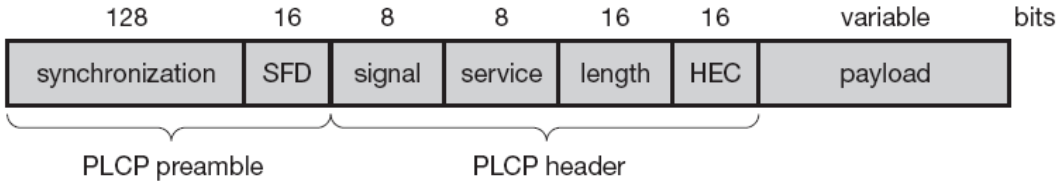


Fig 3.10: Frame Format of DSSS

The frame has 2 parts

1. PLCP Part-transmitted at 1 MBPS
2. Payload part-Transmitted at 1 or 2 MBPS.

Functions of Fields

Synchronization (128 bits)
This field is used for

- Synchronization,

- Gain setting,
- Energy detection,
- Frequency offset compensation.

SFD (Start Frame Delimiter) 16 bits:

- Used for synchronization at the beginning of the frame.
- The pattern used is 1111 0011 1010 0000 (8 bits).

Signal: This field indicates the data rate of transmission of payload.

- Value of the field is OXOA- 1 MBPS (DBPSK)
- Value of the field is OX14-2 MBPS (DQPSK)
- Other Value reserved for future use.

Service (8 bits): Reserved for future use. when the service field has 0x00 indicates a compliant frame.

Length (16 bits): Length of the payload in microseconds.

Header Error Check(HEC) 16 bits: This filed is used for protection of

- Signal
- Service
- Length.

They are protected by checksum using ITU-T CRC 16 standard Polynomial $\lambda^{16}+ \lambda^{12}+ \lambda^{5}+1$.

Infra-Red:

The physical layer is based on Infra red transmission.

Characteristics:

- Doesn"t require line of sight between sender and receiver.
- Allows point to multipoint communication.
- Maximum range of transmission is 10m provided no interference with transmission.
- Best suited for network with in a building.
- Reuse of frequency is simple.

3.5.5 Medium Access Control Layer (Mac Layer Functions)

- Control the medium access
- Support roaming
- Authentication
- Power conversation.

Traffic Service Provided by MAC

- Asynchronous Data Service-Mandatory
- Time bounded service(Optional).Used for transfer of data.

Asynchronous Data Service

- Exchange of packets based on best efforts.
- It supports broadcast and multicast transmission.

Time Bounded Service:

1. This service is implemented using point co-ordination function PCF.

802.11 offers asynchronous data service in ad hoc mode.

802.11 offers asynchronous data and time bounded services in infrastructure mode.

To access the medium three methods are available.

- DFWMAC-DCF CSMA/CA(mandatory)
- DFWMAC-DCF W/RTS/CTS (optional)
- DFW MAC-PCF (optional)

DFW: Distributed foundation wireless
MAC: Medium Access control
DCF: Distributed co-ordination function
PCF: Point co-ordination function
The I method mandatory is based on CSMA/CA.
The II method is based on RTS/CTS used to avoid hidden terminal problem.
The II method is based on polling for time bounded service.
DCF offers only asynchronous service.
PCF offers both Asynchronous and time bounded service.

- The MAC mechanisms are called as DFW MAC.
- When a node wants to transmit a packet it has to wait one DIFS amount of time before sensing the medium. If the Medium is idle immediately the node transmits a packet. Else it has to wait.
- The waiting time depends upon SIFS,PIFS,DIFS based upon the data/control.
- The waiting time depends upon PHY and slot time.
- The slot time is dependent upon
  - Propagation Delay
  - Transmitter Delay
  - Other PHY dependent parameters

Slot time is 50 µs FHSS
20 µs DSSS.

SIFS:
Short Inter Frame Spacing. This waiting time has highest priority, shortest waiting time. Its is used to transmit ACK,CTS and polling response.
PIFS: PCF IFS
Point Co-ordination Function Inter Frame Space. This waiting time has medium priority SIFS waiting time is between SIFS and DIFS. It is used for time bounded service.
DIFS: DLF IFS
Distributed Co-ordination Function Inter Frame Space.
This has the lowest priority longest waiting time.It is used for asynchronous data service.

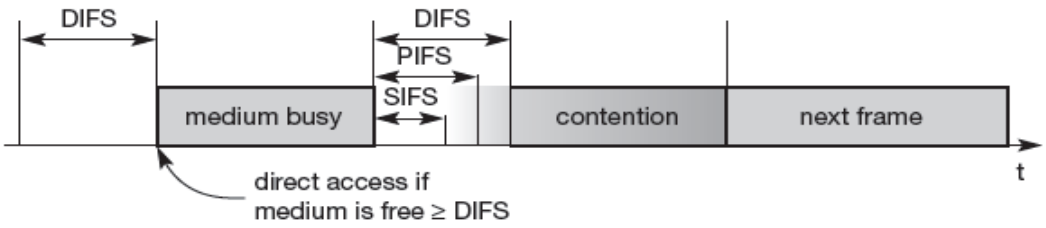


Fig 3.11: Medium Access and Interframe Spacing

3.5.5.1 Access Method 1 DFW Mac-DCF using CSMA/CA

This method is used to check whether the medium is idle or busy. This is the mandatory access method. This method is based on CSMA/CA.

Concept:

When the device is ready to send it starts sensing the medium. Carrier sense based on clear channel assessment.

If the medium is free for the duration of Inter Frame space the station can start sending. The IFS depends upon the service type.

If the medium is busy the station has to wait for a free IFS. When more than one node compete after IFS they entering the contention phase. During the contention phase each node chooses a random back off time within the contention window.

- The Nodes delays the medium sense for chosen random amount of time.
- After the random amount of time the node senses the medium, two scenario"s exist.
  (a) Medium is idle, the node can access the medium.
  (b) The medium is busy, the cycle is lost and the node has to wait once again for on DIFS the idle medium.
- The additional waiting time is measured in multiple of the slots.
- The advantage of randomness is that it avoids collision.
- The disadvantage is that this method is not fair because irrespective of the waiting time all the nodes have chance of transmitting data in the next cycle.

To have fairness 802.11 adds back off timer.

Concept of Back off timer:

All the nodes need to wait for IFS (Free). Then each nodes selects a random waiting time within the contention window.

If the station does not get the access to the medium, it stops the back off timer. Waits for the channel to be free for I DIFS and starts the counter again. As soon as the counter expires the nodes access the medium.

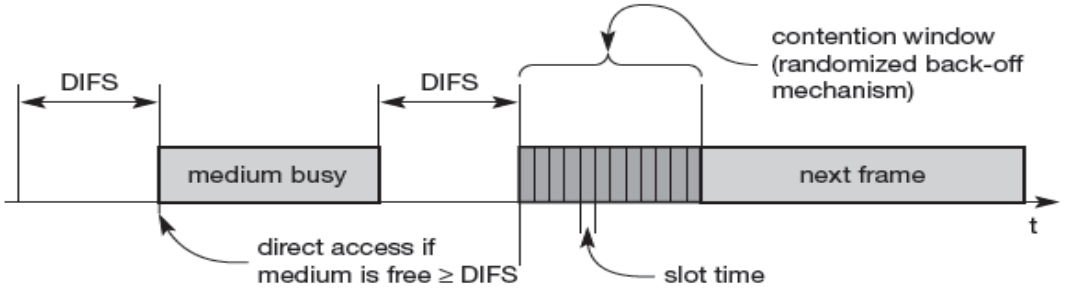
This states that the deferred station do not choose the back off timer again but counts down.

Advantage:

Station waiting for a longer time has an edge over the nodes that have just entered, because it has to wait only for the remainder of the back off timer from the previous cycles.

Broadcast Data Transmission

To illustrate the concept consider 5 stations STA1 to STA5 are trying to send a packet at some point of timer.



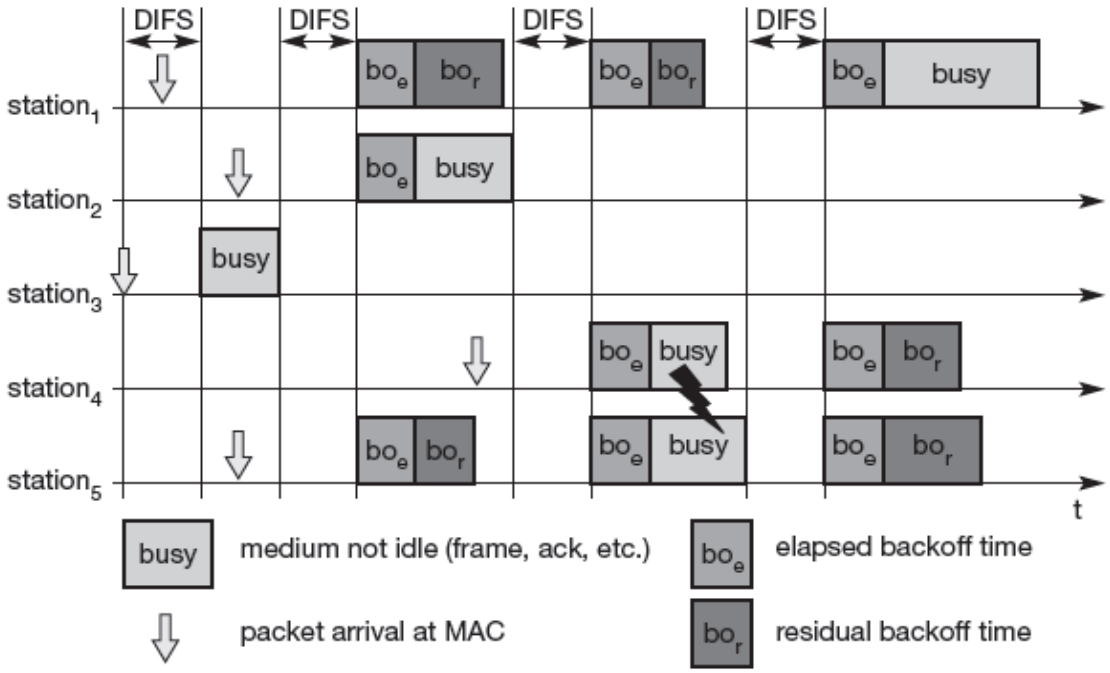


Fig 3.12: Broadcast Data Transmission

From the figure station 3 has the first request to send a packet. The station 3 senses the medium, finds the waits for medium is idle 1 DIFS and finds that the medium is idle throughout and sends the packet. Station1, Station2, Station5 need to wait for 1 DIFS after station 3 window and starts coming down their timer. The stations need to choose back off times because more stations compete.

Back off time=$BO_e + BO_r$

The back off timer for station 2 is very low. Hence it accesses the medium.

The station 1 , and station 5 stops the clock and store their residual back off timer.

Now station 4 wants to send a packet. It waits for 1 DIFS. Three stations try to get access the medium. Accidentally two stations can have the same back off time. Station 4 and Station 5- This results in collision and need to wait. Hence station 1 gets access to the medium. Due to the collision station 4 and 5 need to select a new back off timer.

The problem in this method is the selection of contention window size. If the window size is large causes unnecessary delay over the other hand when it is small results in unnecessary collisions.

The system tries to select the value based upon the number of stations trying to send.
The size of the contention window follows exponential back off.
(e.g.) Starts with CW=7.

When collision occurs, CW size doubles CW=49 and goes on until maximum of CW, 255. The above scenario is for heavy load. Under light load, it starts decreasing until CW=7.

For Unicast Data Transmission

- In the following unicast transmission the sender transmits data and receiver transmits acknowledgement. After receiving the data, the receiver waits for one **SIFS,** only because it is ACK.

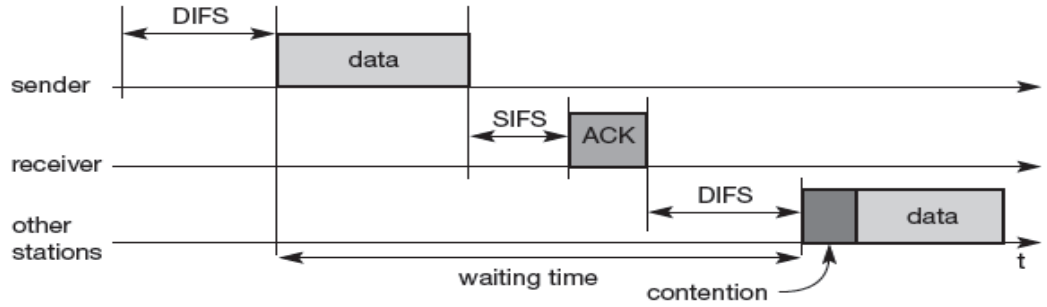


Fig 3.13: Unicast Data Transfer

- When the sender does not receive acknowledgement, it automatically retransmits the frame.
- No rules for Retransmissions.
- When more than one station complete for the medium, the system follows the regular 1 DIFS followed by contention window.

3.5.5.2 DFW MAC-DCF with RTS/CTS

- In order to avoid the hidden terminal problem and for contention free access RTS and CTS are used.

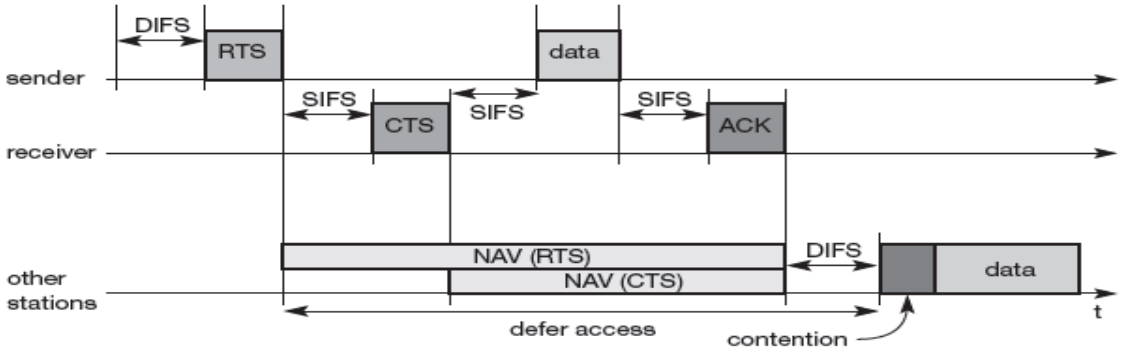


Fig 3.14: IEEE 802.11 contention – free access

- When a sender wishes to send data to a receiver, waits for DIFS if the medium is free or DIFS

+ Back off when the medium is busy contended by many users.

The sender sends RTS packet.(Request to send) a control packet.

Contents of RTS packet

1. Receiver address.
2. Duration (Data transmission plus acknowledgement).

Every node in the range of sender receiving this RTS has its Net Allocation Vector (NAV) in accordance to duration field of RTS. NAV resolves the hidden terminal problem.

If the receiver receives RTS, it sends CTS (Clear to send)control packet after waiting for SIFS.

Contents of CTS Packet

- Sender and receiver address.
- Duration (Data and Acknowledge).

Every node in the range of the receiver receiving this CTS has to set the Allocation Vector (NAV) in accordance to the duration field of CTS.

N**ote:** The receivers of RTS need not be the same set of CTS.

Advantage: Medium is Exclusive to one sender.

- After receiving the CTS the sender sends the data packet after 1 SIFS.
- The receiver waits for SIFS after receives the data packet, then acknowledges to the sender.
- Thus the transmission is complete –NAV marks the medium as free.

Advantage and Disadvantage:

- Collisions can occur at the beginning while the RTS is sent.
- Non negligible overhead in wastage of bandwidth for the transmissions of CTS and RTS.
- When the data size is high ,it needs to be fragmented.

Fragmentations:

Generally in wireless LAN, bit error rate is higher .To decrease the bit error rate fragmentations needs to be done.

Concept:

A Sender can send RTS control packet to reserve the medium after waiting time of DIFS. The RTS packet include the durations for the transmission of the first fragment and the corresponding acknowledgement. The nodes that receives the RTS set their NAV according the durations.

The receives answers with a CTS including the durations of data transfer and acknowledgement.

The nodes that receive the CTS set their NAV according the durations.

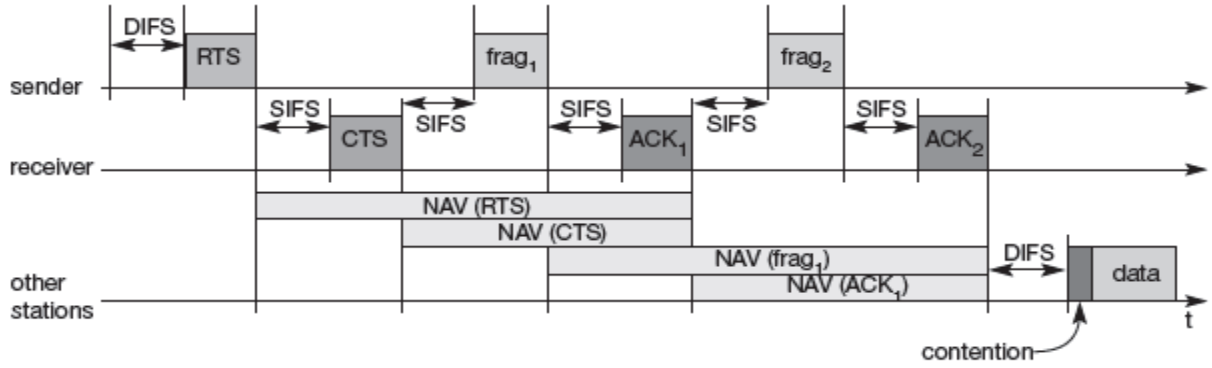


Fig 3.15: IEEE 802.11 fragmentation of user data

The sender after the initial waiting, sending of RTS, Receiving CTS ,is ready to send the data which is fragmented**.**

Content of Fragment:

- Data
- Duration of transmissions for the following fragment, its acknowledgement.

The receiver of fragment responds in the acknowledgement after SIFS.

The fragment contains the duration for the next frame, until the last fragment. For the last fragments the sender does not reserve the medium any longer.

3.5.5.3 DFW MAC-PCF with Polling: The disadvantage of the above 2methods:

- Cannot guarantee a maximum delay.
- Minimum transmission bandwidth**.**

Advantages:

- Provides at time bounded serviced MAC follows PCF (Point Co-ordinate Function)
- Requires an access point to control the medium access and polling.
- The access point splits the access time into super frame period.
- The super frame period has
    1. Contentions free period,
    2. Contention period.

The Contention Period: The nodes can use any one of the above methods to gain access to the medium.

Concept of Contention free period:

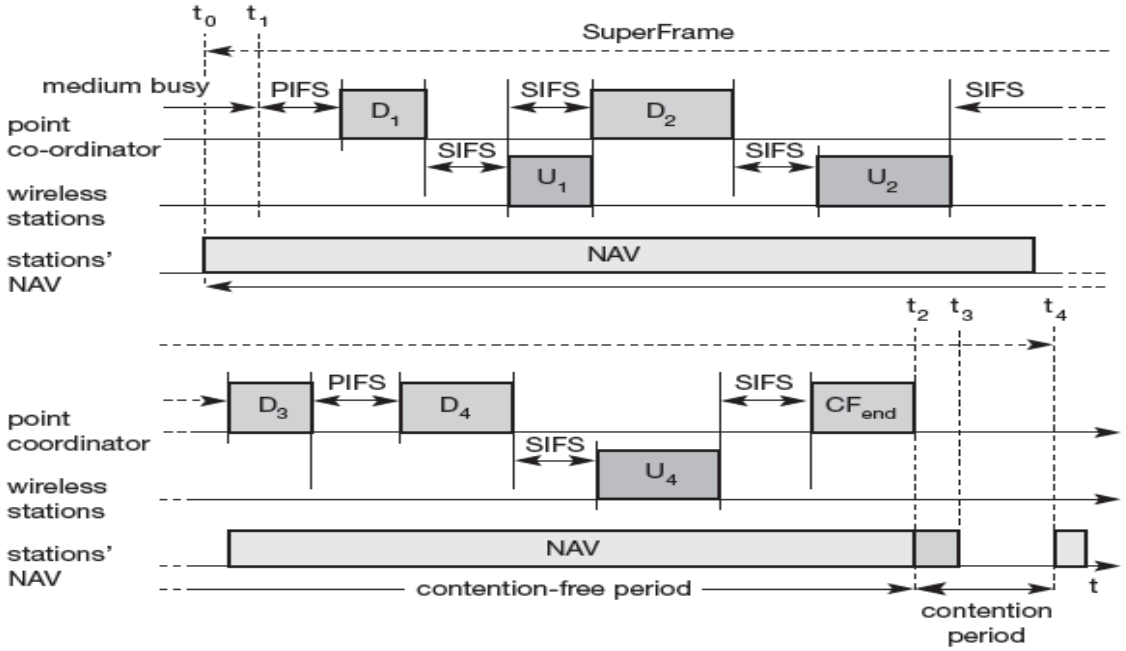


Fig 3.16: Contention-Free Access using Polling Mechanisms (PCF)

The super frame starts from t0 to t4.But the actual period is from t1 to t3 as it has no data from t3 to t4.

The medium needs to be free from t0.But the medium is busy till t1.Hence the contention free periods starts from t1 only.

After waiting for PIFS, the point co-coordinator can access the medium.

As PIFS is smaller than DIFS no other stations can use the medium .The PCF can send data D1 to the first wireless station as round robin. It has to transfer hence replies with U1.

The stations after receiving the data waits for SIFS. The point co-ordinates waits for SIFS and POLLS the seconds station by sending D2.The station may answer to the coordinator with U2 polling. When it has to transfer else remains unanswered. In the above figure D3 has no data hence it remains unanswered.

Merits and Demerits:

- As PCF needs access point the control and poll, Ad hoc network cannot use this function so no QOS but best effort services.
- If only PCF is used and polling is distributed evenly, bandwidth is also distributed evenly resembles TDMA.
- This method has overhead if nodes have nothing to send but access poll them.

3.5.6 MAC Frames:

The MAC frame structure of IEEE802.11 is: The frame control field contains:

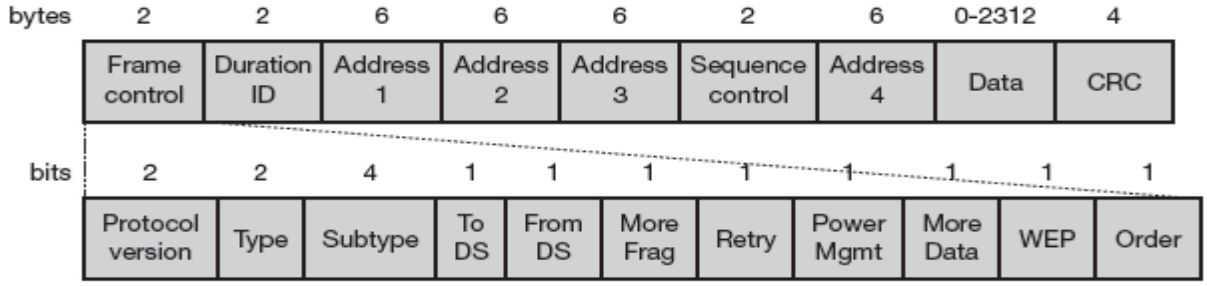


Fig 3.17: MAC Structure

(1) Protocol Versions:

Indicate the current protol version. Now fixed to).

Type: This field determines the functions of the frame. If the representation for the value is

00-Management
01-Control
10-Data
11-Reserved

Each type has several subtypes.

Subtype:

Example:

0000-Association Request
1000-Beacon
1011-RTS
1100-CTS

User Data:

Sub type=0000.

TODS/From DS:

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

The Explanation is that the MAC frames can be transmitted between mobile stations between access points to DS.

More Fragments: Set to 1 for data or management frame.

Retry: This field is set to 1 when the current frame is a retransmissions of a frame.
Power management: This field indicates the mode of a station after successful transmission of a frame.

When value = 1 implies the station goes to power mode.
= 0 the station is active.

More Data: This field is indicates the receiver that the sender has more data to transmit.

This field can be used by access point to inform that station that when it is in the power save mode that the access points has buffered the data for the station.

This can be used by the station to indicate the access point that more polling is necessary as it has more data ready to transmit.

WEP: Wired Equivalent Privacy.

Indicates the security mechanism of 802.11 is applied. But due to weakness of WEP algorithm, higher layer security is needed.

Order: When set, indicate that the received frame must be processed in strict order.

Coming back to MAC

Duration/ID: when the field value is < 32,768 indicates that the value indicates the period of time in which the medium is occupied in μs. when value is >32,768 they are reserved for identifiers.

Address 1 to Address 4: the four address field contain MAC addresses. The meaning of the address depends on the DS bit in the frame control field.

Sequence Control: the sequence number is used to filter duplicates.

Data: the data transmitted is up to a maximum of 2312 byte. Which is transferred transparently from a sender to the receiver.

CRC: finally a 32 bit checksum is used to protect the frame.

3.5.7 Synchronization

What is synchronization?

- Each node is 802.11 network maintains an internal clock.
- To synchronize the clocks of all nodes 802.11 specifies a Timing Synchronization Function (TSF) is used.

Why to have Synchronization?

- The synchronized clocks are needed for power managements of the devices.
- Co-ordination of PCF.
- Synchronization of the hopping sequence in FHSS.

Working principle of how to do synchronization:

Within a BSS the synchronization is done by the quasi periodic transmission of a beacon frame.

- The beacon frame contains a time stamp of the sender and other management function related to power management and roaming.
- The nodes after receiving the beacon frame adjusts its local clock.
- The transmission of the beacon frame is deferred if the medium is busy. Hence it is quasi periodic transmission.

Synchronization in Infrastructure based Network:

- In the infrastructure based network the access point performs Synchronization.

- It transmits the quasi periodic beacon signal, all the other nodes adjust their local timer to the time stamp.

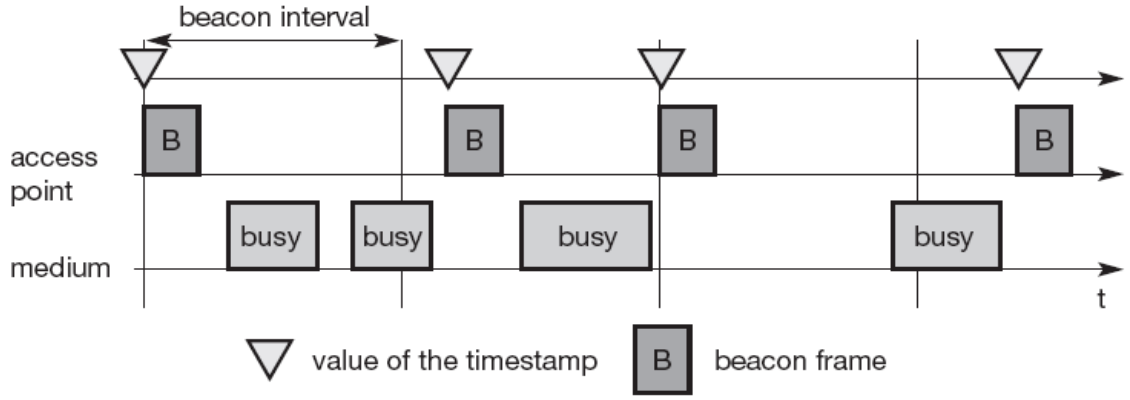


Fig 3.18: Beacon transmission in a busy 802.11 infrastructure network

- In the first interval. And 3rd interval the Ap senses the medium to be idle, transmits the Beacon frame.
- In the second interval and fourth interval.
- The access point defers the beacon frame as the medium is busy.
- But the access point tries to schedule transmissions according to the expected beacon interval (Target Beacon Transmission Time).
  Beacon interval is not shifted if one beacon is delayed.
- The time stamp refers to the real transmit time.
- The Beacon frame has got the time stamp of the AP.

Synchronization in Adhoc Network

- The Synchronization is more complicated as there is no central arbitrar.
- They do not have the access point for transmission of beacon frame.
- Each node starts the transmission of a beacon frame after the beacon interval.
- As more than one compete standard random back off algorithm is applied. Hence only one beacon wins.
- All other stations adjust their internal dock in accordance with the received beacon.
- If collision occurs the beacon is lost. Hence the beacon interval is slightly shifted because all clocks may vary as the start of the beacon interval.

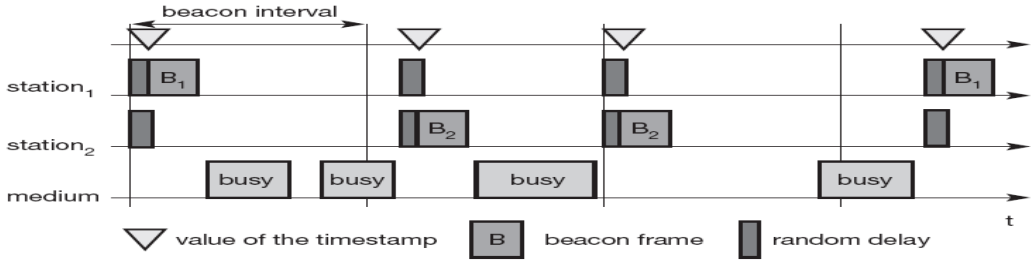


Fig 3.19: Beacon transmission in a busy 802.11 ad-hoc network

- In the above figure station 1 and 2 competes for the medium to transit beacon frame. Station 2 succeeds as it has smaller back off time and transmits its time as time stamp in Cycle1.
- In Cycle 2, Station 1 succeeds the medium and transmits its time as the timestamp.

3.5.8 Power Management

- Wireless devices are battery powered. So powers saving mechanisms are needed for the success of such devices commercially.
- The standard LAN protocols think that the stations are always ready to receive the data, but the receivers are idle most of the time in the lightly loaded networks.
- Hence the standard LAN protocols cannot be used without modifications.
- Basic idea of IEEE 802.11
  Switch-off the transceiver whenever the node is idle.
- To switch on the transceiver in sender in quite easy because transceiving is triggered by the device itself.
- To switch on the receiver is difficult because the receiver cannot know in advance when the node has to wake up.
- Longer off period implies more life to battery but reduces throughput.

Concept:

For power saving the station can be any one state

1. Sleep,
2. Awake.

- Senders need to have buffers to store data for sleeping node.
- The sleeping station needs to wakeup periodically and remain awake for a certain period of time.
- When the nodes are awake, during this time. All the senders announce the destination of their buffered data.
- If a receiver detects that it has a frame. It has to stay awake until the transmission is over.
- To wake up the stations timing synchronization function is needed(previously discussed)
- All stations have to wakeup or be awake at the same time.

Power Management in infrastructure based network

- Power management is simple because of the presence of access points.
- Access points buffers all the frames which are desired for stations in the sleeping mode.
- Along with beacon AP transits TIM (traffic Indication Map) or DTIM (Delivery Traffic Indication Map) is transmitted.

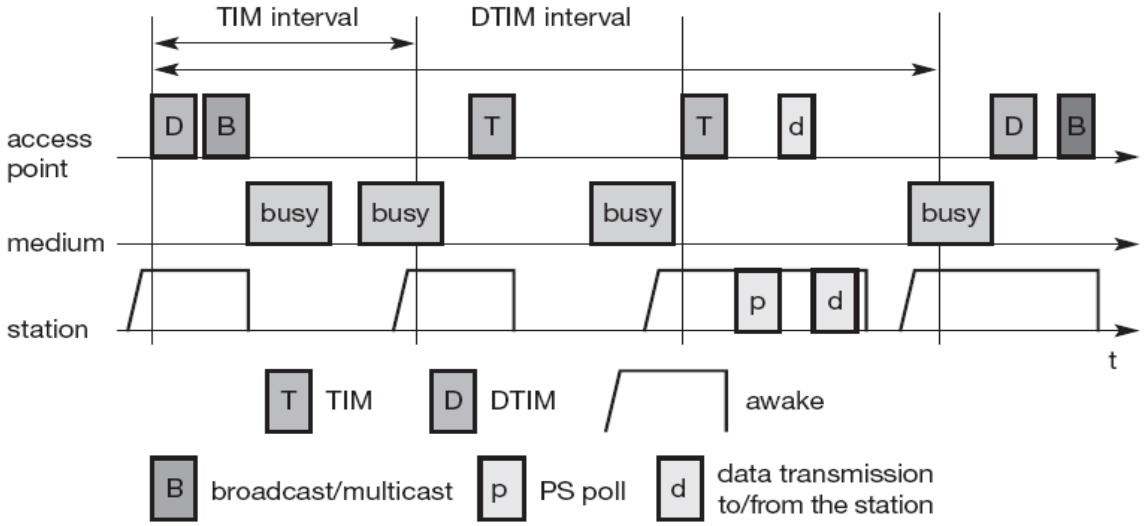


Fig 3.20: Power management in IEEE 802.11 infrastructure networks

- TIM contains to the list of stations for which unicast data is buffered in the access point. DTIM is used to contain the broadcast and multicast frame.
- All the stations wake up prior to TIM/DTIM.
- The Timing Synchronization Function (TSF) assures that the sleeping stations will wake up periodically and listen to the beacon and TIM or DTIM.
- If the station finds its address in the TIM/DTIM then it stays awake for the transmission referring to the above figure.

Interval 1:

The AP transmits DTIM, and the station remains awake to receive the broadcast/multicast frame. After receiving the broadcast frame B the station goes to sleep mode.

Interval 2:

As the medium is bury in the start of the second interval, the AP postpones the transmission of TIM and beacon.

When the medium is idle, AP transmits the TIM. This station address is not present hence the station goes to sleep mode.

Interval 3:

The medium is idle. Hence AP transmits beacon and TIM. The stations address is present in TIM. To inform its awake state the station transmits PS poll to AP.

Then the AP transmits the data to the station.

After the receipt of the data, the station sends back acknowledgment via d to AP.

Interval 4:

AP has a broadcast data to send at the next DTIM interval. DTIM is deferred because the medium is busy.

Power Management in Adhoc Networks:

- Power Management is complicated in Adhoc network because of the absence of AP.
- Hence the station itself need to buffer the data for the sleeping stations. All the station need to be awake at the same time.
- As usual, the station compete to send the Beacon (Synchronize) frame.

- The station which succeeded to send will send the Beacon (Adhoc Traffic Indication Map).
- This ATIM will have the stations to which the data is buffered by the station which sends the ATIM.
- The interval is called as ATCM window.

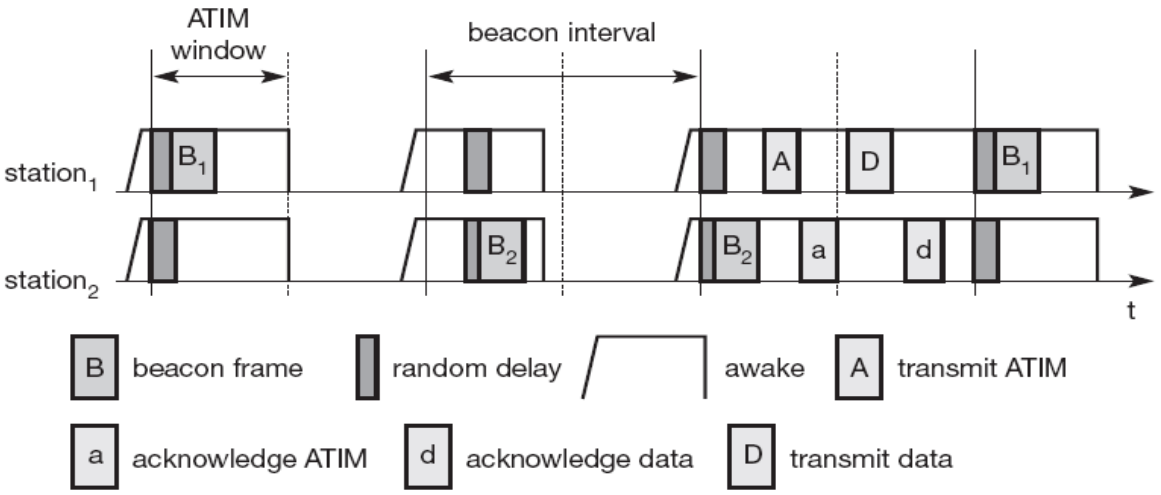


Fig 3.21: Power management in IEEE 802.11 ad-hoc networks

Interval 1:

Station 1 succeeds in sending the Beacon. It has not buffered any frame.

Interval 2:

Station 2 succeeds in sending the Beacon which too has not buffered any frame.

Interval 3:

Station 2 succeeds in sending the Beacon. Station 1 has buffered data to station 2. 1 replies with ATIM to station2. The station 2 acknowledges by sending acknowledgement ATIM (a).

After receiving this acknowledgement Station 1 transmits data.

The station 2 acknowledges the same by sending d.

The stations remain awake in the full interval. Does not enter into sleep mode.

Problems:

1. Does not scale.
2. If many station operate in power save mode all the stations compete to transmit their ATIM within the ATIM within the ATIM window. Which results in collision hence more deferred.
3. Access delay cannot be predicted.
4. QOS cannot be guaranteed under heavy load.

3.5.9 Roaming

- If a user walks around with a wireless station, the station has to move from one access point to another to provide, uninterrupted service.
- Moving between access point is called as roaming is another important function
- Steps needed for roaming between access points.

1. A station decides that the current link quality is too poor9 at present the station is connected to access point AP_1). Hence the station starts scanning for another access point.
2. Scanning mean the active search for another BSS that can be used for setting up a new BSS.

   Scanning can be done on single or multiple channels.

Types of Scanning

1) Passive Scanning: Listening to the medium , to find other networks(i.e.) receiving the beacon of another network which was issued by the access point for synchronization/
2) Active Scanning: sending a probe on each channel and waiting for response. Beacon and probe contain the necessary information to join a new BSS.
3) The station selects the best access points based on scanning. The station sends the association request to the selected access points based on scanning. The station sends the association request to the selected access point AP_2.
4) The new access point AP_2 answers with an association response.
   If the response is successful the station has associated with a new access point. Else to has to continue scanning.
5) The access point indicates the new station in its BSS to the DS. The DS updates its data base which contains the current location of the wireless station.
   The data base is needed for forwarding frames between different CSS.
   DS informs the old access point AP_1, that the station is no longer with in its BSS.

3.6 HIPERLAN

3.6.1 BRAN

In response to growing market pressure for low-cost, high capacity radio links, ETSI European Telecommunications Standards Institute, established a standardization project for Broadband Radio Access Networks (BRAN)in the spring of 1997.

The project prepares standards for equipment providing broadband (25 Mbit/s or more) wireless access to wire-based networks in both private and public environments, operating in either licensed or license exempt spectrum. These systems address both business and residential applications. Fixed wireless access systems are intended as high performance, quick to set up, competitive alternatives for wire-based access systems.

3.6.2 HIPERLAN 1

ETSI BRAN currently produces specifications for three major Standard Areas:

- HiperLAN 1 standard to provide high speed communications between portable devices.
- HiperLAN 2 , a mobile broadband short-range access network
- HIPERACCESS, a fixed wireless broadband access network
- HIPERMAN, a fixed wireless access network which operates below 11 GHz

HiperLAN 1

HiperLAN 1: European Telecommunication Standards Institute, ETSI, ratified in 1996 with High performance Radio LAN (HiperLAN 1) standard to provide high speed communication (20Mbps) between portable devices in the 5GHz range. Similarly to IEEEE802.11, HiperLAN/1 supports isochronous traffic for different type of data such as video, voice, text, etc.

HiperLAN/2

Later, ETSI, in June 2000, gave a flexible Radio LAN standard called HiperLAN 2, designed to provide high speed access (up to 54 mbps at PHY layer) to a variety of networks including 3G mobile core networks, ATM networks and IP based networks, and also for private use as a wireless LAN system, basic applications include data, voice and video, with specific QoS. HiperLAN /2 is used by consumers in corporate, public and home environments wireless access to the Internet and future multimedia,. Easy to install and provide interworking with several core networks including the Ethernet, IEEE 1394, and ATM.HIPERLAN/2 has a very high transmission rate up to 54 Mbps. This is achieved by making use of a modularization method called Orthogonal Frequency Digital Multiplexing (OFDM). OFDM is particularly efficient in time-dispersive environments, i.e. where the radio signals are reflected from many points, e.g. in offices.

HIPERACCESS

THE HIPERACCESS standard is a standard for broadband multimedia fixed wireless access. The HIPERACCESS specifications will allow for a flexible and competitive alternative to wired access networks. It will be an interoperable standard, in order to promote a mass market and there by low cost products.

HIPERACCESS is targeting high frequency bands, especially it will be optimized for the 40, 5 - 43, 5 GHz band.

HIPERMAN

HIPERMAN will be an interoperable broadband fixed wireless access system operating at radio frequencies between 2 GHz and 11GHz. The HIPERMAN standard is designed for fixed Wireless Access provisioning to SMEs and residences using the basic MAC(DLC and CLs)of the IEEE 802.16,such that the HIPERMAN standard and a subset of the IEEE802.16a -2003 standard will interoperate seamlessly. HIPERMAN is capable of supporting ATM, though the main focus is on IP traffic. It offers various service categories, full Quality of Service, fast connection control management, strong security, fast adaptation of coding, modulation and transmit power to propagation conditions and is capable of non-line-of-sight operation. HIPERMAN also supports both FDD and TDD frequency allocations and H-FDD terminals. All this is achieved with a minimum number of options to simplify implementation and interoperability.

3.6.2.1 HIPERLAN1'S Medium Access Scheme

- EY-NPMA [Elimination-Yield Non-Priority multiple Access] is a complex scheme to access the medium which avoids collision.
- EY-NPMA provides priorities and different access schemes.
- EY-NPMA places the competing nodes into 3 phases.

(1) Prioritization: this phase determines the priorities of the packets which are ready to be sent by competing nodes.

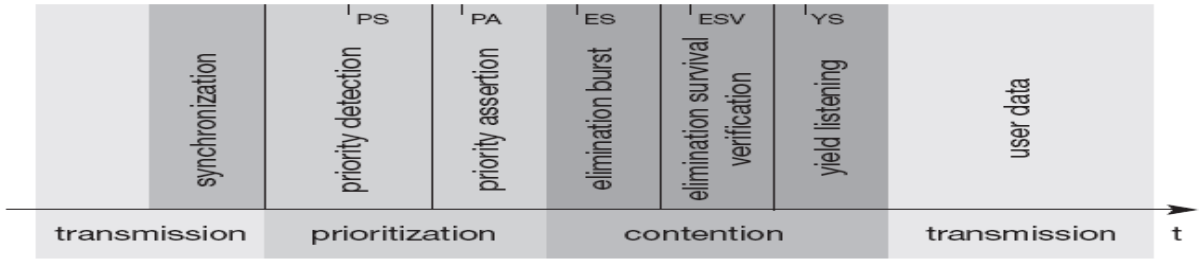


Fig 3.22: Phases of the HYPERLAN 1 EY-NPMA access scheme

(2) **Contention:** This phase eliminates all but one of the contenders in case of tie (if more than one has the highest current priority).
(3) **Transmission:** This phase transmit the packet of the remaining node.

- When many nodes compete for the medium all the three phases are necessary called **channel access in synchronized channel condition.**
- When the channel is free for at least 2000 high rate bit period, dynamic extension then only the third phase is needed called as **channel access in channel free condition Dynamic Extension.**
- Dynamic Extension is randomly chosen between 0-3 times 200 high rate bit period with equal likelyhood.
- Supports channel access in the Hidden elimination condition to handle the problem of hidden terminal.
- For every node ready to send data the access cycle starts with prioritization, contention and transmission.
- Every phase has a certain duration which is measured by slots.
- The prioritization phase is subdivided into priority detection (PS) and priority assertion (PA).
- The contention phase is subdivided into elimination phase and yield phase.

Prioritization phase

- HIPERLAN 1 offers five different priorities for the data packets ready to be sent.
- **Objective 1:**

This ensures that no node with a lower priority gains access to the medium while packets with higher priority are there with other nodes.

Step 1: Priority Detection

The time is divided into five slots, slot0 to slot4. Slot 0 has the highest priority and slot 4 has the lowest priority. Each slot has a duration of IPS= 168 high rate but period.

If a node has the access priority P, it has to listen for P slots into the medium (Priority detection).

Step 2: Priority Assertion.

If the node senses the medium is idle for whole period of P slots, the node asserts the priority. To assert the priority the node immediately transmits a burst for the duration I_{PA}=168 high rate bit period.

The sequence of the burst is 1111 1010 1000 1001 1100 0001 1001 0110.

The sequence can be repeated as many times for the duration of the burst. On the other hand if the node senses the medium is busy, it stops the attempt in this cycle and waits for the next one.

At the end of the prioritization phase one or more nodes with the highest priority will survive and enters the contention phase.

3.6.2.2 Contention Phase

The contention phase is further subdivided into (1) Elimination phase (2) Yield phase

3.6.2.2.1 Elimination Phase

- The purpose of the elimination phase is to eliminate as many contending nodes as possible. The result of the elimination phase is in lesser number of remaining nodes independent of the number of competing nodes that enter the yield phase.
- Several nodes enter the elimination phase.
- Time is divided into slots using the slot interval I_{ES} =212 high rate bit periods.
- The length of the individual elimination burst 0-12 slot intervals long, probability of bursting within a slot is
- The probability $P_E(n)$of an elimination burst to be „n" elimination slot interval long is

  $P_E(n) = 0.5^{n+1}$ for $0 < n < 12$

  $P_E(n) = 0.5^{12}$ for $n = 12$
- The elimination phase resolves contention by means of elimination bursting and elimination survival verification.
- Each contending node selects between 0 to 12 and sends an elimination burst with length ***n*** determined via probabilities and listens to the channel during the verification interval I_{ESv} = 256 high rate bit period.
- A contending node survives elimination phase iff it senses the channel is idle during it survival verification period, else stops its attempt in this transmission cycle.
- The elimination phase will last for the duration of the longest elimination burst among the contending nodes to the survival verification time.
- One or more nodes will survive the elimination phase.

3.6.2.2.2 Yield phase

In this phase the remaining nodes only listen to the medium without sending any additional burst.

Time is divided into slots. Slot is called as yield slot with a duration of Iys = 168 high rate bit period.

The length of the yield listening period can be 0 to 9 slots with equal likelihood.

The probability P_y (a) for a yield listening period to be n slots in 0.1 for all $0 \leq n \leq 9$.

Each node selects between 0 to 9 listen for the whole of its yield listening period. If the node senses the channel is idle for the whole period, the node survives. Else withdraws from the current transmission cycle.

The length of the yield phase in determined by the shortest yield listening period among the contending nodes.

At least one node will survive and can start to transmit data.

Here also more than one node can survive resulting in collision.

3.6.2.2.3 Transmission Phase

- The node has survived the above two phases is ready to transmit data. The data is called low bit rate high bit rate HIPERLAN 1 CAC protocol data unit (LBRHBRHCPDU)
- The PDU can be multicast or unicast.

- For unicast the sender5 expects immediate acknowledgement called HCPDU (AK-HCPDU).

3.7 HIPER LAN 2

3.7.1 General Features of HIPER LAN 2

- Official name HIPER LAN Type 2
- Standardized by ETSI
- Wireless network work at 5 GHZ
- Data rate is 54 MBPS.
- QOS and enhanced security features.

3.7.2 Features of HIPER LAN2

(1) High throughput Transmission:

- Uses OFDM in physical layer.
- Dynamic TDMA/TDD IN MAC protocol.
- Offers data rate of 54 MBPs at the physical layer, 15 MBPS physical layer, 35 MBPS as the network layer.
- The overheads remains constant.
- MAC frame length is 2 ms which is constant.

(2)ConnectionOriented:

before data transmission, HiperLAN2 network establish logical connections between sender and receiver.

- Using the connection setup the QOS parameters are negotiated.
- All connections are TDM.
- Unidirectional, Bi-directional, Broadcast channel are available.

(3) Quality of Service Support:

- As to is connection oriented QOS is simple.
- Each connection has its own QOS parameters.

(4) Dynamic Frequency Selection:

- Does not need frequency planning.
- Access points have built in support which automatically selects appropriate frequency within their coverage area.
- AP"s listen to neighboring AP"s also.
- The best frequency is chosen depending on the interference level and usage of radio channels.

(5) Security Support:

- Authentication and encryption are supported.
- MT and AT can authenticate each other.
- Hence authorized access to the network.
- User data are encrypted using DES TDES /AES.

(6) Mobility Support:

- Mobile Terminals can move around during transmission.
- Handover is performed automatically.
- If enough resources are available the QOS will be supported.
- But some packet will be lost during handover.

(7)Application and Network Independence:

- Hyper LAN was designed for various applications and it"s not network specific.

(8)Power Save:

- Mobile Terminals can have certain wake up pattern to save power.
- During the sleep period show latency or low power can be supplied.

3.7.3 Reference Model and Configuration

Standard architecture of an infrastructure based HiperLAN2.

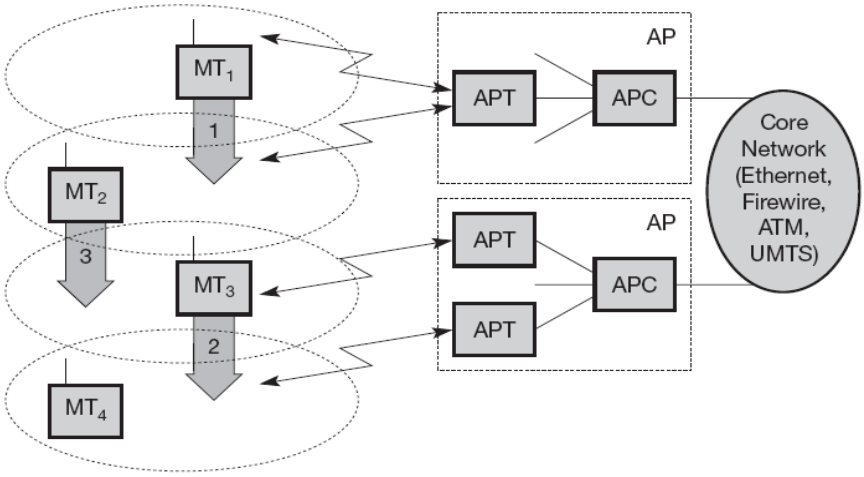


Fig.3.23:HiperLAN2 basic structure and scenarios

- In the figure there are access points AP which is attached to the core network.
- The core network can be Ethernet LAN or ATM network or UMTS.
- The Access points has an Access Point Controllers (APC) and one or more Access Points transceiver (APT).
  - APT can have one or more sectors or cells.
  - Four mobile terminals are present.
  - MT"s can move around the cells.
  - The system automatically assigns the APT/AP with best transmission quality.
  - As it uses dynamic frequency selection (DFS) no frequency planning is needed.

3.7.4 Handover Situations in Hiper LAN2

(1) Sector Handover:

- If the sector antennas are used for an AP this type of handover is supported.
- This type of handover is handled inside the DLC layer, hence not visible outside AP.

(2)Radio Handover :(Inter APT/Intra AP)

- This handover is also handled within AP; hence no external interaction is needed.

- All context data is needed for connection is already in the AP hence no negotiation.

(3)Network Handover :*(* Inter AP /Intra-network)

- Complex situation of handover
- Here the core network and higher networks are also involved.
- Handover must be supported by core network.

3.7.5 Modes of operation in Hiper LAN2

Hiper LAN network operate in two different modes. They are

(1) Centralized Mode :

- Infrastructure based mode
- All AP"s are connected to core network
- MT"s are associated with AP"s
- If two MT share cell, all the data is transmitted via AP.
- AP takes complete control.

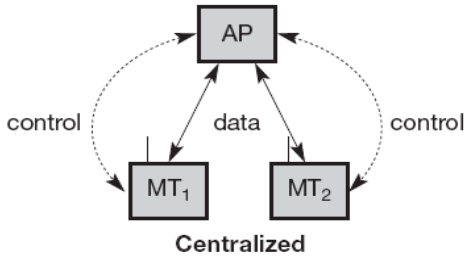


Fig.3.24: Hiper LAN2 centralized mode

(2) Direct Mode:

- Adhoc mode of Hiper LAN2
- Data is exchanged directly between MT"s if they can receive each other
- Network is controlled by AP which contains central controller

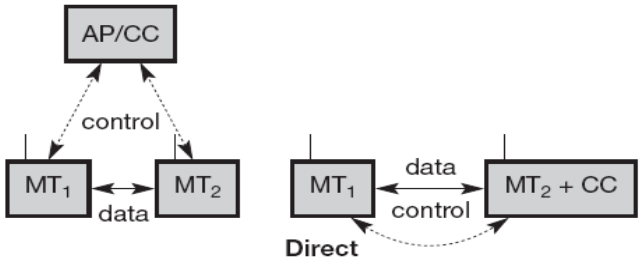


Fig. 3.25: Direct mode

3.7.6 Hiper LAN2 Protocol Stack

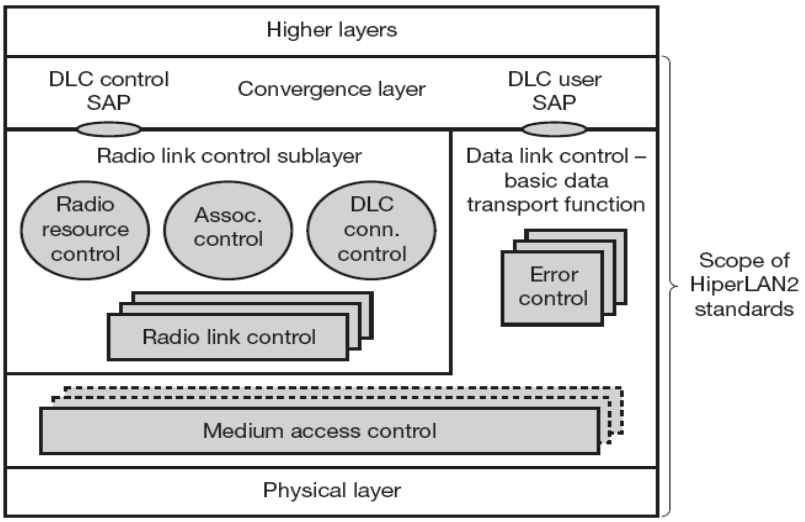


Fig. 3.26: Hiper LAN2 protocol Stack

- The figure shows the Hyper LAN2 protocol stack.
- The lowest layer is the Physical layer. This layer handles the functions of modulation, FEC, signal detection etc.
- The next higher layer is the data link control. This layer contains the MAC function, RLC sub layer and error control functions.
- If AP has several APT each APT has its own MAC instances.
- The MAC of an AP assigns each MT a certain capacity to guarantee connection quality.
- The DLC is divided in to a control and user part .The user part contains error control mechanisms.
- Hiper LAN2 offers reliable transmission using acknowledgments and retransmissions.
- The Radio Link Control (RLC) has the control functions.
- The Association Control Function (ACF) controls association and authentication of MT"s.
- The DLC user control connection DCC or DUCC service control connection setup, modification and release.
- Radio Resources Control (RRC) does the handover functions for Inter AP and Intra AP.
- On the top of OLC there is convergence layer .This does the segmentation and reassembly functions, adoptions to fixed LAN , 3G network.

3.7.6.1 Physical Layer

The figure shows the physical layer reference configuration.

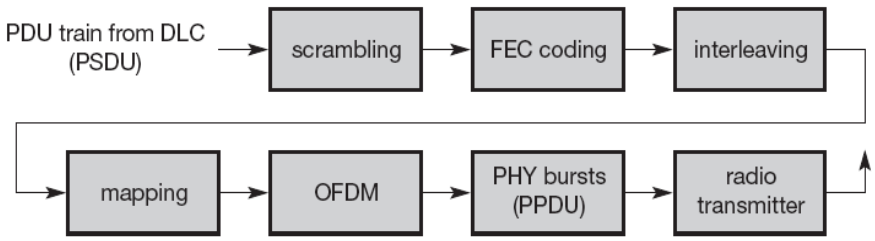


Fig. 3.27: HiperLAN2 physical layer reference configuration.

- The first Step is scrambling of all data bits with generator polynomial x^7+x^4+1 for DC blocking and whitening of spectrum .The output is scrambled bits.
- The next step is FEC coding for error protection coding depends upon the
  (i) Type of data,
  (ii) Uses of sector
  (iii) Omnidirectional antennas
  Output is encoded bits
- Third step is interleaving.
  - This phase is done for mitigation of frequency.
  - For this selective fading interleaving is applied.
  - Output is that adjacent encoded bits are mapped onto non-adjacent subcarriers.
  - Adjacent bits are mapped onto MSB of the constellation.
  - Thus we get interleaved bit
- Fourth step is mapping
  - This process divides the bit sequence in groups of 1,2,4,6 bits depending on the
  - modulation scheme.
  - The groups are mapped onto the appropriate symbol of modulation.
  - Output is that subcarrier modulation symbol.
- Fifth step is OFDM modulation
  - Converts these symbols into baseband signal with the help of inverse FFT.
- The final step is creation of PHY bursts.
  - Each burst has a preamble and a payload.
  - Five types of PHY buses are defined Broadcast, Downlinks, and Uplink with short
  - preamble, uplinks with long preamble and direct link.
- The last step is radio transmission
  - Shifts the baseband signal to a carrier frequency depending on the channel number and formula.

3.7.6.2 Data Link Control Layer

- The DLC layer is divided into MAC, control and data part
- The MAC creates frames of 2 ms duration.
- Each frame is divided into 4 phases with variable boundaries.

Structure of MAC Frame:

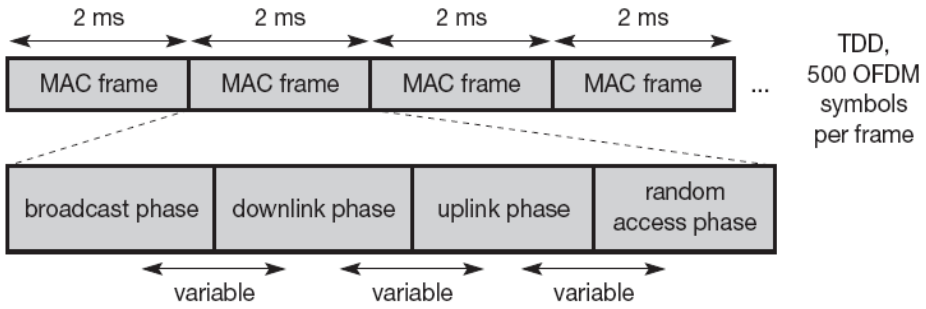


Fig. 3.28: Structure of HiperLAN2 MAC frame

The phases are

Broadcast phase: The AP of a cell broadcasts the content of the current frame plus information about the cell.

Down Link Phase: Transmission of user data from AP to MT.

Uplink Phase: Transmission of user data from MT to AP.

Random Access Phase: Capacity requests from registered MT and access requests from non-registered MT are considered.

Direct Link Phase:

- This is an optional Phase.
- Inserted between downlink and uplink phase.
- The access point to common physical medium is controlled by CC.

3.7.6.3 Transport Channels

HiperLAN2 defines 6 Transport channels for the data transmission.

The channels are

(1)Broadcast Channel: (BCH)

- The Broadcast channel conveys basic information to all MT.
- Identifiers the current transmission power of AP.
- Channel contains pointers to FCH, RCH which gives flexible structure of MAC
- frame.
- Length is 15 bytes

(2)Frame Channel: (FCH)

- Contains the directory of the downlink and uplink phases
- Has the PHY mode used
- Length is multiples of 27 bytes.

(3)Access Feedback Channel: (ACH)

- Channel gives the feedback to MT regarding the random access during the RCH of the previous Frame.
- The access during the RCH is based on slotted aloha, hence collision at AP occurs.
- ACH signals back which slow was successfully transmitted.
- Length is 9 bytes.

(4)Long Transport Channel: (LCH)

- Channel supports user and control data for downlink and uplink length is 54 bytes.

(5) Short Transport Channel: (SCH)

- Channel transport control data for downlink and uplink.

(6)Random Channel:

- Channel gives the MT the opportunity to send information to the AP/CS even without a granted SCH.
- Here the access is via slotted Aloha hence collisions occur.
- Collision is resolved by exponential back off scheme.
- Length is 9 bytes.
  - BCH, FCH and ACH can be used in broadcast phase only
  - Use BPSK with code rate ½.
  - LCH, SCH can be used in downlink, uplink, direct link phase.
  - RCH is used in the uplink phase for random access. Use BPSK code rate ½.

3.7.6.4 Logical channels

- Data between entities of DLC layer are transferred over logical channels
- Logical is another name to any district data path
- The type of logical channel is defined by the type of information it carries, and the interpretation of the values in the messages. Classification of logical channels.

(1)Broadcast control Channel: (BCCH)

- This channels on the downlink coveys a constant amount of broadcast information concessing the whole radio cell.

(2)Frame control Channel: (FCCH)

- FCCH describes the structure of the remaining parts of MAC frames
- Contains resource grant for SCH and LCH
- Resource grant contains MAC address, the number of LCH and SCH, PHY modes.
- Reservation of medium with required QOS is permissible.

(3)Random Access Feedback Channel: (RFCH)

- Channel informs MT"s that have used an RCH in the previous frame about the success of their access attempt.

(4)RLC Broadcast Channel: (RBCH)

- Channel transfers information about RLC control information, MAC ID, information from convergence layer, seas for the encryption function.

(5)Dedicated Control Channel: (DCCH)

- Carrier RLC message related to a certain MT
- Channel is established during association of an MT

(6)User Broadcast Channel: (UBCH)

- UBCH transfers broadcast messages from the convergence layer.
- Transmission is performed in the unacknowledged or repetition mode.

(7)User Multicasts Channel: (UMCH)

- Channel performs unacknowledged transmission of data to group of MT"s

(8)User Data Channel (UDCH):

- Point to point data between AP & MT or between 2 MT"s
- Error control via ARQ.

(9)Link Control Channel (LCCH):

- Bi-directional channel.
- Conveys ARQ feedback and discards messages between error control function of an AP and MT.
- LCCH is assigned to UDCH.

(10)Association Control Channel:

- Channel is used only in uplink
- Used with non-associated MT
- This is used as new association request or handover request.

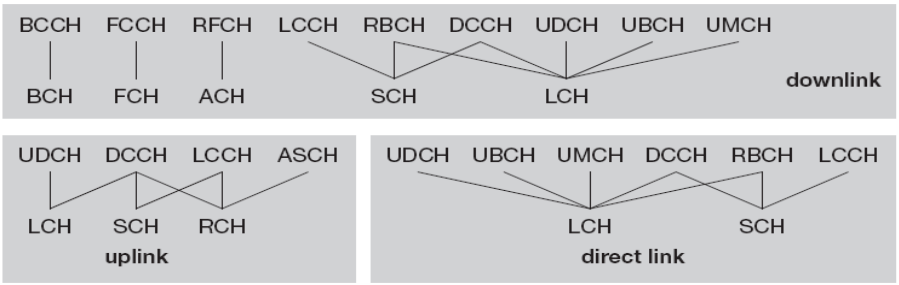


Fig. 3.29: Mapping of logical and transport channels

3.7.6.5 Radio Link Control

- RLC sub layer is connection oriented system offer QOS.
- ETSI has defined 3 main services for the RLC sub layer.

(1)Association Control Function:

- ACF contains all the procedures for association, authentication and encryption.
- MT starts the association procedure
- MT sends the synchronization with a beacon (guide) signal is transmitted in each BCCH of a MAC frame.
- The network ID is obtained via RBCH
- The second step is obtained via MAC ID assignment. This unique ID is used to
- address the MT. From here onwards all RLC control messages are transmitted via DCCH.

Then comes link capability negotiations support of convergence layer, authentication encryption procedures are exchanged.

Based on these parameters the following take place

(1) Encryption start up
(2) Authentication and encryption procedures
(3) Obtaining the ID of MT.

- If all the steps are successful the MT is associated with the AP.
- Disassociation takes place at any time either explicitly or implicitly
- The AP may send MT, alive message to check if an MT is still available.

(2)Radio Resource Control

- Important function of the RRC is handover support

- Each associated MT measures the link quality
- To find handover candidates the MT checks other frequencies
- If one transceiver is available, MT announces the AP that is temporarily unavailable.
- Based on the radio quality an AP can be change carries frequency dynamically.
- RLC has the procedure to inform all MT"s
- To minimize the interference power control must be done by RRC
  - Power saving by MT can be done by negotiating with AP, sleeping period of x MAC frames.
  - After x MAC frames the MT wakeup. The MT wakes up via data ready to be sent or The AP signals data to be received.
- If MT misses the wakeup message from AP to starts the MT alive procedure.
- If no data has to be transmitted the MT goes sleep phase for frames.

(3)DLC User Connection Control (DCC or DUCC):

- This service is used for setting up, realising or modifying unicast connections
- Multicast and Broadcast connections are implicitly setup by a group join during the association procedure.

3.7.6. Convergence Layer (CL)

The convergence layer is needed to adopt the special features of the network protocols.

- HiperLAN2 supports 2 types of CL.

(1)Cell based CL : This layer expects the data packets of fixed size.

(2)Packets based CL: This layer expects the data packets of variable size.

As the packet is of variable size, segmentation and reassembly is needed.

Examples of convergence layer are

(1) Ethernet,
(2) IEEE 1394,
(3) ATM.

3.7.7 Services offered by HIPERLAN

- Speciality services is its QOS

The QOS depends upon 3 parameters called HMQOS parameters. They are:

- The user can set priority for data
  - Priority=0 implies high priority
  - Priority=1 implies low priority
- The user can determine the life time of an MSDU to specify time bounded delivery.

The **MSDU lifetime** specifies the maximum time that can lapse between sending and receiving an MSDU.

The MSDU life time can range between 0-16000 MS.

- The residual life time shows the remaining life time of a packet.
- MAC offers looking up other HIPERLAN within the radio range.
- Power conservation
  - Power conservation is achieved by setting up recurring patterns when a node can receive data.

- MAC offers encryption and decryption
  - The data is XOred with random numbers, key is chosen from a key identifier and key identifier has a set of keys.
- Decryption is done via versa.
- The important function is how MAC selects the next PDU for transmission.

The selection depends upon priority and residual lifetime.
The MAC maps this information onto a channel access priority used by CAC competing with other nodes to transmit.
The MAC determines the normalized residual life time (NRL)

$$NRL = \frac{\text{Lifetime}}{\text{Estimated no. of hopes the PDU has to travel}}$$

The final selection depends upon

(1) HMPDU with the highest priority
(2) Among these the HMPDU with shortest NRL is selected
(3) Finally one without further preference is selected from the remaining.

3.8 Blue Tooth

Bluetooth is an industry specification for short-range RF-based connectivity for portable personal devices with its functional specification released out in 1999 by Bluetooth special Interest Group. Bluetooth communicates on a frequency of 2.45 gigahertz, which has been set aside by international agreement for the use of industrial, scientific and medical devices (ISM). One of the ways Bluetooth devices avoid interfering with other systems is by sending out very weak signals of 1 milliwatt. The low power limits the range of Bluetooth devices to about 10 meters, cutting the chances of interference between a computer system and a portable telephone or television.

Bluetooth makes use of a technique called spread-spectrum frequency hopping. In this technique, a device will use 79 individual, randomly chosen frequencies within a designated range, changing from one to another on a regular basis. Bluetooth devices essentially come in two classes, both using point-to-point communication to speak. Classes 3 devices operate at 0 dBm range and are capable of transmitting 30 feet, through walls or other objects and other class are termed as class 1 product. These devices operate at 20 dBm, which allows for the signal to travel about 300 feet through walls or other solid objects. Bluetooth classes are rated at travelling at about 1 Mbps, with next generation products allowing anywhere from 2 to 12 Mbps.

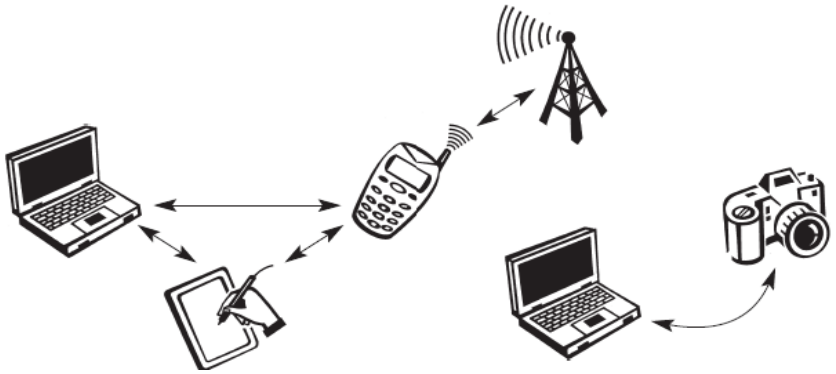


Fig. 3.30: Example configuration with a Bluetooth-based piconet

3.8.1 Introduction

A study group under IEEE 802.11 discussed wireless Personal Area network under the following criteria for Bluetooth.

(1) Market Potential :
What is the market for the available technology?

(2) Compatibility:
Compatible with IEEE 802.

(3) Distinct Identity:
Topic like low cost, low power which is not addressed in 802.11 is addressed.

(4) Technical Feasibility:
Building of prototypes was considered important.

(5) Economic Feasibility:
The cost should be cheaper than the existing one.

3.8.2 Uses of Wireless PAN (or) PICONETS

(1)Connection of Peripheral Devices:

- Now the trend is that the devices are connected to the system without wires.
- They need battery for power supply.

(2)Support of ad hoc Networking:

- To build the network for short duration without any plan Bluetooth can be used.
- Because small devices may not have WLAN adapters.
- Hence it can be done via Bluetooth.

(3)Bridging of Networks:

- Using Piconets a mobile phone can be connected to laptop.
- Mobile phones cannot have full WLAN adapters, hence is needs a Bluetooth.

The main goal of Bluetooth when compared with WLAN technology is that provide local wireless access at very low cost.

3.8.3 Key Features of Bluetooth

- Operates on 79 Channels in 2.4 GHz band with 1 MHz carrier spacing.
- Frequency hopping is the rate of 1600 Lops/sec.
- Applies FHSS for interference mitigation.
- Important Terminology is Pi-conet.

Piconet:

A piconet is a collection of Bluetooth devices which are synchronized to the same hopping sequence of the master.

- One device in the piconet act as a master (M).
- Other devices are connected to the master as slave.
- The master determines the hopping pattern in the piconet and the slave has to synchronize to this pattern.
- Each piconet has a unique pattern
- If a device needs to participate it has to synchronize to this pattern.

Two additional types of devices are present in the pi-conet.

(a)Parked devices (P): They are the devices which cannot actively participate in the pi-conets but can be reactivated.

(b)Standby devices (SB): Devices which do not participate are called standby devices.

- Each pi-conet can have one master and 1 to 7 slaves, 7200 Parked devices.
  - The reason behind the upper limit on the slave is that 3 bit addressing is used in Bluetooth.
  - If any one of the parked devices needs to communicate, then the one of the seven active slaves should switch to the parked mode so that the parked mode device can be made active.

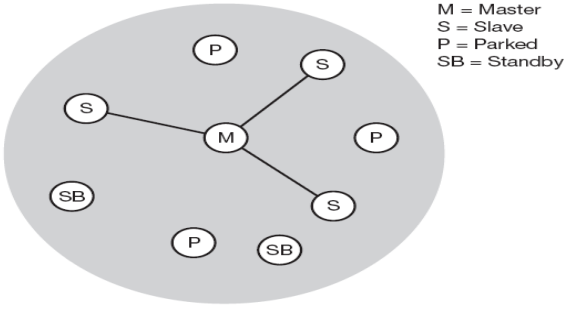


Fig. 3.31: Simple Bluetooth Piconet

Formation of Piconet:

1) Master sends its clock and device ID to all other nodes as hopping sequence.
2) All the Bluetooth devices either master/slave or terminal/base station with the same hopping sequence from a pi-conet.
3) The unit which sends the clock becomes the master and others are slave.
4) The hopping pattern is determined by the device ID which is 48 bit unique identifier worldwide.
5) The phase in the hopping pattern is determined by master clock.
6) A node can adjust its internal clock in accordance with the master clock and become a member of piconet.
7) All the active devices are given 3 bit active member address (AMA)
8) Parked devices has 8 bit parked member address (PMA)
9) Standby devices do not need address

Thus piconet is formed.

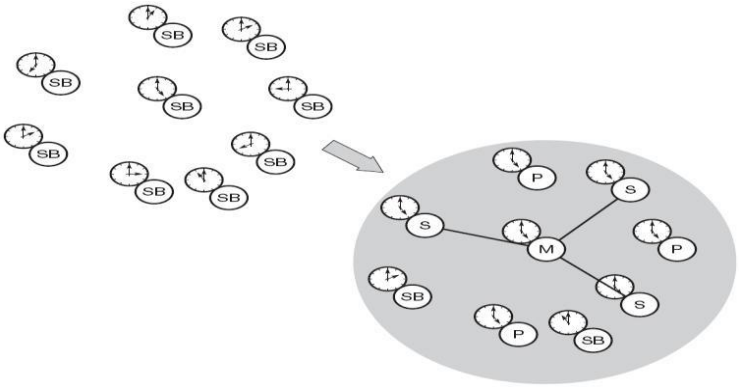


Fig. 3.32: Forming a Bluetooth Piconet

- All the users within one piconet have the same hopping and share the same 1 MHz channel.
- When more units join the pi-conet the throughput decreases.
- To overcome that disadvantage scatternet was formed

Scatter net:

- Groups of pi-conet are called scatter net. The units which are in need of real data exchange share the same piconet.
- Hence many pi-conets with overlapping can exist simultaneously.
- A device can participate in more than one piconet. Under that scenario it has to
- synchronize to the hopping sequence of the piconet it wants to participate.
- After synchronization it acts as a slave in that piconet.
- Before leaving the piconet a slave informs the current master that will be unable for a certain amount of time.
- The remaining devices in the pi-conet communicate as usual.
- The master can also leave the pi-conet and act as a slave in another piconet.

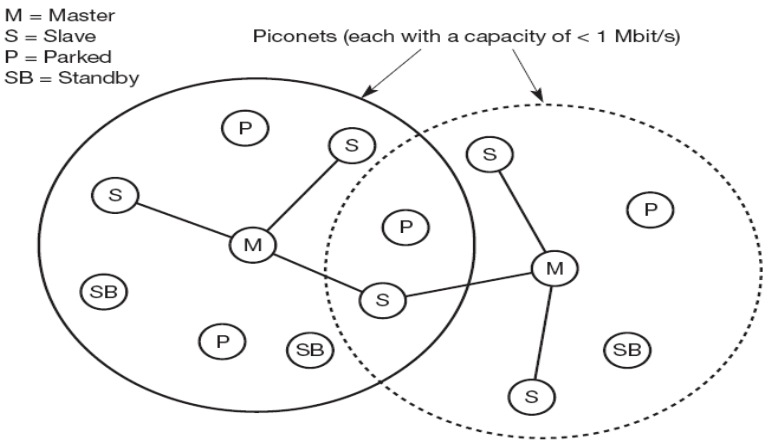


Fig 3.33 Bluetooth Scatternet

As soon as the master leaves a pi-conet all traffic with in this pi-conet is suspended until the master returns.

Communication between different pi-conets takes place by device jumping between the nets.

3.8.4 Protocol Stack

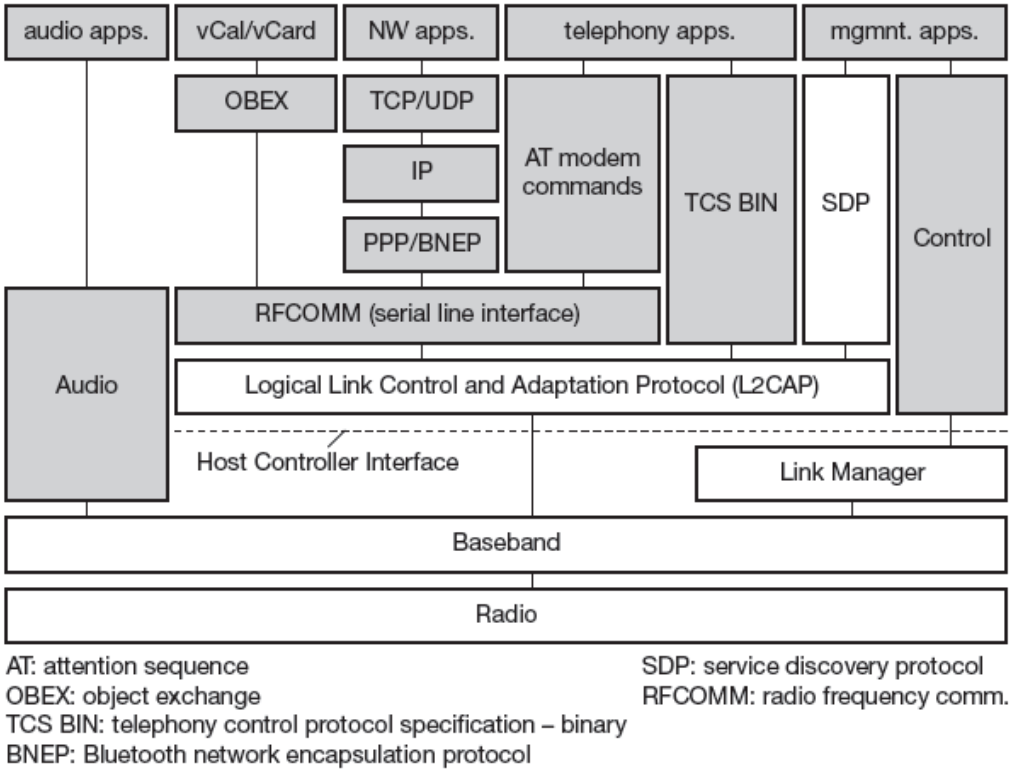


Fig 3.34: Bluetooth protocol stack

The Bluetooth Protocol stacks can be divided into

(a) **Core Specification**: Describes the protocol from physical layer to the data link layer along with management function.

(b) **Profile Specification**: Describes the protocol and functions needed to adapt the wireless technology to legacy and new application.

The core protocol comprises of

(1) Radio: This deals with frequencies, modulation and transmits power.

(2) Base band: Describes the basis of connection establishment, packet formats, and timing and QOS parameters.

(3) Link manager protocol: Deals link setup and management between devices including security function and parameter negotiation.

(4) Logical link control and Adaptation protocol (L2CAP): Deals with adaptation of higher layers to the base band.

(5) Service discovery protocol: Deals with device discovery in close proximity and query service.

Profile Specification protocols

(1) On the top of L2CAP is the cable replacement protocol RFCOMM

- This emulator A serial interface following the E/A-232 which was early called as RS-232

- This allows A simple replacement of serial line cables and allows other protocols to run over Bluetooth.
- RFCOMM supports multiple serial ports.

(2) The telephony control protocol specification llurairy (TCS BIN) specifies a bit oriented protocol which defines call control signal and establish voice and data calls between devices.

(3) The host control interface (HCI) between the base band and L2CAP, provides the interface to the base band controller and link manager. Access to hardware status and control registers.

- The real difference between other protocols and that of this that blue tooth supports audio.

3.8.4.1 Radio layer

- Radio layer define the carrier frequencies and output power
- Blue tooth devices will be integrated into mobile devices and rely on battery power
- Hence small, low power chips are needed to build into hand held deices.
- Blue tooth has to support multimedia data.
- Blue tooth uses license free frequency band at 2.4 GHz
- Hoping rate 1600 hops/sec.Time between two hops is called slot and interval is 625ms
- Blue tooth uses 79 hops
- Transceivers use Gaussian FSK for modulation available in 3 classes:

Power Class 1 : Maximum power in 100 MW
Minimum power is 1 MW
Power control is mandatory
Power Class 2 : Maximum power in 2.5MW
Nominal Power is 1 MW
Minimum power is 0.25 MW
Power control is optional.
Power Class 3 : Maximum power in 1 MW

3.8.4.2 Base band Layer

- Complex layer
- Function: Perform frequency hopping for interference mitigation and medium access, defines physical links and packet formats
- Packet is called 1 slot, 3 slot and 5 slot. 1 Slot: A packet is called one slot when the data transmission uses one 625 ms Slot
- Within each slot the master or one of 7 slaves transmit data
- 3 Slot/5 Slot: If the data transmission covers 3 or 5 slot then it is called as 3 Slot/5 Slot. When the master / slave use 3 or 5 slots the radio to the receiver remains in the same frequency.
- After transmission the radio returns to the frequency required for hopping because every slave will not have transmission, and cannot react on multi bit transmission.
- The slave who is not involved in transmission remains in the hopping sequences.
- This is needed for synchronization.

The component of a blue tooth packet at base band layer

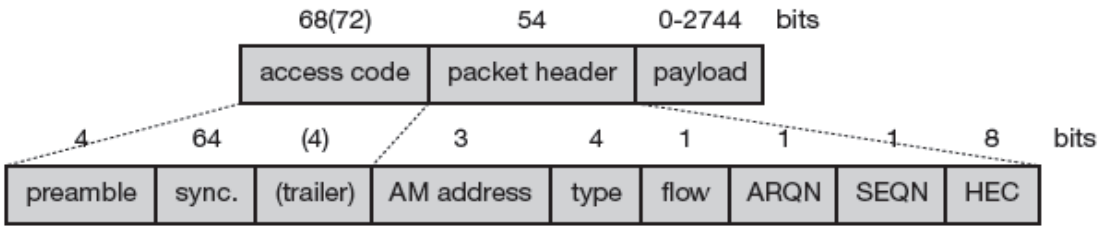


Fig 3.35 Baseband packet format

- This is needed for synchronization. Each device in the Pico net has the same hoping sequence and uses the same carrier frequency. Hence TDD is used for separation of trans mission of data.
  The explanation of the above format is:

Access code

- This packet is needed for timing synchronization and Pico net identification.
- Represent special code during paging.
- The access code consists of

4 Bits	64	4
Preamble	Sync	Trailer

Fig 3.36: Access code

Preamble: synchronization and trailer
Trailer is present if the packet header follows:

- The synchronization field 64 Bits is derived from the lower 24 bit of the address
- If the access code is used for channel access LAP derived from unique 48 bit address

Packet Header
This field has

3	4	1	1	1	8
AM Address	Type	Flow	ARQN	SEQN	HEC

Fig 3.37: Packet Header

This field contains
Address, Packet type, flow, error control, checksum

AMA Address:
The 3 Bit active member address represents the active address of the slave.

- The active address is temporarily assigned to A slave
- Only the master can communicate with the slave
- Value 0 is used as broadcast address.
- Type packet: Type field determines the type of packet can carry control , synchronous or asynchronous data.

Flow:
This field is used for asynchronous traffic
The flow bit = 0 implies asynchronous data; transmission must stop.
The flow bit = 1 implies transmission may resume.

- Alternating bit protocol with SEQN and ARQN can be used

ARQN= Acknowledgement power
HEC: 8 bit header error check

- Used to protect the header
- The header is protected by 1/3 FEC code

For 18 bit header 54 bits are needed.

Pay load

343 bytes of payload can be transferred. the structure of the payload depends upon the link.

Blue tooth offers two types of links

- Synchronous connection oriented
- Asynchronous connection less link

Synchronous connection oriented link

- Used in classical telephone connection for voice
- For this link the master reserves two consecutive slots (forward and return) at fixed intervals
- Master can support three simultaneous SCO links to the same slave or different slaves.
- A slave supports up to two links from different master
- IN SCO three types of single slot packets can be forwarded.
- Each links carries voice at 64 kbps and no FEC,2/3 FEC,1/3 FEC. 1/3 implies FEC Headers and triple the amount of data.
- Voice data is never retransmitted. But continuous variable slope delta is applied on robust voice encoding scheme.

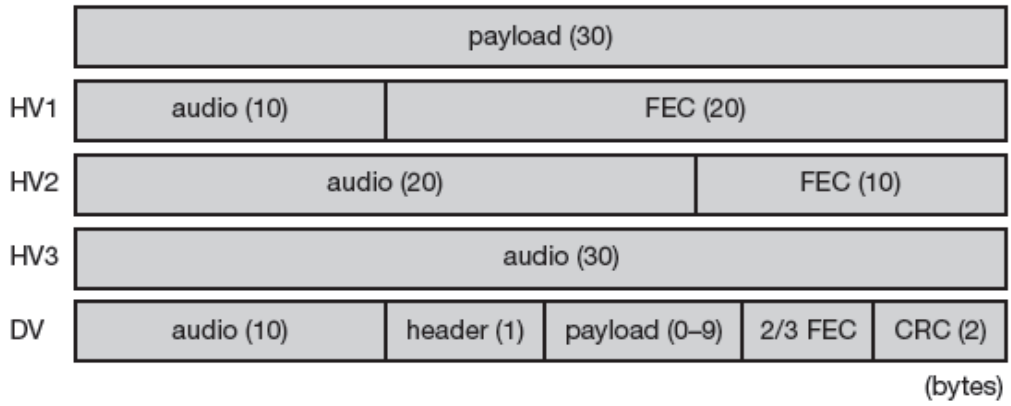


Fig 3.38 SCO payload types

Asynchronous connection oriented link

- Certain application need symmetrical or asymmetrical, packet switched point to multipoint transfer.
- The mater using polling
- A slave may answer if has used the proceeding slot
- Only one ACL can be between master and slot
- For data can be 1 slot, 3 slot or 5 slot packets are used
- The overhead by FES is very high
- Reliable transmission by ARQ
- The payload header Contains an id for logical channel between L2CAP entities

- Payload is always CRC protected

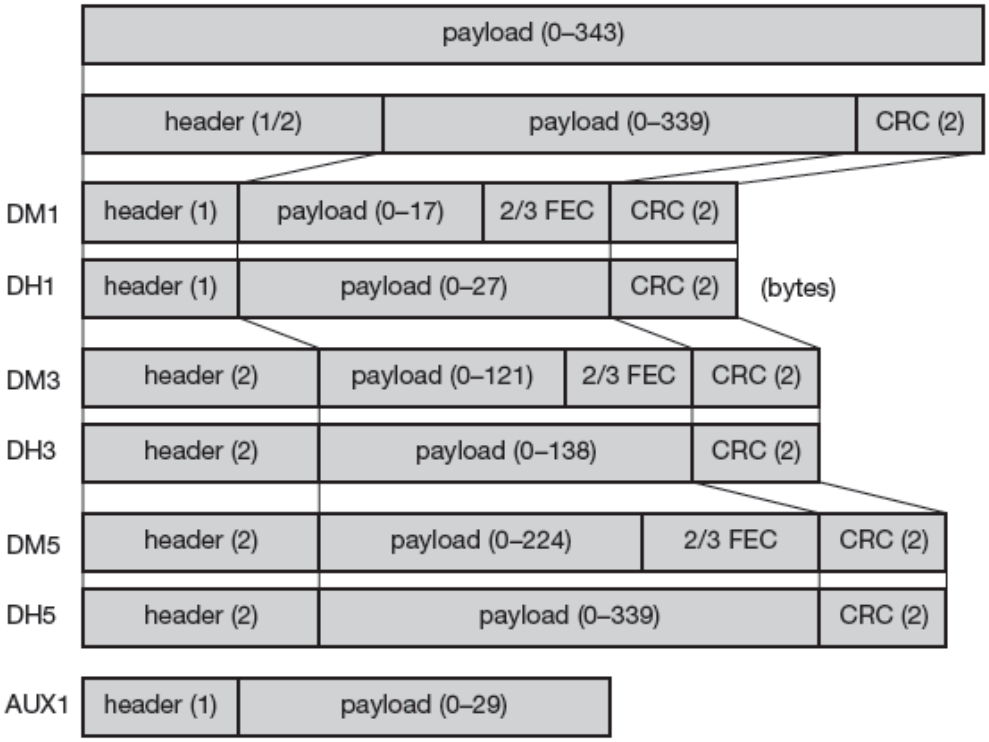


Fig 3.39: Asynchronous connection link payload types

3.8.4.3 Link Manager Protocol

Manages the aspect of radio link between master and slave.

Function covered by LMP:

Authentication pairing and expansion:

- Basic authentication is handled by base band
- LMP has to control the exchange of random number and signed responses.
- Pairing service is needed to establish an initial trust
- The result is a link key

Synchronization:

- Precise Synchronization is major importance
- Clock offset is updated each time a packet is received from the master
- Devices exchange timing information between 2 adjacent Pico nets

(1) Capability negotiation

- Version LMP can be exchanged
- Information about the supported features

(2) Quality of service negotiation

- Parameters control the QOS are poll interval, latency, transfer capacity
- No. of Repetitions for broadcast packets are controlled
- Master can limit the number of slots available for slave

(3) Power control

- Device can measure the received signal strength
- Depending on this strength the device can direct the sender to increase or decrease the transmit power.

(4) Link supervision

- The LMP has to control the activity of link. It may set up new SCO or declare the link as a failure.

(5) State and transmission mode change

- Device changes its role (master or slave) /its mode (unconnected, connecting, and connected).

3.8.4.4 Major states of a Blue Tooth Device

I Stand by Mode

- Any device which is not currently not participating in A Pico net is in standby mode. This is the low power mode 1 only the native clock is running.

II Inquiry mode

- A device in A standby mode can enter into the inquiry mode (for getting connected to the Pico net)

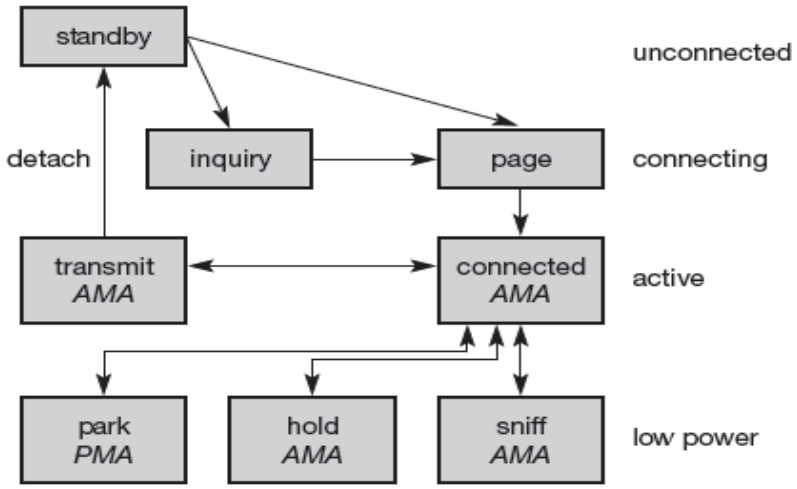


Fig 3.40: Major baseband states of a bluetooth device

For getting connected the device may follow either.

(1) A device want to establish A piconet and act as A master

- Here the user of a devices scans for other devices in the radio range
- The user starts the procedure by sending IAC (Inquiry Access Code)
- This IAC is broadcasted via wake up carrier. (Or)

(2) Devices in the standby mode listen periodically and act as slave

- The devices in the standby mode may enter periodically the inquiry mode
- The devices searches for IAC message on the wakeup carrier
- When the devices detects its address asks the master to initiate the connection
- Here onwards the device is a slave

Page mode: This mode is also a part of getting connected.

- If the inquiry was successful the device enters a page mode
- The page mode is not coordinated Hence collision occurs
- After collision the device finds all the other devices in the radio range
- When A device is in the page mode two roles are defined.

Role 1: After finding all the required devices the master sets up he connection

- Based upon the addresses the master calculate hopping sequences

- The slaves synchronize with the master clock

Role 2: The master continue to page more devices that will be added to the Pico net

III Connection state

The connection states consists of

(1) Active State (2) Low power states

Active State

- The slave participate in the Pico net by listening , transmitting and receiving .
- ACL And SCO link can be used
- Master periodically synchronizes with all slaves
- Active devices will have active Member address
- The active state devices can transmit or simply connected
- From here the device can go to stand by mode via detach procedure.

Low Power states

A blue tooth device can be in one of the three low power states.

(i) Sniff state

- This state has the higher power consumption of the low power states
- The device listens to the piconet at reduced rate at different slots
- The interval for listening depends upon the application and can be programmed
- The device keeps the AMA

(ii) Hold state:

- The device does not release the AMA
- Stops ACL Transmission
- Slave exchange SCO Packet
- If there is no activity the slave reduce the power consumption or move to other piconet

(iii) Park state

- The lowest power consumption
- The device releases AMA and receives PMA
- The device is member of piconet
- The PDU sent to parked slave or broadcast
- Parked devices are synchronized

3.8.4.5 L2CAP

- This is the data link control protocol
- Used by ACL only
- L2CAP provides 3 types of logical channel between master and slave via ACL

Logical Channel types

(i) Connectionless

The unidirectional channel used to broad cast from master to slave

(ii) Connection oriented

- Bidirectional channel
- Support QOS: Flow specification
- The QOS Parameters define

Average data rate, peak data rate latency, and jitter.

(iii) Signaling

The channel is used to exchange signal messages between L2CAP entities

Channels:

Channel is identified by channel id. CID can take 1,2 – reserved for connectionless. The connection oriented channels CID > = 64 dynamically assigned to each end 3 to 63 are reserved.

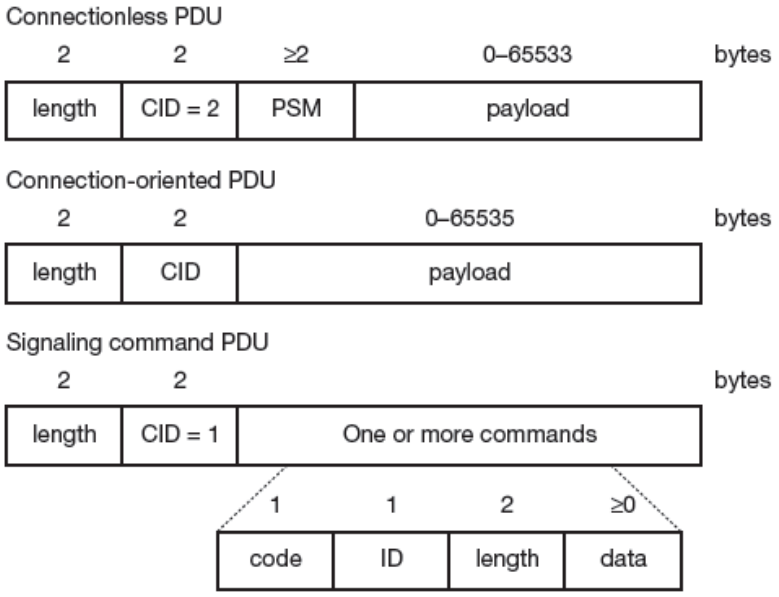


Fig 3.41: L2CAP packet formats

The format specifies.

Length : Indicates the length of payload PSM in case of connectionless PDU

CID: Multiplexing and demultiplexing

PSM: PSM protocol is present for connectionless PDU.PSM (Protocol Service Multiplexes) recipient for the payload.

For connection oriented this function is done by CID.

Command: PDU contains commands. This field is present for signaling command.

- Each command has its own code and ID that matches A request with its reply

Length: Indicate the length of the data field for this command.

3.8.4.6 Security

- Blue tooth devices uses radio for transmission
- This is easily eaves dropped. Hence security is needed
- Hence authentication and encryption are needed
- The security features offered are (1) authentication (2)Encryption stream cipher mode (3) session key is needed
- A connection may need one way, two way or no authentication
- The security algorithms use public identity of a device private user key, random key as input parameters.
- For each transaction a new random number is generated.

Security Architecture of Blue tooth

The Security Architecture is done by 4 steps

Step 1 : Pairing

This step is necessary if two Bluetooth devices have never met before

- To develop trust between the two system user can enter PIN (secret) on to both devices
- The length can be up to 16 bytes, but restricted to 4 digits

Authentication

- Here they are authenticated
- Based on the PIN, device address and random number the key is computed for authentication. The key generated is called link key of 128 bit.
- Link keys are stored in persistent storage
- The authentication is A challenge response process.
- The authentication is based on link key, random number generated by the device and the device address of the device that is authenticated.

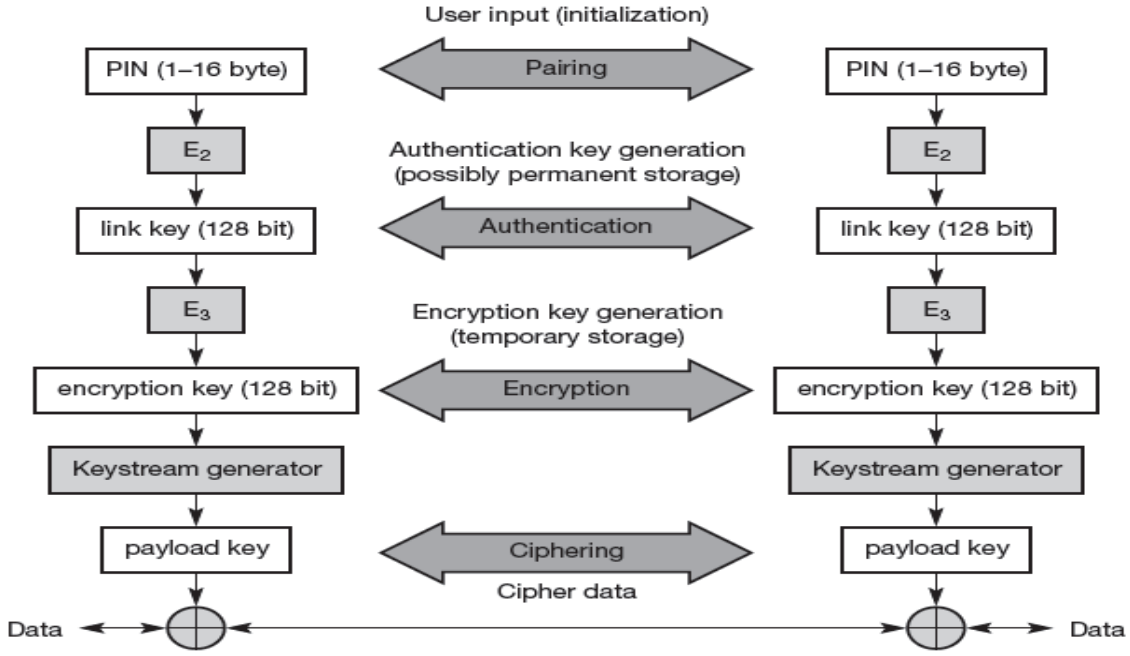


Fig 3.42: Bluetooth security components and protocols

Encryption

- Link key and another random number is used to generate A key which is used as encryption key called as encryption key.
- The key size is max of 128 bits.
- Key is generated for each transmission
- It is stored in temporary storage.

Ciphering

- Based on the encryption key the device address and the current clock A payload key is generated.
- This key is used for ciphering user data
- The payload key is A XOred with user data and payload key

3.8.4.7 SDP: Service Discovery Protocol

- The Bluetooth devices needs to work with other devices in unknown environment
- For this they need to identify what are the device and what services are present in the same radio frequency
- For this SDP protocol is used.
- SDP provides only discovery not usage to this server
- Discovered services are cached and later can be used
- The device which wants to offer A service has to initiate SDP server
- The SDP server contains service records service record contains
  - Service attributes
  - Service record handle 32 bit
- SDP does not inform about the added service or removed service
- Service attribute has attribute ID and attribute value.

Attribute ID is 16 bits, used to identify the semantics of association in A service record.

Attribute Value

It is an integer/UUID value/String/Boolean/URL

UUID= universally unique Identifier

The ID list contains UUID of the service classes.

The protocol descriptor list has the protocol needed to access the service

3.8.4.8 Profiles

- To provide interoperability between the device offering same services profiles are specified
- Profiles represent default solution for certain models
- For inter operability they use protocols and parameters
- Protocols are horizontal profiles are slices
- Types of profile

(A) Basic Profile

The basic profiles are generic access, service discovery, cordless telephony, intercom, serial port, fax, LAN

(B) Additional Profile

Advanced audio distribution, PAN, audio video remote control, basic printing and basic imaging.

3.9 WATM-Wireless ATM

ATM (Asynchronous Transfer Mode) is an important technology for all types of services and networks. Most people believe that ATM will be the standard for the future B-ISDN (Broadband Integrated Services Digital Network). From the service point of view, ATM combines both the data and multimedia information into the wired networks while scales well from backbones to the customer premises networks. To ensure the success of ATM, lots of the design issues have been standardized by ATM forum.

Due to the success of ATM on wired networks, wireless ATM (WATM) is a direct result of the ATM “everywhere” movement. WATM will support integrated data transmission (data, voice, video) with guaranteed QoS.

3.9.1 Reasons that led to the development of WATM

- The need for seamless integration of wireless terminals into an ATM network. This is a basic requirement for supporting the same services as ATM does in fixed networks.
- ATM networks scale well from LAN to WAN and mobility is needed in local and wide area.
- For ATM to be successful it must offer a wireless extension otherwise the field will be absolute.
- WATM can offer QoS to support multimedia data streams.
- For telecommunication service providers it appears merging of mobile wireless and ATM leads to wireless ATM.

3.9.2 Wireless ATM working Group

To develop the complex system the ATM forum formed, wireless ATM working group.

Goal of this group is that the new proposals should be compatible with the existing ATM standards Should be possible to upgrade existing ATM network to support mobility and radio access.

Issues to be covered are

- Extension of Fixed ATM to support mobility
- Protocols related to access the medium

3.9.3 Extension needed for ATM to be mobile ATM

Location Management: WATM network must be able to locate wireless terminal or mobile user as the user will be roaming.

Mobile Routing: The System has to route the traffic through the network to access the wireless terminal.

Hand over Signaling: The network must provide mechanisms for searching new access points, setup new connection; signal the change in access point.

QOS and Traffic Control: The WATM should offer QOS parameters. The network must concentrate on the incoming traffic as the ATM"s do.

Network Management: The extension of protocols needs an extension of management functions to control the network.

Services of the Radio access layer

1. **Radio resource Control:** The radio resources like frequency, modulations etc have to be determined.
2. **Wireless media access:** Various media access schemes like multimedia, voice etc are possible. For each the media should support such data.
3. **Wireless Data Link Control:** The data link control has header compressed.ARQ or FEC schemes are used to improve reliability.
4. **Handover issues:** The issues like resequencing, reliable transmission has to be considered.

WATM Service/Uses of WATM

1. **Office environment:** Using WATM the office can be visually expanded to the location of the employer.
2. **Universities/Schools:** Using WATM distance learning, wirelss and mobile access to data base is possible.

3.Industry: Using WATM we can have Intranet supporting the data base connection and also have factory management.

4.Hospitals: In hospitals we can have transfer of medical images, remote access to patient records,telemedicine,remote monitoring of patients.

5.Home: Electronic devices in home can be connected using WATM.

6.Networked Vehicles: (e.g.) Call Taxi, the Police vehicles are networked.
These have limited communication.

3.9. 4 Reference model

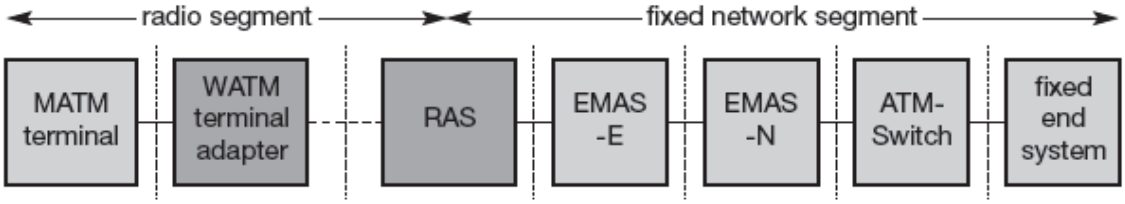


Fig 3.43: Wireless ATM generic reference model

The above figures show a generic reference model for wireless mobile access to an ATM network.

- A mobile ATM(MATM)uses a WATM adapter to gain access with WATM RAD (Radio Access System) MATM (e.g.)Laptop
- The WATM terminal adapter includes transceiver, but does not support mobility.
- RAS is connected to a mobility enhanced ATM switch (EMAS-E) which intern in connected to most aware switches (EMAS-N) and other switches.
- Finally wired, on mobility ATM end system is connected.
- The radio segment spans from the terminal to the access point. The fixed network segment spans from access point to the fixed end system.

3.9.5 Handover

- Handover is important in WATM environment.
- The Main problem for WATM during handover is rerouting all connections and maintaining connection quality.
- WATM could maintain many connection each with different quality of service requirements.
- Handover needs routing of connections reserving resources in switches, testing of availability of radio bandwidth etc.

Requirements needed for Handover

- **Handover of multiple connection:** ATM is connection oriected,where the end systems can support many connections at the same time.
  WATM should support more than only one connection.
  This results in rerouting of every connection after hand over.
- Handover of point to multipoint connection seamless support of point to multipoint connection is the advantage of ATM.
  - WATM should support these types of connection.

- **QOS support:** Handover should aim to preserve the QOS of all connection during handover. But due to limited resources it is not always possible. Hence re-negotiation and dropping on priority may be needed.
- **Data Integrity and security:** WATM should minimize cell loss, duplication reordering during handover. Moreover security association between the network and terminal should not be compromised.
- **Signaling and Rerouting Support:** WATM should identify mobility enabled switches in the network to determine radio adjacent switches by another switch to re-route partial connection during handover.
- **Performance and Complexity:**

  WATM systems are complex, because they support connection with QOS.

  Simplicity of handover should be limited.
  - Modification should be limited.
  - Functions needed should have less time requirements.
  - Handover code needed should be simple because when the code size increases, needs more processing power.

3.9.6 Location Management

For all the networks supporting mobility, functions are needed for looking with current positions of the terminal, for providing moving terminal with a permanent address, for providing security features. These functions are called as location management.

Requirement for Location Management

1. **Transparency of Mobility:**
   - A user should not notice the location management function under normal operation.
   - Any change of location should be done without user activity.
   - Transparent roaming between different domain should be possible.
   - Roaming between networks based on different technology should be feasible.
2. **Security:**
   - To provide high level security WATM system needs special features.
   - All location and use information should be protected.
     - The protection is important for roaming profiles.
     - Users should be able to determine the network their terminal is allowed to access.
3. **Efficiency and Scalability:**
   - Every function involved in location management should be scalable and efficient.
   - The performance of the operation should be independent of the network.
   - Clustering of witches and hierarchies of domain should be possible to increase the performance.
   - Signaling needed for location management should be implemented within the existing signaling mechanisms.

(4) **Identification:**
   - Location management must provide means to identify all the entities of the network.
   - Radiocells, WATM Network, Terminals need to have unique identifiers and mechanisms to exchange the identity information.
   - A terminal need to have permanent ATM end system address AESA, a routable temporary AESA in the foreign network.

(5) Interworking and Standards:

- All the location management function should co-operate with existing ATM functions.
- WATM location management has to be harmonized with other location management schemes as that of GSM, UMTS networks.

3.9.7 Mobile Quality of Service:

- QOS guarantees are the main advantages of WATM networks.
- WATM networks should provide(M-QOS) mobile quality of service.
- M-QOS is composed of 3 parts.

(1) Wired QOS: The QOS parameters are link delay, cell delay variation, bandwidth, etc.

(2) Wireless QOS: The QOS parameters are link delay, error rate channel reservation, multiplexing influence cell delay.

(3) Handover QOS: The QOS parameters are handover blocking, cell loss, speed of handover.

- The WATM system has to emap the QOS specified by an application into these sets of QOS parameters.
- The application will not specify any parameter in detail.
- The WATM system should map.
- WATM networks will offer a set 3.

Service Classes to Applications

Handover QOS: The protocols can support 2 different types of QOS during handover.

i. **Hard Handover QOS:** The QOS with the current RAS can be guaranteed. But he guarantee cannot be given after the Handover. If the applications cannot adapt to the new situation the connection is cut-off.

ii. **Soft Handover QOS :** Even for the current wireless segment only statistical QOS guarntees can be given and the applications have to adapt after the handover.

3.9.8 Access Scenario's of WATM

The figure 3.22 shows the various possible scenarios for WATM.

The componets present are :

T – Terminal

T is a Standard ATM Terminal Offering ATM Services for fixed ATM networks.

MT-Mobile Terminal.

A standard ATM with additional capability of reconnectiong after accomplish change.

WT – Wireless terminal

The termianla is accessed via a Wireless link, the terminal is fixed. Terminal keeps the access point to the network.

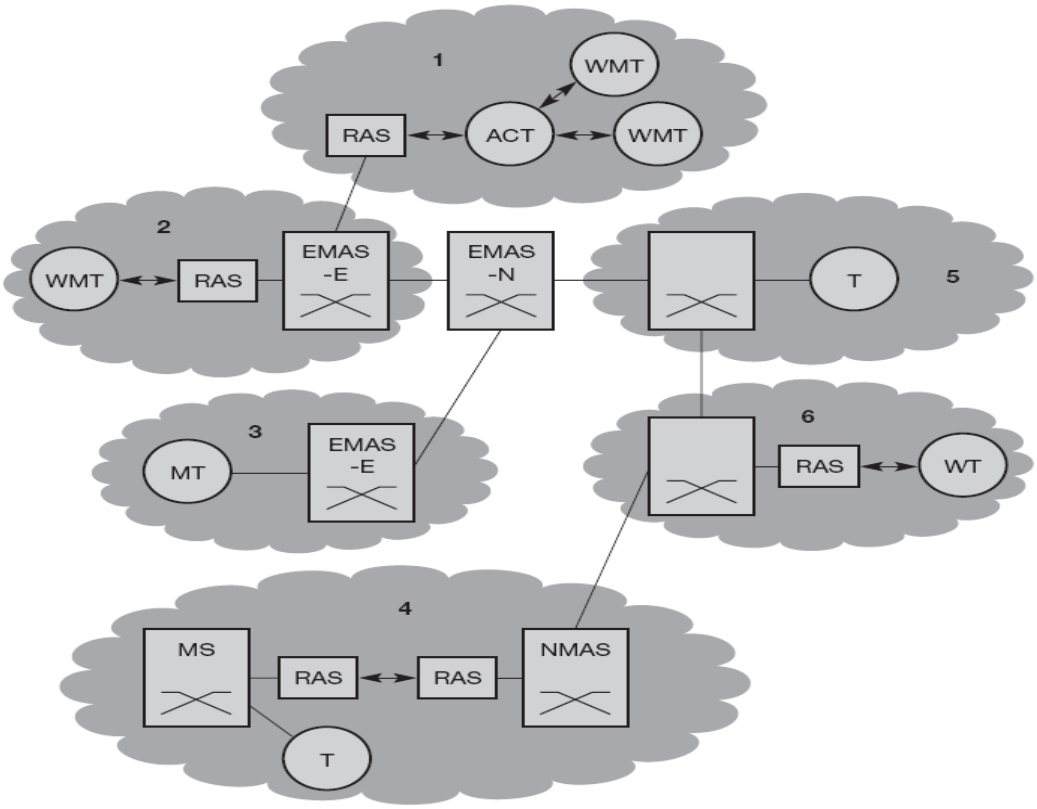


Fig 3.44: WATM reference model with several access scenarios

WMT: Wireless mobile Terminal. This is a combination of wireless and a mobile terminal which is WMT.

RAS: Radio Acccess System.

Point of access to a network via a radio link.

EMAS: End user mobility supporting ATM switch, E-edge, N-network. They are the swiches that support the end user mobility.

MS: Mobile ATM Switch.

ATM switches can also be mobile can use – wireless access to another part of ATM network.

ACT: Ad hoc Controller Terminal.

For ad hoc network special terminal"s are needed.

There can be 6 scenario"s, which the WATM should satisfy to be successful.

Scenario 1: Wireless –ad hoc ATM network.

- WMT can communicate each other without fixed network. Communication without infrastructure.
- Access control is via ACT.
- If connection to a fixed network is needed RAS does this .

Scenario 2:**Wireless mobile ATM Terminal.**

- Wireless and mobnile access the fixed network via a RAs.
- WMT cannot communiacte without EMASE switches.

Scenario 3: Mobile ATM Terminals

Supports device portability

- Users can change the access points without the need for reconfigurati9on
- Needs switches, EMAS-E.

Scenario 4: Mobile ATM swtiches.

- Complex configuration.
- Mobile switches using wireless access to fixed AM networks.
- Need switches NMAS .
- Used in Aircraft, Ships.

Scenario 5: Fixed ATM Terminals.

- Standard configuration
- Terminals and switches donnot have mobiulity.
- Referece configuration.

Scenario 6 : Fixed wireless ATM Terminals

- Provides simple access to ATM network.
- No need of wiring, a fixedx wireless link.
- Needs no changes in the fcixed network.