Unit-2

Mobile Ip & Mobile Data Networks

Mobile Ip: (Mobile Internet protocol)

→ It is a Standard Communication protocol that is designed to allow mobile device users to move from one Network to another network, while maintaining a permanent 'Ip' address.

or

→ Mobile Ip was developed to enable mobile devices to maintain Internet Connectivity while moving from one Internet attachment point to another.

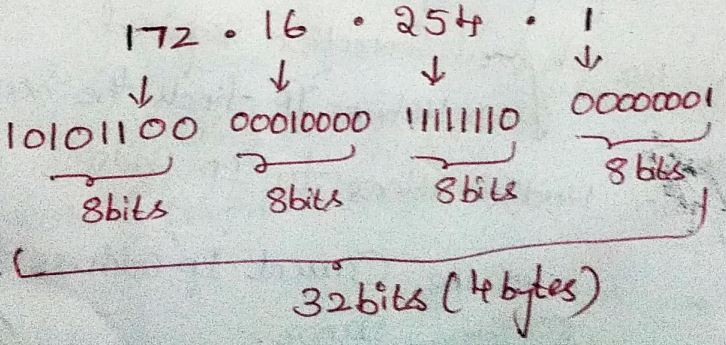
Ip address (Internet protocol address):-

→ An 'Ip' address is a numerical label assigned to each device Connected to a Computer Network that uses the Internet protocol for Communication.

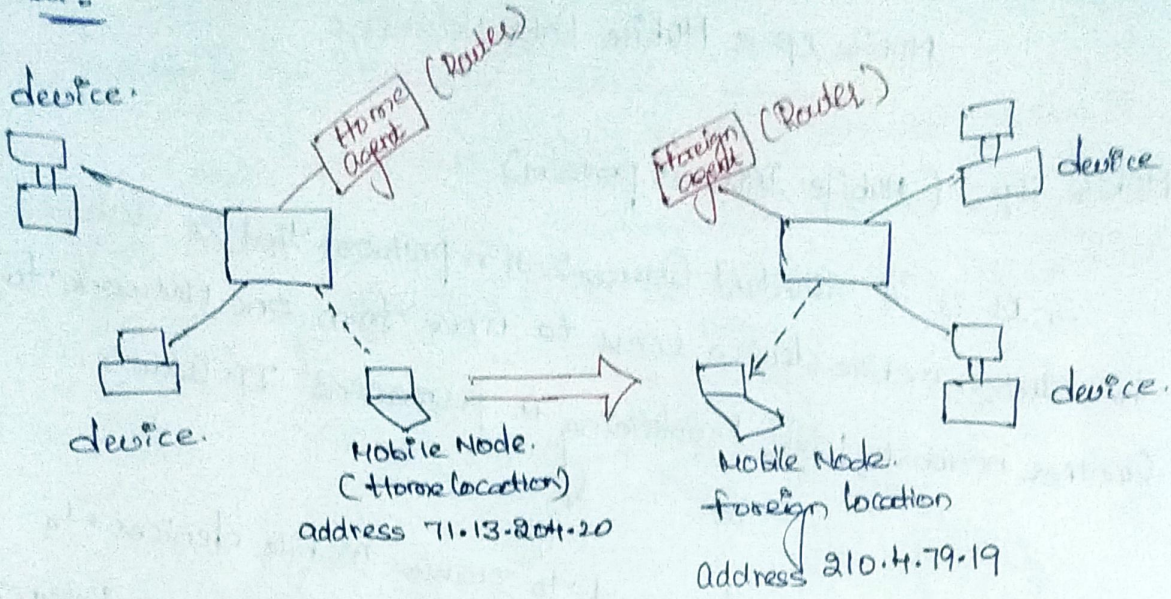
→ The 'Ip' addresses are written and displayed in human readable notations such as 172.16.254.1 in IPV4 (Internet protocol version 4)

→ The Network Administrator assigns the 'Ip' address to each device Connected to a Network.

Ex: IPv4 address in dotted decimal notation.



Ex:



Earlier Situation :-

In the above example Assume a mobile node at home location London when it moves to a foreign network Tokyo there is need for the mobile node to change its Ip address to maintain internet Connectivity.

With introduction of Mobile Ip:

The Mobile Ip enables to retain the same 'Ip' address when mobile moves from home location to foreign location, which eliminates the need for changing the 'Ip' address when device moves from one location to another location.

Features of Mobile Ip:

(1) No geographical limitations: The user can take mobile, laptop anywhere and without losing the Connection to home Network.

(2) No physical Connection required.
→ Mobile 'Ip' finds the Routers and Connects automatically.

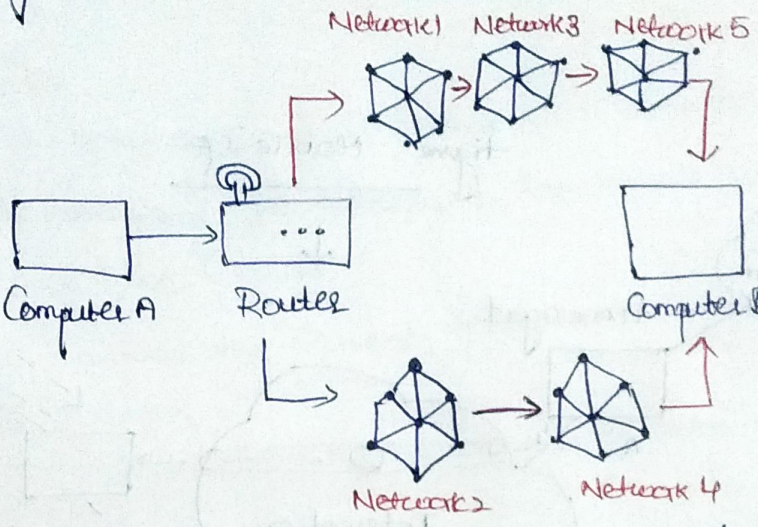
(3) No Modifications to 'Ip' address.
→ The Current 'Ip' address format remains the same.

Importance of Router:

As we know that Routing is the process of Selecting a path across one or more networks. The internet routing decisions are made by specialized pieces of N/w hardware called routers.

(Network)

Ex:



In the figure above for a data packet to get from 'Computer A' to 'Computer B', the two paths it can follow is through Networks 1, 3, 5 or Networks '2' and '4'?.

The packet will take the shorter path through Networks '2' and '4' and these kinds of choices Network routers constantly make.

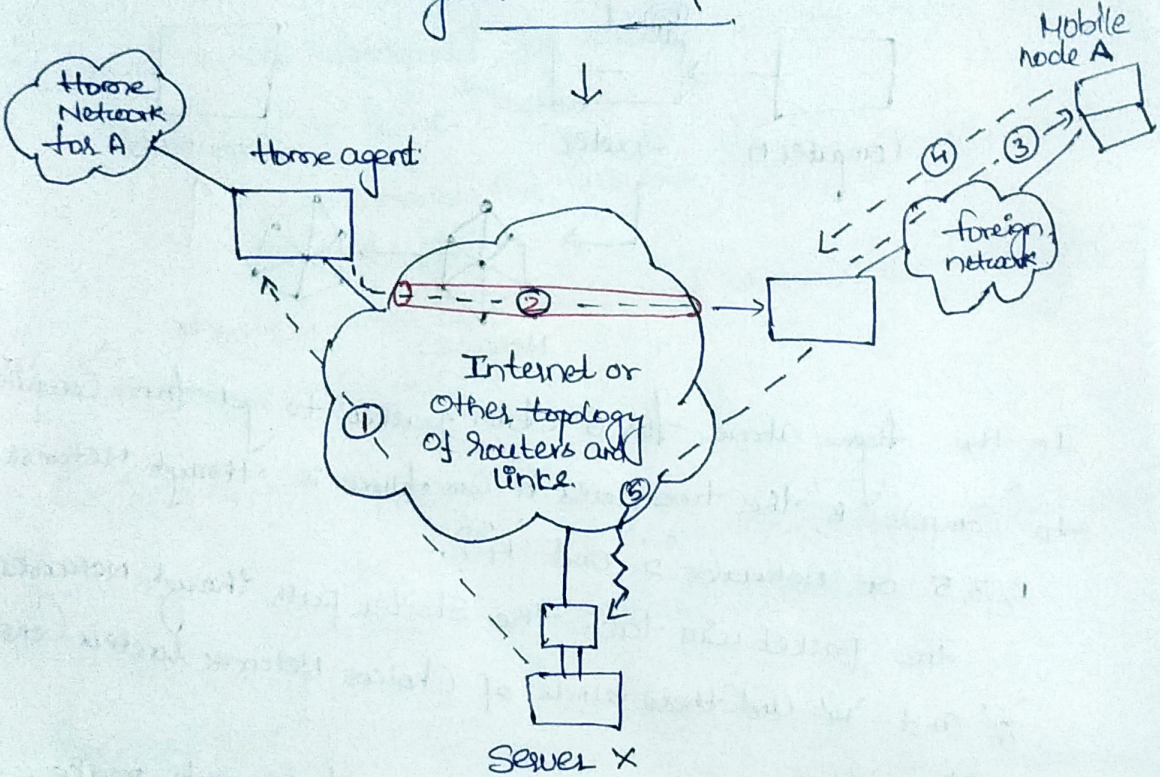
→ The Routers find the internal routing tables to make decisions about how to route packets along Network paths.

Functions of Routers:

1. provide a link between networks.
2. provide for routing and delivery of data between end systems (source and destination systems)

Mobile Ip Scenario
or
Mobile Ip Architecture.

figure: Mobile Ip.



The above figure shows how the Mobile Ip works, And what are the components involved. The components are explained as.

Mobile Node :- The Mobile node is a device such as.

- → Cellphone
- → Laptop
- → personal digital assistant.
- → The device software which enables network roaming facilities and Communication with users.

Home Network :

→ It is a Network to which the mobile node originally belongs to as per its assigned Ip address (home address)

→ The 'Ip' address on that Network, known as home address. (permanent)

Home agent :→

→ A home agent is a Router on mobile node's home N/w which tunnels datagrams for delivery to the mobile node when it is away from home. (Packets)

→ It maintains the Current 'Ip' address information for the mobile node.

→ A Tunnel is established between the home agent and the foreign agent.

Foreign Network :→

It is the Current Network to which the mobile node is visiting (away from its home network).

foreign agent :→

→ A foreign agent is a Router that stores information about mobile nodes visiting its Network.

→ It delivers packets from home agent to mobile node.

Corresponding Node :-

A Server, is a Computer that provides data to other Computers. It may Serve data to systems on Local Area N/w (LAN) or a wide area Network (WAN) over the Internet.

Care of address :- The care of address is the one its gets when it is visiting foreign Network.

→ The care of address identifies the foreign agent location.

Datagram :- → The datagram is an independent, Self Contained message Sent over the Network.

Steps how the process works :-

Step1 :-

The Server 'X' transmits an 'Ip' datagram destined for the Mobile node 'A', with A's home address in the Ip header to home agent.

It means with the Corresponding node (Server 'X'), you are Registering your mobile node at home network.

Assume my mobile is moving form home network to the foreign network (Some where between Chittoor to bangalore).

Step2 :- Now the home agent pass the information over the Tunnel which carries the datagram. The datagram Consists of Registred location and Ip address of your registered mobile node.

Step3 :- Now your foreign agent receives the information regarding your mobile node and passes information to your mobile node.

Step4 :- After Receiving that, the mobile node will again Send back to the foreign agent, and the foreign agent Send back to Corresponding node (Server X).

Note :- → As the transfer is triangular fashion, it is also called as Triangular Ip protocol.

Dr.K.Gopi,
Department of ECE.

Unit-4

BLUE TOOTH

Overview, Radio specification, Base band specification, Links manager specification, and Logical link control and adaptation protocol. Introduction to WLL Technology.

Introduction:

- **Bluetooth** is a wireless technology which is used for exchanging data between fixed and mobile devices over short distances.
- It uses UHF(Ultra High frequency) radio waves, where the frequency lies between 300MHz to 3 GHz. It is an industrial, scientific and medical radio bands(ISM) from 2.402 GHz to 2.480 GHz, and building personal area networks.
- The name of the Bluetooth came from a King Harald "**Bluetooth**" who was well known for two things: Uniting Denmark and Norway.
- Ericsson's Bluetooth project in 1994 defines the standard to enable communication between mobile phones using low power and low cost radio interfaces.

The Bluetooth Logo is 

- In May 1988, Companies such as IBM, Intel, Nokia and Toshiba joined Ericsson to form the Bluetooth Special Interest Group (SIG) whose aim was to develop standard for Personal area network(PAN).

Features of Bluetooth

- Mobile computing devices and accessories are connected wirelessly by Bluetooth using short-range, low-power, inexpensive radios.
- UHF radio waves within the range of 2.400 to 2.485 GHz are using for data communications.
- Presently, 2 to 8 devices may be connected.
- Bluetooth protocols allow devices within the range to find Bluetooth devices and connect with them. This is called pairing. Once, the devices are paired, they can transfer data securely.

- Bluetooth has lower power consumption and lower implementation costs than Wi-Fi. However, the range and transmission speeds are typically lower than Wi-Fi.
- The lower power requirements make it less susceptible to interference with other wireless devices in the same 2.4GHz bandwidth.
- Bluetooth version 3.0 and higher versions can deliver a data rate of 24 Mbps.
- In May 1988, Companies such as IBM, Intel, Nokia and Toshiba joined Ericsson to form the Bluetooth Special Interest Group (SIG) whose aim was to develop standard for Personal area network(PAN).

Bluetooth Range

- Bluetooth operating range depends on the device Class 3 radios have a range of up to 1 meter or 3 feet, Class 2 radios are most commonly found in mobile devices have a range of 10 meters or 30 feet, Class 1 radios are used primarily in industrial use cases have a range of 100 meters or 300 feet.

Data rate

- Bluetooth supports 1Mbps data rate for version 1.0 and 3Mbps data rate for Version 2.0 .

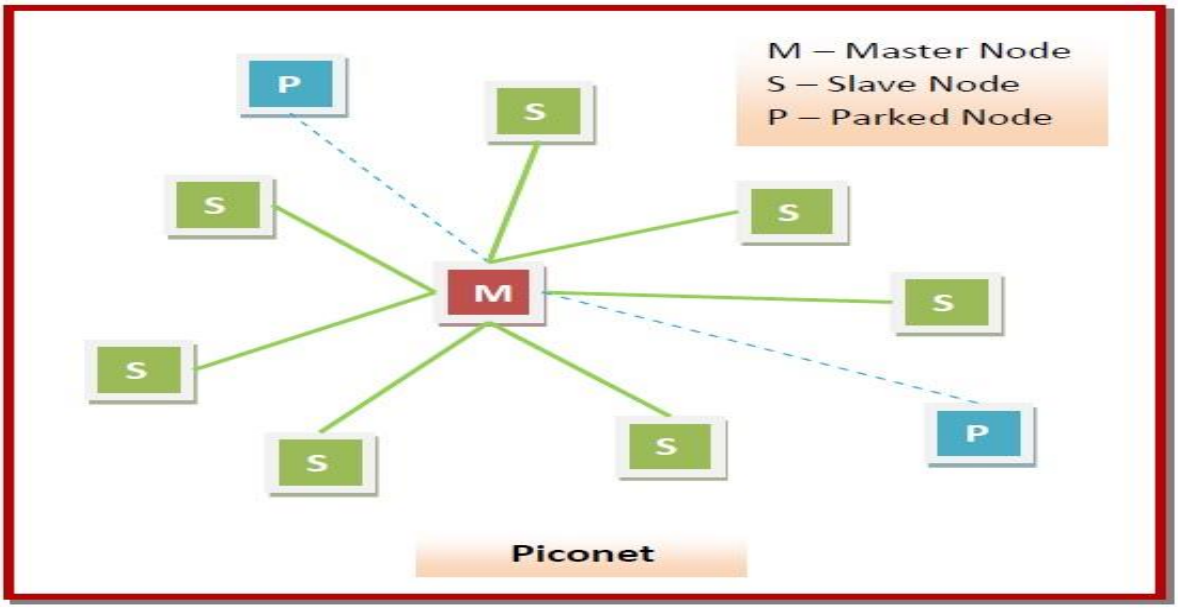
Class	Maximum Permitted Power (mW)	Range (approximate)
Class 1	100 mW	~100 meters
Class 2	2.5 mW	~10 meters
Class 3	1 mW	~1 meter

There are two types of Bluetooth networks –(Architectures)

- Piconets
- Scatternets

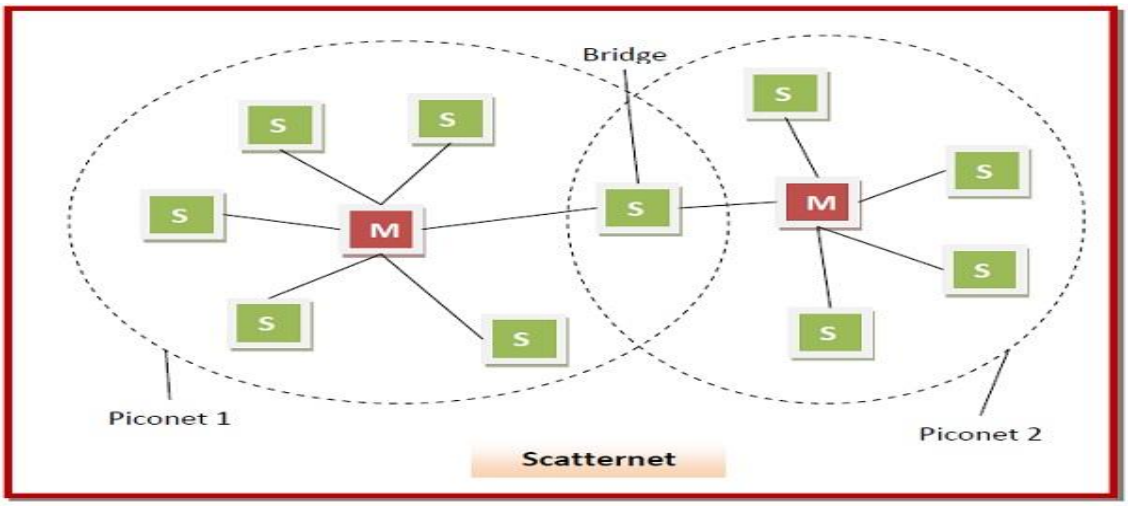
Piconets

- Piconets are small Bluetooth networks, formed by at most 8 stations, one of which is the master node and the rest slave nodes (maximum of 7 slaves). Master node is the primary station that manages the small network. The slave stations are secondary stations that are synchronized with the primary station.
- Communication can take place between a master node and a slave node in either one-to-one or one-to-many manner. However, no direct communication takes place between slaves. Each station, whether master or slave, is associated with a 48-bit fixed device address.
- Besides the seven active slaves, there can be parked nodes. The only work that they can do is respond for activation from the master node



Scatternet

- A scatternet is an interconnected collection of two or more piconets. They are formed when a node in a piconet, whether a master or a slave, acts as a slave in another piconet. This node is called the bridge between the two piconets, which connects the individual piconets to form the scatternet.



Bluetooth Usage

Usage of Bluetooth can be broadly categorized into three areas −

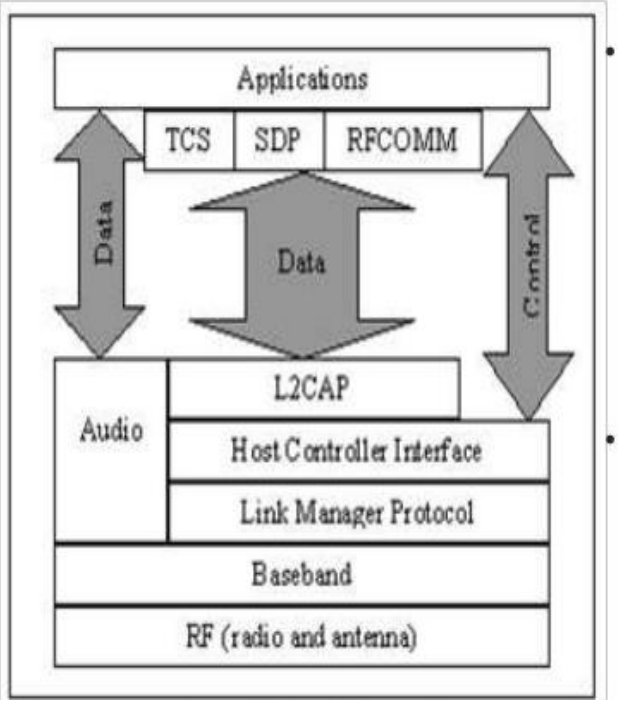
- **Access Points for Data and Voice** − Real-time voice and data transmissions are provided by Bluetooth by connecting portable and stationary network devices wirelessly.
- **Cable replacement** − Bluetooth replaces the need for a large number of wires and cables of wired networks. The connections can be made instantly and are retained even when the devices are not within range. The range of the devices is typically 10m. However, the range can be extended by using amplifiers.
- **Ad hoc networking** −. Bluetooth networks are ad hoc in nature, since a Bluetooth enabled device can form an instant connection with another Bluetooth enabled device as soon as it comes into range.

Dr.K.Gopi,
Department of ECE.

Bluetooth Applications:

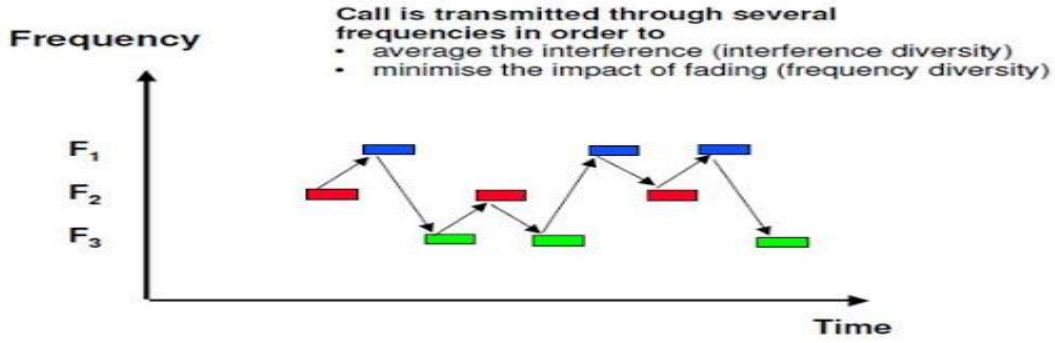
- In laptops and wireless PCs
- In mobile phones, tablets.
- In printers.
- In wireless headsets.
- To transfer data files, videos, and images and MP3 or MP4.
- In wireless peripheral devices like mouse and keyboards.
- In the short-range transmission of data from sensors devices to sensor nodes like mobile phones.

Bluetooth Architecture Protocol



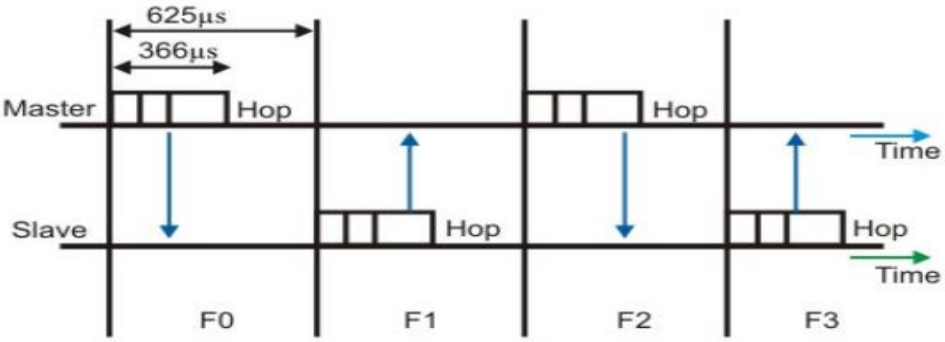
- **The heart of the Bluetooth specification is the Bluetooth protocol stack By providing well-defined layers of functionality, the Bluetooth specification ensures interoperability of Bluetooth devices and encourages adoption of Bluetooth technology.**
- **Bluetooth is defined as a layered protocol architecture consisting of core protocols, cable replacement and telephony control protocols, and adopted protocols .**

- **Radio RF protocol:** It specifies the use of air interface, Frequency hopping, Modulation scheme and transmit power. The radio layer defines the requirements for a bluetooth transceiver operating at 2.4Ghz ISMS BAND.

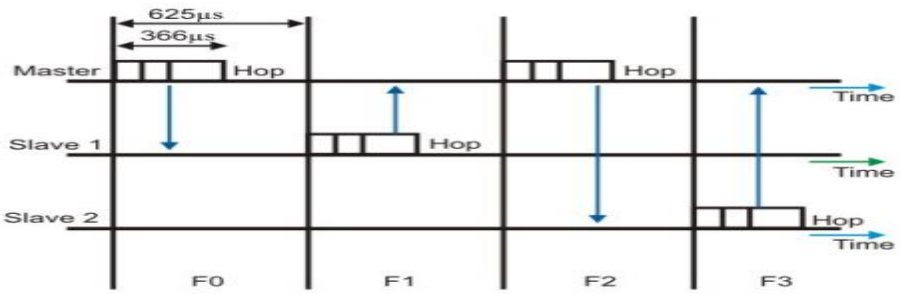


- **Baseband Protocol:** Concerened with Connection establishment with in a piconet, addressing packet, packet format , timing and power control.
- The packet is a small segment of the larger message. The data sent is divided into small packets and routed between source and destination address.

Master and Slave communication



Master and Multi slave communication



- The data exchange takes place with every clock tick. The clock synchronization is with respect to that of the master. Transmission takes place by way of TIME DIVISION DUPLEXING (TDD). The channel is divided into time slots, each 625 μs in length.
- The time slots are numbered according to the Bluetooth clock of the piconet master. A TDD scheme is used where master and slave alternatively transmit.
- The master shall start its transmission in even-numbered time slots only, and the slave shall start in odd number slots.
- If a slave is to establish a connection with the master, then the slave has to synchronize its own clock according to that of the master.
- In the multiple-slave scenario, the slave uses even numbered slots, but only one slave communicates in the next odd-numbered slot if the packet in the previous slot was addressed to it. Slave transmission in the Odd number slots only.

- The baseband layer is responsible for the process of searching for other devices and establishing a connection with them. It is also responsible for assigning the master and slave roles.
- This layer also controls the Bluetooth unit's synchronization and transmission frequency hopping sequence. This layer also manages the links between the devices and is responsible for determining the packet types supported for synchronous and asynchronous traffic.

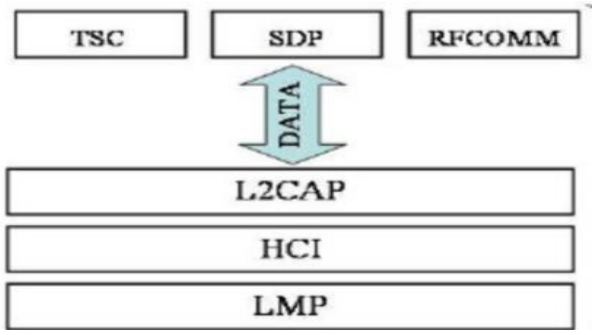
Link manager Protocol(LMP): Responsible for Link setup between Bluetooth devices and maintains the links for enabling communication **.** It is responsible for Authentication and message encryption.

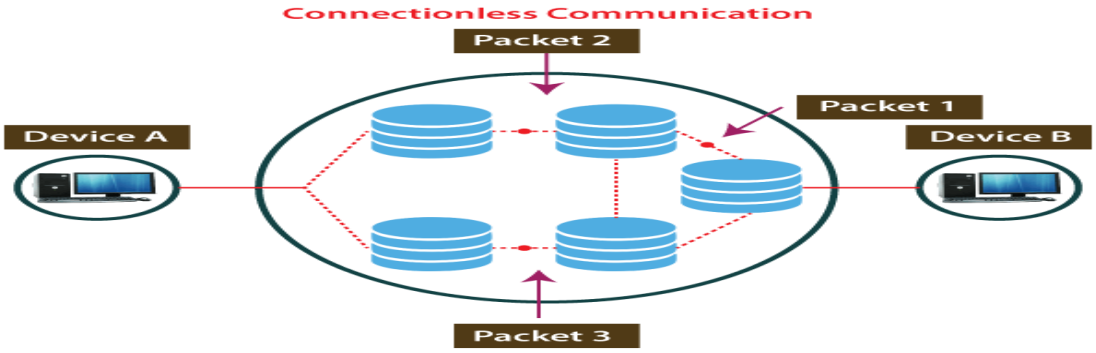
- This layer is responsible for supervising device pairing. Device pairing is the creation of a trust relationship between the devices by generating and storing an authentication key for future device authentication.
- **Encryption** transforms meaningful data into some other text which cannot be understand by Third party(Converts plain text into Cipher text). Reversing the process is called decryption.
- **Authentication** is the process of convincing a gatekeeper that you are who you say you are, typically by proving with a secret key.

Host control Interface(HCI): An interface controller is a device or module that controls and configures the interface of a processor system to a network or other interconnection. It has access to hardware status and control registers.

Logical link control and adaption protocol (L2CAP): It provides connection less and connection oriented services.Connection oriented protocol makes a connection and checks whether message is received or not and sends again if an error occurs, while connectionless service protocol does not guarantees a message delivery.

- It interfaces between the upper layers and the lower layers.
- It performs segmentation and multiplexing



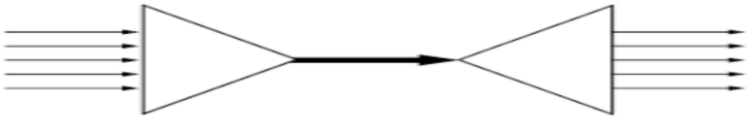


- **Service Datagram protocol(SDP):**SDP takes care of service-related queries like device information so as to establish a connection between contending Bluetooth devices. It defines which services are provided by the Bluetooth devices.

- In Bluetooth wireless communications any two devices can start communicating on the spur of the moment. Once a connection is established there is a need for the devices to find and understand the services the other devices have to offer. This is taken care of in this layer

RFCOMM: It provides connection to multiple devices by relying on L2CAP to handle multiplexing over signal connection. Serial ports are the most common communication interface in use today. These serial ports invariably involve the use of cable.

- Bluetooth's prime aim is to eliminate cables and provide support for serial communication without cables. RFCOMM provides a virtual serial port to applications. The advantage provided by this layer is that it is easy for applications designed for cabled serial ports to migrate to Bluetooth. The applications can use RFCOMM much like a serial port to accomplish scenarios like dial-up networking, etc.



Telephony control protocol: it defines how the telephone calls can be send over the Bluetooth link.

- This layer is designed to support telephony functions, which include call control and group management. These are associated with setting up voice calls.

- Once a call is established a Bluetooth audio channel can carry the call's voice content. TCS can also be used to set up data calls. The TCS protocols are compatible with ITU specifications

LINK MANAGER SPECIFICATION

1. LMP manages various aspects of the radio link between a master and a slave. The protocol involves the exchange of messages in the form of LMP PDUs (protocol data units) between the LMP entities in the master and slave.
2. Messages are always sent as single slot packets with a 1-byte payload header that identifies the message type and a payload body that contains additional information pertinent to this message.
3. The procedures defined for LMP are grouped into 24 functional areas, each of which involves the exchange of one or more messages.
4. Table lists these areas, together with the PDUs involved in each area. We briefly look at each area in turn. The two general response messages are used to reply to other PDUs in a number of different procedures.
5. The accepted PDU includes the opcode of the message that is accepted. The not accepted PDU includes the opcode of the message that is not accepted and the reason why it is not accepted. LMP supports various security services with mechanisms for managing authentication, encryption, and key distribution. These services include

•**Authentication:** Authentication is defined in the baseband specification but involves the exchange of two LMP PDUs, one containing the random number and one containing the signed response (Figure 15.14).

•**Pairing:** This service allows mutually authenticated users to automatically establish a link encryption key. As a first step, an initialization key is generated by both sides and used in the authentication procedure to authenticate that the two sides have the same key. The initialization key is generated from a common personal identification number (PIN) entered in both devices. The two sides then exchange messages to determine if the link key to be used for future encryptions will be a secret key already configured or a combination key that is calculated based on the master's link key.

Change link key: If two devices are paired and use a combination key, then that key can be changed. One side generates a new key and sends it to the other side XOR with the old link key. The other side accepts or rejects the key

Dr.K.Gopi,
Department of ECE.

L2CAP Channels

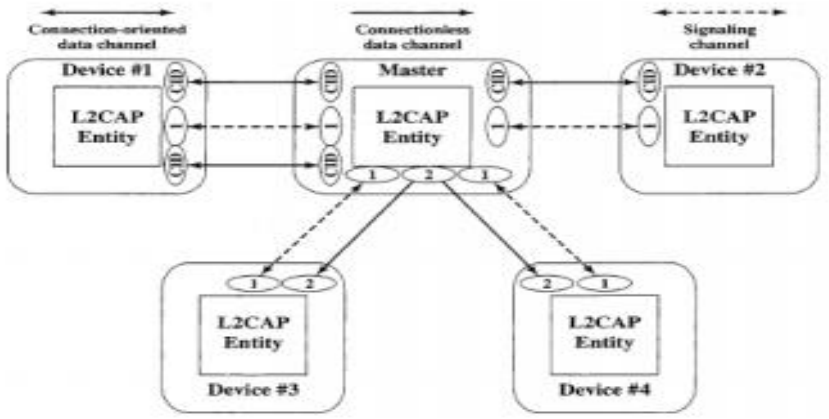
L2CAP provides three types of logical channels:

• Connectionless: Supports the connectionless service. Each channel is unidirectional. This channel type is typically used for broadcast from the master to multiple slaves.

• Connection oriented: Supports the connection-oriented service. Each channel is bidirectional (full duplex). A quality of service (QoS) flow specification is assigned in each direction.

• Signaling: Provides for the exchange of signaling messages between L2CAPentities.

Figure provides an example of the use of L2CAP logical channels. Associated with each logical channel is a channel identifier (CID). For connection-oriented channels, a unique CID is assigned at each end of the channel to identify this connection and associate it with an L2CAP user on each end.



Connectionless channels are identified by a CID value of 2, and signaling channels are identified by a CD value of 1. Thus, between the master and any slave, there is only one connectionless channel and one signaling channel, but there may be multiple connection-oriented channels.L2CAP Packets .

BLUETOOTH PACKETS:

. For the connectionless service, the packet format consists of the following fields:

The data on the piconets is conveyed in packets. A packet is shown below.

ACCESS CODE [72]	HEADER [54]	PAYLOAD [0-2745]

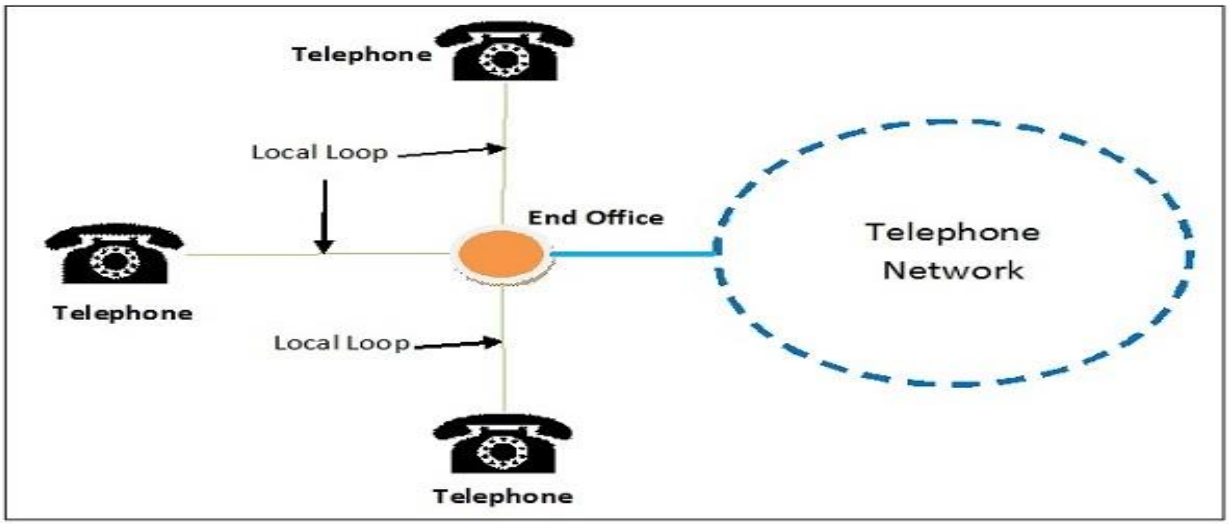
The access code is used for timing synchronization, paging and inquiry. There are three different types of access codes ; Channel access code which identifies a piconet; Device access code is used for paging and its responses and Inquiry access code is for inquiry purposes.

The header contains information of packet acknowledgement, packet numbering , flow control, slave address and error check.

Wireless Local LOOP(WLL)

INTRODUCTION:

- In a telephone system, the local loop is a two-wire connection between the subscriber's house and the end office of the telephone company. The loop may run from 1km to as far as 10 km. The connection is usually a pair of copper wires.
- Earlier it is used for voice transmission only using Analog transmission. Today's the Modem makes the conversion between analog to digital signals. With ISDN(integrated service Digital Network) the local loop can carry digital signals directly at much higher bandwidth.



- Central Office: It is an office where the subscriber home, business lines are connected on local loop. This office has Telephone switches to switch the calls locally or long distance.
- PSTN(Public switched telephone network): It is a combination of telephone networks used world wide, including telephone lines, fiber optic cables, switching offices, cellular networks. They help to communicate with each other.

Dr.K.Gopi,
Department of ECE.

Need for Wireless Local Loop(WLL):

- The implementation of local loop is risky for the operators especially in remote or rural areas due to less number of users & cost of installation.
- Hence the solution for this the Wireless local Loop(WLL), which uses wireless links rather than the copper wires to connect subscriber to the central offices.
- WLL provides wireless communication link for fixed telephone or internet customers, while GSM provides the wireless accces to moving or mobile subscribers.

The three words of WLL is explained as:

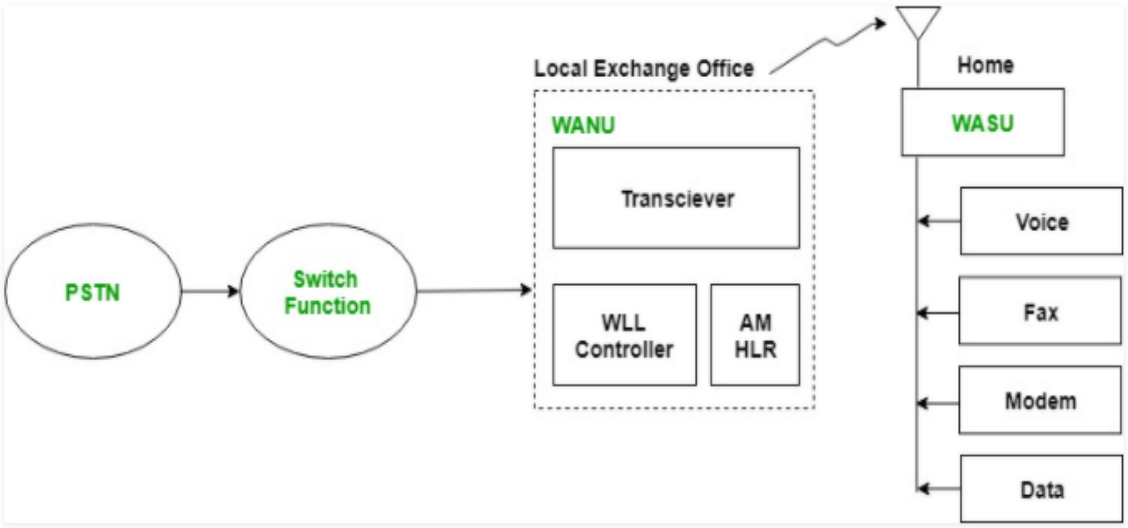
Wireless: The term describes the radio frequency for communication.

Local: it defines the short distance(Rural or small area).

Loop: The circuit that connects telephone to central office.

- Definition: It is a technology for connecting the subscriber to the telephone network with the help of wireless technology.
- It utilizes the radio signals which provide telephone services to subscribers.
- The WLL is also called as Fixed Radio access(FRA) or RLL(Radio Local Loop).

WLL Architecture:



Dr.K.Gopi,
Department of ECE.

Wireless access network Unit(WANU):

- It acts as an Interface between wired side(PSTN & Switch function) and the wireless side(WASU).
- It is the one responsible for taking and delivery of the data across the wired and wireless network.
- It is present at the Exchange office and all the local WASUs are connected to it.
- The functions of it are

1. **Authentication:** Responsible for user validity (i,e when you dial a number, whether it is registered or not).

2. **Operation & Maintenance:** It is used to Monitor and maintenance the performance of equipments in the system.

3.**Privacy via AIR Interface:** Call security is maintained over the air interface with the help of encryption(Converting the information to a form which is not noticeable by third party).

4.**Routing & switching:** Selecting a path for traffic in the network & switch the data packets on the same network.

- The devices present in the WANU are:
  - **Transceiver:** It transmits/receives data.
  - **WLL Controller**: It controls the wireless local loop component with WASU.
  - **AM:** It is short for **Access Manager**. It is responsible for authentication(verifying the user validity) I,e when the user places the call whether he is authenticated or not.
  - **HLR:** It is short for **Home Location Register**. It stores the details of all local WASUs. It is a database that contain information such as customer profile(telephone number, services and location of subscriber).

Switch Function:
Switch Function switches the PSTN among WANUs.

PSTN(Public switched telephone network): It is the voice telephone network around the globe. It is Public Switched Telephone Network which is a circuit switched network. It is a collection of world's interconnected circuit switched telephone networks.

Wireless access subscriber unit(WASU):

It is short for Wireless Access Subscriber Units. It is present at the house of the subscriber. It connects the subscriber to WANU and the power supply for it is provided locally.

- It provides the air interface i,e the data comes from WASU and transferred to WANU with the help of radio signals.
- The key role of WASU is to encode the data i,e When the data is coming from the wired network then it will find the right encoding to translate the signals to the wireless network and vice versa.
- **Advantages of WLL:**
  - Low cost due to no use of conventional copper wires.
  - Much more secure due to digital encryption techniques used in wireless communication.
  - Highly scalable as it doesn't require the installation of more wires for scaling it.
- **Features of WLL:**
  - Internet connection via modem(People can share information and communicate any where with the help of this facility)
  - Data service(it can be variety of forms, text, images etc..)
  - Voice service(voice conversations)
  - Fax service(A **fax machine** is a device that is used to send documents electronically over a telephone network.)

Difference between WLL and Mobile networks:

- The main difference between WLL and GSM is, WLL provide wireless communication link for fixed telephone or internet customers, while GSM provide the wireless access for moving or mobile subscribers.
- MOBILE SYSTEM:
  - Connects people on move

- Universal coverage
- Voice quality is moderate

Wirless local loop(WLL):

- Serve subscriber at home or at offices supporting fixed telephone.
- Voice quality is high
- Limited distance

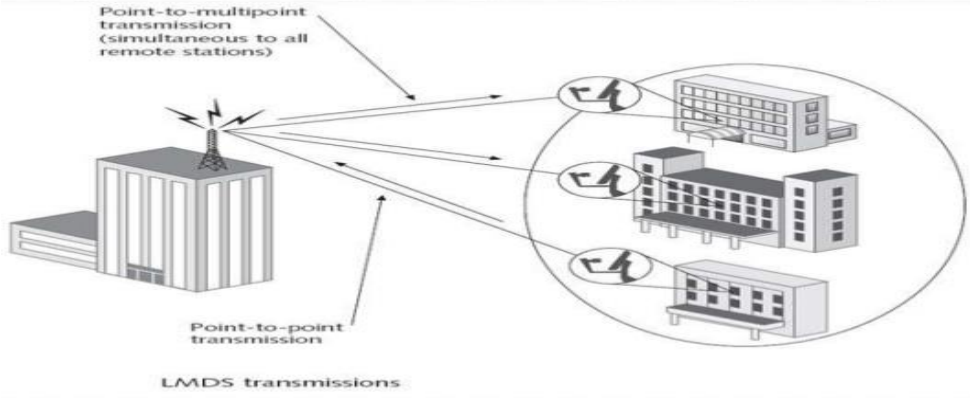
TYPES OF WLL

- There are two type of WLL technique available. They are

i. Local Multipoint Distribution Service (LMDS)

ii. Multichannel Multipoint Distribution Service(MMDS)

LDMS TRANSMISSION



Advantages and Disadvantages

- **Advantages**
  1. High signal strength
  2. Cell size is small
  3. Less cost than LMDS
  4. Larger wavelength

- **Disadvantages**
  1. Physical limitations

The transmitted power as the FCC did not allow the power transmitted of the base station serving area that is more than 50 km.

Multichannel Multipoint Distribution Service

- MMDS is a broadcasting and communications service that operates in the ultra-high-frequency(UHF) portion of the radio spectrum between 2.1 and 2.7 GHz. MMDS is also known as wireless cable.

- In MMDS, a medium-power transmitter is located with an Omni-directional broadcast antenna at or near the highest topographical point in the intended coverage area. The workable radius can reach up to 70 miles in flat terrain.

- Fixed broadband wireless technology similar to LMDS.

- Can transmit video, voice, or data signals at 1.5 to 2 Mbps downstream and 320 Kbps upstream.

Dr.K.Gopi,
Department of ECE.

UNIT-V

WIRELESS LAN TECHNOLOGY: Infrared LANs, Spread spectrum LANs, Narrow bank microwave LANs,IEEE802.11 architecture and services.

Wireless ATM & HIPER LAN: Introduction, Wireless ATM, HIPERLAN, Adhoc Networking and WPAN.

Definition:

- Wireless LAN stands for Wireless Local Area Network. It is also called LAWN (Local Area Wireless Network). WLAN is one in which a mobile user can connect to a Local Area Network (LAN) through a wireless connection.

Or

- A wireless LAN (WLAN) is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, office building etc.
- Wireless LANs provide high speed data communication in small areas such as building or an office. WLANs allow users to move around in a confined area while they are still connected to the network.

Different types of LANS are

1. Infrared LAN

2.Narrowband Microwave LAN

3.Spread spectrum LAN

Advantages of WLANs

- **Flexibility:** Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.).
- **Design:** Wireless networks allow for the design of independent, small devices for example be put into a pocket. Cables not only restrict users but also designers of small notepads, PDAs, etc.

- **Robustness:** Wireless networks can handle disasters, e.g., earthquakes, flood etc. whereas, networks requiring a wired infrastructure will usually break down completely in disasters.
- **Cost:** The cost of installing and maintaining a wireless LAN is on average lower than the cost of installing and maintaining a traditional wired LAN, for two reasons.
  - First, after providing wireless access to the wireless network via an access point for the first user, adding additional users to a network will not increase the cost.
  - And second, wireless LAN eliminates the direct costs of cabling and the labor associated with installing and repairing it.

Disadvantages of WLANs:

- **Quality of Services:** Quality of wireless LAN is typically lower than wired networks. The main reason for this is the lower bandwidth due to limitations is radio transmission, higher error rates due to interference and higher delay/delay variation due to extensive error correction and detection mechanisms.
- **Restrictions:** Several govt. and non-govt. institutions world-wide regulate the operation and restrict frequencies to minimize interference.
- **Global operation:** Wireless LAN products are sold in all countries so, national and international frequency regulations have to be considered.
- **Low Power:** Devices communicating via a wireless LAN are typically power consuming, also wireless devices running on battery power. Whereas the LAN design should take this into account and implement special power saving modes and power management functions.
- **Robust transmission technology:** If wireless LAN uses radio transmission, many other electrical devices can interfere with them.

Dr.K.Gopi,
Department of ECE.

INFRARED LAN

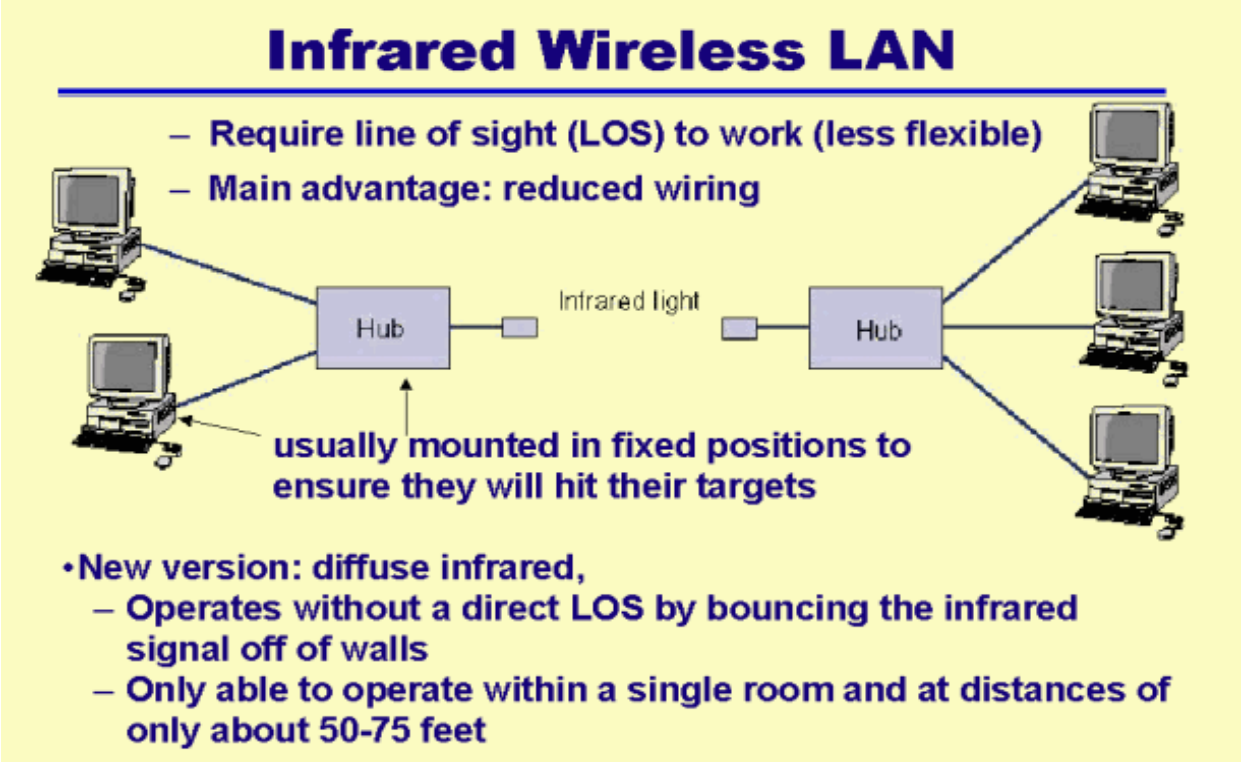
- Infrared LANs use infrared signals to transmit data. This is the same technology used in products like remote controls for televisions and VCRs.
- Infrared networking enables computing devices to send and receive data wirelessly within a short range using infrared beams.
- Devices with infrared can be recognized by the infrared port that is visible on the side of the product which is used to detect and send the infrared beams.
- IR wireless is used for short- and medium-range communications and control.

Advantages:

- **Infrared** transmission requires minimum power to operate and can be set up at a low cost.
- This is a secure way to transfer data between devices as the signal cannot pass beyond a room or chamber.

Disadvantages:

Infrared can be used for a small range distance.



Advantages of infrared:

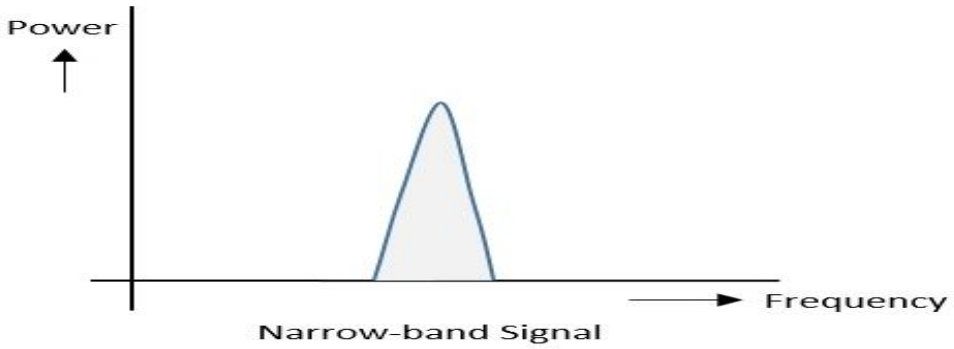
- The main advantage of infrared technology is its simple and extremely cheap senders and receivers which are integrated into nearly all mobile devices available today.
- No licenses are required for infrared and shielding is very simple.
- PDAs, laptops, notebooks, mobile phones etc. have an infrared data association (IrDA) interface.
- Electrical devices cannot interfere with infrared transmission.
- **Disadvantages of Infrared**
- Disadvantages of infrared transmission are its low bandwidth compared to other LAN technologies.
- Limited transfer rates to 115 Kbit/s and we know that even 4 Mbit/s is not a particular high data rate.
- Infrared transmission cannot penetrate walls or other obstacles.
- Typically, for good transmission quality and high data rates a LOS (Line of site), i.e. direct connection is needed.

Narrow Band Microwave LAN

- Microwave technology is not really a LAN technology.
- It's main use is to interconnect LANs between buildings. This requires microwave dishes on both ends of the link.
- The dishes must be in line-of-sight to transmit and collect the microwave signals.
- One major drawback to the use of microwave technology is that the frequency band used requires licensing by the FCC.
- Once a license is granted for a particular location, that frequency band cannot be licensed to anyone else, for any purpose, within a 17.5 mile radius.

Narrowband Microwave

- Microwave technology is not really a LAN technology.
- It's main use is to interconnect LANs between buildings. This requires microwave dishes on both ends of the link.
- The dishes must be in line-of-sight to transmit and collect the microwave signals.
- One major drawback to the use of microwave technology is that the frequency band used requires licensing by the FCC.
- Once a license is granted for a particular location, that frequency band cannot be licensed to anyone else, for any purpose, within a 17.5 mile radius.



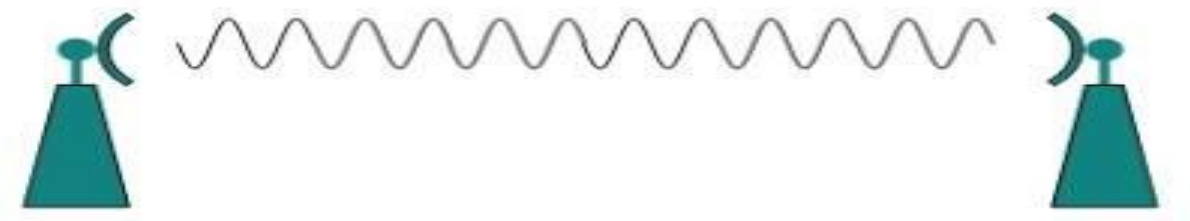
Microwave Transmission

- Because Microwaves travels in straight lines, both sender and receiver must be aligned to be strictly in line-of-sight.
- Microwaves can have wavelength ranging from 1 mm – 1 meter and frequency ranging from 300 MHz to 300 GHz.
- Microwave antennas concentrate the waves making a beam of it. As shown in picture multiple antennas can be aligned to reach farther. Microwaves have higher frequencies and do not penetrate wall like obstacles.

- Microwave transmission depends highly upon the weather conditions and the frequency it is using.

Features of Microwaves

- Microwaves travel in straight lines, and so the transmitter and receiver stations should be accurately aligned to each other.

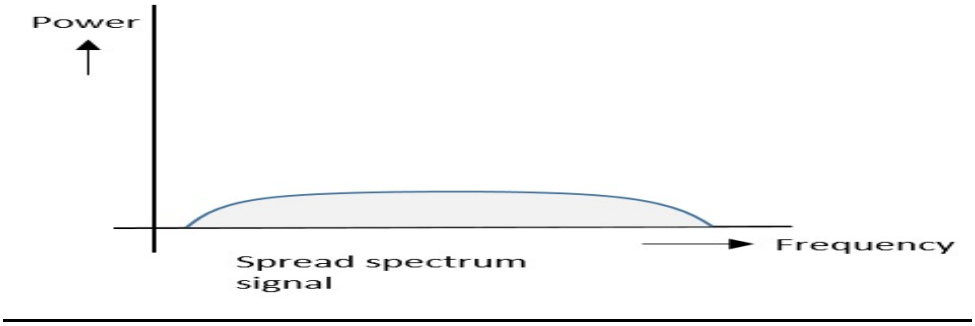


- Microwave propagation is line – of – sight propagation. So, towers hoisting the stations should be placed so that the curvature of the earth or any other obstacle does not interfere with the communication.
- Since it is unidirectional, it allows multiple receivers in a row to receive the signals without interference.

SPREAD SPECTRUM COMMUNICATION

- Most wireless LAN systems use spread-spectrum technology, a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. Spread-spectrum is designed to trade off bandwidth efficiency for reliability, integrity, and security.
- In other words, more bandwidth is consumed than in the case of narrowband transmission, but the tradeoff produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast.
- If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise.

- The spread spectrum signals have the signal strength distributed as shown in the following frequency spectrum figure.



Following are some of its features −

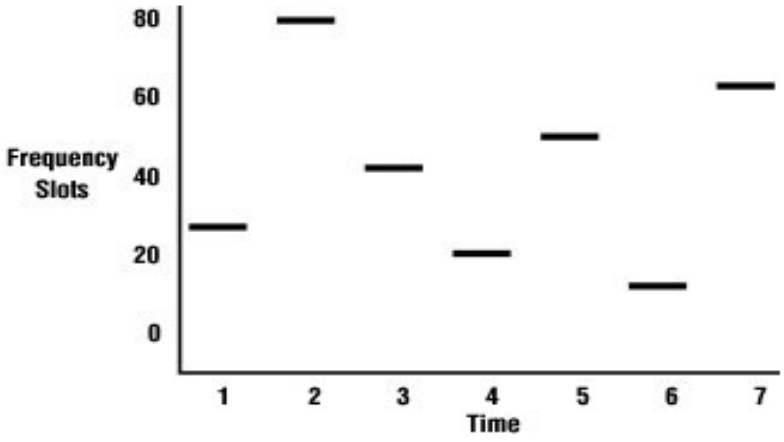
Band of signals occupy a wide range of frequencies.

Energy is wide spread.

With these features, the spread spectrum signals are highly resistant to interference or jamming. Since multiple users can share the same spread spectrum bandwidth without interfering with one another, these can be called as **multiple access techniques**.

Frequency-Hopping Spread Spectrum Technology

- Frequency-hopping spread spectrum is a method of transmitting radio signals by rapidly changing the carrier frequency among many distinct frequencies occupying a large spectral band.



Dr.K.Gopi,
Department of ECE.

WIRELESS LANS

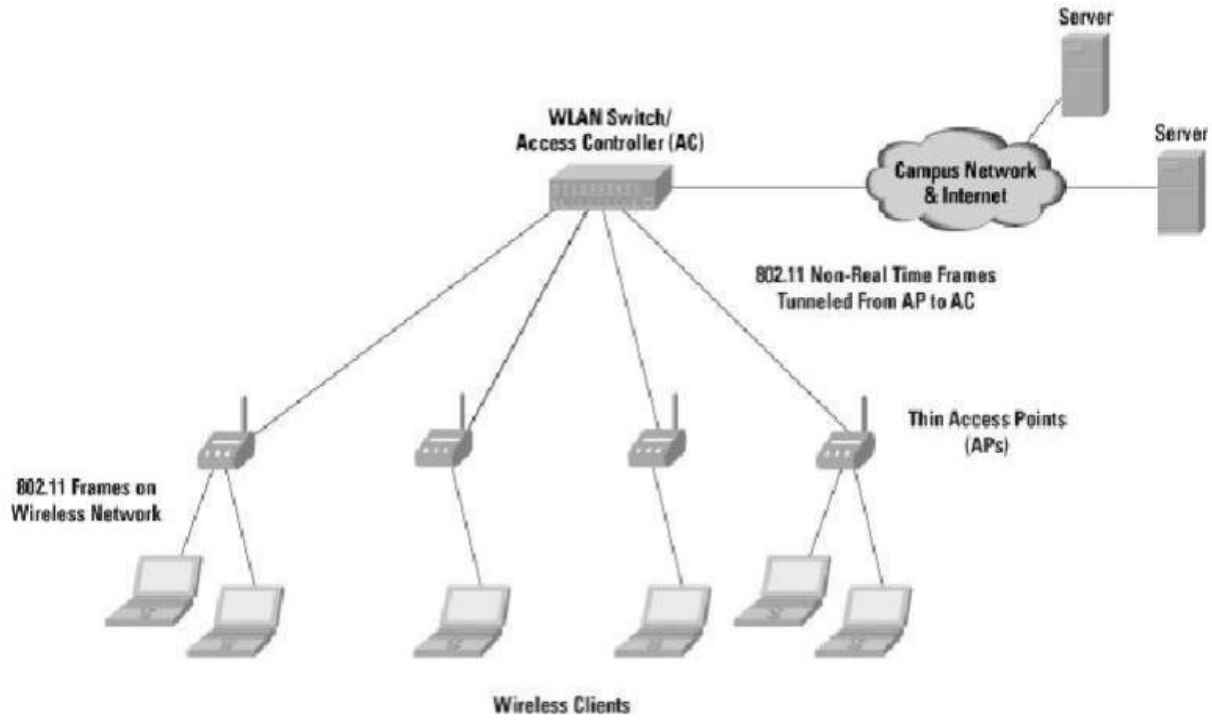
- wireless LAN standard is 802.11.Wireless LANs can also be used to let two or more nearby computers communicate without using the Internet.
- popular, and homes, offices, cafes, libraries, airports, zoos, and other public places are being outfitted with them to connect computers, PDAs, and smart phones to the Internet.

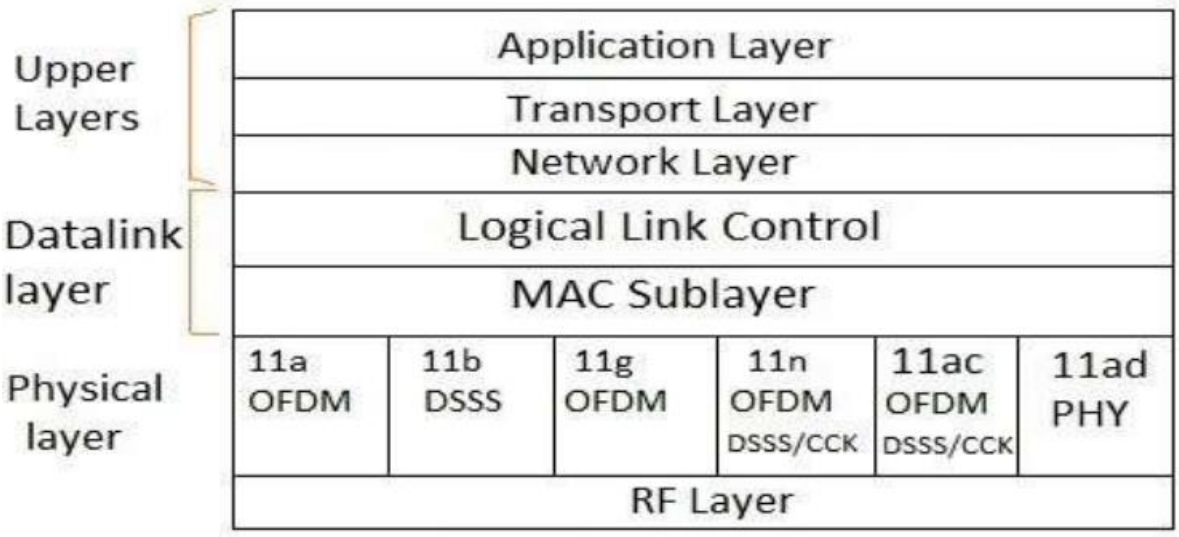
Architecture and Protocol Stack

- Has two modes(Infrastructure mode, Adhoc network)
- The most popular mode is to connect clients, such as laptops and smart phones, to another network, such as a company intranet or the Internet.
- In infrastructure mode, each client is associated with an AP (Access Point) that is in turn connected to the other network.
- The client sends and receives its packets via the AP.
- Several access points may be connected together, typically by a wired network called a distribution system, to form an extended 802.11 network.
- The other mode is called an ad hoc network. • This mode is a collection of computers that are associated so that they can directly send frames to each other.

  • There is no access point. Since Internet access is the killer application for wireless, ad hoc networks are not very popular.

  • The protocols of the 802 protocols, including 802.11 and Ethernet, have a certain commonality of structure.





WLAN protocol stack

Two of the initial techniques, infrared in the manner of television remote controls and frequency hopping in the 2.4-GHz band, are now defunct.

• The third initial technique, direct sequence spread spectrum at 1 or 2 Mbps in the 2.4-GHz band, was extended to run at rates up to 11 Mbps and quickly became a hit. It is now known as 802.11b.

• New transmission techniques based on the OFDM (Orthogonal Frequency Division Multiplexing).

• The first is called 802.11a and uses a different frequency band, 5 GHz.

• The second stuck with 2.4 GHz and compatibility. It is called 802.11g.

• Both give rates up to 54 Mbp

The 802.11 Physical Layer

802.11 techniques use short-range radios to transmit signals in either the 2.4-GHz or the 5-GHz ISM frequency bands.

• Manufacturers of cordless phones, microwave ovens, and countless other devices, all of which compete with laptops for the same spectrum.

• If the wireless signal is weak, a low rate can be used. • If the signal is clear, the highest rate can be used. • This adjustment is called rate adaptation.

The 802.11a method is based on OFDM (Orthogonal Frequency Division Multiplexing) because OFDM uses the spectrum efficiently and resists wireless signal degradations such as multipath.

• The use of multiple antennas gives a large speed boost, or better range and reliability instead. MIMO, like OFDM, is one of those clever communications ideas that is changing wireless designs.

The 802.11 MAC Sublayer Protocol

The 802.11 MAC sublayer protocol is quite different from that of Ethernet, due to two factors that are fundamental to wireless communication.

• First, radios are nearly always half duplex, meaning that they cannot transmit and listen for noise bursts at the same time on a single frequency.

• With wireless, this collision detection mechanism does not work., Instead, 802.11 tries to avoid collisions with a protocol called CSMA/CA (CSMA with Collision Avoidance).

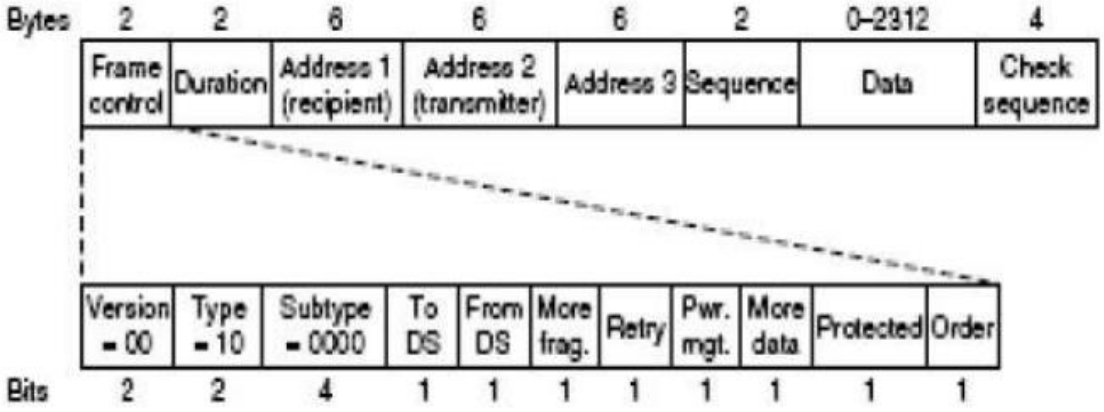
Dr.K.Gopi,
Department of ECE.

The 802.11 Frame Structure

• It defines three different classes of frames in the air are data, control, and management.

• Each of these has a header with a variety of fields used within the MAC sublayer.

• In addition, there are some headers used by the physical layer, but these mostly deal with the modulation techniques used.



The To DS and From DS bits are set to indicate whether the frame is going to or coming from the network connected to the APs, which is called the distribution system.

• The Retry bit marks a retransmission of a frame sent earlier.

• The Power management bit indicates that the sender is going into power-save mode.

• The More data bit indicates that the sender has additional frames for the receiver.

• The Protected Frame bit indicates that the frame body has been encrypted for security.

Duration field-tells how long the frame and its acknowledgement will occupy the channel, measured in microseconds.

• Addresses field-Data frames sent to or from an AP have three addresses, all in standard IEEE 802 format. The Address1 is the receiver, and the Address2 is the transmitter.

• The Address3 gives this distant endpoint.

• The Sequence field numbers frames so that duplicates can be detected. Of the 16 bits available, 4 identify the fragment and 12 carry a number that is advanced with each new transmission.

• The Data field contains the payload, up to 2312 bytes. • The Frame check sequence, which is the same 32-bit CRC. • Management frames have the same format as data frames, plus a format.

Services:

The association service is used by mobile stations to connect themselves to APs.

• Reassociation lets a station change its preferred AP. This facility is useful for mobile stations moving from one AP to another AP in the same extended 802.11 LAN, like a handover in the cellular network.

• Either the station or the AP may also disassociate, breaking their relationship. • Stations must also authenticate before they can send frames via the AP,

• recommended scheme, called WPA2 (WiFi Protected Access 2), implements security as defined in the 802.11i standard.

HIGH PERFORMANCE LAN (HIPERLAN)

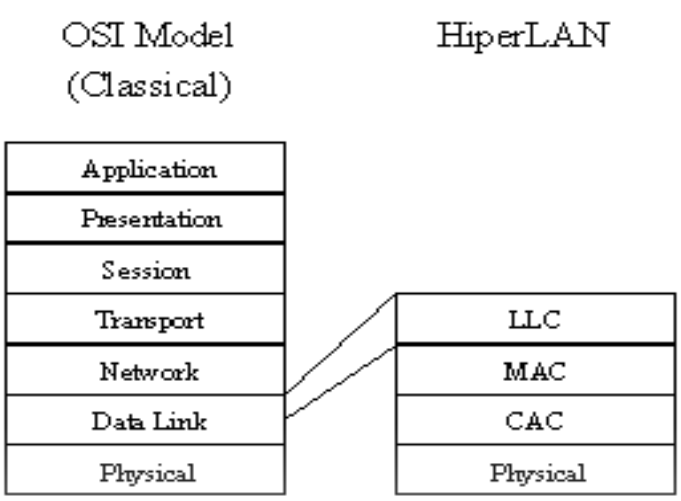
- HiperLAN (High Performance Radio LAN) is a wireless LAN standard. It is defined by the European Telecommunications Standards Institute (ETSI).
- A wireless LAN (WLAN) is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, or office building. This gives users the ability to move around within the area and remain connected to the network.
- The HiperLan is derived from traditional LAN environments and support multimedia data and Asynchronous data effectively at data rate of 23.5Mbps.
- The HiperLAN operates at 5.15Mhz with a coverage of 100m. With up to 800m distance a data rate of 1Mbps are provided.
- It is a digital High speed wireless communication and an alternate for IEEE802.11 standard, as this wireless standard which gives the ability to move around and remain connected to the network.
- In Hiperlan radio waves are used instead of a cable as transmission medium to connect stations. Radio transceivers is mounted to the movable stations as an odd on and no base station has to be installed separately.

It has two variants

- HIPERLAN1
- HIPERLAN2

HIPERLAN1 :

- The goal of the HiperLAN was the high data rate, higher than 802.11. The standard was approved in 1997.
- The standard covers the Physical layer, Media Access Control part of the Data link layer like 802.11.
- It uses single carrier modulation such as GMSK and uses Equalizer to take care of delay spread. The GMSK is a form of frequency modulation that is used in the Radio communication system. With no phase discontinuities it provides efficient use of spectrum and enables high efficiency.
- range 100 m
- supports asynchronous and synchronous traffic
- Bit rate - 23.59 Mbit/s
- Description- Wireless Ethernet
- Frequency range- 5 GHz



Dr.K.Gopi,
Department of ECE.

HIPERLAN REFERENCE MODEL

Components of a HIPERLAN include:

Physical Layer: This layer provides the standard functions, including radio frequency functions. This layer deals with the setup of physical connection to the network and with transmission and reception of signals.

Channel Access Control Layer: The channel access control mechanisms provided by the MAC layer are also known as a multiple access method. This makes it possible for several stations connected to the same physical medium to share it.

- A channel access method is based on multiplexing, that allows several data streams or signals to share the same communication channel or transmission medium.

Medium Access Control Layer:

Medium access control deals with issues such as addressing, assigning channels to different users and avoiding collisions.

- It resolves the addressing of source station as well as the destination station, or groups of destination stations.
- It performs multiple access resolutions when more than one data frame is to be transmitted. It determines the channel access methods for transmission.
- It also performs collision resolution and initiating retransmission in case of collisions.It generates the frame check sequences and thus contributes to protection against transmission errors.

Logical Link control:

The Logical Link Control (LLC) sub layer provides the logic for the data link; thus it controls the synchronization, flow control. With connection-oriented communication, each LLC frame that is sent is acknowledged.

HIPERLAN 2:

- HiperLAN 2 was developed as part of a family of high-speed wireless access standards able to connect to Universal Mobile Telecommunications Systems (UMTS), ATM, and Internet Protocol (IP)-based networks.

- Like its American companion IEEE 802.11a, HiperLAN 2 employs OFDM modulation technology employing 455MHz of the Unlicensed National Information Infrastructure (U-NII) frequency bands, from 5.150GHz to 5.350Ghz and from 5.470GHz to 5.725GHz.
- Data rates for HiperLAN 2 range from 6Mbps to 54Mbps.
- It uses OFDM(orthogonal frequency division multiplexing). It uses two band which supports both Indoor and outdoor environment.
- Orthogonal Frequency Division Multiplexing, is a form of signal modulation that divides a high data rate modulating stream placing them onto many slowly modulated narrowband close-spaced subcarriers, and in this way is less sensitive to frequency selective fading.

Difference between Hiperlan1 and Hiperlan 2

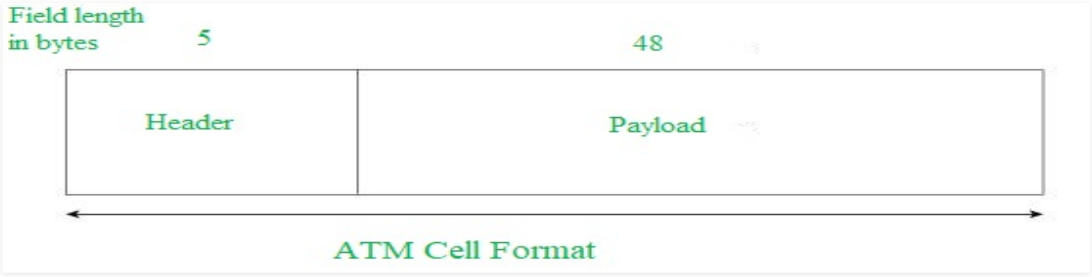
Specifications	HIPERLAN1	HIPERLAN2
Access techniques	TDMA	TDMA
Modulation technique	GMSK	OFDM
Data rates	23Mbps	Up to 54Mbps
frequency	5.1Ghz to 5.3 Ghz	5.1Ghz to 5.3 Ghz
Antenna type	Omni Directional	Omni Directional
Coverage area	50m	50 to 100 m

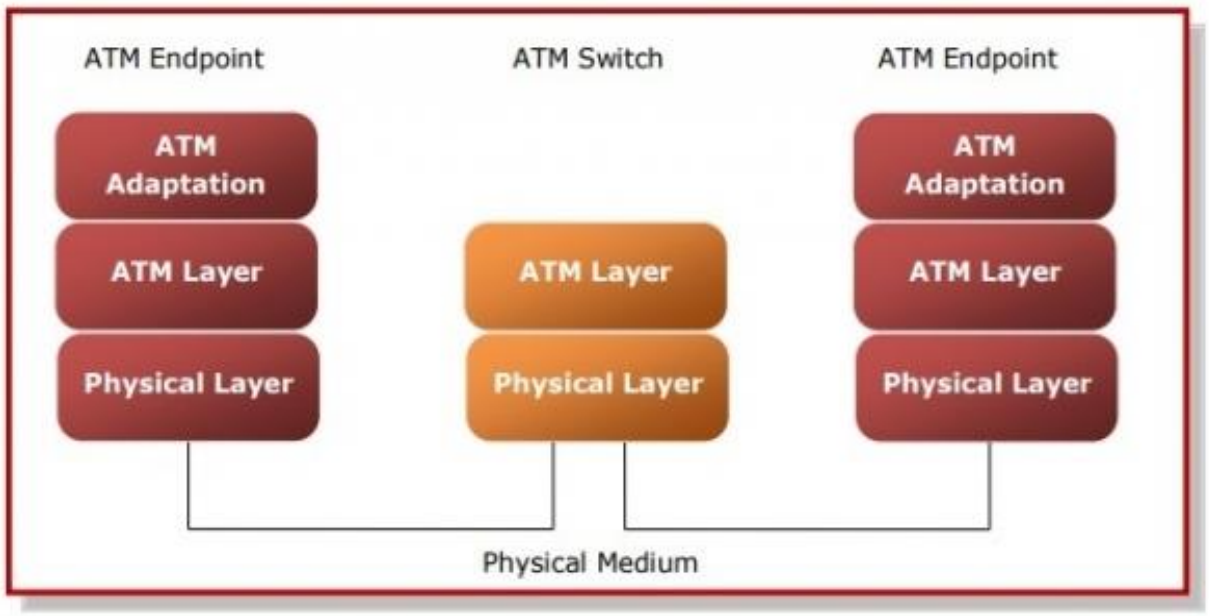
Dr.K.Gopi,
Department of ECE.

ATM Network

- ATM stands for Asynchronous Transfer Mode. It is a switching technique that uses time division multiplexing (TDM) for data communications. ATM networks are connection oriented networks for cell relay that supports voice, video and data communications.
- Asynchronous Transfer Mode (ATM) is an adaptable technology that can be used in LANs and WANs (Wide-Area Networks). Asynchronous, in the context of ATM, means that sources are not limited to sending data during a set time slot, which is the case with circuit switching.
- ATM uses fixed-size packets called “cells.” Each 53-byte ATM cell contains 48 bytes of data payload and 5 bytes of routing information in the header.
- The header provides addressing information for switching the packet to its destination. The payload section carries the actual information, which can be data, voice, or video. The payload is properly called the user information field.
- The fixed size of an ATM cell makes ATM traffic simple and predictable and makes it possible for ATM to operate at high speeds.
- The pre specified bit rates are either 155.520 Mbps or 622.080 Mbps. Speeds on ATM networks can reach 10 Gbps.

STRUCTURE OF PACKET:





ATM ARCHITECTURE

ATM Reference Model

- ATM reference model comprises of three layers −
- **Physical Layer** − This layer corresponds to physical layer of OSI model. At this layer the cells are converted into bit streams and transmitted over the physical medium. This layer has two sub layers − PMD sub layer (Physical Medium Dependent) and TC sub layer (Transmission Covergence) sub layer.
- **ATM Layer** − This layer is comparable to data link layer of OSI model. It accepts the 48 byte segments from the upper layer, adds a 5 byte header to each segment and converts into 53 byte cells. This layer is responsible for routing of each cell, traffic management, multiplexing and switching.
- **ATM Adaptation Layer (AAL)** − This layer corresponds to network layer of OSI model. It provides facilities to the existing packet switched networks to connect to ATM network and use its services. It accepts the data and converts them into fixed sized segments. The transmissions can be of fixed or variable data rate.

Dr.K.Gopi,
Department of ECE.

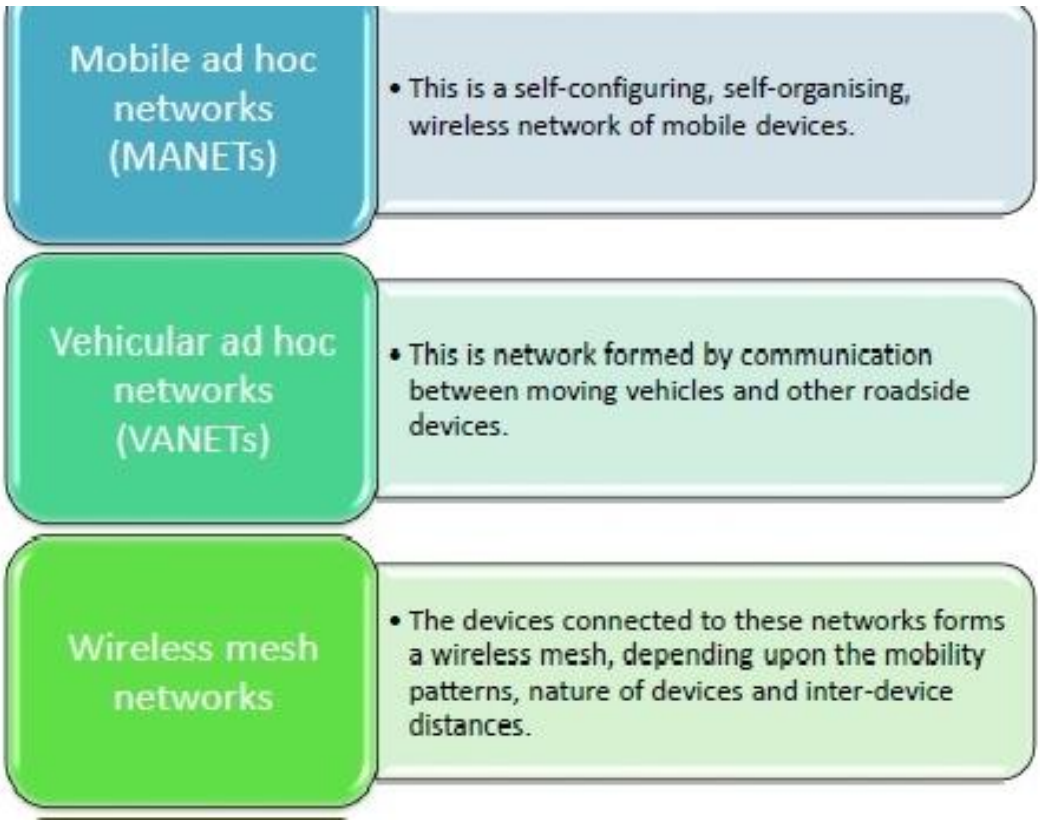
Adhoc Networks

An ad hoc network is one that is spontaneously formed when devices connect and communicate with each other. The term ad hoc is a Latin word that literally means "for this," .

Ad hoc networks are mostly wireless local area networks (LANs). The devices communicate with each other directly instead of relying on a base station or access points as in wireless LANs for data transfer co-ordination. Each device participates in routing activity, by determining the route using the routing algorithm and forwarding data to other devices via this route.

Classifications of Ad Hoc Networks

Ad hoc networks can be classified into several types depending upon the nature of their applications. The most prominent ad hoc networks that are commonly incorporated are illustrated in the diagram below −



Dr.K.Gopi,
Department of ECE.

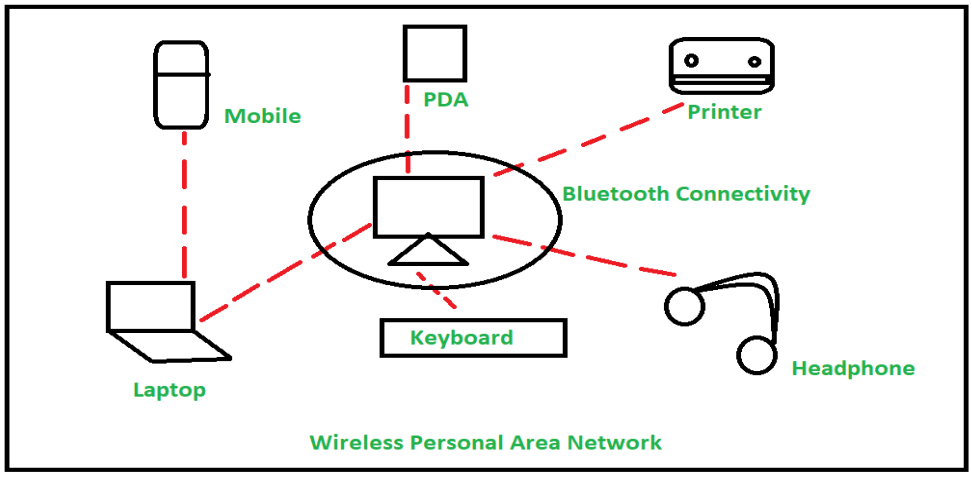
WPAN(Wireless Personal Area Network)

A WPAN (wireless personal area network) is a personal area network - a network for interconnecting devices centered around an individual person's workspace - in which the connections are wireless. Typically, a wireless personal area network uses some technology that permits communication within about 10 meters - in other words, a very short range. One such technology is Bluetooth, which was used as the basis for a new standard, IEEE 802.15.

A WPAN could serve to interconnect all the ordinary computing and communicating devices that many people have on their desk or carry with them today - or it could serve a more specialized purpose such as allowing the surgeon and other team members to communicate during an operation. A key concept in WPAN technology is known as *plugging in*.

In the ideal scenario, when any two WPAN-equipped devices come into close proximity (within several meters of each other) or within a few kilometers of a central server, they can communicate as if connected by a cable. Another important feature is the ability of each device to lock out other devices selectively, preventing needless interference or unauthorized access to information.

The technology for WPANs is in its infancy and is undergoing rapid development. Proposed operating frequencies are around 2.4 GHz in digital modes. The objective is to facilitate seamless operation among home or business devices and systems. Every device in a WPAN will be able to plug in to any other device in the same WPAN, provided they are within physical range of one another



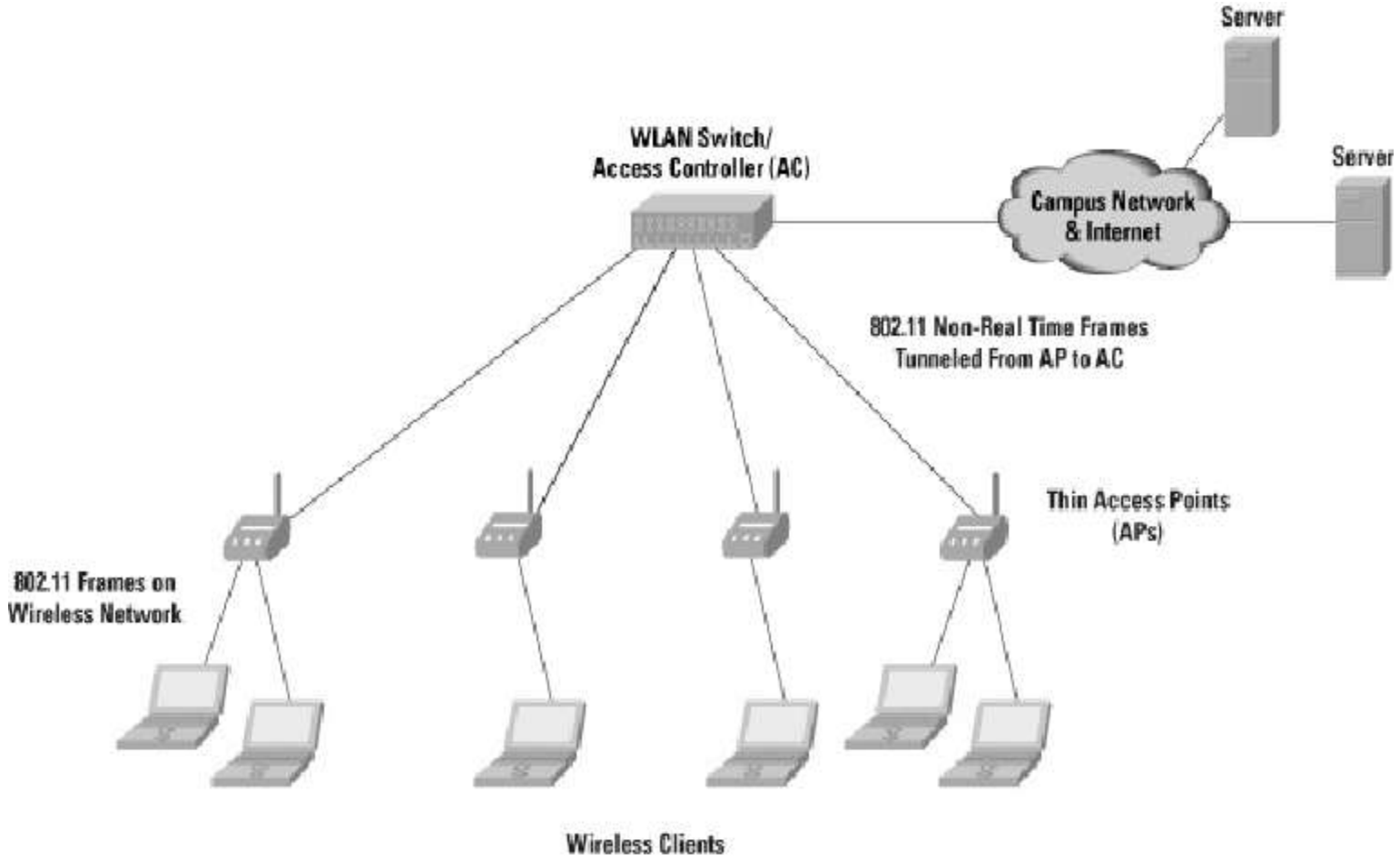
WIRELESS LANS

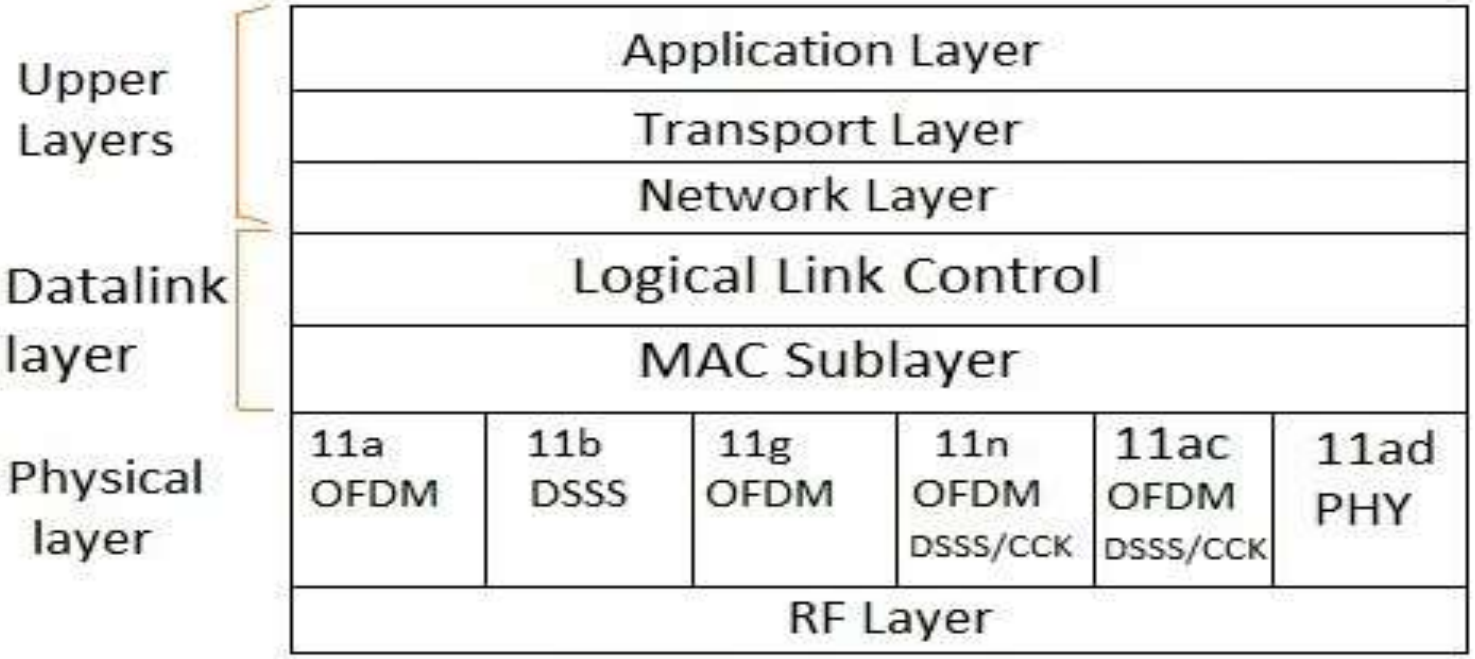
- wireless LAN standard is 802.11.
- Wireless LANs can also be used to let two or more nearby computers communicate without using the Internet.
- popular, and homes, offices, cafes, libraries, airports, zoos, and other public places are being outfitted with them to connect computers, PDAs, and smart phones to the Internet.

Architecture and Protocol Stack

- Has two modes.
- The most popular mode is to connect clients, such as laptops and smart phones, to another network, such as a company intranet or the Internet.
- In **infrastructure mode**, **each client is associated with an AP (Access Point) that is in turn connected to the other network.**
- The client sends and receives its packets via the AP.
- Several access points may be connected together, typically by a wired network called a **distribution system**, **to form an extended 802.11 network.**

- In this case, clients can send frames to other clients via their APs.
- The other mode is called an **ad hoc network.**
- This mode is a collection of computers that are associated so that they can directly send frames to each other.
- There is no access point. Since Internet access is the killer application for wireless, ad hoc networks are not very popular.
- The protocols of the 802 protocols, including 802.11 and Ethernet, have a certain commonality of structure.


Server
WLAN Switch/
Access Controller (AC)
Server
Campus Network
& Internet
802.11 Non-Real Time Frames
Tunneled From AP to AC
Thin Access Points
(APs)
802.11 Frames on
Wireless Network
Wireless Clients



WLAN protocol stack

- Two of the initial techniques, infrared in the manner of television remote controls and frequency hopping in the 2.4-GHz band, are now defunct.
- The third initial technique, direct sequence spread spectrum at 1 or 2 Mbps in the 2.4-GHz band, was extended to run at rates up to 11 Mbps and quickly became a hit. It is now known as 802.11b.
- New transmission techniques based on the **OFDM** **(Orthogonal Frequency Division Multiplexing).**
- The first is called 802.11a and uses a different frequency band, 5 GHz.
- The second stuck with 2.4 GHz and compatibility. It is called 802.11g.
- Both give rates up to 54 Mbps.

The 802.11 Physical Layer

- 802.11 techniques use short-range radios to transmit signals in either the 2.4-GHz or the 5-GHz ISM frequency bands.
- Manufacturers of cordless phones, microwave ovens, and countless other devices, all of which compete with laptops for the same spectrum.
- If the wireless signal is weak, a low rate can be used.
- If the signal is clear, the highest rate can be used.
- This adjustment is called **rate adaptation.**

802.11b

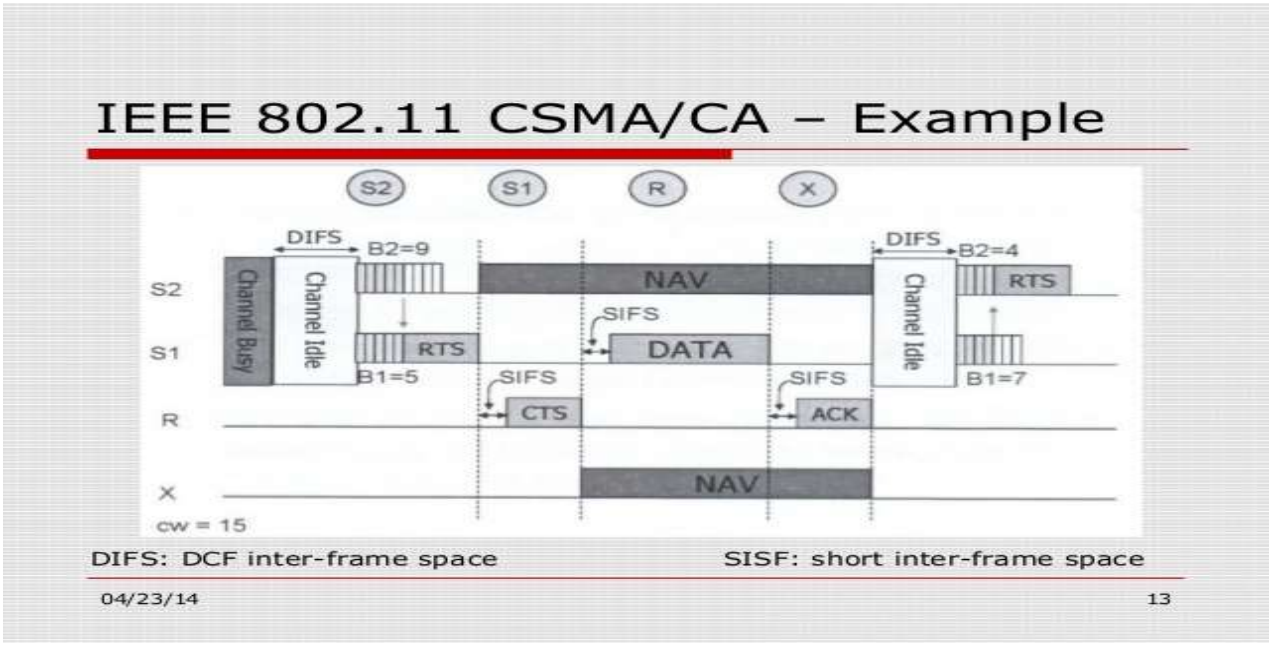
- It is a spread-spectrum method that supports rates of 1, 2, 5.5, and 11 Mbps, though in practice the operating rate is nearly always 11 Mbps. It is similar to the CDMA system.
- The spreading sequence used by 201.11b is a **Barker sequence.**
- the Barker sequence is used with **BPSK modulation** to send 1 bit per 11 chips.
- The chips are transmitted at a rate of 11 Mchips/sec.
- To send at 2 Mbps, it is used with **QPSK modulation** to send 2 bits per 11 chips.
- The higher rates are different. These rates use a technique called **CCK (Complementary Code Keying)** to construct codes instead of the Barker sequence.

- The 802.11a method is based on **OFDM** (Orthogonal Frequency Division Multiplexing) because OFDM uses the spectrum efficiently and resists wireless signal degradations such as multipath.
- The use of multiple antennas gives a large speed boost, or better range and reliability instead. MIMO, like OFDM, is one of those clever communications ideas that is changing wireless designs.

The 802.11 MAC Sublayer Protocol

- The 802.11 MAC sublayer protocol is quite different from that of Ethernet, due to two factors that are fundamental to wireless communication.
- First, radios are nearly always half duplex, meaning that they cannot transmit and listen for noise bursts at the same time on a single frequency.
- With wireless, this collision detection mechanism does not work.
- Instead, 802.11 tries to avoid collisions with a protocol called **CSMA/CA** (CSMA with Collision Avoidance).

- the destination immediately sends a short acknowledgement.
-



- Compared to Ethernet, there are two main differences.
- First, starting backoffs early helps to avoid collisions.
- This avoidance is worthwhile because collisions are expensive, as the entire frame is transmitted even if one occurs.
- Second, acknowledgements are used to infer collisions because collisions cannot be detected.
- This mode of operation is called **DCF** (Distributed Coordination Function) because each station acts independently, without any kind of central control.
- The standard also includes an optional mode of operation called **PCF** (Point Coordination Function) in which the access point controls all activity in its cell, just like a cellular base station.
- However, PCF is not used in practice because there is normally no way to prevent stations in another nearby network from transmitting competing traffic.
- The second problem is that the transmission ranges of different stations may be different. With a wire, the system is engineered so that all stations can hear each other. With the complexities of RF propagation this situation does not hold for wireless stations.

- With virtual sensing, each station keeps a logical record of when the channel is in use by tracking the **NAV** (Network Allocation Vector).
- An optional RTS (Request To Send)/CTS (Clear To Send) mechanism uses the NAV to prevent terminals from sending frames at the same time as hidden terminals.

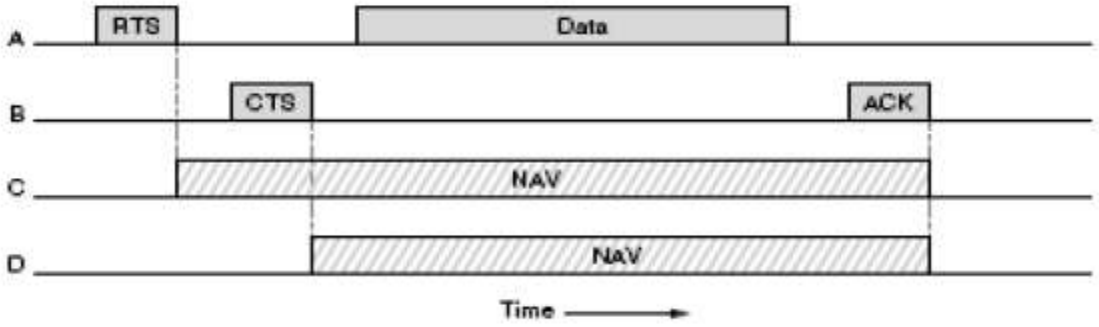
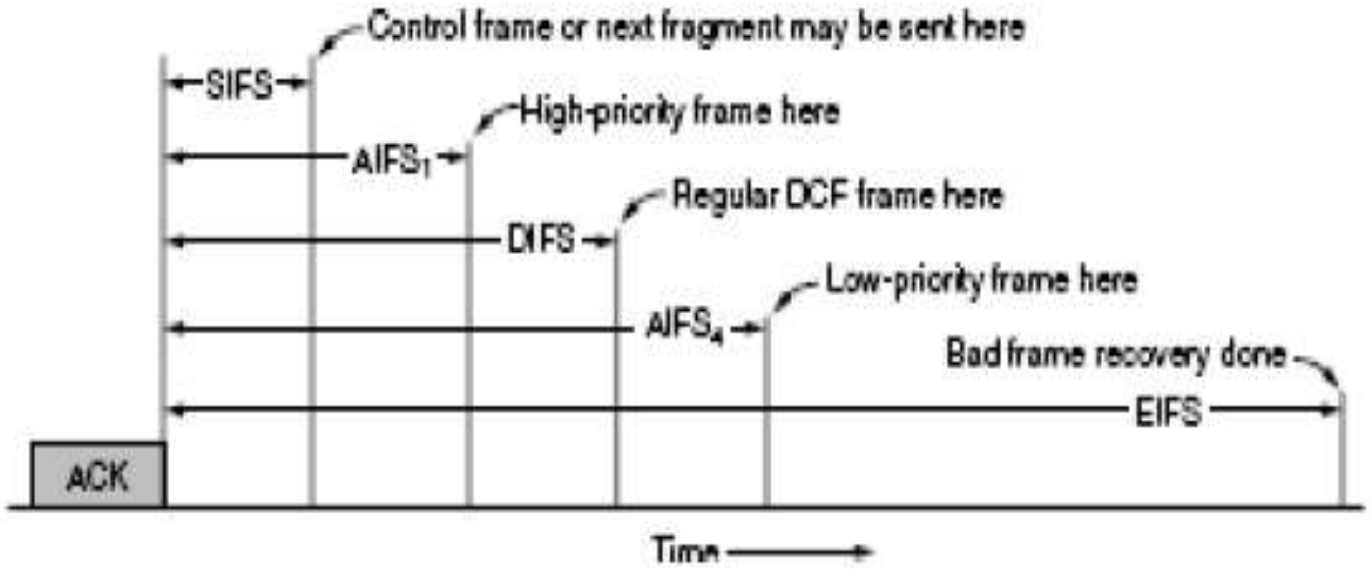


Figure 4-27. Virtual channel sensing using CSMA/CA.

- Alternatively, 802.11 allow frames to be split into smaller pieces, called **fragments**, each with its own checksum.
- The fragment size is not fixed by the standard, but is a parameter that can be adjusted by the AP.
- The fragments are individually numbered and acknowledged using a stop-and-wait protocol.
- Once the channel has been acquired, multiple fragments are sent as a burst.

- The basic mechanism for saving power builds on **beacon frames**.
- Clients can set a power-management bit in frames that they send to the AP to tell it that they are entering **power-save mode**.
- Another power-saving mechanism, called **APSD** (Automatic Power Save Delivery), was also added to 802.11.
- CSMA/CA with carefully defined intervals between frames.
- The trick is to define different time intervals for different kinds of frames.
- The interval between regular data frames is called the **DIFS** (Distributed Coordination Function Inter Frame spacing).
- Any station may attempt to acquire the channel to send a new frame after the medium has been idle for DIFS.
- The usual contention rules apply, and binary exponential backoff may be needed if a collision occurs, this shortest interval is **SIFS** (Short Inter Frame Spacing).


Control frame or next fragment may be sent here
SIFS
High-priority frame here
AIFS1
Regular DCF frame here
DIFS
Low-priority frame here
AIFS4
Bad frame recovery done
EIFS
ACK
Time

- The two **AIFS** (Arbitration InterFrame Space) intervals show examples of two different priority levels. The short interval, AIFS1, is smaller than DIFS but longer than SIFS.
- It can be used by the AP to move voice or other high-priority traffic to the head of the line.
- The last time interval, **EIFS** (Extended Inter Frame Spacing), is used only by a station that has just received a bad or unknown frame, to report the problem.

The 802.11 Frame Structure

- It defines three different classes of frames in the air are **data, control, and management.**
- Each of these has a header with a variety of fields used within the MAC sublayer.
- In addition, there are some headers used by the physical layer, but these mostly deal with the modulation techniques used.

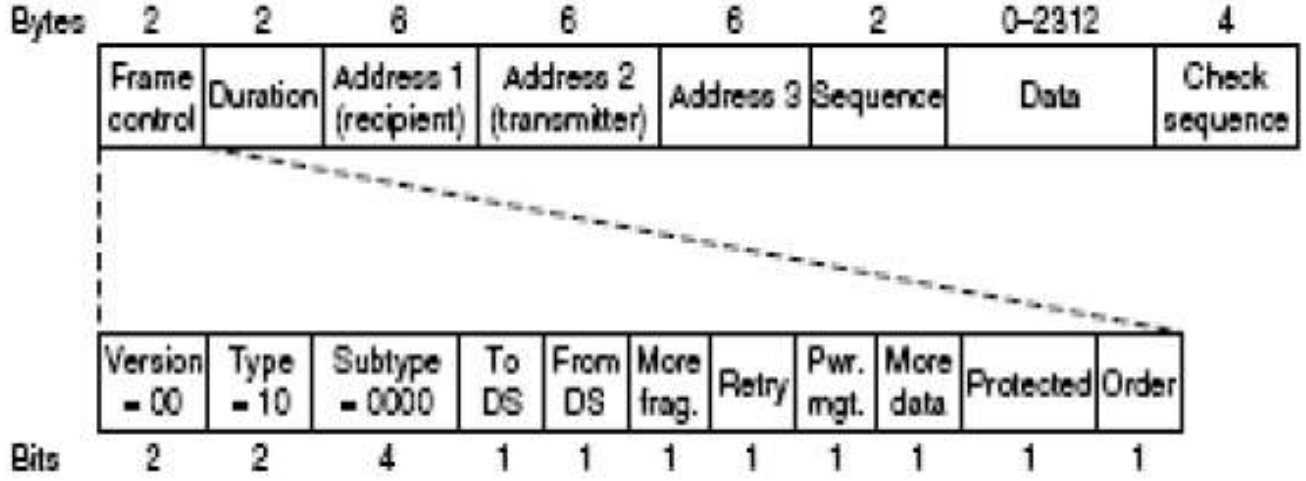


Figure 4-29. Format of the 802.11 data frame.

- The *To DS* and *From DS* bits are set to indicate whether the frame is going to or coming from the network connected to the APs, which is called the distribution system.
- The *More fragments* bit means that more fragments will follow.
- The *Retry bit* marks a retransmission of a frame sent earlier.
- The *Power management bit* indicates that the sender is going into power-save mode.
- The *More data bit* indicates that the sender has additional frames for the receiver.
- The *Protected Frame bit* indicates that the frame body has been encrypted for security.

- Duration field-tells how long the frame and its acknowledgement will occupy the channel, measured in microseconds.
- Addresses field-Data frames sent to or from an AP have three addresses, all in standard IEEE 802 format. The Address1 is the receiver, and the Address2 is the transmitter.
- The Address3 gives this distant endpoint.
- The Sequence field numbers frames so that duplicates can be detected. Of the 16 bits available, 4 identify the fragment and 12 carry a number that is advanced with each new transmission.
- The Data field contains the payload, up to 2312 bytes.
- The Frame check sequence, which is the same 32-bit CRC.
- Management frames have the same format as data frames, plus a format.

- Control frames are short, Like all frames, they have the Frame control, Duration, and Frame check sequence fields.
- However, they may have only one address and no data portion.
- Most of the key information is conveyed with the Subtype field (e.g., ACK, RTS and CTS).

Services

- The association service is used by mobile stations to connect themselves to APs.
- Reassociation lets a station change its preferred AP. This facility is useful for mobile stations moving from one AP to another AP in the same extended 802.11 LAN, like a handover in the cellular network.
- Either the station or the AP may also disassociate, breaking their relationship.
- Stations must also authenticate before they can send frames via the AP,
- recommended scheme, called WPA2 (WiFi Protected Access 2), implements security as defined in the 802.11i standard.

- The scheme that was used before WPA is called WEP (Wired Equivalent Privacy).
- the distribution service determines how to route them. If the destination is local to the AP, the frames can be sent out directly over the air. Otherwise, they will have to be forwarded over the wired network.
- The integration service handles any translation that is needed for a frame to be sent outside the 802.11 LAN, or to arrive from outside the 802.11 LAN.
- Data transmission is what it is all about, so 802.11 naturally provides a data delivery service.

- privacy service that manages the details of encryption and decryption by The encryption algorithm for WPA2 is based on **AES** (Advanced Encryption Standard).
- To handle traffic with different priorities, there is a QOS traffic scheduling service.
- The transmit power control service gives stations the information they need to meet regulatory limits on transmit power that vary from region to region.
- The dynamic frequency selection service give stations the information they need to avoid transmitting on frequencies in the 5-GHz band that are being used for radar in the proximity.