Program : **B.E**

Subject Name: **Advance Computer Networks**

Subject Code: **CS-8004**

Semester: **8th**

CS-8004 Elective –VI (3)
Advance Computer Networks
Subject Notes: UNIT-V

Introduction to Wireless Transmission

Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the air and are received and interpreted by appropriate antennas.

When an antenna is attached to electrical circuit of a computer or wireless device, it converts the digital data into wireless signals and spread all over within its frequency range. The receptor on the other end receives these signals and converts them back to digital data.

A little part of electromagnetic spectrum can be used for wireless transmission.

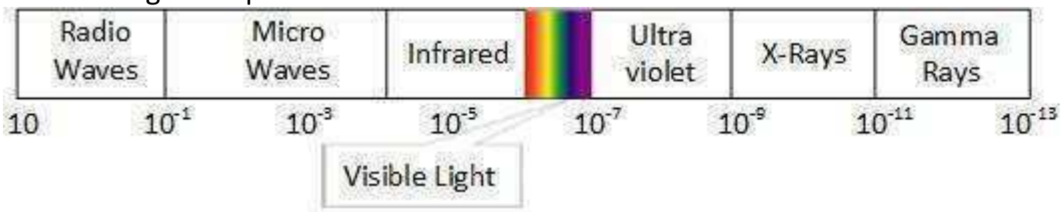


Figure No. 5.1 Wireless transmission

Wireless transmission may refer to:

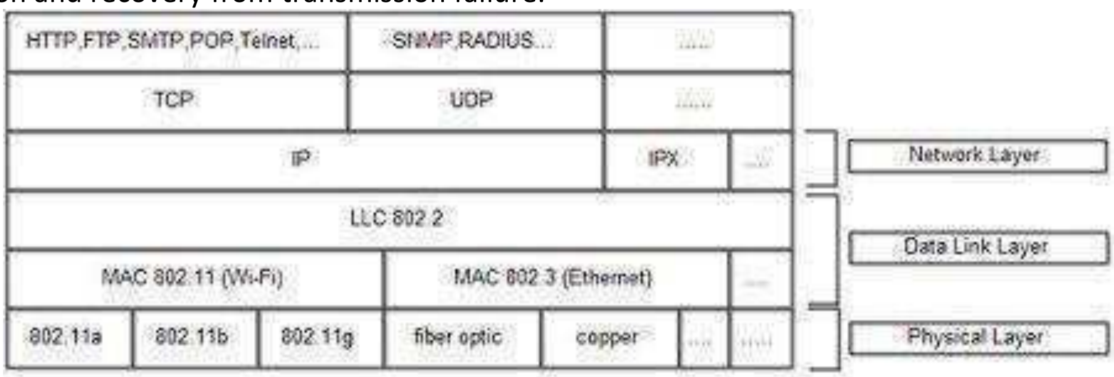
- Radio, the wireless transmission of signals through free space by radio waves instead of cables, like telegraphs
- Wireless communication, all types of non-wired communication
- Wireless power, the transmission of electrical energy without man-made conductors.

The transmission of data or information from one place to another wirelessly is referred as wireless communication. This provides an exchange of data without any conductor through RF and radio signals.

Media Access Control (MAC)

The Media Access Control (MAC) data communication Networks protocol sub-layer, also known as the Medium Access Control, is a sub-layer of the data link layer specified in the seven-layer OSI model. The medium access layer was made necessary by systems that share a common communications medium. The MAC layer is the "low" part of the second OSI layer, the layer of the "data link". The IEEE divided this layer into two layers "above" is the control layer the logical connection (Logical Link Control, LLC) and "down" the control layer the medium access (MAC).

In LAN nodes uses the same communication channel for transmission. The MAC sub-layer has two primary responsibilities: Data encapsulation, including frame assembly before transmission, and frame parsing/error detection during and after reception. Media access control, including initiation of frame transmission and recovery from transmission failure.



Network layers.

Figure No.5.2 Media Access Control (MAC)

IEEE 802.11

Wireless networks are based on the IEEE 802.11 standards. A basic wireless network consists of multiple stations communicating with radios that broadcast in either the 2.4GHz or 5GHz band (though this varies according to the locale and is also changing to enable communication in the 2.3 GHz and 4.9 GHz ranges).

Wireless Operating Mode

The IEEE 802.11 standards specify two operating modes: **infrastructure mode** and **ad hoc mode**.

1. **Infrastructure mode** is used to connect computers with wireless network adapters, also known as wireless clients, to an existing wired network with the help from wireless router or access point. The 2 examples which I specified above operate in this mode.
2. **Ad hoc mode** is used to connect wireless clients directly together, without the need for a wireless router or access point. An ad hoc network consists of up to 9 wireless clients, which send their data directly to each other. Click here to learn more on this ad hoc mode.

#IEEE 802.11 Architecture:

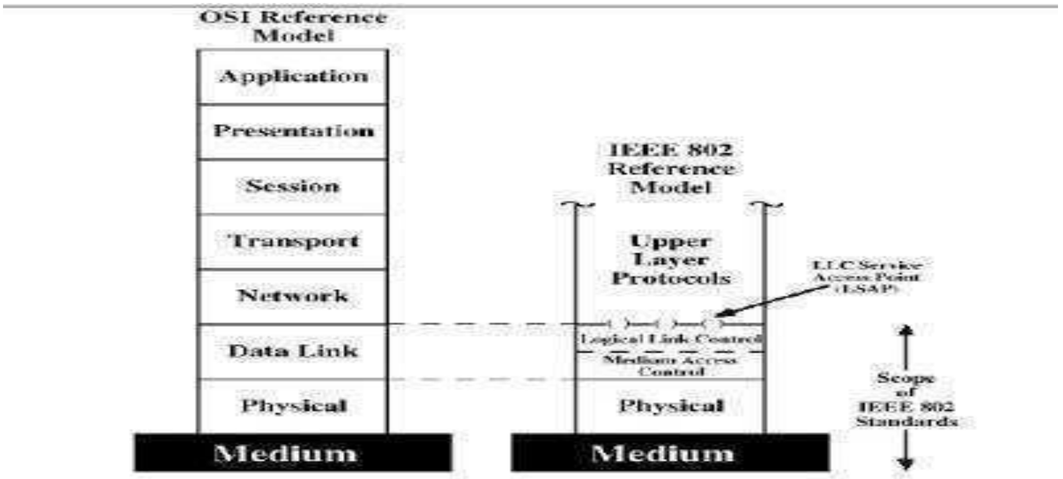


Figure No. 5.3 IEEE 802.11 Architecture

#Functions of physical layer: Functions includes encoding/decoding of signals, Preamble generation/removal (for synchronization), Bit transmission/reception and also includes specification of the transmission medium. It also provides specification for converting bits to a RF signal: FHSS (Frequency Hopping Spread Spectrum), DSSS (Direct Sequence Spread Spectrum), OFDM (Orthogonal Frequency Division), HR-DSS (High Rate-DSSS) and OFDM (802.11 g)

1. **FHSS:** Frequency band is 2.4 GHz ISM Band (2.402 – 2.480 GHz). The band divided into 79 equal sub bands of 1 MHz each. Sender sends one frequency for a short period of time, then hope to another carrier frequency. Thus there are N such hopping in one cycle. The cycle repeats itself after N hopping. Main advantage is that unauthorized person cannot understand transmitted data.
2. **DSSS:** Frequency band is 2.4 GHz ISM Band. Each bit is first converted into a group of bits called as chip code. For example for 0, chip code is 100011, for 1 chip code is 111010 etc.
3. **HR DSSS:** Frequency band is 2.4 GHz ISM Band. Encoding is also used. 4 or 8 bits of original data converted into one symbol.
4. **OFDM:** Frequency band is 5 GHz ISM Band. Band is sub divided into 52 sub bands. 48 are used for sending 48 groups of bits and 4 are used for sending control information. These sub bands are used randomly in order to increase the security of transmitted data

#Functions of medium access control (MAC) layer includes: On transmission, assemble data into a frame with address and error detection fields, on reception, disassemble frame and perform address recognition and error detection. Logical link control (LLC) Layer provides an interface to higher layers and perform flow and error control.

#High-performance local area network (HIPERLAN)

A High-performance local area network (HIPERLAN) is an alternative wireless LAN standard to the IEEE 802.11. It is one of four standards specified by the European telecommunications standards institute (ETSI) to provide a concatenated service of interoperable technologies from different locations. HIPERLAN uses cellular-based data networks to connect to an ATM backbone. The main idea behind HIPERLAN is to provide an infrastructure or ad-hoc wireless with low mobility and a small radius. HIPERLAN supports isochronous traffic with low latency.

#Components of a HIPERLAN include:

1 Physical Layer: This layer provides the standard functions, including radio frequency functions.

Link Adaptation: This standard allows the access point to convey information in an uplink or downlink direction.

The HIPERLAN physical layer also specifies some link adaptation algorithms to be used.

2 Data Link Control (DLC) Layer: This layer includes the Media Access Control (MAC), Radio Link Control (RLC), Dynamic Frequency Selection (DFS) and Error Control (EC) protocols. Convergence Layer: Its basic function is to provide the HIPERLAN DLC and physical access to other data networks.

The standard serves to ensure the possible interoperability of different manufacturers' wireless communications equipment that operate in this spectrum. The HIPERLAN standard only describes a common air interface including the physical layer for wireless communications equipment, while leaving decisions on higher level configurations and functions open to the equipment manufacturers.

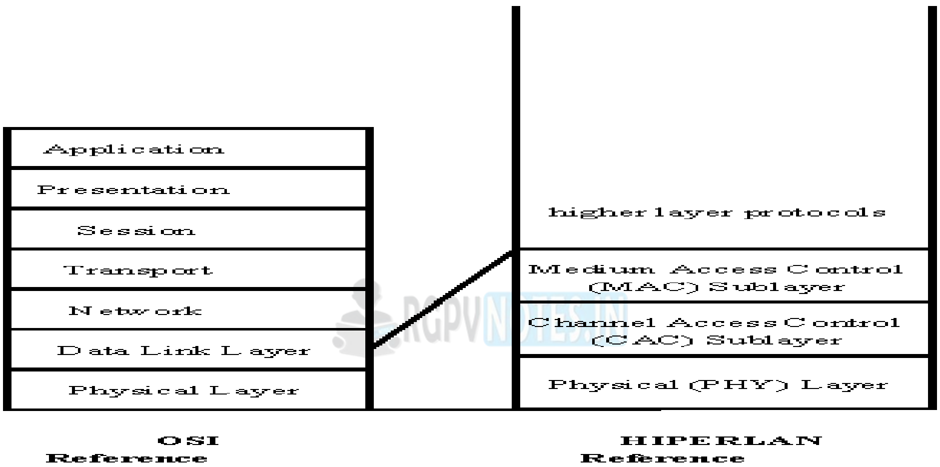


Figure No.5.4 HIPERLAN

HIPERLAN is the short form of High Performance Radio LAN. It is variant of IEEE 802.11 standard developed by ETSI BRAN for use in European region.

Features of HIPERLAN/1:	**Features of HIPERLAN/2:**
Operates at 5GHz • Supports data rate up to 19 Mbps. • It uses SC (Single Carrier) modulation such as GMSK. • It uses complex equalizer to take care of delay spread.	Operates at 5GHz with 455MHz bandwidth. • Supports data rate of 6 Mbps to 54 Mbps similar to 802.11a • it uses multi carrier (i.e. OFDM) modulation like 802.11a • It uses two bands one for indoor use and the other for outdoor use with power at 200 milli Watt and 1 Watt respectively.

Difference between HIPERLAN/1 and HIPERLAN/2

Following table summarizes key difference between HIPERLAN/1 and HIPERLAN/2 standards.

Specifications	HIPERLAN/1	HIPERLAN/2

Access technique	TDMA, EY NPMA	TDMA, TDD
Modulation technique	GMSK, FSK	BPSK-OFDM, QPSK-OFDM, 16QAM-OFDM, 64QAM-OFDM
Data rate (Mbps)	23 (HBR), 1.4 (LBR)	From 6, 9, 12, 18, 27, 36, 48, 54
Frequency of operation	5.1 GHz to 5.3 GHz	5.1 GHz to 5.3 GHz
Data rate	23.2 Mbps	Greater than 20 Mbps
Application	WLAN	Wireless ATM, Indoor Access
Topology	Infrastructure, De-centralised Ad-Hoc	cellular, centralized
Antenna type	Omni-directional	Omni-directional
Coverage Range	50 meters	50 to 100 meters
Interface	LAN	ATM networks
Mobility	less than 10 m/s	less than 10 m/s

Difference between HIPERLAN Type-3 (HIPERACCESS) Vs HIPERLAN Type-4 (HIPERLINK)

Following are the features of HIPERLAN Type-3(HIPERACCESS):

Following are the features of

Features of HIPERLAN Type-3(HIPERACCESS)	Features of HIPERLAN Type-4(HIPERLINK)
• Frequency: 5.1 GHz to 5.3 GHz • Topology: Uni-directional or point to multi-point • Antenna type: directional • Range: 5000 meters • Data rate: >20 Mbps • Mobility: stationary	• Frequency: 17.1 to 17.3 GHz • Topology: Directional • Antenna type: directional • Range: 150 meters • Data rate: 155 Mbps • Mobility: stationary .

#Bluetooth

Bluetooth is, with the infrared, one of the major wireless technologies developed to achieve WPAN. Bluetooth is a wireless LAN technology used to connect devices of different functions such as telephones, computers (laptop or desktop), notebooks, cameras, printers and so on. Bluetooth is an example of personal area network.

• Bluetooth project was started by SIG (Special Interest Group) formed by four companies IBM, Intel, Nokia and Toshiba for interconnecting computing and communicating devices using short-range, lower-power, inexpensive wireless radios.

Bluetooth technology is used for several computer and non computer application:

1. It is used for providing communication between peripheral devices like wireless mouse or keyboard with the computer.
2. It is used by modern healthcare devices to send signals to monitors.
3. It is used by modern communicating devices like mobile phone, PDAs, palmtops etc to transfer data rapidly.
4. It is used for dial up networking. Thus, allowing a notebook computer to call via a mobile phone.
5. It is used for cordless telephoning to connect a handset and its local base station.
6. It also allows hands-free voice comml1nication with headset.
7. It also enables a mobile computer to connect to a fixed LAN.
8. It can also be used for file transfer operations from one mobile phone to another.
9. Bluetooth uses omni directional radio waves that can through wallsor other non-metal barriers.

Bluetooth devices have a built-in short range radio transmitter. The rate provided is 1Mbps and uses 2.4 GHz bandwidth.

Bluetooth is that when the device is within the scope of a other devices automatically start the transfer information without the user noticing. A small network between the devices is created and the user can accessed as if there were cables.

#Bluetooth Architecture

Bluetooth architecture defines two types of networks:

1. Piconet
2. Scattemet

1. Piconet

• Piconet is a Bluetooth network that consists of one primary (master) node and seven active secondary (slave) nodes.

• Thus, piconet can have up to eight active nodes (1 master and 7 slaves) or stations within the distance of 10 meters.

• There can be only one primary or master station in each piconet.

• The communication between the primary and the secondary can be one-to-one or one-to-many.

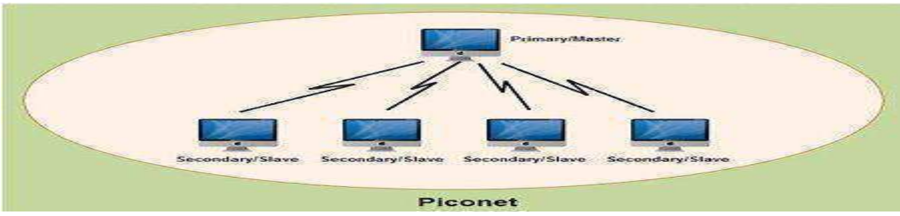


Figure No.5.5 Piconet

• All communication is between master and a slave. Salve-slave communication is not possible.

• In addition to seven active slave station, a piconet can have upto 255 parked nodes. These parked nodes are secondary or slave stations and cannot take part in communication until it is moved from parked state to active state.

2. Scatternet

• Scattemet is formed by combining various piconets.

• A slave in one piconet can act as a master or primary in other piconet.

• Such a station or node can receive messages from the master in the first piconet and deliver the message to its slaves in other piconet where it is acting as master. This node is also called bridge slave.

• Thus a station can be a member of two piconets.

• A station cannot be a master in two piconets.

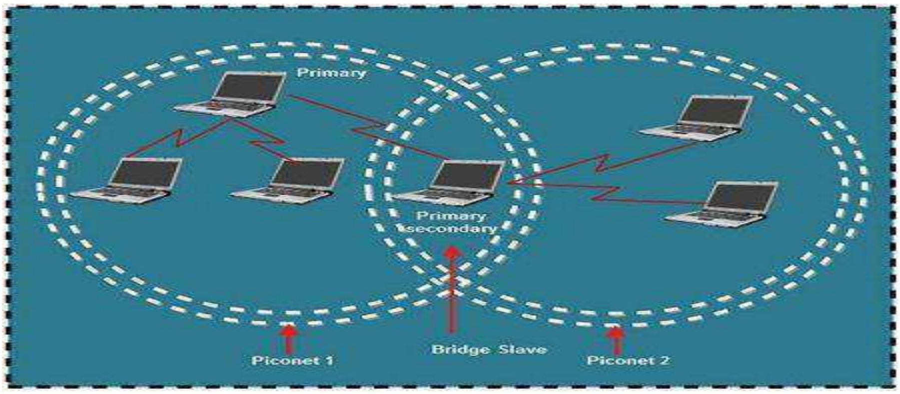


Figure No.5.6 Scatternet

#Bluetooth layers and Protocol Stack

• Bluetooth standard has many protocols that are organized into different layers.
• The layer structure of Bluetooth does not follow OS1 model, TCP/IP model or any other known model.
• The different layers and Bluetooth protocol architecture.

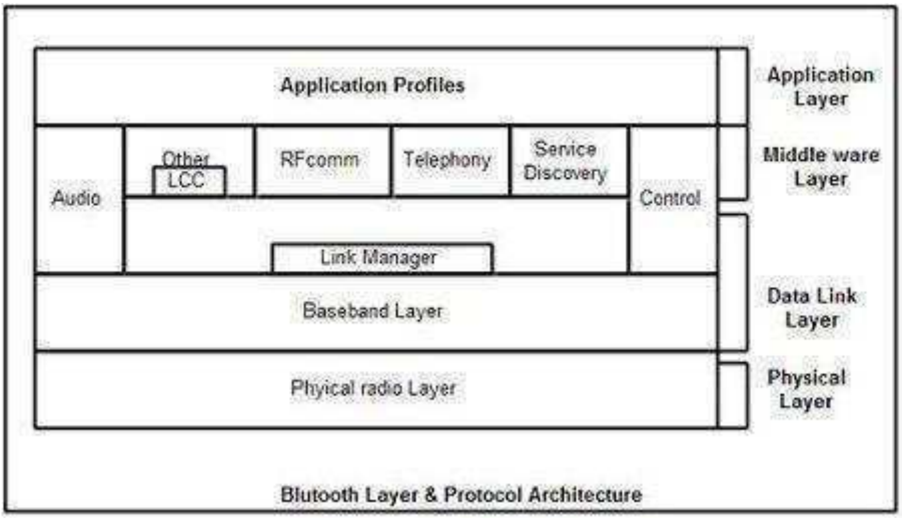


Figure No.5.7 Bluetooth layers and protocol architecture

#Radio Layer

• The Bluetooth radio layer corresponds to the physical layer of OSI model.
• It deals with ratio transmission and modulation.
• The radio layer moves data from master to slave or vice versa.
• It is a low power system that uses 2.4 GHz ISM band in a range of 10 meters.
• This band is divided into 79 channels of 1MHz each. Bluetooth uses the Frequency Hopping Spread Spectrum (FHSS) method in the physical layer to avoid interference from other devices or networks.
• Bluetooth hops 1600 times per second, i.e. each device changes its modulation frequency 1600 times per second.

#Baseband Layer

• Baseband layer is equivalent to the MAC sublayer in LANs.
• Bluetooth uses a form of TDMA called TDD-TDMA (time division duplex TDMA).
• Master and slave stations communicate with each other using time slots.
• The master in each piconet defines the time slot of 625 µsec.
• In TDD- TDMA, communication is half duplex in which receiver can send and receive data but not at the same time.
• If the piconet has only no slave; the master uses even numbered slots (0, 2, 4, ...) and the slave uses odd-numbered slots (1, 3, 5, ...). Both master and slave communicate in half duplex mode. In slot 0, master sends & secondary receives; in slot 1, secondary sends and primary receives.

• If piconet has more than one slave, the master uses even numbered slots. The slave sends in the next odd-numbered slot if the packet in the previous slot was addressed to it.

In Baseband layer, two types of links can be created between a master and slave. These are:

1. Asynchronous Connection-less (ACL)

• It is used for packet switched data that is available at irregular intervals.
• ACL delivers traffic on a best effort basis. Frames can be lost & may have to be retransmitted.
• A slave can have only one ACL link to its master.
• Thus ACL link is used where correct delivery is preferred over fast delivery.
• The ACL can achieve a maximum data rate of 721 kbps by using one, three or more slots.

2. Synchronous Connection Oriented (SCO)

• sco is used for real time data such as sound. It is used where fast delivery is preferred over accurate delivery.
• In an sco link, a physical link is created between the master and slave by reserving specific slots at regular intervals.
• Damaged packet; are not retransmitted over sco links.
• A slave can have three sco links with the master and can send data at 64 Kbps.

#Logical Link, Control Adaptation Protocol Layer (L2CAP)

• The logical unit link control adaptation protocol is equivalent to logical link control sublayer of LAN.
• The ACL link uses L2CAP for data exchange but sco channel does not use it.

The various function of L2CAP is:

1. Segmentation and reassembly

• L2CAP receives the packets of upto 64 KB from upper layers and divides them into frames for transmission.
• It adds extra information to define the location of frame in the original packet.
• The L2CAP reassembles the frame into packets again at the destination.

2. Multiplexing

• L2CAP performs multiplexing at sender side and demultiplexing at receiver side.
• At the sender site, it accepts data from one of the upper layer protocols frames them and deliver them to the Baseband layer.
• At the receiver site, it accepts a frame from the baseband layer, extracts the data, and delivers them to the appropriate protocol1ayer.

3. Quality of Service (QOS)

• L2CAP handles quality of service requirements, both when links are established and during normal operation.
• It also enables the devices to negotiate the maximum payload size during connection establishment.

#Bluetooth Frame Format

The various fields of blue tooth frame format are:

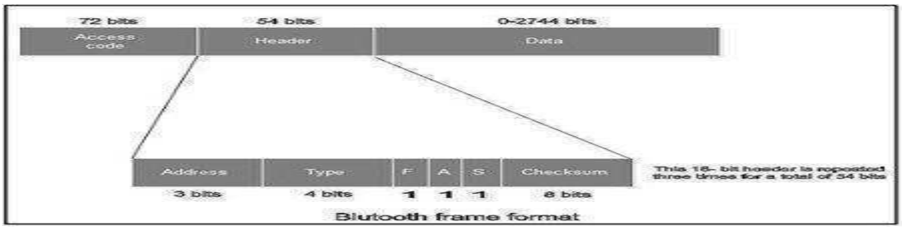


Figure No.5.8 Bluetooth Frame Format

1. Access Code: It is 72 bit field that contains synchronization bits. It identifies the master.

2. Header: This is 54-bit field. It contain 18 bit pattern that is repeated for 3 time.

The header field contains following subfields:

(i) Address: This 3 bit field can define upto seven slaves (1 to 7). If the address is zero, it is used for broadcast communication from primary to all secondary's.

(ii)Type: This 4 bit field identifies the type of data coming from upper layers.

(iii) F: This flow bit is used for flow control. When set to 1, it means the device is unable to receive more frames.

(iv) A: This bit is used for acknowledgement.
(v) S: This bit contains a sequence number of the frame to detect retransmission. As stop and wait protocol is used, one bit is sufficient.
(vi) Checksum: This 8 bit field contains checksum to detect errors in header.
3. Data: This field can be 0 to 2744 bits long. It contains data or control information coming from upper layers.

 # WAP (Wireless Application Protocol)

WAP (Wireless Application Protocol) is a specification for a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access, including e-mail, the World Wide Web, newsgroups, and instant messaging. While Internet access has been possible in the past, different manufacturers have used different technologies. In the future, devices and service systems that use WAP will be able to interoperate.

The WAP layers are:

- Wireless Application Environment (WAE)
- Wireless Session Layer (WSL)
- Wireless Transport Layer Security (WTLS)
- Wireless Transport Layer (WTP)

The WAP was conceived by four companies: Ericsson, Motorola, Nokia, and Unwired Planet (now Phone.com). The Wireless Mark-up Language (WML) is used to create pages that can be delivered using WAP.

#Application Layer

Wireless Application Environment (WAE). This layer is of most interest to content developers because it contains among other things, device specifications, and the content development programming languages, WML, and WML Script.

Session Layer

Wireless Session Protocol (WSP). Unlike HTTP, WSP has been designed by the WAP Forum to provide fast connection suspension and reconnection.

Transaction Layer

Wireless Transaction Protocol (WTP). The WTP runs on top of a datagram service, such as User Datagram Protocol (UDP) and is part of the standard suite of TCP/IP protocols used to provide a simplified protocol suitable for low bandwidth wireless stations.

Security Layer

Wireless Transport Layer Security (WTLS). WTLS incorporates security features that are based upon the established Transport Layer Security (TLS) protocol standard. It includes data integrity checks, privacy, service denial, and authentication services.

Transport Layer

Wireless Datagram Protocol (WDP). The WDP allows WAP to be bearer-independent by adapting the transport layer of the underlying bearer. The WDP presents a consistent data format to the higher layers of the WAP protocol stack, thereby offering the advantage of bearer independence to application developers.

Each of these layers provides a well-defined interface to the layer above it. This means that the internal workings of any layer are transparent or invisible to the layers above it. The layered architecture allows other applications and services to utilise the features provided by the WAP-stack as well. This makes it possible to use the WAP-stack for services and applications that currently are not specified by WAP.

The WAP protocol architecture is shown below alongside a typical Internet Protocol stack.

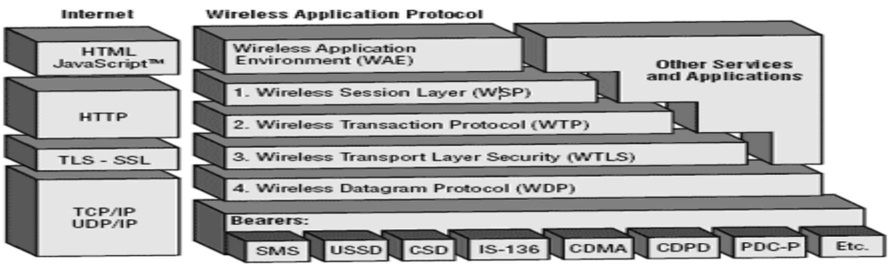


Figure No.5.9 Wireless Application Protocol

WAP works as follows –

- The user selects an option on their mobile device that has a URL with Wireless Markup language (WML) content assigned to it.
- The phone sends the URL request via the phone network to a WAP gateway using the binary encoded WAP protocol.
- The gateway translates this WAP request into a conventional HTTP request for the specified URL and sends it on to the Internet.
- The appropriate Web server picks up the HTTP request.
- The server processes the request just as it would any other request. If the URL refers to a static WML file, the server delivers it. If a CGI script is requested, it is processed and the content returned as usual.
- The Web server adds the HTTP header to the WML content and returns it to the gateway.
- The WAP gateway compiles the WML into binary form.
- The gateway then sends the WML response back to the phone.
- The phone receives the WML via the WAP protocol.
- The micro-browser processes the WML and displays the content on the screen.

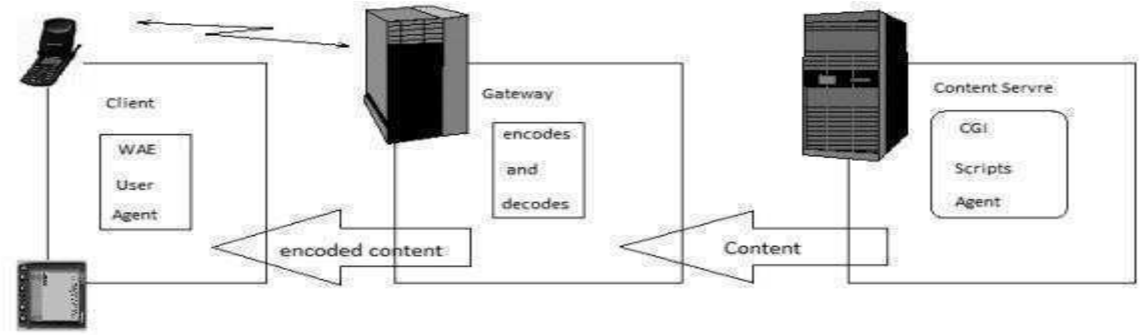


Figure No.5.10 working of Wireless Application Protocol

Global System for Mobile Communication

GSM stands for Global System for Mobile communication. Today, GSM is used by more than 800 million end users spread across 190 countries which represent around 70 percent of today's digital wireless market. So, let's see how it works.

In GSM, geographical area is divided into hexagonal cells whose side depends upon power of transmitter and load on transmitter (number of end user). At the center of cell, there is a base station consisting of a transceiver (combination of transmitter and receiver) and an antenna.

#General Features of GSM

- GSM (Global System for Mobile Communications) is a second-generation (2G) digital mobile telephones standard using a combination Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA) to share the bandwidth among as many subscribers as possible.
- GSM provides only 9.6 kbps data connection. Increase in data rates can be achieved when GSM changes into a radio service based on wide band code division multiple access, and not TDMA.
- GSM digitizes and compresses voice data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900, 1800 or 1,900 MHz frequency bands.
- The uplink and down link frequencies for GSM are different and therefore a channel has a pair of frequencies 80 MHz apart. The separation between uplink and downlink frequencies is called duplex distance.
- In a channel the separation between adjacent carrier frequencies is known as channel separation which is 200 kHz in case of GSM.
- The services supported by GSM are telephony, fax and SMS, call forwarding, caller 10, call waiting and the like.
- GSM supports data at rates up to 9.6 kbps on POTS (Plain Old Telephone Service), ISDN, Packet Switched Public Data Networks, and Circuit Switched Public Data Networks.
- The access methods and protocols for GSM may be fromX.25 or X.32.

- Being a digital system, GSM does not require a modem between subscriber and GSM network. However, an audio modem is required inside the GSM network to establish connection with POTS.

#Architecture of the GSM Network

The generic GSM network architecture is composed of three subsystems as the Radio Subsystem (RSS), the network and Switching Subsystem (NSS) and the Operation Subsystem (OSS). The subscriber carries the Mobile Station, which is part or RSS.

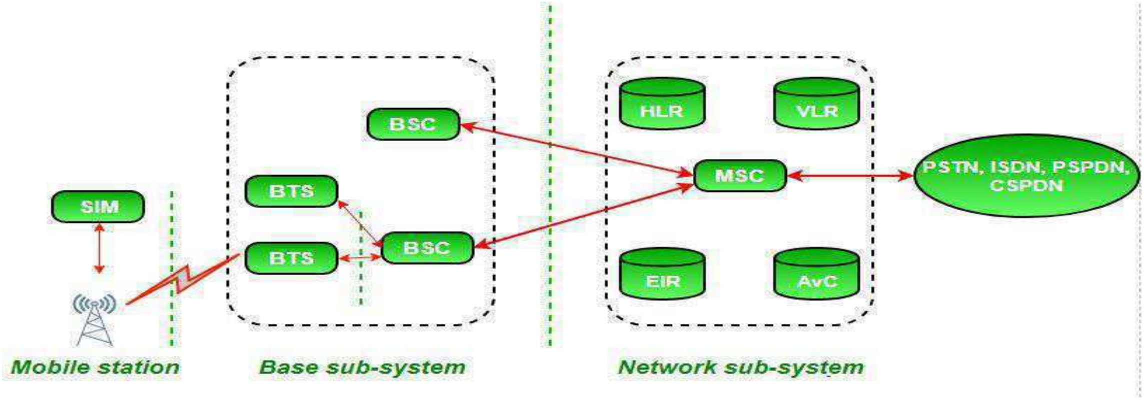


Figure No.5.11 Architecture of the GSM Network

#Function of Components:

1. Mobile station (MS): It refers for mobile station. Simply, it means a mobile phone.
2. Base trans-receiver system (BTS): It maintains the radio component with MS.
3. Base station controller (BSC): Its function is to allocate necessary time slots between the BTS and MSC.
4. Home location register (HLR): It is the reference database for subscriber parameter like subscriber's ID, location, authentication key etc.
5. Visitor location register (VLR): It contains copy of most of the data stored in HLR which is temporary and exist only until subscriber is active.
6. Equipment identity register (EIR): It is a database which contains a list of valid mobile equipment on the network.
7. Authentication centre (AuC): It perform authentication of subscriber.

Carrier Sensed Multiple Accesses (CSMA): CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network. Devices attached to the network cable listen (carrier sense) before transmitting. If the channel is in use, devices wait before transmitting. MA (Multiple Access) indicates that many devices can connect to and share the same network. All devices have equal access to use the network when it is clear.

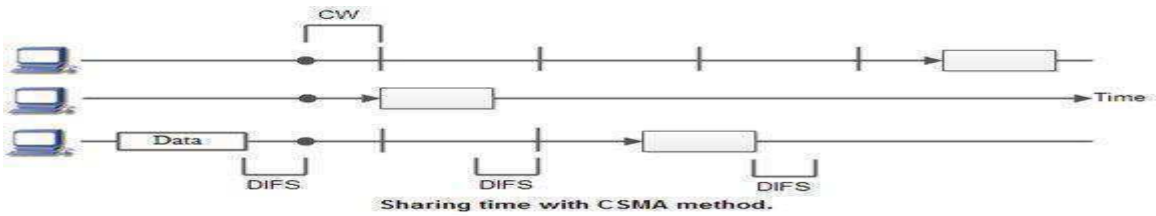


Figure No.5.11 Carrier Sensed Multiple Accesses

CSMA protocol was developed to overcome the problem found in ALOHA i.e. to minimize the chances of collision, so as to improve the performance. CSMA protocol is based on the principle of 'carrier sense'. The station senses the carrier or channel before transmitting a frame. It means the station checks the state of channel, whether it is idle or busy.

Even though devices attempt to sense whether the network is in use, there is a good chance that two stations will attempt to access it at the same time. On large networks, the transmission time between one end of the cable and another is enough that one station may access the cable even though another has already just accessed it.

The chances of collision still exist because of propagation delay. The frame transmitted by one station takes some time to reach other stations. In the meantime, other stations may sense the channel to be idle and transmit their frames. This results in the collision.

There Are Three Different Type of CSMA Protocols
(I) I-persistent CSMA
(ii) Non- Persistent CSMA
(iii) p-persistent CSMA

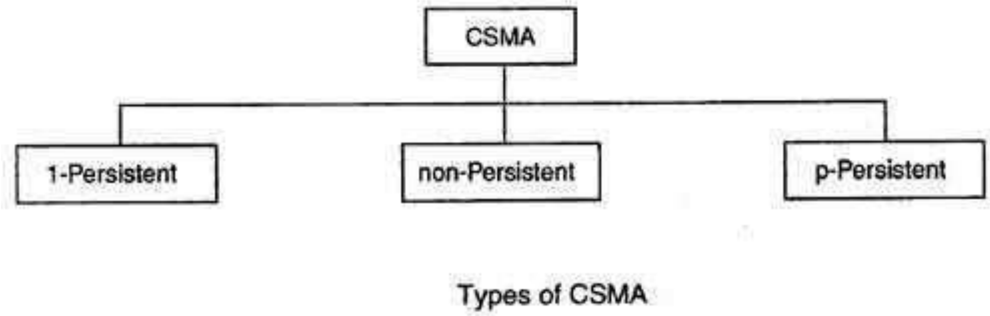


Figure No.5.12 Types of CSMA

(i) I-persistent CSMA
• In this method, station that wants to transmit data continuously senses the channel to check whether the channel is idle or busy.
• If the channel is busy, the station waits until it becomes idle.
• When the station detects an idle-channel, it immediately transmits the frame with probability 1. Hence it is called I-persistent CSMA.
• This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and transmit their frames.
• When the collision occurs, the stations wait a random amount of time and start allover again.
Drawback of I-persistent
• The propagation delay time greatly affects this protocol. Let us suppose, just after the station I begins its transmission, station 2 also became ready to send its data and senses the channel. If the station I signal has not yet reached station 2, station 2 will sense the channel to be idle and will begin its transmission. This will result in collision.

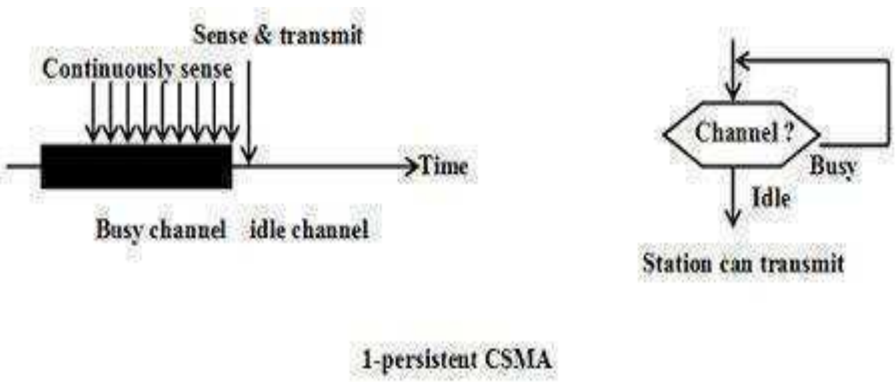


Figure No.5.13 1 Persistent CSMA

(ii) Non-persistent CSMA
• In this scheme, if a station wants to transmit a frame and it finds that the channel is busy (some other station is transmitting) then it will wait for fixed interval of time.
• After this time, it again checks the status of the channel and if the channel is free it will transmit.
• A station that has a frame to send senses the channel.
• If the channel is idle, it sends immediately.
• If the channel is busy, it waits a random amount of time and then senses the channel again.
• In non-persistent CSMA the station does not continuously sense the channel for the purpose of capturing it when it detects the end of previous transmission.
Advantage of non-persistent

• It reduces the chance of collision because the stations wait a random amount of time. It is unlikely that two or more stations will wait for same amount of time and will retransmit at the same time.

Disadvantage of non-persistent

• It reduces the efficiency of network because the channel remains idle when there may be stations with frames to send. This is due to the fact that the stations wait a random amount of time after the **collision.**

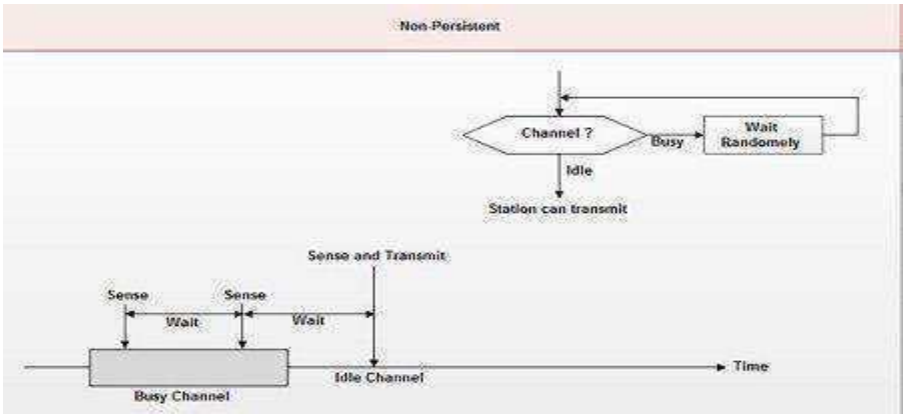


Figure No.5.14 Non-persistent

(iii) p-persistent CSMA

• This method is used when channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time.
• Whenever a station becomes ready to send, it senses the channel.
• If channel is busy, station waits until next slot.
• If channel is idle, it transmits with a probability p.
• With the probability q=l-p, the station then waits for the beginning of the next time slot.
• If the next slot is also idle, it either transmits or waits again with probabilities p and q.
• This process is repeated till either frame has been transmitted or another station has begun transmitting.
• In case of the transmission by another station, the station acts as though a collision has occurred and it waits a random amount of time and starts again.

Advantage of p-persistent

• It reduces the chance of collision and improves the efficiency of the network.

#Frame format of CSMA/CD

The frame format specified by IEEE 802.3 standard contains following fields.

7 byte	1 byte	6 byte	6 byte	2 byte	46 to 1500 byte	4 byte
Preamble	Start Frame Delimiter	Destination Address	Source Address	Length	Data	Frame Check Sequence

Frame format of IEEE 802.3 CSMA/CD frame

Figure No.5.15 Frame format of CSMA/CD

1. Preamble: It is seven bytes (56 bits) that provides bit synchronization. It consists of alternating Os and 1s. The purpose is to provide alert and timing pulse.
2. Start Frame Delimiter (SFD): It is one byte field with unique pattern: 10 10 1011. It marks the beginning of frame.
3. Destination Address (DA): It is six byte field that contains physical address of packet's destination.
4. Source Address (SA): It is also a six byte field and contains the physical address of source or last device to forward the packet (most recent router to receiver).
5. Length: This two byte field specifies the length or number of bytes in data field.
6. Data: It can be of 46 to 1500 bytes, depending upon the type of frame and the length of the information field.
7. Frame Check Sequence (FCS): This for byte field contains CRC for error detection.

