THIRUVALLUVAR UNIVERSITY

E-NOTES

BECS 63B / BECA 63B

MOBILE COMPUTING

(6th SEMESTER B.Sc CS / BCA)

STEERED BY

Dr. S. THAMARAI SELVI, M.E., Ph.D.,
Vice Chancellor, Tiruvalluvar University, Serkkadu, Vellore

COMPILED BY

1. **Dr. S. SELVAKANI, M.C.A.,M.Phil.,M.Tech., Ph.D.,**
   Assistant professor & Head, Department of Computer Science, Thiruvalluvar University College of Arts and Science, Arakkonam.
2. **Ms. A. SIVASANKARI, M.Sc.,M.Phil., DCP.,**
   Assistant Professor , Department of Computer Applications, Shanmuga Industries arts and science college, Tiruvannamalai.
3. **Mr. V. SAKTHIVEL, M.C.A., M.Phil.,**
   Assistant Professor & Head , Department of Computer Applications, Shanmuga Industries arts and science college, Tiruvannamalai.
4. **Mrs. G. KOMALA, M.C.A., M. Phil., B.Ed.,**
   Assistant Professor , Department of Computer Applications, Shanmuga Industries arts and science college, Tiruvannamalai.
5. **Ms. S. R. RATHINA PRIYA, M.C.A.,M.Phil.,**
   Assistant Professor , Department of Computer Applications, Shanmuga Industries arts and science college, Tiruvannamalai.
6. **Mrs. E. SUGANYA, M.C.A.,M.Phil.,**
   Assistant Professor , Department of Computer Applications, Shanmuga Industries arts and science college, Tiruvannamalai.,

ACKNOWLEDGEMENT

Writing an e-content is harder than we thought and more rewarding than we could have ever imagined. None of this would have been possible without our honourable Vice Chancellor – Professor ***Dr. S. Thamarai Selvi****. Her dynamism, vision, sincerity, guidance and motivation have deeply inspired us. She worked her magic on every page in this e-content, reorganised content wherever necessary, bringing value added words in every line. She has taught us the way to present the content to the students in a best possible way to have clear and crisp understanding. She was able to tune into the task and identify the ones that diverted our team focus and energy keeping us from getting our things done. It was a great privilege and honour to work under her guidance. We are extremely grateful for what she has offered us.*

Dr. S. SELVAKANI

A. SIVASANKARI

V. SAKTHIVEL

G. KOMALA

S. R. RATHINAPRIYA

E. SUGANYA

SYLLABUS

MOBILE COMPUTING

Objective: To impart good knowledge of wireless communication to students

UNIT I WIRELESS COMMUNICATION FUNDAMENTALS

Cellular systems- Frequency Management and Channel Assignment- types of handoff and their characteristics, dropped call rates & their evaluation -MAC – SDMA – FDMA –TDMA – CDMA – Cellular Wireless Networks.

UNIT II TELECOMMUNICATION NETWORKS & WIRLESS LAN

Telecommunication systems – GSM – GPRS - Satellite Networks ,Wireless LAN – IEEE 802.11 - Architecture – services – MAC – Physical layer – IEEE 802.11a -802.11b standards – HIPERLAN – Blue Tooth.

UNIT III MOBILE NETWORK LAYER & TRANSPORT LAYER

Mobile IP – Dynamic Host Configuration Protocol - Routing – DSDV – DSR – Alternative Metrics. Traditional TCP, Mobile TCP

UNIT IV APPLICATION LAYER

WAP Model- Mobile Location based services -WAP Gateway –WAP protocols – WAP user agent profile- caching model-wireless bearers for WAP - WML – WML Scripts

UNIT V DATABASE ISSUES

Database Issues : Hoarding techniques, caching invalidation mechanisms, client server computing with adaptation, power-aware and context-aware computing, transactional models, query processing, recovery, and quality of service issues.

TEXT BOOKS:

1. Jochen Schiller, “Mobile Communications”, Second Edition, Pearson Education, 2003. 2. William Stallings, “Wireless Communications and Networks”, Pearson Education, 2002.

REFERENCE BOOKS:

1. KavehPahlavan, PrasanthKrishnamoorthy, “Principles of Wireless Networks”, PHI/Pearson Education, 2003.
2. UweHansmann, LotharMerk, Martin S. Nicklons and Thomas Stober, “Principles of Mobile Computing”, Springer, 2003..
3. Raj Kamal, “Mobile Computing”,Oxford University Press, 2007
4. Asoke K. Talukdar, “Mobile Computing”, Tata McGraw-Hill Education,2010.
5. Mohammad Ilyas , Imad Mahgoub,” Mobile Computing Handbook” ,AUERBACH,2004.
6. Vilas S. Bagad , “Mobile Computing Introduction”, Technical Publications,2014
7. DR SANJAY Sharma, “Mobile Computing”,S.K. Kataria & Sons Publication,2014.
8. Dr. Ashish N.Jani, Dr. N.N. Jani , Neeta Kanabar ,” Mobile Computing - Technologies and Applications”, 2010
9. Pattnaik, Prasant Kumar, Mall, Rajib, “Fundamentals Of Mobile Computing”, Second Edition, PHI Learning Pvt. Ltd., 2015.

UNIT - I

MOBILE COMPUTING

1. WIRELESS COMMUNICATION

1.1 INTRODUCTION

Wireless communication involves the transmission of information over a distance without the help of wires, cables or any other forms of electrical conductors.

Wireless communication is a broad term that incorporates all procedures and forms of connecting and communicating between two or more devices using a wireless signal through wireless communication technologies and devices.

1.1.1 FEATURES OF WIRELESS COMMUNICATION

- The evolution of wireless technology has brought much advancement with its effective features.
- The transmitted distance can be anywhere between a few meters (for example, a television's remote control) and thousands of kilometers (for example, radio communication).
- Wireless communication can be used for cellular telephony, wireless access to the internet, wireless home networking, and so on.
- Other examples of applications of radio wireless technology include GPS units, garage door openers, wireless computer mice, keyboards and headsets, headphones, radio receivers, satellite television, broadcast television and cordless telephones.

FIGURE 1.1 WIRELESS COMMUNICATION

1.1.2 WIRELESS - ADVANTAGES

Wireless communication involves transfer of information without any physical connection between two or more points. Because of this absence of any 'physical infrastructure', wireless communication has certain advantages. This would often include collapsing distance or space.

Wireless communication has several advantages; the most important ones are discussed below

Cost effectiveness

Wired communication entails the use of connection wires. In wireless networks, communication does not require elaborate physical infrastructure or maintenance practices. Hence the cost is reduced.

Example − Any company providing wireless communication services does not incur a lot of costs, and as a result, it is able to charge cheaply with regard to its customer fees.

Flexibility

Wireless communication enables people to communicate regardless of their location. It is not necessary to be in an office or some telephone booth in order to pass and receive messages.

Miners in the outback can rely on satellite phones to call their loved ones, and thus, help improve their general welfare by keeping them in touch with the people who mean the most to them.

Convenience

Wireless communication devices like mobile phones are quite simple and therefore allow anyone to use them, wherever they may be. There is no need to physically connect anything in order to receive or pass messages.

Example − Wireless communications services can also be seen in Internet technologies such as Wi-Fi. With no network cables hampering movement, we can now connect with almost anyone, anywhere, anytime.

Speed

Improvements can also be seen in speed. The network connectivity or the accessibility were much improved in accuracy and speed.

Example − A wireless remote can operate a system faster than a wired one. The wireless control of a machine can easily stop its working if something goes wrong, whereas direct operation can’t act so fast.

Accessibility

The wireless technology helps easy accessibility as the remote areas where ground lines can’t be properly laid, are being easily connected to the network.

Example − In rural regions, online education is now possible. Educators no longer need to travel to far-flung areas to teach their lessons. Thanks to live streaming of their educational modules.

Constant connectivity

Constant connectivity also ensures that people can respond to emergencies relatively quickly.

Example − A wireless mobile can ensure you a constant connectivity though you move from place to place or while you travel, whereas a wired land line can’t.

1.1.3 TERMS IN MOBILE TELEPHONY

Among the various terms used in Mobile telephony, the most used ones will be discussed here.

Mobile Station (MS) − The Mobile Station (MS) communicates the information with the user and modifies it to the transmission protocols of the air interface to communicate with the BSS. The user information communicates with the MS through a microphone and speaker for the speech, keyboard and display for short messaging and the cable connection for other data terminals. The mobile station has two elements Mobile Equipment (ME) and Subscriber Identity Module (SIM).

Mobile Equipment (ME) − ME is a piece of hardware that the customer purchases from the equipment manufacturer. The hardware piece contains all the components needed for the implementation of the protocols to interface with the user and the air-interface to the base stations.

FIGURE 1.2 MOBILE EQUIPMENT

FIGURE 1.3 MOBILE EQUIPMENT- SIM

Subscriber Identity Module (SIM) − This is a smart card issued at the subscription to identify the specifications of a user such as address and type of service. The calls in the GSM are directed to the SIM rather than the terminal.

SMS are also stored in the SIM card. It carries every user's personal information which enables a number of useful applications.

Base Station (BS) − A base station transmits and receives user data. When a mobile is only responsible for its user's data transmission and reception, a base station is capable to handle the calls of several subscribers simultaneously.

Base Transceiver Station (BTS) − The user data transmission takes place between the mobile phone and the base station (BS) through the base transceiver station. A transceiver is a circuit which transmits and receives, i.e., does both.

Mobile Switching Center (MSC) − MSC is the hardware part of the wireless switch that can communicate with PSTN switches using the Signaling System 7 (SS7) protocol as well as other MSCs in the coverage area of a service provider. The MSC also provides for communication with other wired and wireless networks as well as support for registration and maintenance of the connection with the mobile stations.

The following image illustrates the parts of different sub-systems. HLR, VLR, EIR and AuC are the sub-systems of Network sub-system.

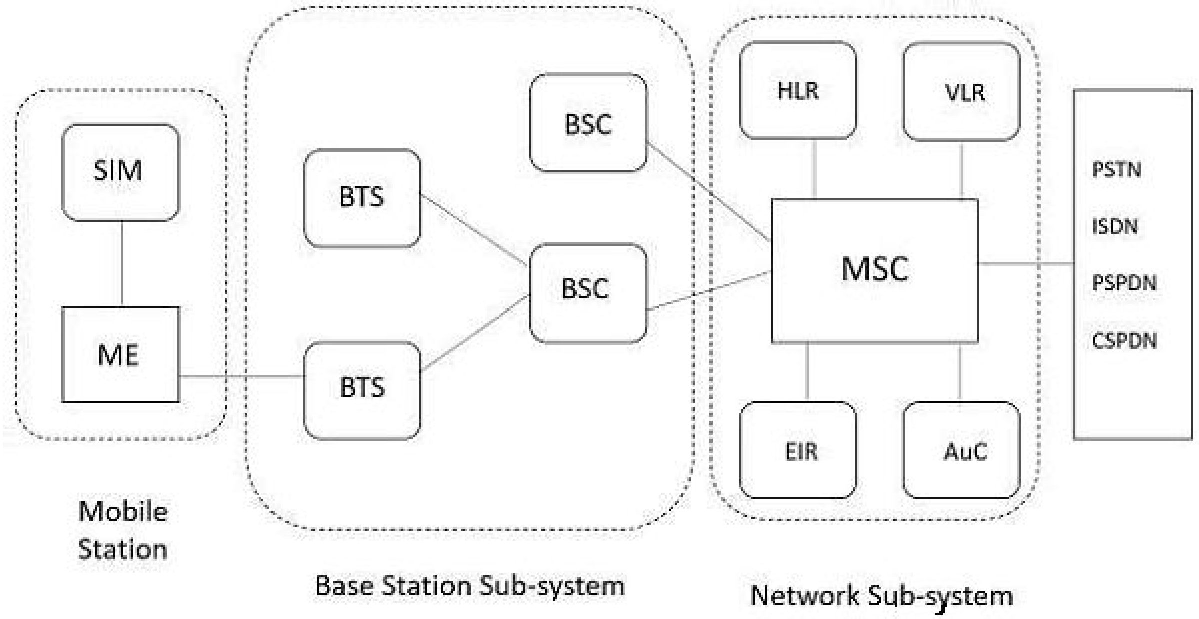


FIGURE 1.4 NETWORK SUB-SYSTEM

Channels − It is a range of frequency allotted to particular service or systems.

Control Channel − Radio channel used for transmission of call setup, call request, call initiation and other beacon or control purposes.

Forward Control Channel(FCC) − Radio channel used for transmission of information from the base station to the mobile

Reverse Channel(RC) − Radio channel used for transmission of information from the mobile to base station.

Voice Channel(VC) − Radio channel used for voice or data transmission.

Handoff − It is defined as the transferring a call from the channel or base station to another base station.

Roamer − A mobile station which operates in a service area other than that from which service has been subscribed

Transceiver − A device capable of simultaneously transmitting and receiving radio signals.

Wireless communications is, by any measure, the fastest growing segment of the communications industry. As such, it has captured the attention of the media and the imagination of the public. Cellular systems have experienced exponential growth over the last decade and there are currently around two billion users worldwide. Indeed, cellular phones have become a critical business tool and part of everyday life in most developed countries, and are rapidly supplanting antiquated wireline systems in many developing countries.

In addition, wireless local area networks currently supplement or replace wired networks in many homes, businesses, and campuses. Many new applications, including wireless sensor networks, automated high ways and factories, smart homes and appliances, and remote telemedicine, are emerging from research ideas to concrete systems.

The explosive growth of wire- less systems coupled with the proliferation of laptop and palmtop computers indicate a bright future for wireless networks, both as stand-alone systems and as part of the larger networking infrastructure. However, many technical challenges remain in designing robust wireless networks that deliver the performance necessary to support emerging applications.

In this introductory chapter we will briefly review the history of wireless networks, from the smoke signals of the pre-industrial age to the cellular, satellite, and other wireless networks of today. We then discuss the wireless vision in more detail, including the technical challenges that must be overcome to make this vision a reality. We describe current wireless systems along with emerging systems and standards. The gap between current and emerging systems and the vision for future wireless applications indicates that much work remains to be done to make this vision are ability.

1.1.4 HISTORY OF WIRELESS COMMUNICATIONS

A digital radio can transmit a continuous bit stream or it can group the bits into packets. The latter type of radio is called a **packet radio** and is characterized by bursty transmissions: the radio is idle except when it transmits a packet. The first network based on packet radio, ALOHANET, was developed at the University of Hawaii in 1971. This network enabled computer sites at seven campuses spread out over four islands to communicate with a central computer on Oahu via radio transmission.

The history of Wireless Communications started with the understanding or magnetic and electric properties observed during the early days by the Chinese, Greek and Roman cultures and experiments carried out in the 17th and 18th centuries. Here are some selected events in the development of Wireless Communications (material taken from the book History of Wireless, Tapan Sarkar, et al., Wiley, 2006).

1807 – French mathematician Jean Baptiste Joseph Fourier discovered Fourier's theorem

1820 – Danish physicist Hans Christian Orsted discovered the electromagnetic field caused by electric current. The French physicist Dominique Francois Jean Arago showed that a wire became a magnet when current flowed through it. French mathematician and physicist Andre-Marie Ampere discovered electrodynamics and proposed an Electromagnetic Telegraph.

1831 – British scientist Michael Faraday discovered electromagnetic induction and predicted existence of electromagnetic waves.

1834 – American inventor Samuel Finley Breese Morse invented the code for telegraphy named after him.

1847 – German physiologist and physicist Hermann Ludwig Ferdinand von Helmholtz suggested electrical oscillation

1853 – William Thomson (Lord Kelvin) calculated the period, damping and intensity as a function of the capacity, self-inductance and resistance of an oscillatory circuit.

1857 – Feddersen verified experimentally the resonant frequency of a tuned circuit as suggested by Helmholtz in 1847.

1864 – Scottish mathematician and physicist James Clerk Maxwell formulated the electromagnetic theory of light and developed the general equations of the electromagnetic field. He formulated 20 equations that were later simplified into the 4 basic equations we use today.

1866 - American dentist Dr. Mahlon Loomis described and demonstrated a wireless transmission system which he patented in 1866. Loomis demonstrated the transmission of signals between two mountains, a distance of 22 km.

1882 – American physicist, Amos Emerson Dolbear, was granted a patent for a wireless transmission system using an induction coil, microphone and telephone receiver and battery. Nathan Stubblefield transmitted audio signals without wires.

1883 – Irish physicist and chemist George Francis FitzGerald published a formula for the power radiated by a small loop antenna.

1884 – German physicist Heinrich Rudolf Hertz wrote Maxwell's equations in scalar form by discarding the concept of aether reducing it from 20 to 12 equations.

1885 – Thomas Edison patented a system of wireless communication by electrostatic induction.

1886 – Heaviside introduced impedance as the ratio of voltage over current. Hertz started his work to demonstrate the existence of radio waves and published his results in 1888.

1887 – English physicist Oliver Joseph Lodge discovered Sympathetic Resonance (standing waves) in wires.

1888 – Hertz produced, transmitted, and received electromagnetic waves (5 m to 50 cm) using reflectors to concentrate the beam. Hertz also discovered the principle for Radar. Heaviside wrote Maxwell's equations in vector form – the four equations we use today. Italian Galileo Farrari and Croatian-American Nilola Tesla independently produced rotating fields using 2-phase currents. Austrian engineer Ernst Lecher established the relation between frequency, wire length, velocity of propagation and the electrical constants of the wire.

1890 – Lecher used standing waves produced in parallel wires to measure frequency. Tesla introduced high frequency currents in therapeutics as he observed that current of high frequency could raise the temperature of living tissue. Tesla also patented his Tesla Coil which was used later in every spark gap generator to produce high frequency signals. Heinrich Rubens and R. Titter made a sensitive bolometer which measured the intensity of electromagnetic waves by means of the heat generated in a thin wire.

1893 – English physicist Joseph John Thomson published the first theoretical analysis of electric oscillations within a conducting cylindrical cavity of finite length suggesting the possibility of wave propagation in hollow pipes (waveguides). Hertz conducted experiments of EM shielding and for coaxial configuration.

1895 – Marconi transmitted and received a coded message at a distance of 1.75 miles near his home in Bologna, Italy. Indian physicist, Sir Jagadis Chunder Bose generated and detected wireless signals and produced many devices such as waveguides, horn antennas, microwave reflectors and more.

1897 – Marconi demonstrated a radio transmission to a tugboat over an 18 mile path over the English Channel. The first wireless company, Wireless Telegraph and Signal Company was founded – they bought most of Marconi's patents. Lord Rayleigh suggests EM wave propagation in waveguides and analysis of propagation through dielectrically filled waveguides. Lodge patented various types of antennas.

1899 – Marconi sent the first international wireless message from Dover, England to Wimereux, France.

1900 – Tesla obtained patents on System of Transmission of Electrical Energy which the US recognized as the first patents on Radio. Tesla is the first person to describe a system of determining the location of an object using radio waves – Radar.

1902 – Fessenden patented the Heterodyne receiver. American Cornelius D. Ehret filed patents covering the transmission and reception of coded signals or speech (Frequency Modulation – FM). Poulsen was the first to develop the CW transmitter.

1903 – Marconi established a transmission station in South Wellfleet, MA – the dedication included exchanges of greetings between American President Theodore Roosevelt and British King Edward VII. G.

1904 – Frank J. Sprague developed the idea of the printed circuit. W. Pickard filed a patent application for a crystal detector where a thin wire was in contact with silicon. It was the central component in early radio receivers called crystal radios. J. C. Bose was granted a patent on point contact diodes that were used for many years as detectors in the industry. Fleming suggested the rectifying action of the vacuum-tube diode for detecting high frequency oscillation – the first practical radio tube.

1905 – Fessenden invented the superheterodyne circuit.

1906 – Lee de Forest patented the general principle of omni-range using a rotating radio beam keyed to identify the sector forming 360 degree sweep of the beam. He also invented the three-electrode valve or vacuum tube triode that was instrumental in the development of transcontinental telephony in 1913. Poulsen transmitted music by wireless using an arc transmitter with 1 kW of input power and a 200 feet high antenna that was heard 300 miles away.

1909 – Marconi and Braun shared the Nobel Prize for Physics for their contributions to the physics of electric oscillations and radiotelegraphy.

1911 – Von Lieben and Eugen Riesz developed a cascade amplifier. Hugo Germsback, an American novelist, envisaged the concept of pulse radar in one of his works where he proposed the use of a pulsating polarized wave, the reflection of which was detected by an actinoscope.

1911 – Engineers start to realize that the triode can also be used for transmitter and oscillator – the three-electrode vacuum tube was included in designs for telephone repeaters in several countries.

1912 – G. A. Campbell developed guided wave filters. Sinding and Larsen transmitted TV by wireless using 3 channels. The Institute of Radio Engineers was formed in the US.

1914 – The German physicist Walter Schottky discovered the effect of electric field on the rate of electron emission from thermionic-emitters named after him. Fleming discovered the atmospheric refraction and its importance in the transmission of EM waves around the Earth. Carl R. Englund was the first to develop the equation of a modulated wave (AM) and also discovered the frequencies related to sidebands. Frequency modulation of a carrier was proposed to accommodate more channels within the available bandwidths.

1915 – Schottky stated work on the space-charge-grid tube and a screen grid tube or Tetrode that achieved good amplification by placing a screen grid between the grid and the anode.

1916 – Leon m Brillouin and Georges A. Beauvais patented the R-C coupled amplifier. F. Adcock used open vertically spaced aerials for direction finding in aircraft and granted British patent.

1918 – Armstrong invented the Super heterodyne Radio Receiver using 8 valves – most receivers still use this design today. Langmuir patented the feedback amplifier. E. H. O Shaughnessy development of direction finding was one of the key weapons in England during WWI – Bellini-Tosi aerials were installed around the coast to locate transmission from ships and aircrafts. Louis Alan Hazeltime invented the neutrodyne circuit with tuned RF amplifier with neutralization.

1919 – Marconi-Osram company developed the U-5 twin-anode full-wave rectifier. Joseph Slepian filed a patent application for a vacuum tube electron multiplier. Sir Robert Alexander Watson-Watt patented a device for radiolocation by means of short-wave radio waves – the forerunner of the Radar system.

1921 - E. S. Purington made the all-electric frequency modulator. A.W. Hull invented the Magnetron oscillator operating at 30 kHz and output power of 8 kW and 69 percent efficiency. E. H. Colpitt and O. B. Blackwell developed modulation of an audio frequency carrier by signals of lower audio frequency for carrying telephony over wires. S. Butterworth published a classic paper on HF resistance of single coil considering skin and proximity effect.

1922 – Walter Guiton Cady invented the piezoelectric (Quartz) crystal oscillator. The BBC broadcasts is first news program.

1923 – The decibel (1/10th of a bel, after A. G. Bell, inventor of the telephone) was used to express the loss in a telephone cable. H. W. Nichols developed point-to-point communication using single side-band communication. D.C Prince analyzed Class A and Class C amplifiers. Scottish engineer Antoine Logie Barid built and patented the first practical TV. Watson-Watt perfected the radiolocation device by displaying radio information on a cathode ray oscilloscope telling the radar operator the direction, distance and velocity of the target. Ralph Vinton Lyon Hartley showed that the amount of information that can be transmitted at a given time is proportional to the bandwidth of the communication channel. H. Flurschein filed a patent on radio warning system for use on vehicles.

1924 – J.R. Carson showed that energy absorbed by a receiver is directly proportional to its bandwidth and extended Lorentz's reciprocity theory to EM fields to antenna terminals. Lloyd Espenschied invented the first radio altimeter. The mobile telephone was invented by Bell Telephone Company and introduced to NYC police cars.

1925 – First conference on frequency allocation was held in Geneva. Joseph Tykocinski-Tykociner demonstrated that the characteristics of a full size antenna can be replaced with sufficient accuracy from measurements made on a small short wave in the rage of 3 to 6 m.

1926 – L.E. Lilienfield patented the theory of the Field-Effect Transistor. Japanese engineers Hidetsugu Yagi and Shintaro Uda developed the Yagi antenna, a row of aerials consisting of one active antenna and twenty undriven members as a wave canal. Hulsenback and Company patented identification of buried objects using CW radar.

1927 – R. V. Hartley developed the mathematical theory of communications. Harold Stephen Black of Bell Laboratories conceived the negative feedback amplifier. A. de Hass studied fading and independently developed diversity reception system.

1928 – Baird conducted the first transatlantic TV broadcast and built the first color TV. Nyquist published a classic paper on the theory of signal transmission in telegraphy. He developed the criteria for the correct reception of telegraph signals transmitted over dispersive channels in the absence of noise. C.S. Franklin patented the coaxial cable in England to be used as an antenna feeder.

1929 – L. Cohen proposed circuit tuning by wave resonance (resonant transmission line) and its application to radio reception. H.A. Affel and L. Espenscheid of AT&T/Bell Labs created the concept of coaxial cable for a FDMA multi-channel telephony system. K. Okabe made a breakthrough in cm-waves when operating his slotted-anode magnetron (5.35 GHz). Hans Erich Hollmann patented the idea of a reflex klystron with his double-grid retarding-field tube. W.H. Martin proposed the Decibel as a transmission unit.

1931 – H. diamond and F. W. Dunmore conceived a radio beacon and receiving system for blind landing of aircraft. H. E. Hollmann built and operated the first decimeter transmitter and receiver at the Heinrich Hertz Institute. He called the device the magnetron.

1932 – The word Telecommunication was coined and the International Telecommunications Union (ITU) was formed. George C. Southworth and J. F. Hargreaves developed the circular waveguide. Karl Jansky accidentally discovered radio noise coming from outer space giving birth to radio astronomy. R. Darbord developed the UHF Antenna with parabolic reflector.

1933 – Armstrong demonstrated Frequency Modulation (FM) and proposed FM radio in 1936. C.E. Cleeton and N. H. Williams made a 30 GHZ CW oscillator using a split-anode magnetron.

1934 – The Federal Communications Commission (FTC) was created in the US. W.L. Everitt obtained the optimum operating conditions for Class C amplifiers. F. E. Terman demonstrated a transmission line as a resonant circuit. German physicist Oskar Ernst Heil applied for a patent on technology relating electrical amplifiers and other control arrangements that was the theoretical invention of capacitive current control in FETs.

1935 – C. J. Frank of Boonton Radio Corp demonstrated Q-meter at the fall meeting of IRE – the ratio of reactance to resistance of a coil as its "Quality Factor" was first suggested about 1926. A French TV transmitter was installed on top of the Eiffel Tower. Watson-Watt developed and patented the first practical radar for use in the detection of airplanes in England. H. E. Hollmann filed a patent for the multi-cavity magnetron (granted in 1938).

1936 – H. W. Doherty developed a new high efficiency power amplifier for modulated waves, Doherty amplifier, at Bell Labs. English engineer Paul Eisler devised the Printed Circuit. N. H. Jack patented the semi-rigid coaxial cable using thin soft copper tube as the outer conductor. Harold Wheeler used two flat copper strips side by side to make a low loss transmission line that could be rolled to save space. H. T. Friis and A. C. Beck invented the horn reflector antenna with dual polarization.

1937 – Grote Rober constructed the first radio telescope. W. R. Blair patented the first anti-aircraft fire control radar. Russell H. Varian and his brother Sigurd Varian along with William Hansen developed the reflex Klystron. Alex H. Reeves invented pulse-code modulation for digital encoding of speech signals.

1938 – E. L. Chaffee determined the optimum load for Class B amplifiers. IRE published standards on transmitters, receivers and antennas. Claude Elwood Shannon recognized the parallels between Boolean algebra and the functioning of electrical switching systems. W. R. Hewlett developed the Wien-bridge (RC) oscillator. P. H Smith at RCA developed the well known Smith Chart. N. E. Lindenblad of RCA developed a coaxial horn antenna. John Turton Randall and Albert Boot developed the cavity magnetron that becomes the central components to radar systems.

1941 – W. C. Godwin developed the direct-coupled push-pull amplifier with inverse feedback. Siemens & Halske made the Ge diode – R. S. Ohl made the Si junction diode. Sidney Warner realized a two-way police FM radio.

1943 – H. J. Finden developed the frequency synthesizer. Austrian engineer Rudolf Kompfner developed the traveling wave tube. C. K. Chang developed frequency modulation of RC oscillators. C. F. Edwards developed microwave mixers. H. T. Friis developed noise figures of radio receivers.

1944 – Harold Goldberg suggested pulse frequency position modulation. E. C Quackenbush of Amphenol developed the VHF coaxial connectors. Paul Neil of Bell Labs developed Type N connectors. Maurice Deloraine, P. R. Adams and D. H. Ranson applied for patents covering switching by pulse displacement a principle later defined as time-slot interchange – Thus, Time-Division Multiplexing (TDMA) was invented. Radio Research Lab developed radar countermeasures (jamming) in the 25 MHz to 6 GHz range.

1946 – S. L. Ackerman and G. Rappaport developed a radio control systems for guided missiles. E. M. Williams developed the radio frequency spectrum analyzer.

1947 – G. E. Mueller and W. A. Tyrrel developed the dielectric rod antenna. John D. Kraus invented the helical antenna. W. Tyrell proposed hybrid circuits for microwaves, H. E. Kallaman constructed the VSWR indictor meter.

1948 – W. H. Branttain, J. Bardeen and W. Shockley of Bell Labs built the junction transistor. E. L. Ginzton and others developed distributed wideband amplifier using pentodes in parallel. Shannon laid out the theoretical foundations of digital communications in a paper entitled "A Mathematical Theory of Communication." Paine described the BALUN.

1949 – E. J. Barlow published the principle of operation of Doppler Radar.

1950- J. M. Janssen developed the sampling oscilloscope.

1951- Charles Hard Townes published the principle of the MASER (Microwave Amplification by Stimulated Emission of Radiation). The Laboratoire Central des Telecommunications in Paris developed the first model of a time-division multiplex system connecting subscriber line by electronic gates handling amplitude modulated pulses.

1952 – C. L. Hogan demonstrated a microwave circulator.

1955 – R. H. DuHamel and D. E. IsBelll develop the log periodic antenna. John R. Pierce proposed using satellites for communications. Sony marketed the first transistor radio.

1957 – Soviet Union launched Sputnik I that transmitted telemetry signals for about 5 months. German physicist Herbert Kroemer originated the concept of the heterostructure bipolar transistor (HBT).

1958 – Robert Noyce (Intel) and Jack Kilby (TI) produced the first Si integrated circuit (IC).

1962 – G. Robert-Pierre Marie patented the wide band slot antenna. S. R. Hofstein and F. P. Heiman developed MOS IC.

1963 – W. S. Mortley and J. H. Rowen developed surface acoustic wave (SAW) devices. John B. Gunn of IBM demonstrated microwave oscillations in GaAs and InP diodes. The Institute of Electrical and Electronic Engineers (IEEE) was formed by merging the IRE and AIEE.

1964 – R. L. Johnson, B. C. De Loach and B. G. Cohen developed the IMPATT diode oscillator. COMSAT and INTELSAT started launching a series of communications satellites that were the building blocks in the global network of international communications satellites.

1969 – The first digital radio-relay system went into operation in Japan using 2 GHz operating frequency. ARPANET was launched (precursor to Internet).

1971 – Statek began manufacturing and marketing quartz oscillators that were made using their patented photolithographic process.

1978 – AT&T Bell Labs started testing a mobile telephone system based on cells.

1980 – CW performance of GaAs MESFET reached 10 W at 10 GHz. ATLAS I EM pulse simulator was built for testing large aircraft – it was the largest wooden structure in the world (400 x 105 x 75 m).

1989 – F. Laleari invented the broadband notch antenna

1990 – WWW was developed

1.2 CELLULAR WIRELESS NETWORKS

Cellular network is an underlying technology for mobile phones, personal communication systems, wireless networking etc. The technology is developed for mobile radio telephone to replace high power transmitter/receiver systems. Cellular networks use lower power, shorter range and more transmitters for data transmission.

FEATURES OF CELLULAR SYSTEMS

Wireless Cellular Systems solves the problem of spectral congestion and increases user capacity. The features of cellular systems are as follows −

- Offer very high capacity in a limited spectrum.
- Reuse of radio channel in different cells.
- Enable a fixed number of channels to serve an arbitrarily large number of users by reusing the channel throughout the coverage region.
- Communication is always between mobile and base station (not directly between mobiles).
- Each cellular base station is allocated a group of radio channels within a small geographic area called a cell.

- Neighboring cells are assigned different channel groups.
- By limiting the coverage area to within the boundary of the cell, the channel groups may be reused to cover different cells.
- Keep interference levels within tolerable limits.
- Frequency reuse or frequency planning.
- Organization of Wireless Cellular Network.

Cellular network is organized into multiple low power transmitters each 100w or less.

SHAPE OF CELLS

The coverage area of cellular networks are divided into **cells**, each cell having its own antenna for transmitting the signals. Each cell has its own frequencies. Data communication in cellular networks is served by its base station transmitter, receiver and its control unit.

The shape of cells can be either square or hexagon −

SQUARE

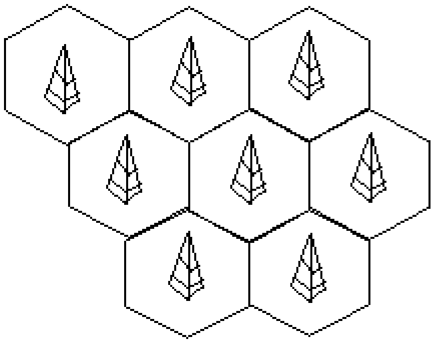
A square cell has four neighbors at distance **d** and four at distance Root **2 d**

- Better if all adjacent antennas equidistant
- Simplifies choosing and switching to new antenna

HEXAGON

A hexagon cell shape is highly recommended for its easy coverage and calculations. It offers the following advantages −

- Provides equidistant antennas
- Distance from center to vertex equals length of side



FREQUENCY REUSE

Frequency reusing is the concept of using the same radio frequencies within a given area, that are separated by considerable distance, with minimal interference, to establish communication.

Frequency reuse offers the following benefits −

- Allows communications within cell on a given frequency
- Limits escaping power to adjacent cells
- Allows re-use of frequencies in nearby cells
- Uses same frequency for multiple conversations
- 10 to 50 frequencies per cell

For example, when **N** cells are using the same number of frequencies and **K** be the total number of frequencies used in systems. Then each **cell frequency** is calculated by using the formulae **K/N**.

In Advanced Mobile Phone Services (AMPS) when K = 395 and N = 7, then frequencies per cell on an average will be 395/7 = 56. Here, **cell frequency** is 56.

1.3 FREQUENCY MANAGEMENT AND CHANNEL ASSIGNMENT

Numbering and grouping, Setup access and paging channels, Channel assignments to cell sites and mobile units, Channel sharing and barrowing, sectorization, Overlaid cells, Non fixed channel assignment.

1.3.1 FREQUENCY MANAGEMENT

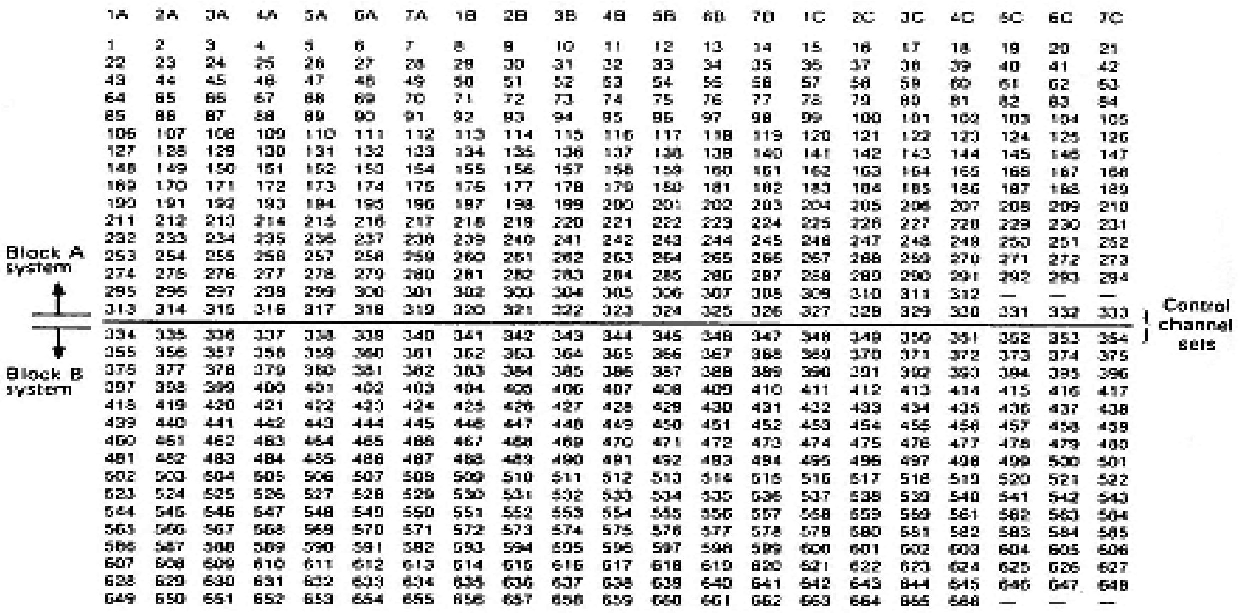
- Designating set-up channels and voice channels (done by the FCC),
- Numbering the channels(done by the FCC), and
- Grouping the voice channels into subsets (done by each system according to its preference).

1.3.2 CHANNEL ASSIGNMENT

- Means the allocation of specific channels to cell sites and mobile units.
- A fixed channel set – Cell site- long-term basis
- During a call- Mobile unit - short-term basis (handled by MTSO).
- Ideally channel assignment should be based on causing the least interference in the system.

1.3.3 NUMBERING THE CHANNELS

- The total number of channels (January 1988) is 832.
- But most mobile units and systems are still operating on 666 channels.
- **A channel consists of two frequency channel bandwidths**,
- one in the low band
- one in the high band
- **Two frequencies in channel 1 are**
- 825.030 MHz (mobile transmit) and
- 870.030 MHz (cell-site transmit)
- **The two frequencies in channel 666 are**
- 844.98 MHz (mobile transmit) and
- 889.98 MHz (cell-site transmit)
- **The 666 channels are divided into two groups:**
- block A system
- block B system



	1A	2A	3A	4A	5A	6A	7A	1B	2B	3B	4B	5B	6B	7B	1C	2C	3C	4C	5C	6C	7C	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	
	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	
	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	
	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	
	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105	
	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	
	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	
	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	
	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	
	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	
	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	
	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	
Block A system	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	
	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	
	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	—	—	—	
	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	Control channel sets
	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	
	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	
Block B system	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	
	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	
	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	
	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	
	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	
	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	
	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	522	
	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	
	544	545	546	547	548	549	550	551	552	553	554	555	556	557	558	559	560	561	562	563	564	
	565	566	567	568	569	570	571	572	573	574	575	576	577	578	579	580	581	582	583	584	585	
	586	587	588	589	590	591	592	593	594	595	596	597	598	599	600	601	602	603	604	605	606	
	607	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623	624	625	626	627	
	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	
	649	650	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	—	—	—	

FIGURE 1.5 FREQUENCY-MANAGEMENT CHART.

- Each block has 333 channels
- The 42 set-up channels are assigned as follows.
- Channels 313 - 333 block A
- Channels 334 - 354 block B
- The voice channels are assigned as follows.
- Channels 1 - 312 (312 voice channels) block A
- Channels 355 - 666 (312 voice channels) block B
- New additional spectrum allocation - 10 MHz -additional 166 channels are assigned
- a 1 MHz is assigned below 825 MHz (or 870 MHz)
- additional channels will be numbered up to 849 MHz (or 894 MHz) and will then circle back
- The last channel number is 1023 (=210)
- There are no channels between channels 799 and 991.

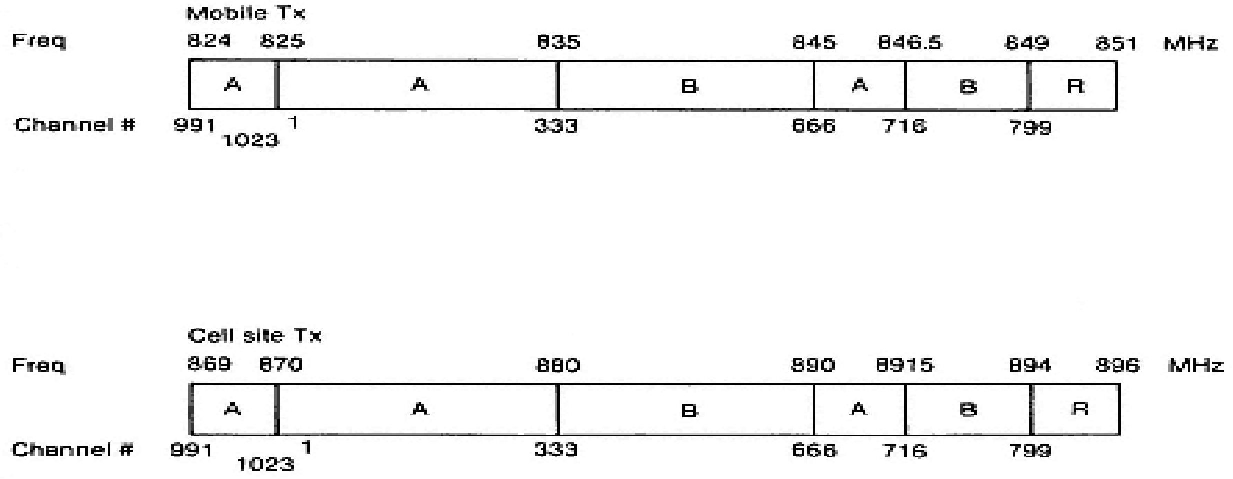
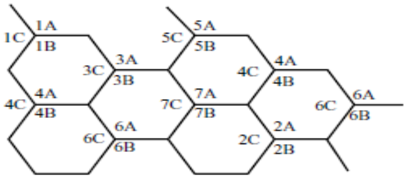


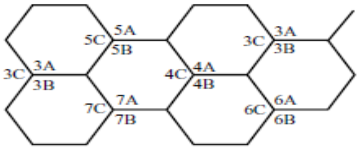
FIGURE 1.6 NEW ADDITIONAL SPECTRUM ALLOCATION



Block A

1A	2A	3A	4A	5A	6A	7A	1B	2B	3B	4B	5B	6B	7B	1C	2C	3C	4C	5C	6C	7C
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42
43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90												102	103	104	105
106	107	108	109	110	111												123	124	125	126
127	128	129	130	131	132												144	145	146	147
148	149	150	151	152	153												165	166	167	168
169	170	171	172	173	174												186	187	199	190
190	191	192	193	194	195												207	208	209	210
211	212	213	214	215	216												228	229	230	231
232	233	234	235	236	237												249	250	251	252
253	254	255	256	257	258												270	271	272	273
274	275	276	277	278	279												291	292	293	294
295	296	297	298	299	300												312	X	X	X
313*	**314**	**315**	**316**	**317**	**318**	**319**	**320**	**321**	**322**	**323**	**324**	**325**	**326**	**327**	**328**	**329**	**330**	**331**	**332**	**333**
667	668	669	670	671	672	673	674	675	676	677	678	679	680	681	682	683	684	685	686	687
688	689	690	691	692	693	694	695	696	697	698	699	700	701	702	703	704	705	706	707	708
709	710	711	712	713	714	715	716	X	991	992	993	994	995	996	997	998	999	1000	1001	1002
1003	1004	1005	1006	1007	1008	1009	1010	1011	1012	1013	1014	1015	1016	1017	1018	1019	1020	1021	1022	1023

FIGURE 1.7 FULL SPECTRUM FREQUENCY MANAGEMENT



Block B

1A	2A	3A	4A	5A	6A	7A	1B	2B	3B	4B	5B	6B	7B	1C	2C	3C	4C	5C	6C	7C
334	**335**	**336**	**337**	**338**	**339**	**340**	**341**	**342**	**343**	**344**	**345**	**346**	**347**	**348**	**349**	**350**	**351**	**352**	**353**	**354**
355	356	357	358	359	360	361														375
376	377	378	379	380	381	382														396
397	398	399	400	401	402	403														417
418	419	420	421	422	423	424														438
439	440	441	442	443	444	445														459
460	461	462	463	464	465	466														480
481	482	483	484	485	486	487														501
502	503	504	505	506	507	508														522
523	524	525	526	527	528	529														543
544	545	546	547	548	549	550														564
565	566	567	568	569	570	571														585
586	587	588	589	590	591	592	593	594	595	596	597	598	599	600	601	602	603	604	605	606
607	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623	624	625	626	627
628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648
649	650	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	717	718	719
720	721	722	723	724	725	726	727	728	729	730	731	732	733	734	735	736	737	738	739	740
741	742	743	744	745	746	747	748	749	750	751	752	753	754	755	756	757	758	759	760	761
762	763	764	765	766	767	768	769	770	771	772	773	774	775	776	777	778	779	780	781	782
783	784	785	786	787	788	789	790	791	792	793	794	795	796	797	798	799				

FIGURE 1.8 FULL SPECTRUM FREQUENCY

Grouping into Subsets

- Voice channels for each system is 312
- We can group these into any number of subsets
- 21 set-up channels for each system
- it is logical to group the 312 channels into 21 subsets
- Each subset then consists of 16 channels
- In each set, the closest adjacent channel is 21 channels away
- The 16 channels in each subset - connected to a channel combiner
- Wide separation between adjacent channels -requirement of minimum isolation
- Each 16-channel subset is idealized for each 16-channel combiner
- In a seven-cell pattern system each cell contains three subsets,

  iA + iB + iC

- where i is an integer from 1 to 7
- The total number of voice channels in a cell is about 45
- The minimum separation between three subsets is 7 channels (21/3)
- If six subsets are equipped in an omnicell site,
- Minimum separation between two adjacent channels can be only three (21/6 > 3) physical channel bandwidths
- For Example
- **1A+1B+1C+4A+4B+4C OR 1A+1B+1C+5A+5B+5C**
- Techniques for increasing frequency spectrum
- Increasing the number of radio channels using narrow banding, spread spectrum, or time division
- Improving spatial frequency-spectrum reuse
- Frequency management and channel assignment

- Improving spectrum efficiency in time
- Reducing the load of invalid calls

Voice storage service for No-Answer calls

Call forwarding

- Call waiting for Busy-Call situations
- Queuing
- Off air call setup
- Reducing the customer keep dialling case

Set-up Channels

- Set-up channels, also called control channels,
- Channels designated to set up calls
- A system can be operated without set-up channels
- Set-up channels can be classified by usage into two types
    - access channels
    - paging channels

Access channels - Operational functions

- Power of a forward set-up channel [or forward control channel (FOCC)]
- The set-up channel received level (Threshold)-RECC
- Change power at the mobile unit(Messages)
    - Mobile station control message
    - System parameter overhead message
    - Control-filler message
- Direct call - retry

Paging Channels

- The assigned forward set-up channel (FOCC) of each cell site is used to page the mobile unit with the same mobile station control message

1.3.4 SELECTING A VOICE CHANNEL

- For mobile-originating calls
- For paging calls

1.3.5 FIXED CHANNEL ASSIGNMENT

Setup-channels

21 channels

- N = 4, 7, 12 cell reuse patterns
- Omni-directional antennas
- One channel per cell
- Unused set-up channels
- Avoid interference between block A and B
- Voice Channels
- 21 subsets
- Min. co channel& Adjacent channel interference
- 3 SAT Tones
- (supervisory audio tone)

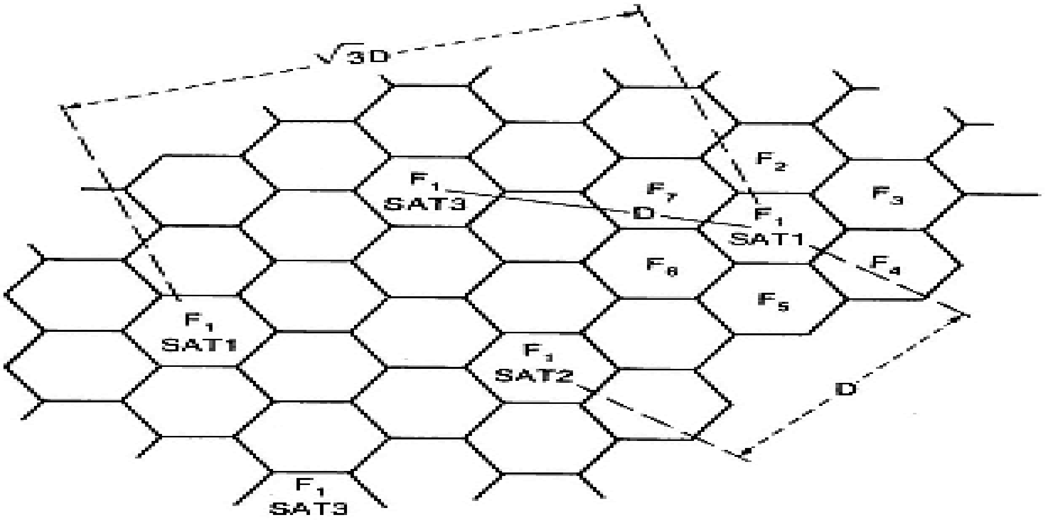


FIGURE 1.9 FIXED CHANNEL ASSIGNMENT

1.3.6 CHANNEL ASSIGNMENT TO TRAVELLING MOBILE UNITS

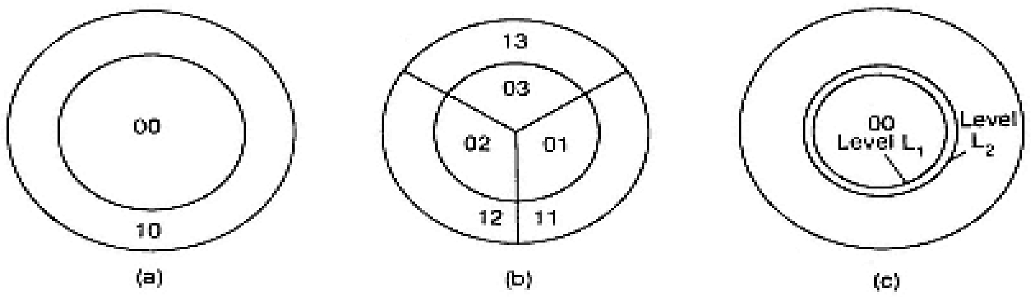


FIGURE 1.10 CHANNEL ASSIGNMENT TO TRAVELLING MOBILE UNITS

Underlaid-overlaid cell arrangements

(*a*) Undelay-overlay in omnicell

(*b*) underlay-overlay in sectorized cells

(*c*) two-level handoff scheme

1.3.7 UNDERLAY-OVERLAY ARRANGEMENT

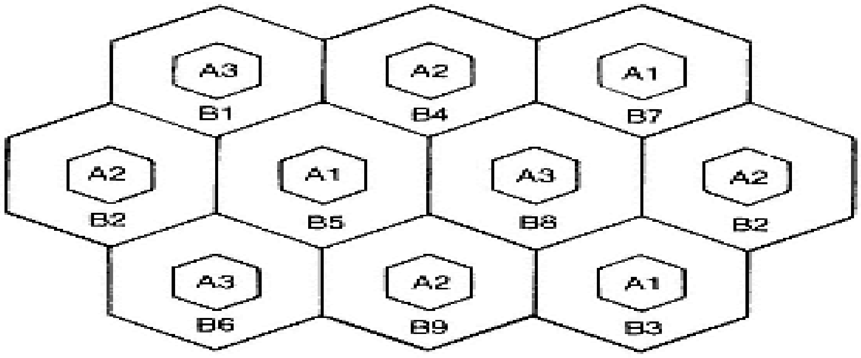


FIGURE 1.11 UNDERLAY-OVERLAY ARRANGEMENT

- Adjacent-Channel Assignment
- Channel Sharing and Borrowing
- Sectorization

1.3.8 ADJACENT-CHANNEL ASSIGNMENT

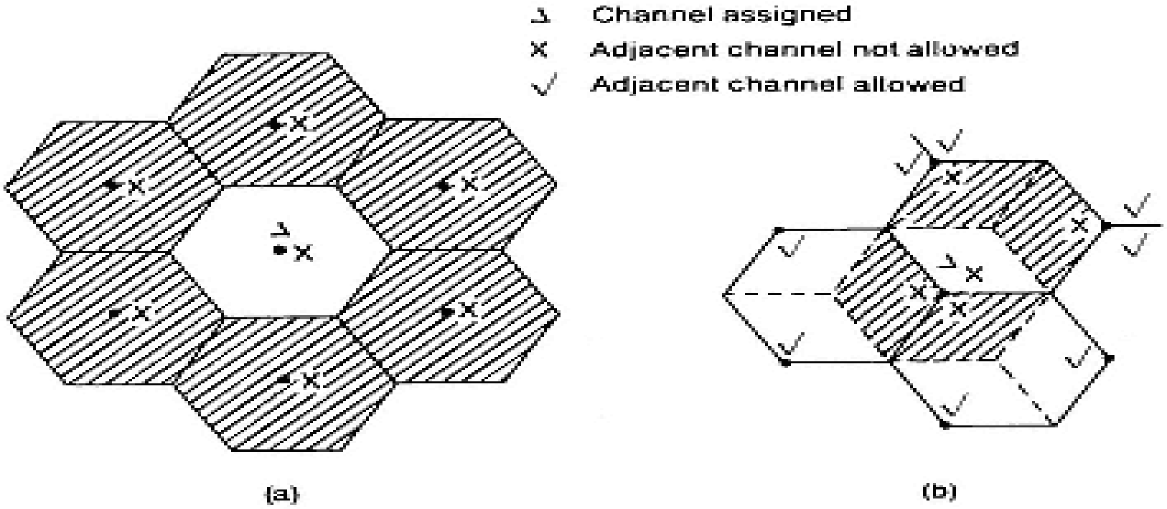


FIGURE 1.12 ADJACENT CHANNEL ASSIGNMENT.

ADJACENT CHANNEL ASSIGNMENT.

- **Omnidirectional-antenna cells**
- **Directional-antenna cells**

1.3.9 CHANNEL SHARING AND BORROWING

- **Channel Sharing**

Algorithm

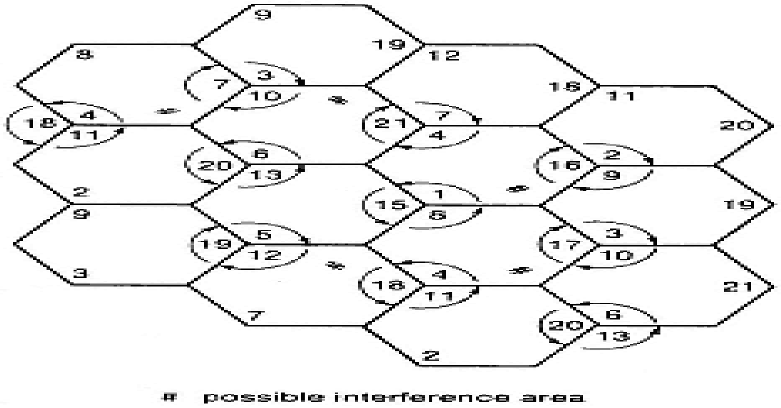


FIGURE 1.13 CHANNEL SHARING AND BORROWING

1.3.10 SECTORIZATION

- The 120o sector cell for both transmitting and receiving
- The 60o sector cell for both transmitting and receiving
- 120o or 60o sector cell for receiving sectorization only , and transmitting antenna is omni-directional
  - **Non-Fixed Channel Assignment**
  - Dynamic Channel Assignment
  - Hybrid channel Assignment
  - Borrowing channel Assignment
  - Forcible-borrowing channel Assignment

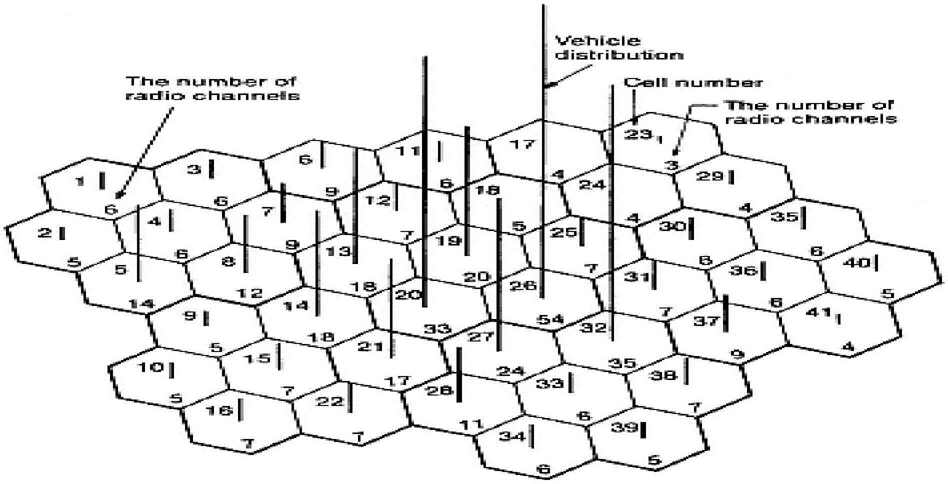


FIGURE 1.14 SIMULATION PROCESS AND RESULTS

CELLULAR SYSTEM.

Vehicle and radio channel distribution in the bus rush hour

- Average Blocking
- Handoff Blocking

1.4 HANDOFF IN MOBILE CONNECTIONS

In cellular communications, the handoff is the process of transferring an active call or data session from one cell in a cellular network or from one channel to another. In satellite communications, it is the process of transferring control from one earth station to another. Handoff is necessary for preventing loss of interruption of service to a caller or a data session user. Handoff is also called handover.

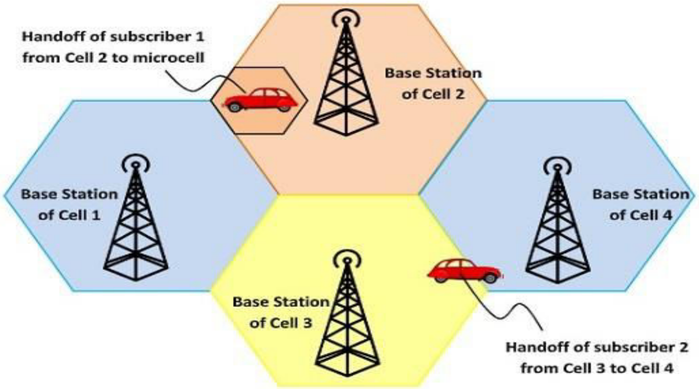

Handoff of subscriber 1 from Cell 2 to microcell
Base Station of Cell 2
Base Station of Cell 1
Base Station of Cell 4
Base Station of Cell 3
Handoff of subscriber 2 from Cell 3 to Cell 4

FIGURE 1.15 HANDOFF IN MOBILE CONNECTIONS

1.4.1 SITUATIONS FOR TRIGGERING HANDOFF

Handoffs are triggered in any of the following situations −

- If a subscriber who is in a call or a data session moves out of coverage of one cell and enters coverage area of another cell, a handoff is triggered for a continuum of service. The tasks that were being performed by the first cell are delineating to the latter cell.
- Each cell has a pre-defined capacity, i.e. it can handle only a specific number of subscribers. If the number of users using a particular cell reaches its maximum capacity, then a handoff occurs. Some of the calls are transferred to adjoining cells, provided that the subscriber is in the overlapping coverage area of both the cells.
- Cells are often sub-divided into microcells. A handoff may occur when there is a transfer of duties from the large cell to the smaller cell and vice versa. For example, there is a traveling user moving within the jurisdiction of a large cell. If the traveler stops, then the jurisdiction is transferred to a microcell to relieve the load on the large cell.

Handoffs may also occur when there is an interference of calls using the same frequency for communication.

1.4.2 TYPES OF HANDOFFS

There are two types of handoffs −

- **Hard Handoff** − In a hard handoff, an actual break in the connection occurs while switching from one cell to another. The radio links from the mobile station to the existing cell is broken before establishing a link with the next cell. It is generally an inter-frequency handoff. It is a "**break before make**" policy.
- **Soft Handoff** − In soft handoff, at least one of the links is kept when radio links are added and removed to the mobile station. This ensures that during the handoff, no break occurs. This is generally adopted in co-located sites. It is a "**make before break**" policy.

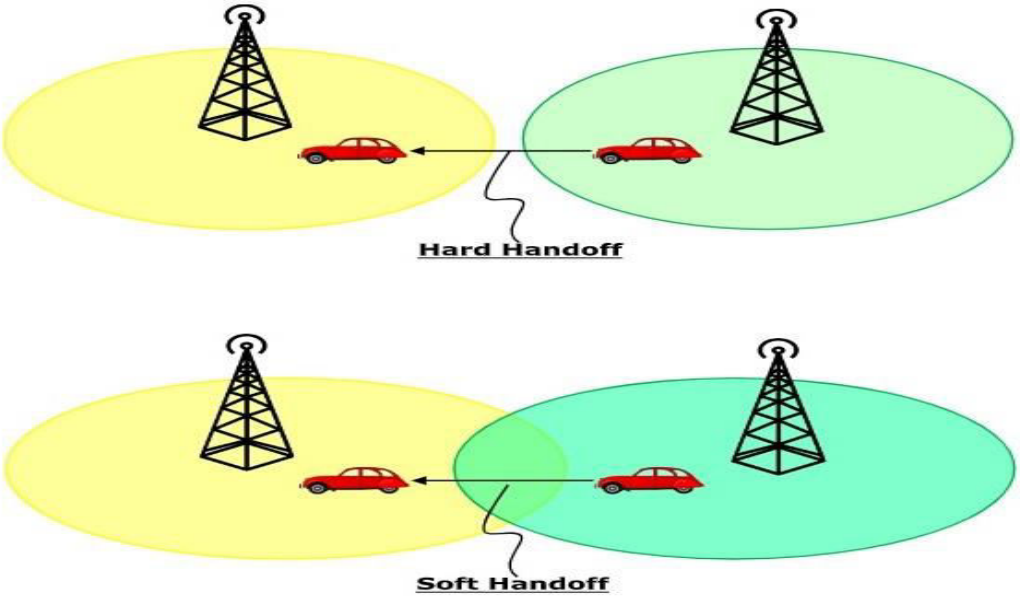


FIGURE 1.16 TYPES OF HANDOFFS

1.4.3 Mobile Assisted Handoff

Mobile Assisted Handoff (MAHO) is a technique in which the mobile devices assist the Base Station Controller (BSC) to transfer a call to another BSC. It is used in GSM cellular networks. In other systems, like AMPS, a handoff is solely the job of the BSC and the Mobile Switching Centre (MSC), without any participation of the mobile device. However, in GSM, when a mobile station is not using its time slots for communicating, it measures signal quality to nearby BSC and sends this information to the BSC. The BSC performs handoff according to this information.

1.5 DROPPED-CALL RATE

Dropped-Call Rate

In telecommunications, the **dropped-call rate** (DCR) is the fraction of the telephone**calls** which, due to technical reasons, were cut off before the speaking parties had finished their conversational tone and before one of them had hung up (**dropped calls**).

In telecommunications, the **dropped-call rate** (DCR) is the fraction of the telephone calls which, due to technical reasons, were cut off before the speaking parties had finished their conversational tone and before one of them had hung up (dropped calls). This fraction is usually measured as a percentage of all calls.[1] A call attempt invokes a call setup procedure, which, if successful, results in a connected call.

A connected call may be terminated (disconnected) due to a technical reason before the parties making the call would wish to do so (in ordinary phone calls this would mean before either of the parties has hung up). Such calls are classified as dropped calls. In many practical cases this definition needs to be further expanded with a number of detailed specifications describing which calls exactly are counted as dropped, at what stage of the call setup procedure a call is counted as connected, etc.

In modern telecommunication systems, such as cellular networks, the call setup procedure may be very complex and the point at which a call is considered successfully connected may be defined in a number of ways, thus influencing the way the dropped-call rate is calculated. The dropped-call rate in conventional (land-line) networks is extremely low and is significantly less than 0.01%. In mobile communication systems using radio channels the dropped-call rate is higher and may range for commercial networks between 0.1% and a few percent.

The main reasons for dropped calls in mobile networks are lack of radio coverage (either in the downlink or the uplink),radio interference between different subscribers, imperfections in the functioning of the network (such as failed handover or cell-reselection attempts), overload of the different elements of the network (such as cells), etc. The dropped-call rate is one of the key performance indicators (KPI) used by the network operators to assess the performance of their networks. It is assumed to have direct influence on the customer satisfaction with the service provided by the network and its operator.

The dropped-call rate is usually included, together with other technical parameters of the network, in a key performance indicator known as call retainability. The operators of telecommunication networks aim at reducing the call dropped rate as much as practical and affordable. In mobile networks this is achieved by improving radio coverage, expanding the capacity of the network and optimising the performance of its elements, all of which may require considerable effort and significant investments on the part of the network operator.

1.6 MEDIUM ACCESS CONTROL

Medium Access Control (MAC) address is a hardware address use to uniquely identify each node of a network. It provides addressing and channel access control mechanisms to enable the several terminals or network nodes to communicate in a specified network. Medium Access Control of data communication protocol is also named as Media Access Control. In IEEE 802 OSI Reference model of computer networking, the Data Link Control (DLC) layer is subdivided into two sub-layers:

- The Logical Link Control (LLC) layer and
- The Medium Access Control (MAC) layer

The MAC sublayer acts as a direct interface between the logical link control (LLC) Ethernet sublayer and the physical layer of reference model. Consequently, each different type of network medium requires a different MAC layer. On networks that don’t conform they are part of IEEE 802 standards but they do conform that they participate OSI Reference Model then the node address is named the Data Link Control (DLC) address. The MAC sublayer emulates a full-duplex logical communication channel in a multipoint network system. These communication channels may provide unicast, multicast and/or broadcast communication services.

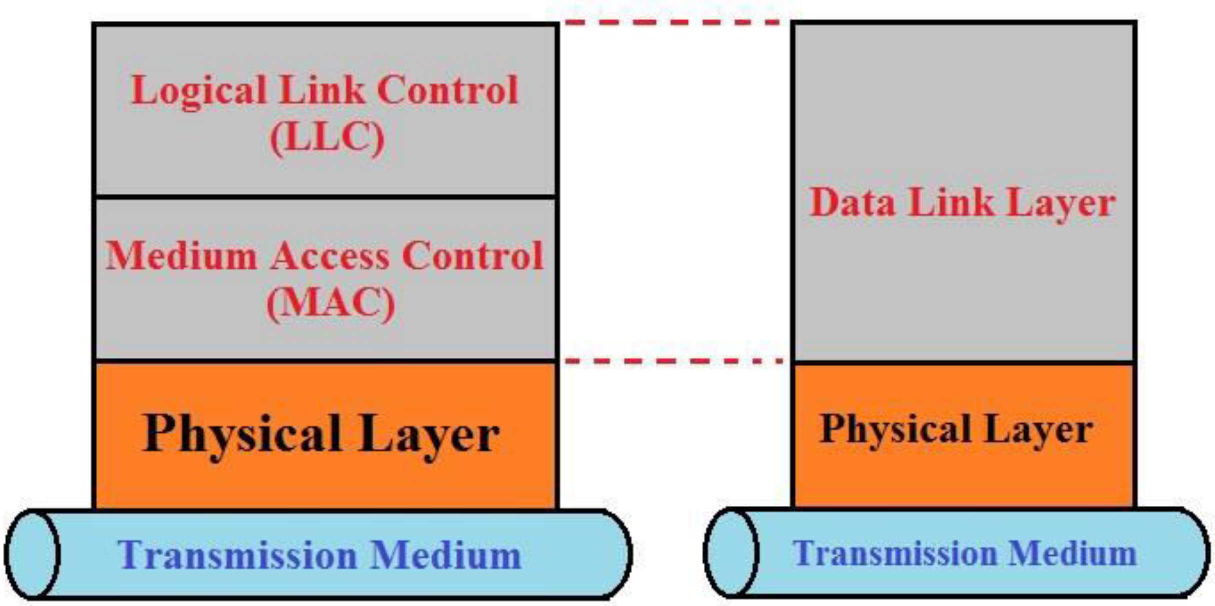


FIGURE 1.17 MEDIUM ACCESS CONTROL

MAC address is suitable when multiple devices are connected with same physical link then to prevent from collisions system uniquely identify the devices one another at the data link layer, by using the MAC addresses that are assigned to all ports on a switch. The MAC sublayer uses MAC protocols to prevent collisions and MAC protocols uses MAC algorithm that accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC address.

1.6.1 Functions performed in the MAC sublayer:

The primary functions performed by the MAC layer as per the IEEE Std 802-2001 section 6.2.3 are as follows:

- **Frame delimiting and recognition:** This function is responsible to creates and recognizes frame boundaries.

- **Addressing:** MAC sublayer performs the addressing of destination stations (both as individual stations and as groups of stations) and conveyance of source-station addressing information as well.
- **Transparent data transfer:** It performs the data transparency over data transfer of LLC, PDUs, or of equivalent information in the Ethernet sublayer.
- **Protection:** MAC sublayer function is to protect the data against errors, generally by means of generating and checking frame check sequences.
- **Access control:** Control of access to the physical transmission medium form unauthorized medium access.

One of the most commonly used of MAC sublayer for wired networks i.e. Carrier Sense Multiple Access with Collision Detection (CSMA/CD). Through MAC schema, a sender senses the medium (a wire or coaxial cable) before transmission of data to check whether the medium is free or not. If MAC senses that the medium is busy, the sender waits until it is free. When medium becomes free, the sender starts transmitting of data and continues to listen into the medium. If any kind of collision detected by sender while sending data, it stops at once and sends a jamming signal. But this scheme does not work well with wireless networks.

Some of the problems that occur when it uses to transfer data through wireless networks are as follow;

- Signal strength decreases proportional to the square of the distance
- The sender would apply Carrier Sense (CS) and Collision Detection (CD), but the collisions happen at the receiver
- It might be a case that a sender cannot “hear” the collision, i.e., CD does not work
- Furthermore, CS might not work, if for e.g., the terminals are“hidden”.
- The directional spot-beam antennas are used and hence the base station in SDMA, can track a moving user.
- Controls the radiated energy for each user in space.

1.6.2 MULTIPLE ACCESS TECHNIQUES

In wireless communication systems, it is often desirable to allow the subscriber to send information simultaneously from the mobile station to the base station while receiving information from the base station to the mobile station.

A cellular system divides any given area into cells where a mobile unit in each cell communicates with a base station. The main aim in the cellular system design is to be able to **increase the capacity of the channel**, i.e., to handle as many calls as possible in a given bandwidth with a sufficient level of quality of service.

There are several different ways to allow access to the channel. These includes mainly the following −

- Frequency division multiple-access (FDMA)
- Time division multiple-access (TDMA)
- Code division multiple-access (CDMA)
- Space division multiple access (SDMA)

Depending on how the available bandwidth is allocated to the users, these techniques can be classified as **narrowband** and **wideband** systems.

Narrowband Systems

Systems operating with channels substantially narrower than the coherence bandwidth are called as Narrow band systems. Narrow band TDMA allows users to use the same channel but allocates a unique time slot to each user on the channel, thus separating a small number of users in time on a single channel.

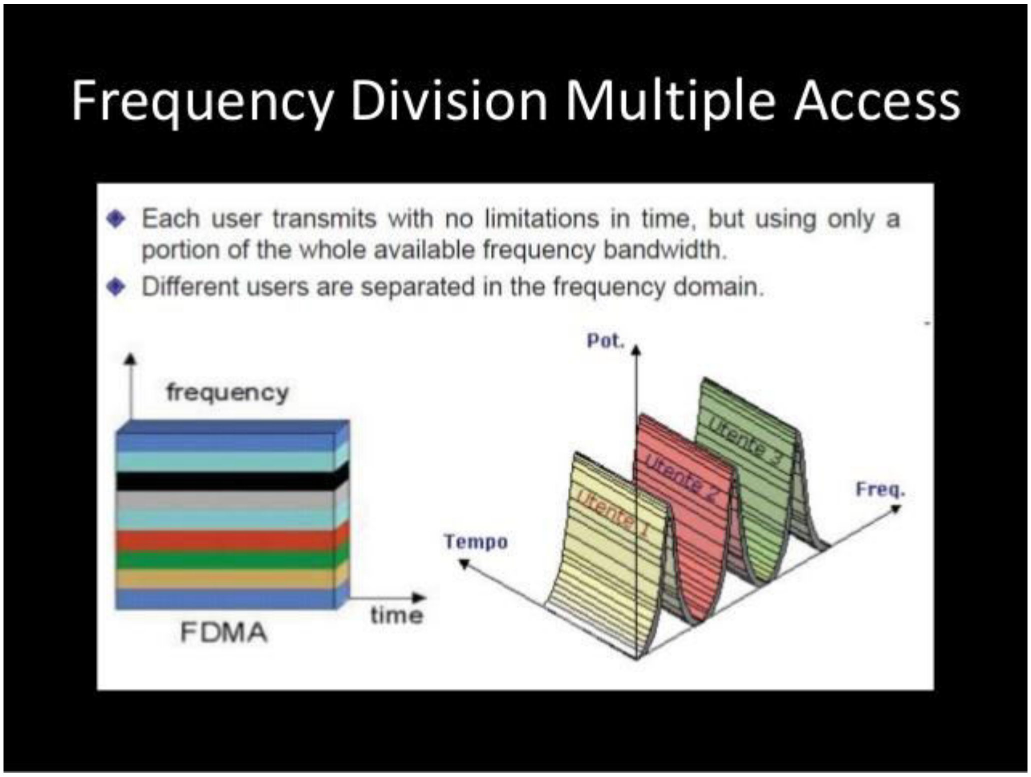
Wideband Systems

In wideband systems, the transmission bandwidth of a single channel is much larger than the coherence bandwidth of the channel. Thus, multipath fading doesn't greatly affect the received signal within a wideband channel, and frequency selective fades occur only in a small fraction of the signal bandwidth.

1.7 FREQUENCY DIVISION MULTIPLE ACCESS (FDMA)

FDMA is the basic technology for advanced mobile phone services. The features of FDMA are as follows.

- FDMA allots a different sub-band of frequency to each different user to access the network.
- If FDMA is not in use, the channel is left idle instead of allotting to the other users.
- FDMA is implemented in Narrowband systems and it is less complex than TDMA.
- Tight filtering is done here to reduce adjacent channel interference.
- The base station BS and mobile station MS, transmit and receive simultaneously and continuously in FDMA.



Frequency Division Multiple Access

- Each user transmits with no limitations in time, but using only a portion of the whole available frequency bandwidth.
- Different users are separated in the frequency domain.

FIGURE 1.18 FREQUENCY DIVISION MULTIPLE ACCESS

FDMA is different from frequency division duplexing (FDD). While FDMA permits multiple users to simultaneously access a transmission system, FDD describes the way the radio channel is shared between the downlink and uplink.

FDMA is also different from Frequency-division multiplexing (FDM). FDM refers to a physical layer method that blends and transmits low-bandwidth channels via a high-bandwidth channel. FDMA, in contrast, is a channel access technique in the data link layer.

1.8 TIME DIVISION MULTIPLE ACCESS (TDMA)

In the cases where continuous transmission is not required, there TDMA is used instead of FDMA. The features of TDMA include the following.

- TDMA shares a single carrier frequency with several users where each users makes use of non-overlapping time slots.
- Data transmission in TDMA is not continuous, but occurs in bursts. Hence handsoff process is simpler.
- TDMA uses different time slots for transmission and reception thus duplexers are not required.
- TDMA has an advantage that is possible to allocate different numbers of time slots per frame to different users.
- Bandwidth can be supplied on demand to different users by concatenating or reassigning time slot based on priority.

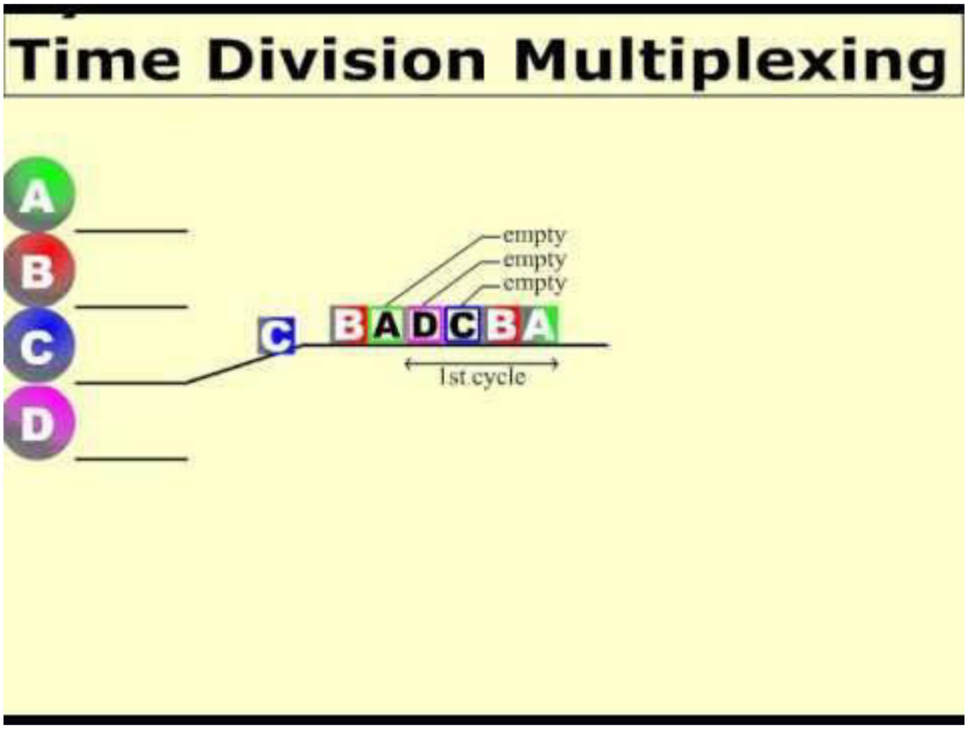


FIGURE 1.19 TIME DIVISION MULTIPLE ACCESS

Time Division Multiple Access (TDMA) is a digital cellular telephone communication technology. It facilitates many users to share the same frequency without interference. Its technology divides a signal into different timeslots, and increases the data carrying capacity.

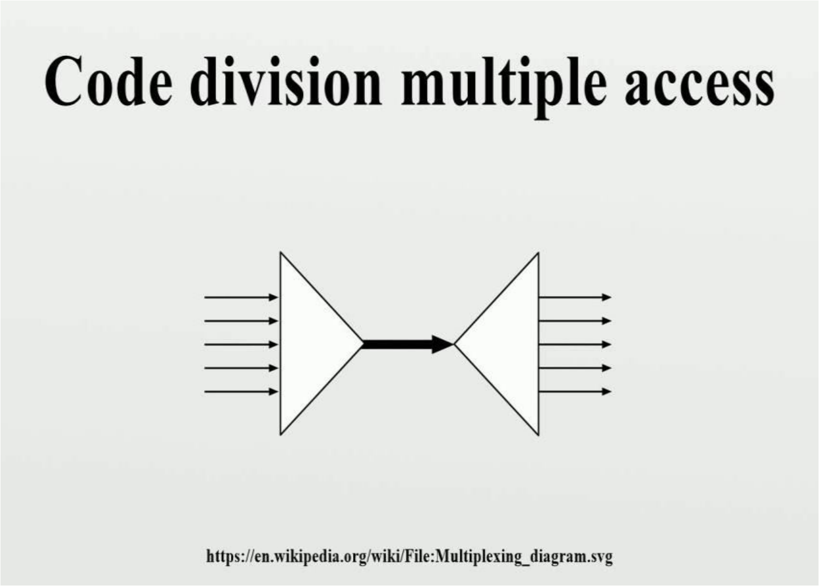
Time Division Multiple Access (TDMA) is a complex technology, because it requires an accurate synchronization between the transmitter and the receiver. TDMA is used in digital mobile radio systems. The individual mobile stations cyclically assign a frequency for the exclusive use of a time interval.

In most of the cases, the entire system bandwidth for an interval of time is not assigned to a station. However, the frequency of the system is divided into sub-bands, and TDMA is used for the multiple access in each sub-band. Sub-bands are known as **carrier frequencies**. The mobile system that uses this technique is referred as the **multi-carrier systems**.

1.9 CODE DIVISION MULTIPLE ACCESS (CDMA)

Code division multiple access technique is an example of multiple access where several transmitters use a single channel to send information simultaneously. Its features are as follows.

- In CDMA every user uses the full available spectrum instead of getting allotted by separate frequency.
- CDMA is much recommended for voice and data communications.
- While multiple codes occupy the same channel in CDMA, the users having same code can communicate with each other.
- CDMA offers more air-space capacity than TDMA.
- The hands-off between base stations is very well handled by CDMA.



https://en.wikipedia.org/wiki/File:Multiplexing_diagram.svg

FIGURE 1.20 CODE DIVISION MULTIPLE ACCESS

Code Division Multiple Access (CDMA) is a sort of multiplexing that facilitates various signals to occupy a single transmission channel. It optimizes the use of available bandwidth. The technology is commonly used in ultra-high-frequency (UHF) cellular telephone systems, bands ranging between the 800-MHz and 1.9-GHz.

1.10 SPACE DIVISION MULTIPLE ACCESS (SDMA)

Space division multiple access or spatial division multiple access is a technique which is MIMO (multiple-input multiple-output) architecture and used mostly in wireless and satellite communication. It has the following features.

- All users can communicate at the same time using the same channel.
- SDMA is completely free from interference.
- A single satellite can communicate with more satellites receivers of the same frequency.
- The directional spot-beam antennas are used and hence the base station in SDMA, can track a moving user.
- Controls the radiated energy for each user in space.

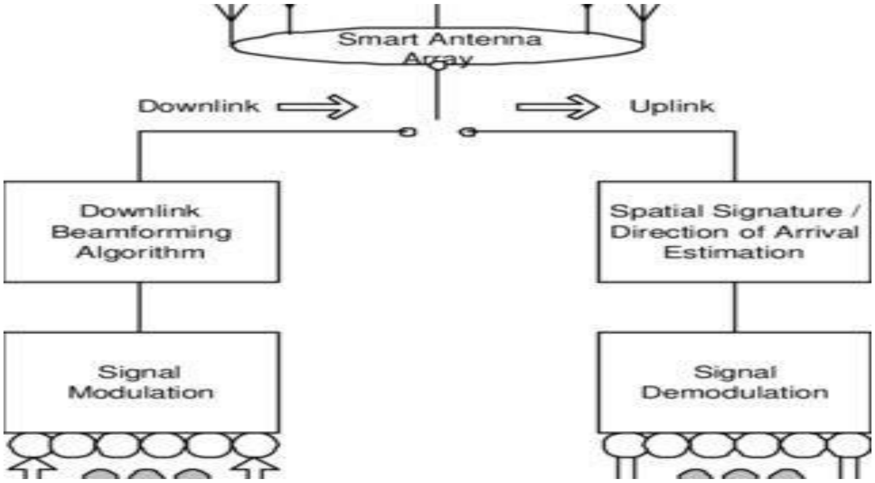

Smart Antenna Array
Downlink
Uplink
Downlink Beamforming Algorithm
Spatial Signature / Direction of Arrival Estimation
Signal Modulation
Signal Demodulation

FIGURE 1.21 SPACE DIVISION MULTIPLE ACCESS

Space-division multiple access (SDMA) is a channel access method based on creating parallel spatial pipes (focused signal beams) using advanced antenna technology next to higher capacity pipes through spatial multiplexing and/or diversity, by which it is able to offer superior performance in radio multiple access communication systems (where multiple users may need to use the communication media simultaneously).

In traditional mobile cellular network systems, the base station has no information on the position of the mobile units within the cell and radiates the signal in all directions within the cell in order to provide radio coverage. This method results in wasting power on transmissions when there are no mobile units to reach, in addition to causing interference for adjacent cells using the same frequency, so called co-channel cells. Likewise, in reception, the antenna receives signals coming from all directions including noise and interference signals. By using smart antenna technology and differing spatial locations of mobile units within the cell, space-division multiple access techniques offer attractive performance enhancements.

The radiation pattern of the base station, both in transmission and reception, is adapted to each user to obtain highest gain in the direction of that user. This is often done using phased array techniques

1.11 SPREAD SPECTRUM MULTIPLE ACCESS

Spread spectrum multiple access (SSMA) uses signals which have a transmission bandwidth whose magnitude is greater than the minimum required RF bandwidth.

There are two main types of spread spectrum multiple access techniques −

- Frequency hopped spread spectrum (FHSS)
- Direct sequence spread spectrum (DSSS)

1.11.1 Frequency Hopped Spread Spectrum (FHSS)

This is a digital multiple access system in which the carrier frequencies of the individual users are varied in a pseudo random fashion within a wideband channel. The digital data is broken into uniform sized bursts which is then transmitted on different carrier frequencies.

1.11.2 Direct Sequence Spread Spectrum (DSSS)

This is the most commonly used technology for CDMA. In DS-SS, the message signal is multiplied by a Pseudo Random Noise Code. Each user is given his own code word which is orthogonal to the codes of other users and in order to detect the user, the receiver must know the code word used by the transmitter.

The combinational sequences called as **hybrid** are also used as another type of spread spectrum. **Time hopping** is also another type which is rarely mentioned.

Since many users can share the same spread spectrum bandwidth without interfering with one another, spread spectrum systems become **bandwidth efficient** in a multiple user environment.

UNIT -II

TELECOMMUNICATION NETWORKS & WIRLESS LAN

2.1 GLOBAL SYSTEM FOR MOBILE COMMUNICATION [GSM]

- GSM stands for **G**lobal **S**ystem for **M**obile Communication. It is a digital cellular technology used for transmitting mobile voice and data services.
- The concept of GSM emerged from a cell-based mobile radio system at Bell Laboratories in the early 1970s.
- GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard.
- GSM is the most widely accepted standard in telecommunications and it is implemented globally.
- GSM is a circuit-switched system that divides each 200 kHz channel into eight 25 kHz time-slots. GSM operates on the mobile communication bands 900 MHz and 1800 MHz in most parts of the world. In the US, GSM operates in the bands 850 MHz and 1900 MHz.
- GSM owns a market share of more than 70 percent of the world's digital cellular subscribers.
- GSM makes use of narrowband Time Division Multiple Access (TDMA) technique for transmitting signals.
- GSM was developed using digital technology. It has an ability to carry 64 kbps to 120 Mbps of data rates.
- Presently GSM supports more than one billion mobile subscribers in more than 210 countries throughout the world.
- GSM provides basic to advanced voice and data services including roaming service. Roaming is the ability to use your GSM phone number in another GSM network.

GSM digitizes and compresses data, then sends it down through a channel with two other streams of user data, each in its own timeslot.

2.1.1 FEATURES OF GSM

Listed below are the features of GSM that account for its popularity and wide acceptance.

- Improved spectrum efficiency

- International roaming
- Low-cost mobile sets and base stations (BSs)
- High-quality speech
- Compatibility with Integrated Services Digital Network (ISDN) and other telephone company services
- Support for new services

2.1.2 HISTORY OF GSM

The following table shows some of the important events in the rollout of the GSM system.

Years	Events
1982	Conference of European Posts and Telegraph (CEPT) establishes a GSM group to widen the standards for a pan-European cellular mobile system.
1985	A list of recommendations to be generated by the group is accepted.
1986	Executed field tests to check the different radio techniques recommended for the air interface.
1987	Time Division Multiple Access (TDMA) is chosen as the access method (with Frequency Division Multiple Access [FDMA]). The initial Memorandum of Understanding (MoU) is signed by telecommunication operators representing 12 countries.
1988	GSM system is validated.
1989	The European Telecommunications Standards Institute (ETSI) was given the responsibility of the GSM specifications.
1990	Phase 1 of the GSM specifications is delivered.

1991	Commercial launch of the GSM service occurs. The DCS1800 specifications are finalized.
1992	The addition of the countries that signed the GSM MoU takes place. Coverage spreads to larger cities and airports.
1993	Coverage of main roads GSM services starts outside Europe.
1994	Data transmission capabilities launched. The number of networks rises to 69 in 43 countries by the end of 1994.
1995	Phase 2 of the GSM specifications occurs. Coverage is extended to rural areas.
1996	June: 133 network in 81 countries operational.
1997	July: 200 network in 109 countries operational, around 44 million subscribers worldwide.
1999	Wireless Application Protocol (WAP) came into existence and became operational in 130 countries with 260 million subscribers.
2000	General Packet Radio Service(GPRS) came into existence.
2001	As of May 2001, over 550 million people were subscribers to mobile telecommunications.

2.1.4 GSM - ARCHITECTURE

A GSM network comprises of many functional units. These functions and interfaces are explained in this chapter. The GSM network can be broadly divided into:

- The Mobile Station (MS)

- The Base Station Subsystem (BSS)
- The Network Switching Subsystem (NSS)
- The Operation Support Subsystem (OSS)

Given below is a simple pictorial view of the GSM architecture.

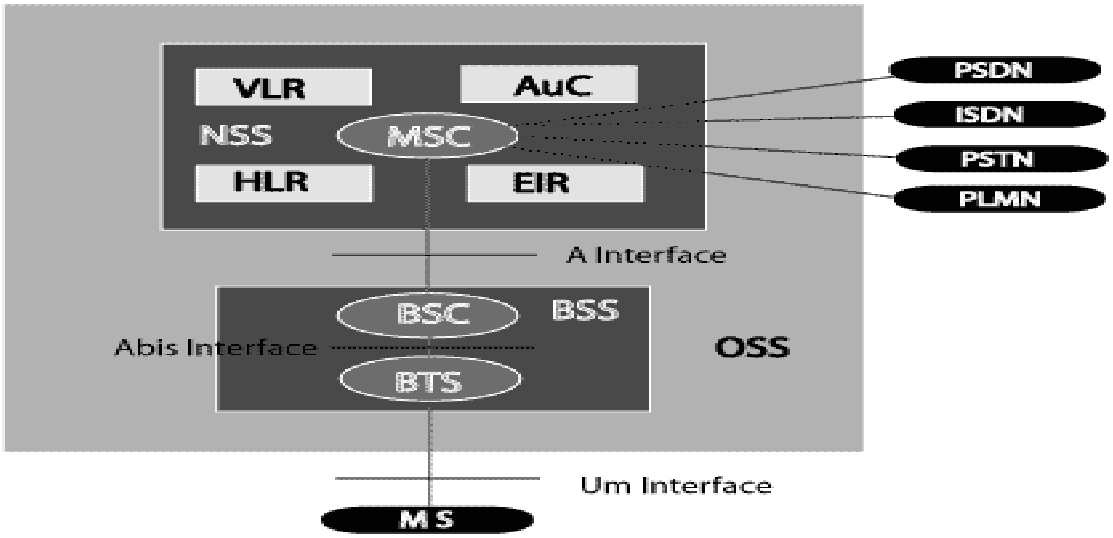


FIGURE 2.1 GSM - ARCHITECTURE

2.1.5 COMPONENTS OF THE GSM ARCHITECTURE

The additional **components of the GSM architecture** comprise of databases and messaging systems functions:

- Home Location Register (HLR)
- Visitor Location Register (VLR)
- Equipment Identity Register (EIR)
- Authentication Center (AuC)
- SMS Serving Center (SMS SC)
- Gateway MSC (GMSC)
- Chargeback Center (CBC)
- Transcoder and Adaptation Unit (TRAU)

The following diagram shows the GSM network along with the added elements:

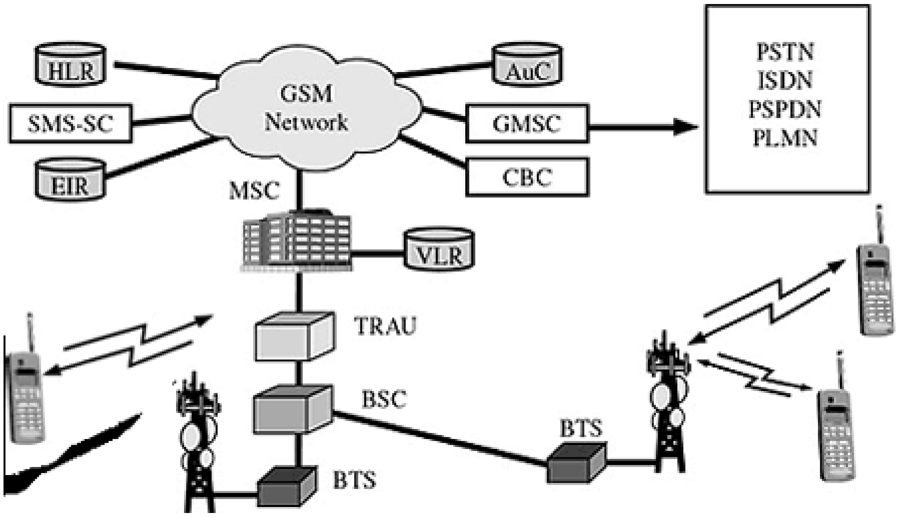


FIGURE 2.2 COMPONENTS OF THE GSM ARCHITECTURE

The MS and the BSS communicate across the Um interface. It is also known as the air interface or the radio link. The BSS communicates with the Network Service Switching (NSS) center across the *A* interface.

2.1.6 GSM NETWORK AREAS

In a GSM network, the following areas are defined:

- **Cell** : Cell is the basic service area; one BTS covers one cell. Each cell is given a Cell Global Identity (CGI), a number that uniquely identifies the cell.
- **Location Area** : A group of cells form a Location Area (LA). This is the area that is paged when a subscriber gets an incoming call. Each LA is assigned a Location Area Identity (LAI). Each LA is served by one or more BSCs.
- **MSC/VLR Service Area** : The area covered by one MSC is called the MSC/VLR service area.
- **PLMN** : The area covered by one network operator is called the Public Land Mobile Network (PLMN). A PLMN can contain one or more MSCs.

2.1.7 GSM - SPECIFICATION

The requirements for different Personal Communication Services (PCS) systems differ for each PCS network. Vital characteristics of the GSM specification are listed below:

Modulation

Modulation is the process of transforming the input data into a suitable format for the transmission medium. The transmitted data is demodulated back to its original form at the receiving end. The GSM uses Gaussian Minimum Shift Keying (GMSK) modulation method.

Access Methods

Radio spectrum being a limited resource that is consumed and divided among all the users, GSM devised a combination of TDMA/FDMA as the method to divide the bandwidth among the users. In this process, the FDMA part divides the frequency of the total 25 MHz bandwidth into 124 carrier frequencies of 200 kHz bandwidth.

Each BS is assigned with one or multiple frequencies, and each of this frequency is divided into eight timeslots using a TDMA scheme. Each of these slots are used for both transmission as well as reception of data. These slots are separated by time so that a mobile unit doesn't transmit and receive data at the same time.

Transmission Rate

The total symbol rate for GSM at 1 bit per symbol in GMSK produces 270.833 K symbols/second. The gross transmission rate of a timeslot is 22.8 Kbps.

GSM is a digital system with an over-the-air bit rate of 270 kbps.

Frequency Band

The **uplink frequency range** specified for GSM is 933 - 960 MHz (basic 900 MHz band only).

The **downlink frequency band** 890 - 915 MHz (basic 900 MHz band only).

Channel Spacing

Channel spacing indicates the spacing between adjacent carrier frequencies. For GSM, it is 200 kHz.

Speech Coding

For speech coding or processing, GSM uses Linear Predictive Coding (LPC). This tool compresses the bit rate and gives an estimate of the speech parameters. When the audio signal passes through a filter, it mimics the vocal tract. Here, the speech is encoded at 13 kbps.

Duplex Distance

Duplex distance is the space between the uplink and downlink frequencies. The duplex distance for GSM is 80 MHz, where each channel has two frequencies that are 80 MHz apart.

- Misc
- Frame duration : 4.615 mS
- Duplex Technique : Frequency Division Duplexing (FDD) access mode previously known as WCDMA.
- Speech channels per RF channel : 8.

2.1.9 GSM - ADDRESSES AND IDENTIFIERS

GSM treats the users and the equipment in different ways. Phone numbers, subscribers, and equipment identifiers are some of the known ones. There are many other identifiers that have been well-defined, which are required for the subscriber's mobility management and for addressing the remaining network elements. Vital addresses and identifiers that are used in GSM are addressed below.

International Mobile Station Equipment Identity (IMEI)

The International Mobile Station Equipment Identity (IMEI) looks more like a serial number which distinctively identifies a mobile station internationally. This is allocated by the equipment manufacturer and registered by the network operator, who stores it in the Equipment Identity Register (EIR). By means of IMEI, one recognizes obsolete, stolen, or non-functional equipment.

Following are the parts of IMEI:

- **Type Approval Code (TAC)** : 6 decimal places, centrally assigned.
- **Final Assembly Code (FAC)** : 6 decimal places, assigned by the manufacturer.
- **Serial Number (SNR)** : 6 decimal places, assigned by the manufacturer.
- **Spare (SP)** : 1 decimal place.

Thus, IMEI = TAC + FAC + SNR + SP. It uniquely characterizes a mobile station and gives clues about the manufacturer and the date of manufacturing.

International Mobile Subscriber Identity (IMSI)

Every registered user has an original International Mobile Subscriber Identity (IMSI) with a valid IMEI stored in their Subscriber Identity Module (SIM).

IMSI comprises of the following parts:

- **Mobile Country Code (MCC)** : 3 decimal places, internationally standardized.
- **Mobile Network Code (MNC)** : 2 decimal places, for unique identification of mobile network within the country.
- **Mobile Subscriber Identification Number (MSIN)** : Maximum 10 decimal places, identification number of the subscriber in the home mobile network.

Mobile Subscriber ISDN Number (MSISDN)

The authentic telephone number of a mobile station is the Mobile Subscriber ISDN Number (MSISDN). Based on the SIM, a mobile station can have many MSISDNs, as each subscriber is assigned with a separate MSISDN to their SIM respectively.

Listed below is the structure followed by MSISDN categories, as they are defined based on international ISDN number plan:

- **Country Code (CC)** : Up to 3 decimal places.
- **National Destination Code (NDC)** : Typically 2-3 decimal places.
- **Subscriber Number (SN)** : Maximum 10 decimal places.

Mobile Station Roaming Number (MSRN)

Mobile Station Roaming Number (MSRN) is an interim location dependent ISDN number, assigned to a mobile station by a regionally responsible Visitor Location Register (VLA). Using MSRN, the incoming calls are channelled to the MS.

The MSRN has the same structure as the MSISDN.

- Country Code (CC) : of the visited network.
- National Destination Code (NDC) : of the visited network.
- Subscriber Number (SN) : in the current mobile network.

Location Area Identity (LAI)

Within a PLMN, a Location Area identifies its own authentic Location Area Identity (LAI). The LAI hierarchy is based on international standard and structured in a unique format as mentioned below:

- Country Code (CC) : 3 decimal places.
- Mobile Network Code (MNC) : 2 decimal places.
- Location Area Code (LAC) : maximum 5 decimal places or maximum twice 8 bits coded in hexadecimal (LAC < FFFF).

Temporary Mobile Subscriber Identity (TMSI)

Temporary Mobile Subscriber Identity (TMSI) can be assigned by the VLR, which is responsible for the current location of a subscriber. The TMSI needs to have only local significance in the area handled by the VLR. This is stored on the network side only in the VLR and is not passed to the Home Location Register (HLR).

Together with the current location area, the TMSI identifies a subscriber uniquely. It can contain up to 4 × 8 bits.

Local Mobile Subscriber Identity (LMSI)

Each mobile station can be assigned with a Local Mobile Subscriber Identity (LMSI), which is an original key, by the VLR. This key can be used as the auxiliary searching key for each mobile station within its region. It can also help accelerate the database access. An LMSI is assigned if the mobile station is registered with the VLR and sent to the HLR. LMSI comprises of four octets (4x8 bits).

Cell Identifier (CI)

Using a Cell Identifier (CI) (maximum 2 × 8) bits, the individual cells that are within an LA can be recognized. When the Global Cell Identity (LAI + CI) calls are combined, then it is uniquely defined.

2.1.10 GSM - OPERATIONS

Once a Mobile Station initiates a call, a series of events takes place. Analyzing these events can give an insight into the operation of the GSM system.

Mobile Phone to Public Switched Telephone Network (PSTN)

When a mobile subscriber makes a call to a PSTN telephone subscriber, the following sequence of events takes place:

- The MSC/VLR receives the message of a call request.
- The MSC/VLR checks if the mobile station is authorized to access the network. If so, the mobile station is activated. If the mobile station is not authorized, then the service will be denied.
- MSC/VLR analyzes the number and initiates a call setup with the PSTN.
- MSC/VLR asks the corresponding BSC to allocate a traffic channel (a radio channel and a time slot).
- The BSC allocates the traffic channel and passes the information to the mobile station.
- The called party answers the call and the conversation takes place.
- The mobile station keeps on taking measurements of the radio channels in the present cell and the neighbouring cells and passes the information to the BSC. The BSC decides if a handover is required. If so, a new traffic channel is allocated to the mobile station and the handover takes place. If handover is not required, the mobile station continues to transmit in the same frequency.

PSTN to Mobile Phone

When a PSTN subscriber calls a mobile station, the following sequence of events takes place:

- The Gateway MSC receives the call and queries the HLR for the information needed to route the call to the serving MSC/VLR.
- The GMSC routes the call to the MSC/VLR.
- The MSC checks the VLR for the location area of the MS.
- The MSC contacts the MS via the BSC through a broadcast message, that is, through a paging request.
- The MS responds to the page request.
- The BSC allocates a traffic channel and sends a message to the MS to tune to the channel. The MS generates a ringing signal and, after the subscriber answers, the speech connection is established.
- Handover, if required, takes place, as discussed in the earlier case.

To transmit the speech over the radio channel in the stipulated time, the MS codes it at the rate of 13 Kbps. The BSC transcodes the speech to 64 Kbps and sends it over a land link or a radio link to the MSC. The MSC then forwards the speech data to the PSTN. In the reverse direction, the speech is received at 64 Kbps at the BSC and the BSC transcodes it to 13 Kbps for radio transmission.

GSM supports 9.6 Kbps data that can be channelled in one TDMA timeslot. To supply higher data rates, many enhancements were done to the GSM standards (GSM Phase 2 and GSM Phase 2+).

2.1.11 GSM - PROTOCOL STACK

GSM architecture is a layered model that is designed to allow communications between two different systems. The lower layers assure the services of the upper-layer protocols. Each layer passes suitable notifications to ensure the transmitted data has been formatted, transmitted, and received accurately.

The GMS protocol stacks diagram is shown below:

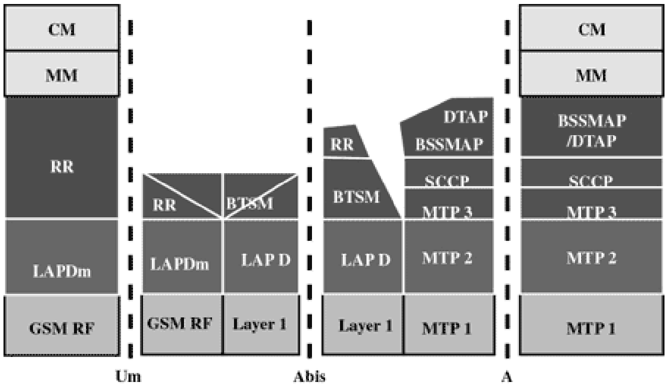


FIGURE 2.3 GSM - PROTOCOL STACK

MS Protocols

Based on the interface, the GSM signaling protocol is assembled into three general layers:

- **Layer 1** : The physical layer. It uses the channel structures over the air interface.
- **Layer 2** : The data-link layer. Across the Um interface, the data-link layer is a modified version of the Link access protocol for the D channel (LAP-D) protocol used in ISDN, called Link

access protocol on the Dm channel (LAP-Dm). Across the A interface, the Message Transfer Part (MTP), Layer 2 of SS7 is used.

- **Layer 3** : GSM signalling protocol's third layer is divided into three sublayers:
    - Radio Resource Management (RR),
    - Mobility Management (MM), and
    - Connection Management (CM).

MS to BTS Protocols

The RR layer is the lower layer that manages a link, both radio and fixed, between the MS and the MSC. For this formation, the main components involved are the MS, BSS, and MSC. The responsibility of the RR layer is to manage the RR-session, the time when a mobile is in a dedicated mode, and the radio channels including the allocation of dedicated channels.

The MM layer is stacked above the RR layer. It handles the functions that arise from the mobility of the subscriber, as well as the authentication and security aspects. Location management is concerned with the procedures that enable the system to know the current location of a powered-on MS so that incoming call routing can be completed.

The CM layer is the topmost layer of the GSM protocol stack. This layer is responsible for Call Control, Supplementary Service Management, and Short Message Service Management. Each of these services are treated as individual layer within the CM layer. Other functions of the CC sublayer include call establishment, selection of the type of service (including alternating between services during a call), and call release.

BSC Protocols

The BSC uses a different set of protocols after receiving the data from the BTS. The Abis interface is used between the BTS and BSC. At this level, the radio resources at the lower portion of Layer 3 are changed from the RR to the Base Transceiver Station Management (BTSM). The BTS management layer is a relay function at the BTS to the BSC.

The RR protocols are responsible for the allocation and reallocation of traffic channels between the MS and the BTS. These services include controlling the initial access to the system, paging for MT calls, the handover of calls between cell sites, power control, and call termination. The BSC still has some radio resource management in place for the frequency coordination, frequency allocation, and the management of the overall network layer for the Layer 2 interfaces.

To transit from the BSC to the MSC, the BSS mobile application part or the direct application part is used, and SS7 protocols is applied by the relay, so that the MTP 1-3 can be used as the prime architecture.

MSC Protocols

At the MSC, starting from the BSC, the information is mapped across the A interface to the MTP Layers 1 through 3. Here, Base Station System Management Application Part (BSS MAP) is said to be the equivalent set of radio resources. The relay process is finished by the layers that are stacked on top of Layer 3 protocols, they are BSS MAP/DTAP, MM, and CM. This completes the relay process. To find and connect to the users across the network, MSCs interact using the control-signalling network. Location registers are included in the MSC databases to assist in the role of determining how and whether connections are to be made to roaming users.

Each GSM MS user is given a HLR that in turn comprises of the user's location and subscribed services. VLR is a separate register that is used to track the location of a user. When the users move out of the HLR covered area, the VLR is notified by the MS to find the location of the user. The VLR in turn, with the help of the control network, signals the HLR of the MS's new location. With the help of location information contained in the user's HLR, the MT calls can be routed to the user.

2.1.12 GSM - USER SERVICES

GSM offers much more than just voice telephony. Contact your local GSM network operator to the specific services that you can avail.

GSM offers three basic types of services:

- Telephony services or teleservices

- Data services or bearer services
- Supplementary services

TELESERVICES

The abilities of a Bearer Service are used by a Teleservice to transport data. These services are further transited in the following ways:

Voice Calls

The most basic Teleservice supported by GSM is telephony. This includes full-rate speech at 13 kbps and emergency calls, where the nearest emergency-service provider is notified by dialing three digits.

Videotext and Facsmile

Another group of teleservices includes Videotext access, Teletex transmission, Facsmile alternate speech and Facsmile Group 3, Automatic Facsmile Group, 3 etc.

Short Text Messages

Short Messaging Service (SMS) service is a text messaging service that allows sending and receiving text messages on your GSM mobile phone. In addition to simple text messages, other text data including news, sports, financial, language, and location-based data can also be transmitted.

BEARER SERVICES

Data services or Bearer Services are used through a GSM phone. to receive and send data is the essential building block leading to widespread mobile Internet access and mobile data transfer. GSM currently has a data transfer rate of 9.6k. New developments that will push up data transfer rates for GSM users are HSCSD (high speed circuit switched data) and GPRS (general packet radio service) are now available.

SUPPLEMENTARY SERVICES

Supplementary services are additional services that are provided in addition to teleservices and bearer services. These services include caller identification, call forwarding, call waiting, multi-party conversations, and barring of outgoing (international) calls, among others. A brief description of supplementary services is given here:

- **Conferencing** : It allows a mobile subscriber to establish a multiparty conversation, i.e., a simultaneous conversation between three or more subscribers to setup a conference call. This service is only applicable to normal telephony.
- **Call Waiting** : This service notifies a mobile subscriber of an incoming call during a conversation. The subscriber can answer, reject, or ignore the incoming call.
- **Call Hold** : This service allows a subscriber to put an incoming call on hold and resume after a while. The call hold service is applicable to normal telephony.
- **Call Forwarding** : Call Forwarding is used to divert calls from the original recipient to another number. It is normally set up by the subscriber himself. It can be used by the subscriber to divert calls from the Mobile Station when the subscriber is not available, and so to ensure that calls are not lost.
- **Call Barring** : Call Barring is useful to restrict certain types of outgoing calls such as ISD or stop incoming calls from undesired numbers. Call barring is a flexible service that enables the subscriber to conditionally bar calls.
- **Number Identification** : There are following supplementary services related to number identification:

○ **Calling Line Identification Presentation** : This service displays the telephone number of the calling party on your screen.

○ **Calling Line Identification Restriction** : A person not wishing their number to be presented to others subscribes to this service.

○ **Connected Line Identification Presentation** : This service is provided to give the calling party the telephone number of the person to whom they are connected. This service is useful in situations such as forwarding's where the number connected is not the number dialled.

○ **Connected Line Identification Restriction** : There are times when the person called does not wish to have their number presented and so they would subscribe to this person. Normally, this overrides the presentation service.

○ **Malicious Call Identification** : The malicious call identification service was provided to combat the spread of obscene or annoying calls. The victim should subscribe to this service, and then they could cause known malicious calls to be identified in the GSM network, using a simple command.

- **Advice of Charge (AoC)** : This service was designed to give the subscriber an indication of the cost of the services as they are used. Furthermore, those service providers who wish to offer rental services to subscribers without their own SIM can also utilize this service in a slightly different form. AoC for data calls is provided on the basis of time measurements.
- **Closed User Groups (CUGs)** : This service is meant for groups of subscribers who wish to call only each other and no one else.
- **Unstructured supplementary services data (USSD)** : This allows operator-defined individual services.

2.1.13 GSM - SECURITY AND ENCRYPTION

- GSM is the most secured cellular telecommunications system available today. GSM has its security methods standardized. GSM maintains end-to-end security by retaining the confidentiality of calls and anonymity of the GSM subscriber.
- Temporary identification numbers are assigned to the subscriber's number to maintain the privacy of the user. The privacy of the communication is maintained by applying encryption algorithms and frequency hopping that can be enabled using digital systems and signalling.
- This chapter gives an outline of the security measures implemented for GSM subscribers.
- Mobile Station Authentication
- The GSM network authenticates the identity of the subscriber through the use of a challenge-response mechanism. A 128-bit Random Number (RAND) is sent to the MS. The MS computes the 32-bit Signed Response (SRES) based on the encryption of the RAND with the authentication algorithm (A3) using the individual subscriber authentication key (Ki). Upon receiving the SRES from the subscriber, the GSM network repeats the calculation to verify the identity of the subscriber.
- The individual subscriber authentication key (Ki) is never transmitted over the radio channel, as it is present in the subscriber's SIM, as well as the AUC, HLR, and VLR databases. If the received SRES agrees with the calculated value, the MS has been successfully authenticated and

may continue. If the values do not match, the connection is terminated and an authentication failure is indicated to the MS.

- The calculation of the signed response is processed within the SIM. It provides enhanced security, as confidential subscriber information such as the IMSI or the individual subscriber authentication key (Ki) is never released from the SIM during the authentication process.
- Signalling and Data Confidentiality
- The SIM contains the ciphering key generating algorithm (A8) that is used to produce the 64-bit ciphering key (Kc). This key is computed by applying the same random number (RAND) used in the authentication process to ciphering key generating algorithm (A8) with the individual subscriber authentication key (Ki).
- GSM provides an additional level of security by having a way to change the ciphering key, making the system more resistant to eavesdropping. The ciphering key may be changed at regular intervals as required. As in case of the authentication process, the computation of the ciphering key (Kc) takes place internally within the SIM. Therefore, sensitive information such as the individual subscriber authentication key (Ki) is never revealed by the SIM.
- Encrypted voice and data communications between the MS and the network is accomplished by using the ciphering algorithm A5. Encrypted communication is initiated by a ciphering mode request command from the GSM network. Upon receipt of this command, the mobile station begins encryption and decryption of data using the ciphering algorithm (A5) and the ciphering key (Kc).
- Subscriber Identity Confidentiality
- To ensure subscriber identity confidentiality, the Temporary Mobile Subscriber Identity (TMSI) is used. Once the authentication and encryption procedures are done, the TMSI is sent to the mobile station. After the receipt, the mobile station responds. The TMSI is valid in the location area in which it was issued. For communications outside the location area, the Location Area Identification (LAI) is necessary in addition to the TMSI.

2.1.14 GSM - BILLING

GSM service providers are doing billing based on the services they are providing to their customers. All the parameters are simple enough to charge a customer for the provided services.

Telephony Service

These services can be charged on per call basis. The call initiator has to pay the charges, and the incoming calls are nowadays free. A customer can be charged based on different parameters such as:

- International call or long distance call.
- Local call.
- Call made during peak hours.
- Call made during night time.
- Discounted call during weekends.
- Call per minute or per second.
- Many more other criteria can be designed by a service provider to charge their customers.

SMS Service

Most of the service providers charge their customer's SMS services based on the number of text messages sent. There are other prime SMS services available where service providers charge more than normal SMS charge. These services are being availed in collaboration of Television Networks or Radio Networks to demand SMS from the audiences.

Most of the time, the charges are paid by the SMS sender but for some services like stocks and share prices, mobile banking facilities, and leisure booking services, etc. the recipient of the SMS has to pay for the service.

GPRS Services

Using GPRS service, you can browse, play games on the Internet, and download movies. So a service provider will charge you based on the data uploaded as well as data downloaded on your mobile phone. These charges will be based on per Kilo Byte data downloaded/uploaded.

Additional parameter could be a QoS provided to you. If you want to watch a movie, then a low QoS may work because some data loss may be acceptable, but if you are downloading a zip file, then a single byte loss will corrupt your complete downloaded file.

Another parameter could be peak and off peak time to download a data file or to browse the Internet.

Supplementary Services

Most of the supplementary services are being provided based on monthly rental or absolutely free. For example, call waiting, call forwarding, calling number identification, and call on hold are available at zero cost.

Call barring is a service, which service providers use just to recover their dues, etc., otherwise this service is not being used by any subscriber.

Call conferencing service is a form of simple telephone call where the customers are charged for multiple calls made at a time. No service provider charges extra charge for this service.

Closed User Group (CUG) is very popular and is mainly being used to give special discounts to the users if they are making calls to a particular defined group of subscribers.

Advice of Charge (AoC) can be charged based on number of queries made by a subscriber.

2.2 GENERAL PACKET RADIO SYSTEM - GPRS

General Packet Radio System is also known as **GPRS** is a third-generation step toward internet access. GPRS is also known as GSM-IP that is a Global-System Mobile Communications Internet Protocol as it keeps the users of this system online, allows to make voice calls, and access internet on-the-go. Even Time-Division Multiple Access (TDMA) users benefit from this system as it provides packet radio access.

GPRS also permits the network operators to execute an Internet Protocol (IP) based core architecture for integrated voice and data applications that will continue to be used and expanded for 3G services.

GPRS supersedes the wired connections, as this system has simplified access to the packet data networks like the internet. The packet radio principle is employed by GPRS to transport user data packets in a structure way between GSM mobile stations and external packet data networks. These packets can be directly routed to the packet switched networks from the GPRS mobile stations.

In the current versions of GPRS, networks based on the Internet Protocol (IP) like the global internet or private/corporate intranets and X.25 networks are supported.

The GPRS specifications are written by the European Telecommunications Standard Institute (ETSI), the European counterpart of the American National Standard Institute (ANSI).

2.2.1 KEY FEATURES

Following three key features describe wireless packet data:

- **The always online feature -** Removes the dial-up process, making applications only one click away.
- **An upgrade to existing systems -** Operators do not have to replace their equipment; rather, GPRS is added on top of the existing infrastructure.
- **An integral part of future 3G systems -** GPRS is the packet data core network for 3G systems EDGE and WCDMA.

2.2.2 GOALS OF GPRS

GPRS is the first step toward an end-to-end wireless infrastructure and has the following goals:

- Open architecture
- Consistent IP services
- Same infrastructure for different air interfaces
- Integrated telephony and Internet infrastructure
- Leverage industry investment in IP
- Service innovation independent of infrastructure

2.2.3 BENEFITS OF GPRS

Higher Data Rate

GPRS benefits the users in many ways, one of which is higher data rates in turn of shorter access times. In the typical GSM mobile, setup alone is a lengthy process and equally, rates for data permission are restrained to 9.6 kbit/s. The session establishment time offered while GPRS is in practice is lower than one second and ISDN-line data rates are up to many 10 kbit/s.

Easy Billing

GPRS packet transmission offers a more user-friendly billing than that offered by circuit switched services. In circuit switched services, billing is based on the duration of the connection. This is unsuitable for applications with bursty traffic. The user must pay for the entire airtime, even for idle periods when no packets are sent (e.g., when the user reads a Web page).

In contrast to this, with packet switched services, billing can be based on the amount of transmitted data. The advantage for the user is that he or she can be "online" over a long period of time but will be billed based on the transmitted data volume.

2.2.4 GPRS - APPLICATIONS

GPRS has opened a wide range of unique services to the mobile wireless subscriber. Some of the characteristics that have opened a market full of enhanced value services to the users. Below are some of the characteristics:

- **Mobility -** The ability to maintain constant voice and data communications while on the move.
- **Immediacy -** Allows subscribers to obtain connectivity when needed, regardless of location and without a lengthy login session.
- **Localization -** Allows subscribers to obtain information relevant to their current location.

Using the above three characteristics varied possible applications are being developed to offer to the mobile subscribers. These applications, in general, can be divided into two high-level categories:

- Corporation

- Consumer

These two levels further include:

- **Communications -** E-mail, fax, unified messaging and intranet/internet access, etc.
- **Value-added services -** Information services and games, etc.
- **E-commerce -** Retail, ticket purchasing, banking and financial trading, etc.
- **Location-based applications -** Navigation, traffic conditions, airline/rail schedules and location finder, etc.
- **Vertical applications -** Freight delivery, fleet management and sales-force automation.
- **Advertising -** Advertising may be location sensitive. For example, a user entering a mall can receive advertisements specific to the stores in that mall.

Along with the above applications, non-voice services like SMS, MMS and voice calls are also possible with GPRS. Closed User Group (CUG) is a common term used after GPRS is in the market, in addition, it is planned to implement supplementary services, such as Call Forwarding Unconditional (CFU), and Call Forwarding on Mobile subscriber Not Reachable (CFNRc), and closed user group (CUG).

2.2.5 GPRS - ARCHITECTURE

GPRS architecture works on the same procedure like GSM network, but, has additional entities that allow packet data transmission. This data network overlaps a second-generation GSM network providing packet data transport at the rates from 9.6 to 171 kbps. Along with the packet data transport the GSM network accommodates multiple users to share the same air interface resources concurrently.

Following is the GPRS Architecture diagram:

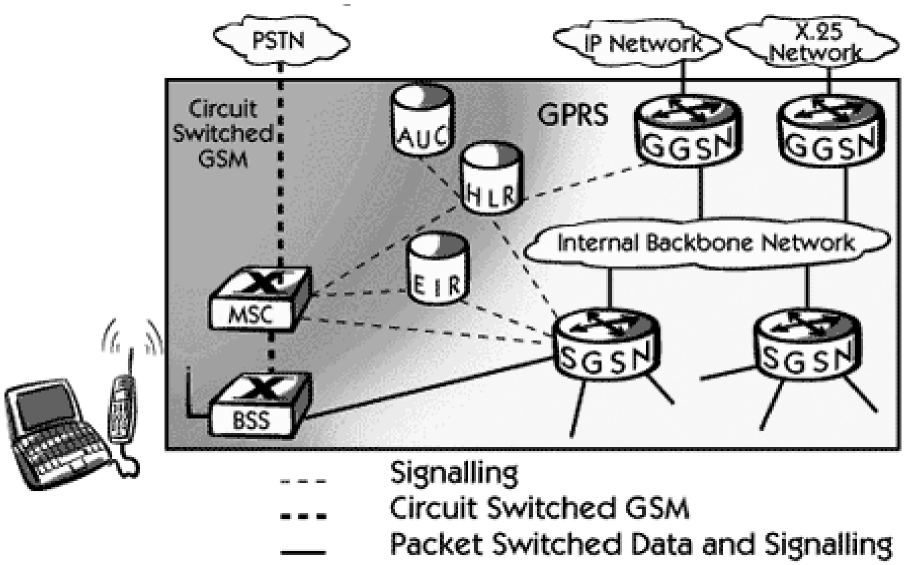


FIGURE 2.4 GPRS - ARCHITECTURE

GPRS attempts to reuse the existing GSM network elements as much as possible, but to effectively build a packet-based mobile cellular network, some new network elements, interfaces, and protocols for handling packet traffic are required.

Therefore, GPRS requires modifications to numerous GSM network elements as summarized below:

GSM Network Element	Modification or Upgrade Required for GPRS.
Mobile Station (MS)	New Mobile Station is required to access GPRS services. These new terminals will be backward compatible with GSM for voice calls.
BTS	A software upgrade is required in the existing Base Transceiver Station(BTS).

BSC	The Base Station Controller (BSC) requires a software upgrade and the installation of new hardware called the packet control unit (PCU). The PCU directs the data traffic to the GPRS network and can be a separate hardware element associated with the BSC.
GPRS Support Nodes (GSNs)	The deployment of GPRS requires the installation of new core network elements called the serving GPRS support node (SGSN) and gateway GPRS support node (GGSN).
Databases (HLR, VLR, etc.)	All the databases involved in the network will require software upgrades to handle the new call models and functions introduced by GPRS.

GPRS Mobile Stations

New Mobile Stations (MS) are required to use GPRS services because existing GSM phones do not handle the enhanced air interface or packet data. A variety of MS can exist, including a high-speed version of current phones to support high-speed data access, a new PDA device with an embedded GSM phone, and PC cards for laptop computers. These mobile stations are backward compatible for making voice calls using GSM.

2.2.6 GPRS BASE STATION SUBSYSTEM

Each BSC requires the installation of one or more Packet Control Units (PCUs) and a software upgrade. The PCU provides a physical and logical data interface to the Base Station Subsystem (BSS) for packet data traffic. The BTS can also require a software upgrade but typically does not require hardware enhancements.

When either voice or data traffic is originated at the subscriber mobile, it is transported over the air interface to the BTS, and from the BTS to the BSC in the same way as a standard GSM call. However, at the output of the BSC, the traffic is separated; voice is sent to the Mobile Switching Center (MSC) per standard GSM, and data is sent to a new device called the SGSN via the PCU over a Frame Relay interface.

GPRS Support Nodes

Following two new components, called Gateway GPRS Support Nodes (GSNs) and, Serving GPRS Support Node (SGSN) are added:

Gateway GPRS Support Node (GGSN)

The Gateway GPRS Support Node acts as an interface and a router to external networks. It contains routing information for GPRS mobiles, which is used to tunnel packets through the IP based internal backbone to the correct Serving GPRS Support Node. The GGSN also collects charging information connected to the use of the external data networks and can act as a packet filter for incoming traffic.

Serving GPRS Support Node (SGSN)

The Serving GPRS Support Node is responsible for authentication of GPRS mobiles, registration of mobiles in the network, mobility management, and collecting information on charging for the use of the air interface.

Internal Backbone

The internal backbone is an IP based network used to carry packets between different GSNs. Tunnelling is used between SGSNs and GGSNs, so the internal backbone does not need any information about domains outside the GPRS network. Signalling from a GSN to a MSC, HLR or EIR is done using SS7.

Routing Area

GPRS introduces the concept of a Routing Area. This concept is similar to Location Area in GSM, except that it generally contains fewer cells. Because routing areas are smaller than location areas, less radio resources are used While broadcasting a page message.

2.2.7 GPRS - PROTOCOL STACK

The flow of GPRS protocol stack and end-to-end message from MS to the GGSN is displayed in the below diagram. GTP is the protocol used between the SGSN and GGSN using the Gn interface. This is a Layer 3 tunneling protocol.

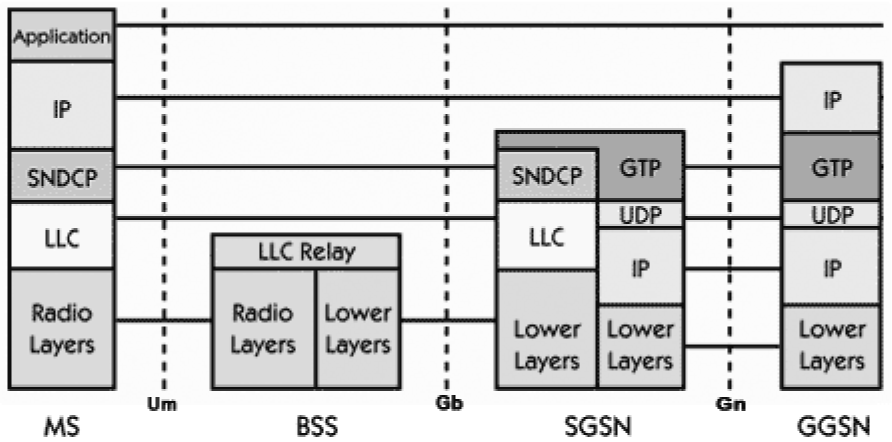


FIGURE 2.5 GPRS - PROTOCOL STACK

The process that takes place in the application looks like a normal IP sub-network for the users both inside and outside the network. The vital thing that needs attention is, the application communicates via standard IP, that is carried through the GPRS network and out through the gateway GPRS. The packets that are mobile between the GGSN and the SGSN use the GPRS tunneling protocol, this way the IP addresses located on the external side of the GPRS network do not have deal with the internal backbone. UDP and IP are run by GTP.

SubNetwork Dependent Convergence Protocol (SNDCP) and Logical Link Control (LLC) combination used in between the SGSN and the MS. The SNDCP flattens data to reduce the load on the radio channel. A safe logical link by encrypting packets is provided by LLC and the same LLC link is used as long as a mobile is under a single SGSN.

In case, the mobile moves to a new routing area that lies under a different SGSN; then, the old LLC link is removed and a new link is established with the new Serving GSN X.25. Services are provided by running X.25 on top of TCP/IP in the internal backbone.

2.2.8 GPRS - Quality of Service

Quality of Service (QoS) requirements of conventional mobile packet data applications are in assorted forms. The QoS is a vital feature of GPRS services as there are different QoS support requirements for assorted GPRS applications like realtime multimedia, web browsing, and e-mail transfer.

GPRS allows defining QoS profiles using the following parameters :

- Service Precedence
- Reliability
- Delay and
- Throughput

These parameters are described below:

Service Precedence

The preference given to a service when compared to another service is known as **Service Precedence**. This level of priority is classified into three levels called:

- high
- normal
- low

When there is network congestion, the packets of low priority are discarded as compared to high or normal priority packets.

Reliability

This parameter signifies the transmission characteristics required by an application. The reliability classes are defined which guarantee certain maximum values for the probability of loss, duplication, mis-sequencing, and corruption of packets.

Delay

The delay is defined as the end-to-end transfer time between two communicating mobile stations or between a mobile station and the GI interface to an external packet data network.

This includes all delays within the GPRS network, e.g., the delay for request and assignment of radio resources and the transit delay in the GPRS backbone network. Transfer delays outside the GPRS network, e.g., in external transit networks, are not taken into account.

Throughput

The throughput specifies the maximum/peak bit rate and the mean bit rate.

Using these QoS classes, QoS profiles can be negotiated between the mobile user and the network for each session, depending on the QoS demand and the available resources.

The billing of the service is then based on the transmitted data volume, the type of service, and the chosen QoS profile.

2.2.9 GPRS - MOBILE STATION CLASSES

Mobile Station Classes talk about the globally-known equipment handset which is also known as Mobile Station (MS) and its three different classes. This equipment, more popular as handset, is used to make phone calls and access data services. The MS comprises of Terminal Equipment (TE) and Mobile Terminal (MT).

TE is the equipment that accommodates the applications and the user interaction, while the MT is the part that connects to the network.

In the following example, Palm Pilot is TE and Mobile phone is MT.

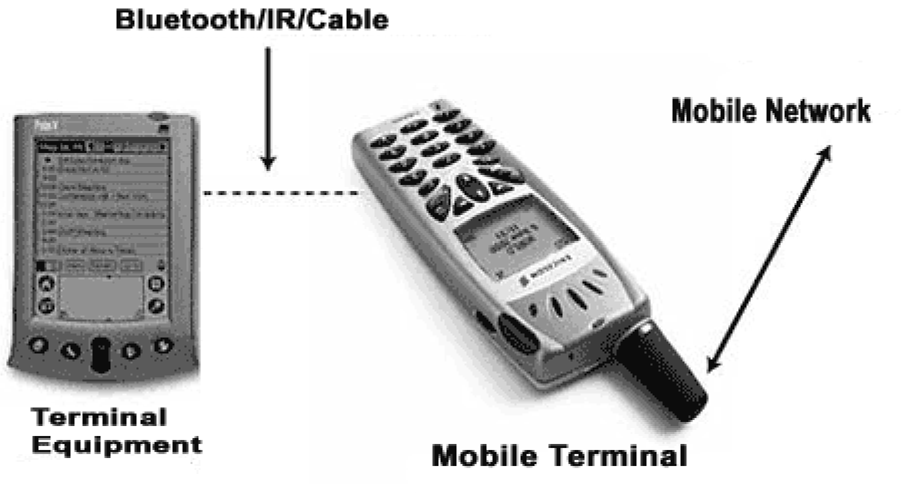


FIGURE 2.6 GPRS - MOBILE STATION CLASSES

In order to take advantage of the new GPRS services, we need new GPRS enabled handsets. There are three different classes of GPRS terminal equipments:

Class A

Class A terminals can manage both packet data and voice simultaneously. Which means, one needs two transceivers, as the handset has to send or receive data and voice at the same time.This is the main reason why class A terminals are high-priced to manufacture than class B and C terminals.

Class B

Class B terminals do not play the same role like Class A. These terminals can manage either packet data or voice at a time. One can use a single transceiver for both, resulting in the low cost of terminals.

For example, If a user is using the GPRS session (like WAP browsing, file transfer, etc.) then this session is halted if he or she receives a call. This terminal does not allow both the sessions active in one go. This backlog needs rectification thereby giving the user a facility of both receiving a call and maintaining the data session.

Class C

Class C terminals can manage either only packet data or only voice. Examples of class C terminals are GPRS PCM/CIA cards, embedded modules in vending machines, and so on.

Due to the high cost of class A handsets, most handset manufacturers have announced that their first handsets will be class B. Currently, work is going on in 3GPP to standardize a lightweight class A in order to make handsets with simultaneous voice and data available at a reasonable cost.

2.2.10 GPRS - PDP CONTEXT

PDP stands for Packet Data Protocol. The PDP addresses are network layer addresses (Open Standards Interconnect [OSI] model Layer 3). GPRS systems support both X.25 and IP network layer protocols. Therefore, PDP addresses can be X.25, IP, or both.

Each PDP address is anchored at a Gateway GPRS Support Node (GGSN), as shown in figure below. All packet data traffic sent from the public packet data network for the PDP address goes through the gateway (GGSN).

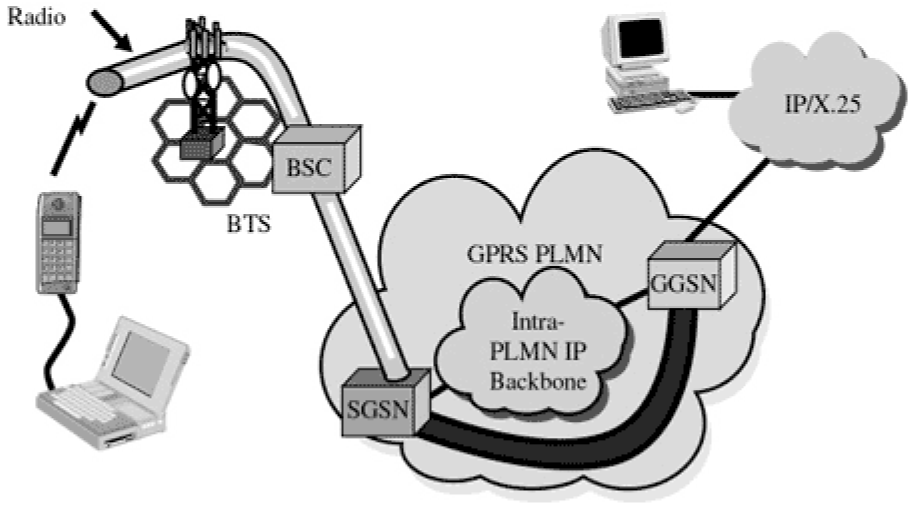


FIGURE 2.7 GPRS - PDP CONTEXT

The public packet data network is only concerned that the address belongs to a specific GGSN. The GGSN hides the mobility of the station from the rest of the packet data network and from computers connected to the public packet data network.

Statically assigned PDP addresses are usually anchored at a GGSN in the subscriber's home network. Conversely, dynamically assigned PDP addresses can be anchored either in the subscriber's home network or the network that the user is visiting.

When a MS is already attached to a SGSN and it is about to transfer data, it must activate a PDP address. Activating a PDP address establishes an association between the current SGSN of mobile device and the GGSN that anchors the PDP address.

The record kept by the SGSN and the GGSN regarding this association is called the PDP context.

It is important to understand the difference between a MS attaching to a SGSN and a MS activating a PDP address. A single MS attaches to only one SGSN, however, it may have multiple PDP addresses that are all active at the same time.

Each of the addresses may be anchored to a different GGSN. If packets arrive from the public packet data network at a GGSN for a specific PDP address and the GGSN does not have an active PDP context corresponding to that address, it may simply discard the packets. Conversely, the GGSN may attempt to activate a PDP context with a MS if the address is statically assigned to a particular mobile device.

2.2.11 GPRS - DATA ROUTING

Data routing or routing of data packets to and fro from a mobile user, is one of the pivot requisites in the GPRS network. The requirement can be divided into two areas:

- Data packet routing
- Mobility management.

Data Packet Routing

The important roles of GGSN involve synergy with the external data network. The GGSN updates the location directory using routing information supplied by the SGSNs about the location of an MS. It routes the external data network protocol packet encapsulated over the GPRS backbone to the SGSN currently serving the MS. It also decapsulates and forwards external data network packets to the appropriate data network and collects charging data that is forwarded to a charging gateway (CG).

There are three important routing schemes:

- **Mobile-originated message -** This path begins at the GPRS mobile device and ends at the host.
- **Network-initiated message when the MS is in its home network -** This path begins at the host and ends at the GPRS mobile device.
- **Network-initiated message when the MS roams to another GPRS network -** This path begins at the host of visited network and ends at the GPRS mobile device.

The GPRS network encapsulates all data network protocols into its own encapsulation protocol called the GPRS tunnelling protocol (GTP). The GTP ensures security in the backbone network and simplifies the routing mechanism and the delivery of data over the GPRS network.

Mobility Management

The operation of the GPRS is partly independent of the GSM network. However, some procedures share the network elements with current GSM functions to increase efficiency and to make optimum use of free GSM resources (such as unallocated time slots).

An MS can be in any of the following three states in the GPRS system. The three-state model is unique to packet radio. GSM uses a two-state model either idle or active.

Active State

Data is transmitted between an MS and the GPRS network only when the MS is in the active state. In the active state, the SGSN knows the cell location of the MS.

Packet transmission to an active MS is initiated by packet paging to notify the MS of an incoming data packet. The data transmission proceeds immediately after packet paging through the channel indicated by the paging message. The purpose of the paging message is to simplify the process of receiving packets. The MS listens to only the paging messages instead of to all the data packets in the downlink channels. This reduces battery usage significantly.

When an MS has a packet to transmit, it must access the uplink channel (i.e., the channel to the packet data network where services reside). The uplink channel is shared by a number of MSs, and its use is allocated by a BSS. The MS requests use of the channel in a random access message. The BSS allocates an unused channel to the MS and sends an access grant message in reply to the random access message.

Standby State

In the standby state, only the routing area of the MS is known. (The routing area can consist of one or more cells within a GSM location area).

When the SGSN sends a packet to an MS that is in the standby state, the MS must be paged. Because the SGSN knows the routing area of the MS, a packet paging message is sent to the routing area. On receiving the packet paging message, the MS relays its cell location to the SGSN to establish the active state.

Idle State

In the idle state, the MS does not have a logical GPRS context activated or any Packet-Switched Public Data Network (PSPDN) addresses allocated. In this state, the MS can receive only those multicast messages that can be received by any GPRS MS. Because the GPRS network infrastructure does not know the location of the MS, it is not possible to send messages to the MS from external data networks.

Routing Updates

When an MS that is in an active or a standby state moves from one routing area to another within the service area of one SGSN, it must perform a routing update. The routing area information in the SGSN is updated, and the success of the procedure is indicated in the response message.

A cell-based routing update procedure is invoked when an active MS enters a new cell. The MS sends a short message containing the identity of the MS and its new location through GPRS channels to its current SGSN. This procedure is used only when the MS is in the active state.

The inter-SGSN routing update is the most complicated routing update. The MS changes from one SGSN area to another, and it must establish a new connection to a new SGSN. This means creating a new logical link context between the MS and the new SGSN and informing the GGSN about the new location of the MS.

2.2.12 GPRS - Access Modes & Access Point Names

The GPRS access modes specify whether or not the GGSN requests user authentication at the access point to a Public Data Network (PDN). The available options are:

- **Transparent -** No security authorization/authentication is requested by the GGSN.
- **Non-transparent -** In this case, GGSN acts as a proxy for authenticating.

The GPRS transparent and non-transparent modes relate only to PDP type IPv4.

Transparent Mode

Transparent access pertains to a GPRS PLMN that is not involved in subscriber access authorization and authentication. Access to PDN-related security procedures are transparent to GSNs.

In transparent access mode, the MS is given an address belonging to the operator or any other addressing space of domain. The address is given either at subscription as a static address or at PDP context activation, as a dynamic address. The dynamic address is allocated from a Dynamic Host Configuration Protocol (DHCP) server in the GPRS network. Any user authentication is done within the GPRS network. No RADIUS authentication is performed; only IMSI-based authentication (from the subscriber identity module in the handset) is done.

Non Transparent Mode

Non-transparent access to an intranet/ISP means that the PLMN plays a role in the intranet/ISP authentication of the MS. Non-transparent access uses the Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) message issued by the mobile terminal and piggybacked in the GTP PDP context activation message. This message is used to build a RADIUS request toward the RADIUS server associated with the access point name (APN).

2.2.13 GPRS ACCESS POINT NAME

The GPRS standards define a network identity called an Access Point Name (APN). An APN identifies a PDN that is accessible from a GGSN node in a GPRS network. In GPRS, only the APN is used to select the target network. To configure an APN, the operator configures three elements on the GSN node:

- **Access point -** Defines an APN and its associated access characteristics, including security (RADIUS), dynamic address allocation (DHCP), and DNS services.
- **Access point list -** Defines a logical interface that is associated with the virtual template.
- **Access group -** Defines whether access is permitted between the PDN and the MS.

2.2.14 GPRS - Network Processes

This chapter gives a brief description of the basic processes used in GPRS networks:

- **Attach process -** Process by which the MS attaches (i.e., connects) to the SGSN in a GPRS network.
- **Authentication process -** Process by which the SGSN authenticates the mobile subscriber.
- **PDP activation process -** Process by which a user session is established between the MS and the destination network.
- **Detach process -** Process by which the MS detaches (i.e., disconnects) from the SGSN in the GPRS network.
- **Network-initiated PDP request for static IP address -** Process by which a call from the packet data network reaches the MS using a static IP address.
- **Network-initiated PDP request for dynamic IP address -** Process by which a call from the packet data network reaches the MS using a dynamic IP address.

2.2.15 GPRS Billing Techniques

As packet data is introduced into mobile systems, the question of how to bill for the services arises. Always online and paying by the minute does not sound all that appealing. Here, we describe the possibilities but it totally depends on different service providers, how they want to charge their customers.

The SGSN and GGSN register all possible aspects of a GPRS user's behavior and generate billing information accordingly. This information is gathered in so-called Charging Data Records (CDR) and is delivered to a billing gateway.

The GPRS service charging can be based on the following parameters:

- **Volume -** The amount of bytes transferred, i.e., downloaded and uploaded.
- **Duration -** The duration of a PDP context session.
- **Time -** Date, time of day, and day of the week (enabling lower tariffs at offpeak hours).
- **Final destination -** A subscriber could be charged for access to the specific network, such as through a proxy server.

- **Location -** The current location of the subscriber.
- **Quality of Service -** Pay more for higher network priority.
- **SMS -** The SGSN will produce specific CDRs for SMS.
- **Served IMSI/subscriber -** Different subscriber classes (different tariffs for frequent users, businesses, or private users).
- **Reverse charging -** The receiving subscriber is not charged for the received data; instead, the sending party is charged.
- **Free of charge -** Specified data to be free of charge.
- **Flat rate -** A fixed monthly fee.
- **Bearer service -** Charging based on different bearer services (for an operator who has several networks, such as GSM900 and GSM1800, and who wants to promote usage of one of the networks). Or, perhaps the bearer service would be good for areas where it would be cheaper for the operator to offer services from a wireless LAN rather than from the GSM network.

2.2.16 GPRS - MOBILE PHONES

GPRS has almost become a default or a mandatory feature of the latest GSM phones. In case you have plans to buy a GPRS enabled mobile phone, then; GSM mobile phone should be opted than going for CDMA technology.

GSMArena.com is a website that has become a one-stop shop for all the latest GSM Mobile Phones. The page below displays a list of latest GSM mobile phones subscribers is a courtesy of GSM Arena. As a staunch follower of this site, I suggest you to go through all the reviews posted on the site, and pick the best suitable mobile phone.

At present, numerous noted mobile device manufacturers provide state–of-the-art mobile handsets:

Alcatel	Amoi
Apple	Asus

Benefon	BenQ
BenQ-Siemens	Bird
BlackBerry	Bosch
Chea	Ericsson
Eten	Fujitsu Siemens
Gigabyte	Haier
HP	HTC
i-mate	Innostream
Kyocera	LG
Maxon	Mitac
Mitsubishi	Motorola
NEC	Neonode
Nokia	O2
Palm	Panasonic
Pantech	Philips
Qtek	Sagem

Samsung	Sendo
Sewon	Sharp
Siemens	Sony
Sony Ericsson	Tel.Me.
Telit	Thuraya
Toshiba	Vertu
VK Mobile	WND
XCute	

2.3 WIRELESS COMMUNICATION - SATELLITE

A satellite is an object that revolves around another object. For example, earth is a satellite of The Sun, and moon is a satellite of earth.

A **communication satellite** is a **microwave repeater station** in a space that is used for telecommunication, radio and television signals. A communication satellite processes the data coming from one earth station and it converts the data into another form and send it to the second earth station.

Two stations on earth want to communicate through radio broadcast but are too far away to use conventional means. The two stations can use a relay station for their communication. One earth station transmits the signal to the satellite.

Uplink frequency is the frequency at which ground station is communicating with satellite. The satellite transponder converts the signal and sends it down to the second earth station, and this is called **Downlink frequency**. The second earth station also communicates with the first one in the same way.

2.3.1 ADVANTAGES OF SATELLITE

The advantages of Satellite Communications are as follows −

- The Coverage area is very high than that of terrestrial systems.
- The transmission cost is independent of the coverage area.
- Higher bandwidths are possible.

2.3.2 DISADVANTAGES OF SATELLITE

The disadvantages of Satellite Communications are as follows −

- Launching satellites into orbits is a costly process.
- The bandwidths are gradually used up.
- High propagation delay for satellite systems than the conventional terrestrial systems.

2.3.3 SATELLITE COMMUNICATION BASICS

The process of satellite communication begins at an **earth station**. Here an installation is designed to transmit and receive signals from a satellite in orbit around the earth. Earth stations send information to satellites in the form of high powered, high frequency (GHz range) signals.

The satellites **receive** and **retransmit** the signals back to earth where they are received by other earth stations in the coverage area of the satellite. **Satellite's footprint** is the area which receives a signal of useful strength from the satellite.

The transmission system from the earth station to the satellite through a channel is called the **uplink**. The system from the satellite to the earth station through the channel is called the **downlink**.

2.3.4 SATELLITE FREQUENCY BANDS

The satellite frequency bands which are commonly used for communication are the **Cband, Ku-band,** and **Ka-band**. C-band and Ku-band are the commonly used frequency spectrums by today's satellites.

It is important to note that there is an inverse relationship between frequency and wavelength i.e. when frequency increases, wavelength decreases this helps to understand the relationship between **antenna diameter** and **transmission frequency**. Larger antennas (satellite dishes) are necessary to gather the signal with increasing wavelength.

2.3.5 EARTH ORBITS

A satellite when launched into space, needs to be placed in certain orbit to provide a particular way for its revolution, so as to maintain accessibility and serve its purpose whether scientific, military or commercial. Such orbits which are assigned to satellites, with respect to earth are called as **Earth Orbits**. The satellites in these orbits are Earth Orbit Satellites.

The important kinds of Earth Orbits are −

- Geo-synchronous Earth Orbit
- Geo-stationary Earth Orbit
- Medium Earth Orbit
- Low Earth Orbit

Geo-synchronous Earth Orbit (GEO) Satellites

A Geo-synchronous Earth orbit Satellite is one which is placed at an altitude of 22,300 miles above the Earth. This orbit is synchronized with a **side real day** (i.e., 23hours 56minutes). This orbit can **have inclination and eccentricity**. It may not be circular. This orbit can be tilted at the poles of the earth. But it appears stationary when observed from the Earth.

The same geo-synchronous orbit, if it is **circular** and in the plane of equator, it is called as geo-stationary orbit. These Satellites are placed at 35,900kms (same as geosynchronous) above the Earth's Equator and they keep on rotating with respect to earth's direction (west to east). These satellites are considered **stationary** with respect to earth and hence the name implies.

Geo-Stationary Earth Orbit Satellites are used for weather forecasting, satellite TV, satellite radio and other types of global communications.

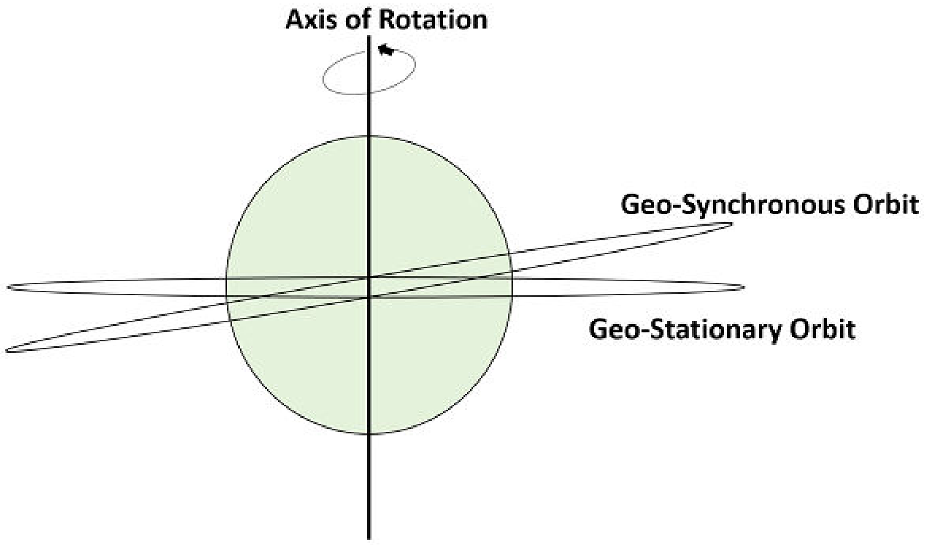


FIGURE 2.18 GEO-SYNCHRONOUS

The above figure shows the difference between Geo-synchronous and Geo- Stationary orbits. The Axis of rotation indicates the movement of Earth.

The main point to note here is that every Geo-Stationary orbit is a Geo-Synchronous orbit. But every Geo-Synchronous orbit is NOT a Geo-stationary orbit.

Medium Earth Orbit (MEO) Satellites

Medium earth orbit (MEO) satellite networks will orbit at distances of about 8000 miles from earth's surface. Signals transmitted from a MEO satellite travel a shorter distance. This translates to improved signal strength at the receiving end. This shows that smaller, more lightweight receiving terminals can be used at the receiving end.

Since the signal is travelling a shorter distance to and from the satellite, there is less transmission delay. **Transmission delay** can be defined as the time it takes for a signal to travel up to a satellite and back down to a receiving station.

For real-time communications, the shorter the transmission delay, the better will be the communication system. As an example, if a GEO satellite requires 0.25 seconds for a round trip, then MEO satellite requires less than 0.1 seconds to complete the same trip. MEOs operates in the frequency range of 2 GHz and above.

Low Earth Orbit (LEO) Satellites

The LEO satellites are mainly classified into three categories namely, little LEOs, big LEOs, and Mega-LEOs. LEOs will orbit at a distance of 500 to 1000 miles above the earth's surface.

This relatively short distance reduces transmission delay to only 0.05 seconds. This further reduces the need for sensitive and bulky receiving equipment. Little LEOs will operate in the 800 MHz (0.8 GHz) range. Big LEOs will operate in the 2 GHz or above range, and Mega-LEOs operates in the 20-30 GHz range.

The higher frequencies associated with **Mega-LEOs** translates into more information carrying capacity and yields to the capability of real-time, low delay video transmission scheme.

High Altitude Long Endurance (HALE) Platforms

Experimental HALE platforms are basically highly efficient and lightweight airplanes carrying communications equipment. This will act as **very low earth orbit geosynchronous satellites**.

These crafts will be powered by a combination of battery and solar power or high efficiency turbine engines. HALE platforms will offer **transmission delays of less than 0.001 seconds** at an altitude of only 70,000 feet, and even **better signal strength** for very lightweight hand-held receiving devices.

Orbital Slots

Here there may arise a question that with more than **200 satellites** up there in geosynchronous orbit, how do we keep them from running into each other or from attempting to use the same location in space? To answer this problem, international regulatory bodies like the International Telecommunications Union (**ITU**) and national government organizations like the Federal Communications Commission (**FCC**) designate the locations on the geosynchronous orbit where the communications satellites can be located.

These locations are specified in degrees of longitude and are called as **orbital slots**. The FCC and ITU have progressively reduced the required spacing down to only 2 degrees for C-band and Ku-band satellites due to the huge demand for orbital slots.

2.4 WIRELESS LAN AND IEEE 802.11

Wireless LANs are those Local Area Networks that use high frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage. Most WLANs are based upon the standard IEEE 802.11 or WiFi.

2.4.1 IEEE 802.11 Architecture

The components of an IEEE 802.11 architecture are as follows

Stations (STA): Stations comprise all devices and equipments that are connected to the wireless LAN. A station can be of two types:

- **Wireless Access Pointz (WAP):** WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.
- **Client. :** Clients are workstations, computers, laptops, printers, smartphones, etc.

Each station has a wireless network interface controller.

2) Basic Service Set (BSS): A basic service set is a group of stations communicating at physical layer level. BSS can be of two categories depending upon mode of operation:

- **Infrastructure BSS:** Here, the devices communicate with other devices through access points.
- **Independent BSS:** Here, the devices communicate in peer-to-peer basis in an ad hoc manner.

3) Extended Service Set (ESS): It is a set of all connected BSS.

4) Distribution System (DS): It connects access points in ESS.

Advantages of WLANs

- They provide clutter free homes, offices and other networked places.
- The LANs are scalable in nature, i.e. devices may be added or removed from the network at a greater ease than wired LANs.
- The system is portable within the network coverage and access to the network is not bounded by the length of the cables.

- Installation and setup is much easier than wired counterparts.
- The equipment and setup costs are reduced.

Disadvantages of WLANs

- Since radio waves are used for communications, the signals are noisier with more interference from nearby systems.
- Greater care is needed for encrypting information. Also, they are more prone to errors. So, they require greater bandwidth than the wired LANs.
- WLANs are slower than wired LANs.

2.4.2 Wireless LAN Protocols

Wireless LANs refer to LANs (Local Area Networks) that use high frequency radio waves instead of cables for connecting the devices. It can be conceived as a set of laptops and other wireless devices communicating by radio signals. Users connected by WLANs can move around within the area of network coverage. Most WLANs are based upon the standard IEEE 802.11 or WiFi.

2.4.3 Configuration of Wireless LANs

Each station in a Wireless LAN has a wireless network interface controller. A station can be of two categories −

- **Wireless Access Point (WAP)** − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access points. The APs are wired together using fiber or copper wires, through the distribution system.
- **Client** − Clients are workstations, computers, laptops, printers, smart phones etc. They are around tens of metres within the range of an AP.

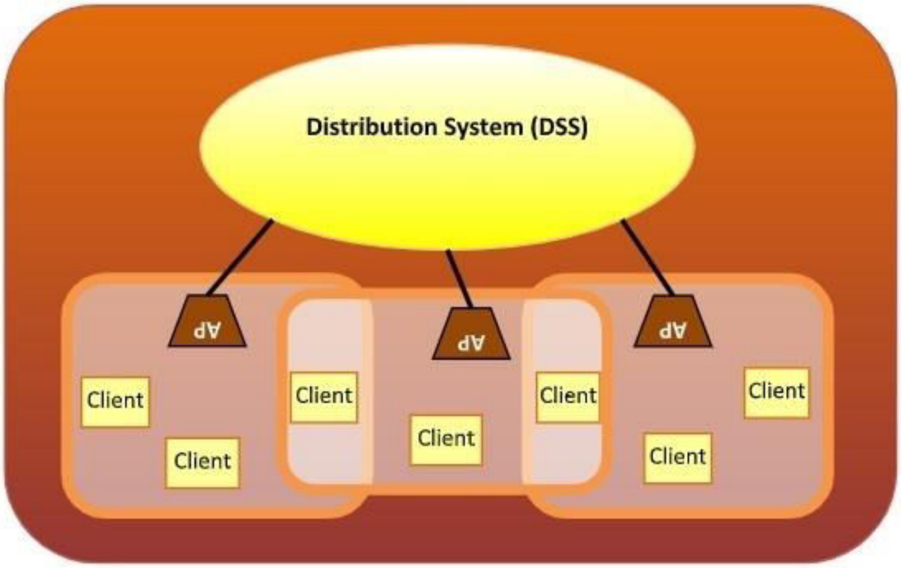


FIGURE 2.19 Types of WLAN Protocols

IEEE 802.11 or WiFi has a number of variations, the main among which are −

- **802.11a Protocol**− This protocol supports very high transmission speeds of 54Mbps. It has a high frequency of 5GHz range, due to which signals have difficulty in penetrating walls and other obstructions. It employs Orthogonal Frequency Division Multiplexing (OFDM).
- **802.11b Protocol** − This protocol operates within the frequency range of 2.4GHz and supports 11Mbps speed. It facilitates path sharing and is less vulnerable to obstructions. It uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with Ethernet protocol.
- **802.11g Protocol** − This protocol combines the features of 802.11a and 802.11b protocols. It supports both the frequency ranges 5GHz (as in 802.11a standard) and 2.4GHz (as in 802.11b standard). Owing to its dual features, 802.11g is backward compatible with 802.11b devices. 802.11g provides high speeds, varying signal range, and resilience to obstruction. However, it is more expensive for implementation.
- **802.11n Protocol** − Popularly known as Wireless N, this is an upgraded version of 802.11g. It provides very high bandwidth up to 600Mbps and provides signal coverage. It

uses Multiple Input/Multiple Output (MIMO), having multiple antennas at both the transmitter end and receiver ends. In case of signal obstructions, alternative routes are used. However, the implementation is highly expensive.

2.5 MEDIUM ACCESS CONTROL

Medium Access Control (MAC) address is a hardware address use to uniquely identify each node of a network. It provides addressing and channel access control mechanisms to enable the several terminals or network nodes to communicate in a specified network. Medium Access Control of data communication protocol is also named as Media Access Control. In IEEE 802 OSI Reference model of computer networking, the Data Link Control (DLC) layer is subdivided into two sub-layers:

- The Logical Link Control (LLC) layer and
- The Medium Access Control (MAC) layer

The MAC sublayer acts as a direct interface between the logical link control (LLC) Ethernet sublayer and the physical layer of reference model. Consequently, each different type of network medium requires a different MAC layer. On networks that don't conform they are part of IEEE 802 standards but they do conform that they participate OSI Reference Model then the node address is named the Data Link Control (DLC) address. The MAC sublayer emulates a full-duplex logical communication channel in a multipoint network system. These communication channels may provide unicast, multicast and/or broadcast communication services.

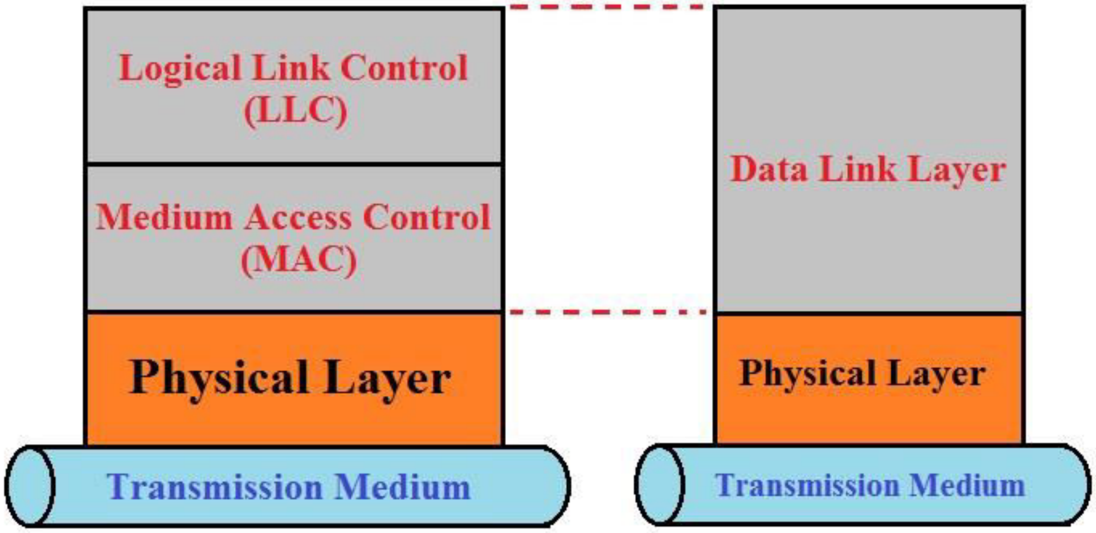


FIGURE 2.20 MEDIUM ACCESS CONTROL

LLC and MAC Sublayer

MAC address is suitable when multiple devices are connected with same physical link then to prevent from collisions system uniquely identify the devices one another at the data link layer, by using the MAC addresses that are assigned to all ports on a switch. The MAC sublayer uses MAC protocols to prevent collisions and MAC protocols uses MAC algorithm that accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC address.

Functions performed in the MAC sublayer:

The primary functions performed by the MAC layer as per the IEEE Std 802-2001

Frame delimiting and recognition: This function is responsible to creates and recognizes frame boundaries.

- **Addressing:** MAC sublayer performs the addressing of destination stations (both as individual stations and as groups of stations) and conveyance of source-station addressing information as well.

- **Transparent data transfer:** It performs the data transparency over data transfer of LLC, PDUs, or of equivalent information in the Ethernet sublayer.
- **Protection:** MAC sublayer function is to protect the data against errors, generally by means of generating and checking frame check sequences.
- **Access control:** Control of access to the physical transmission medium form unauthorized medium access.

One of the most commonly used of MAC sublayer for wired networks i.e. Carrier Sense Multiple Access with Collision Detection (CSMA/CD). Through MAC schema, a sender senses the medium (a wire or coaxial cable) before transmission of data to check whether the medium is free or not. If MAC senses that the medium is busy, the sender waits until it is free. When medium becomes free, the sender starts transmitting of data and continues to listen into the medium. If any kind of collision detected by sender while sending data, it stops at once and sends a jamming signal. But this scheme doest work well with wireless networks. Some of the problems that occur when it uses to transfer data through wireless networks are as follow;

- Signal strength decreases proportional to the square of the distance
- The sender would apply Carrier Sense (CS) and Collision Detection (CD), but the collisions happen at the receiver
- It might be a case that a sender cannot "hear" the collision, i.e., CD does not work
- Furthermore, CS might not work, if for e.g., the terminals are "hidden".

2.6 PHYSICAL LAYER

The physical layer is aimed at consolidating the hardware requirements of a network to enable the successful transmission of data. Network engineers can define different bit transmission mechanisms for the physical layer level, including the shapes and types of connectors, cables and frequencies for each physical medium.

The physical layer sometimes plays an important role in the effective sharing of available communication resources, and helps avoid contention among multiple users. It also handles the transmission rate to improve the flow of data between a sender and receiver.

The physical layer provides the following services:

- Modulates the process of converting a signal from one form to another so that it can be physically transmitted over a communication channel
- Bit-by-bit delivery
- Line coding, which allows data to be sent by hardware devices that are optimized for digital communications that may have discreet timing on the transmission link
- Bit synchronization for synchronous serial communications
- Start-stop signaling and flow control in asynchronous serial communication
- Circuit switching and multiplexing hardware control of multiplexed digital signals
- Carrier sensing and collision detection, whereby the physical layer detects carrier availability and avoids the congestion problems caused by undeliverable packets
- Signal equalization to ensure reliable connections and facilitate multiplexing
- Forward error correction/channel coding such as error correction code
- Bit interleaving to improve error correction
- Auto-negotiation
- Transmission mode control

Examples of protocols that use physical layers include:

- Digital Subscriber Line
- Integrated Services Digital Network
- Infrared Data Association
- Universal Serial Bus
- Bluetooth
- Controller Area Network
- Ethernet

2.7 HIPERLAN

High Performance LAN (Hiperlan)

HIPERLAN is a European (ETSI) standardization initiative for a HIghPER formance wireless Local Area Network. Radio waves are used instead of a cable as a transmission medium to connect stations. Either, the radio transceiver is mounted to the movable station as an add-on and no base station has to be installed separately, or a base station is needed in addition per room.

The stations may be moved during operation-pauses or even become mobile. The max.data rate for the user depends on the distance of the communicating stations. With short distances (<50 m) and asynchronous transmission a data rate of 20 Mbit/s is achieved, with up to 800 m distance a data rate of 1 Mbit/s are provided. For connection-oriented services, e.g. video-telephony, at least 64 kbit/s are offered.

HIPERLAN is a European family of standards on digital high speed wireless communication in the 5.15-5.3 GHz and the 17.1-17.3 GHz spectrum developed by ETSI. The committee responsible for HIPERLAN is RES-10 which has been working on the standard since November 1991.

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.

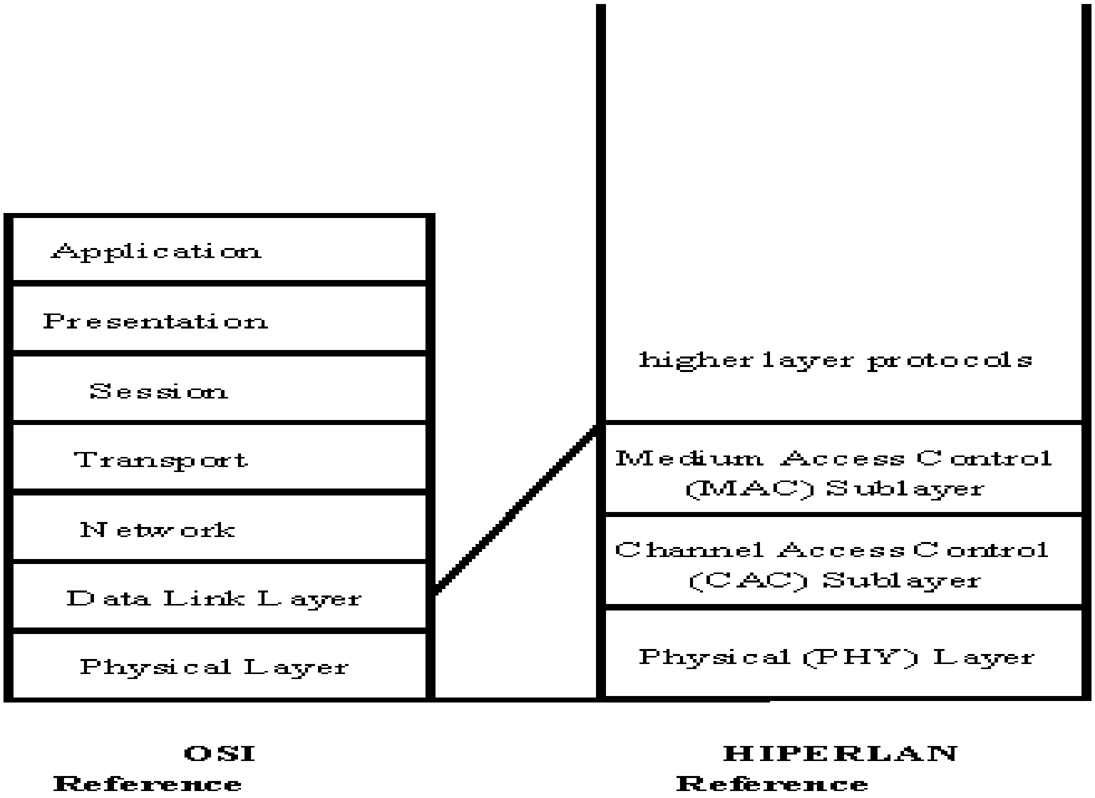


FIGURE 2.21 HIPERLAN

The choice of frequencies allocated to HIPERLAN was part of the 5-5.30 GHz band being allocated globally to aviation purposes. The Aviation industry only used the 5-5.15GHz frequency, thus making the 5.15-5.30 frequency band accessible to HIPERLAN standards.

HIPERLAN is designed to work without any infrastructure. Two stations may exchange data directly, without any interaction from a wired (or radio-based) infrastructure. The simplest HIPERLAN thus consists of two stations. Further, if two HIPERLAN stations are not in radio contact with each other, they may use a third station (i.e. the third station must relay messages between the two communicating stations).

Products compliant to the HIPERLAN 5 GHz standard shall be possible to implement on a PCMCIA Type III card. Thus the standard will enable users to truly take computing power on the road.

The HIPERLAN standard has been developed at the same time as the development of the SUPER net standard in the United States.

2.7.1 HIPERLAN requirements

- Short range - 50m
- Low mobility - 1.4m/s
- Networks with and without infrastructure
- Support isochronous traffic
- audio 32kbps, 10ns latency
- video 2Mbps, 100ns latency
- Support asynchronous traffic
- data 10Mbps, immediate access

Quality of service

Performance is one of the most important factors when dealing with wireless LANs. In contrast to other radio-based systems, data traffic on a local area network has a randomized bursty nature, which may cause serious problems with respect to throughput.

Many factors have to be taken into consideration, when quality of service is to be measured. Among these are:

- The topography of the landscape in general
- Elevations in the landscape that might cause shadows, where connectivity is unstable or impossible.
- Environments with many signal-reflection surfaces
- Environments with many signal-absorbing surfaces
- Quality of the wireless equipment
- Placement of the wireless equipment
- Number of stations
- Proximity to installations that generate electronic noise
- and many more

The sheer number of factors to take into consideration means, that the physical environment will always be a factor in trying to asses the usefulness of using a wireless technology like HIPERLAN.

Simulations show that the HIPERLAN MAC can simultaneously support

- 25 audio links at 32kbit/s, 10ms delivery
- 25 audio links at 16kbit/s, 20ms delivery
- 1 video link at 2Mbit/s, 100ms delivery
- Asynch file transfer at 13.4Mbit/s

2.7.2 Benchmarking HIPERLAN in practice

Once a new HIPERLAN installation is implemented, trying to benchmark it can easily become a mind-boggling task.

Even though a spectrum analyzer can be used for initial evaluation and troubleshooting, the factors influencing performance are so many and so complex, that initial benchmarking should be based evenly on perceived performance and registered performance over a longer period of time.

In contrast to cable based LANs, the testing equipment has to find the communication stream in the air not on a physical cable and it has to monitor several frequencies at once. On top of that, the testing equipment itself can interfere with the signals it intends to monitor.

2.7.3 New HIPERLAN standards ahead

A second set of standards have been constructed for a new version of HIPERLAN - HIPERLAN2. The idea of HIPERLAN2 is to be compatible with ATM.

There is also undergoing work to establish global sharing rules. The WINForum for NII/SUPERNET in the US aim to support HIPERLAN 1 and HIPERLAN 2. This effort involves interaction between ETSI RES10, WINForum, ATM Forum.

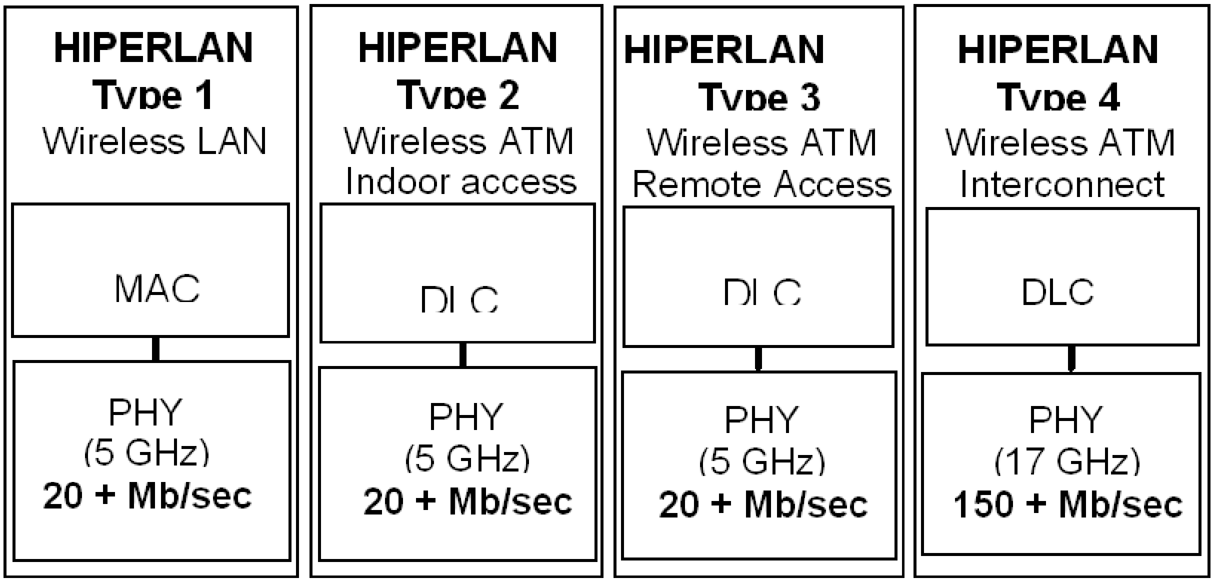


FIGURE 2.22 THE FUTURE OF HIPERLAN

2.8 WIRELESS COMMUNICATION - BLUETOOTH

Bluetooth wireless technology is a short range communications technology intended to replace the cables connecting portable unit and maintaining high levels of security. Bluetooth technology is based on **Ad-hoc technology** also known as **Ad-hoc Pico nets**, which is a local area network with a very limited coverage.

2.8.1 History of Bluetooth

WLAN technology enables device connectivity to infrastructure based services through a wireless carrier provider. The need for personal devices to communicate wirelessly with one another without an established infrastructure has led to the emergence of **Personal Area Networks (PANs)**.

- Ericsson's Bluetooth project in 1994 defines the standard for PANs to enable communication between mobile phones using low power and low cost radio interfaces.

- 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 a defacto standard for PANs.
- IEEE has approved a Bluetooth based standard named IEEE 802.15.1 for Wireless Personal Area Networks (WPANs). IEEE standard covers MAC and Physical layer applications.

Bluetooth specification details the entire protocol stack. Bluetooth employs Radio Frequency (RF) for communication. It makes use of **frequency modulation** to generate radio waves in the **ISM** band.

Symbol of Bluetooth

An example of a Bluetooth device

FIGURE 2.23 BLUETOOTH

The usage of Bluetooth has widely increased for its special features.

- Bluetooth offers a uniform structure for a wide range of devices to connect and communicate with each other.
- Bluetooth technology has achieved global acceptance such that any Bluetooth enabled device, almost everywhere in the world, can be connected with Bluetooth enabled devices.
- Low power consumption of Bluetooth technology and an offered range of up to ten meters has paved the way for several usage models.
- Bluetooth offers interactive conference by establishing an adhoc network of laptops.

- Bluetooth usage model includes cordless computer, intercom, cordless phone and mobile phones.

2.8.2 PICONETS AND SCATTERNETS

Bluetooth enabled electronic devices connect and communicate wirelessly through short range devices known as **Piconets**. Bluetooth devices exist in small ad-hoc configurations with the ability to act either as master or slave the specification allows a mechanism for **master** and **slave** to switch their roles. Point to point configuration with one master and one slave is the simplest configuration.

When more than two Bluetooth devices communicate with one another, this is called a **PICONET**. A Piconet can contain up to seven slaves clustered around a single master. The device that initializes establishment of the Piconet becomes the **master**.

The master is responsible for transmission control by dividing the network into a series of time slots amongst the network members, as a part of **time division multiplexing** scheme which is shown below.

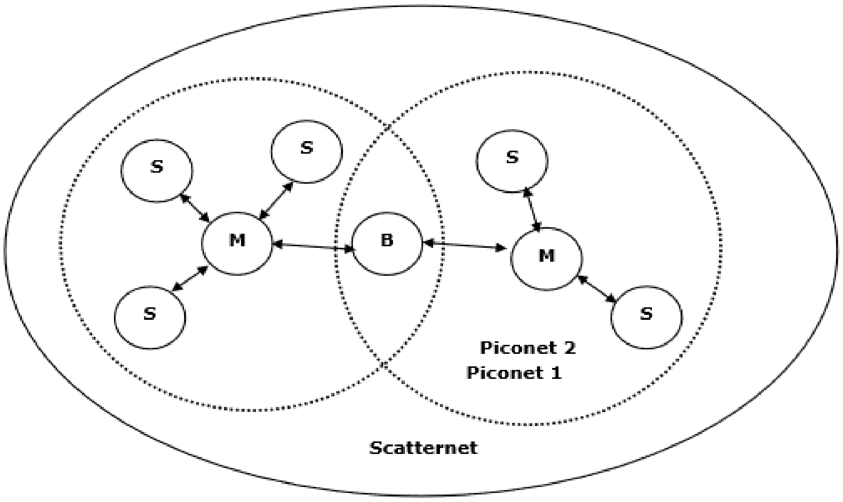


Figure: Piconets and Scatternets

FIGURE 2.24 PICONETS AND SCATTERNETS

The features of Piconets are as follows −

- Within a Piconet, the timing of various devices and the frequency hopping sequence of individual devices is determined by the clock and unique **48-bit address** of master.
- Each device can communicate simultaneously with up to seven other devices within a single Piconet.
- Each device can communicate with several piconets simultaneously.
- Piconets are established dynamically and automatically as Bluetooth enabled devices enter and leave piconets.
- There is no direct connection between the slaves and all the connections are essentially master-to-slave or slave-to-master.
- Slaves are allowed to transmit once these have been polled by the master.
- Transmission starts in the slave-to-master time slot immediately following a polling packet from the master.
- A device can be a member of two or more piconets, jumping from one piconet to another by adjusting the transmission regime-timing and frequency hopping sequence dictated by the master device of the second piconet.
- It can be a slave in one piconet and master in another. It however cannot be a master in more than once piconet.
- Devices resident in adjacent piconets provide a bridge to support inner-piconet connections, allowing assemblies of linked piconets to form a physically extensible communication infrastructure known as **Scatternet**.

Spectrum

Bluetooth technology operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHZ, using a spread spectrum hopping, full-duplex signal at a nominal rate of 1600 hops/sec. the 2.4 GHZ ISM band is available and unlicensed in most countries.

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 1.2 and 3Mbps data rate for Version 2.0 combined with Error Data Rate.

UNIT – III

MOBILE NETWORK LAYER & TRANSPORT LAYER

3. MOBILE IP

3.1 DEFINITION

Mobile IP is a communication protocol (created by extending Internet Protocol, IP) that allows the users to move from one network to another with the same IP address. It ensures that the communication will continue without user's sessions or connections being dropped.

TERMINOLOGIES

- **Mobile Node (MN):**

  It is the hand-held communication device that the user caries e.g. Cell phone.

- **Home Network:**

  It is a network to which the mobile node originally belongs to as per its assigned IP address (home address).

- **Home Agent (HA):**

  It is a router in home network to which the mobile node was originally connected

- **Home Address:**

  It is the permanent IP address assigned to the mobile node (within its home network).

- **Foreign Network:**

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

- **Foreign Agent (FA):**

  It is a router in foreign network to which mobile node is currently connected. The packets from the home agent are sent to the foreign agent which delivers it to the mobile node.

- **Correspondent Node (CN):**

  It is a device on the internet communicating to the mobile node.

- **Care of Address (COA):**

It is the temporary address used by a mobile node while it is moving away from its his is an **IETF (Internet Engineering Task Force)** standard communications protocol designed to allow mobile devices' (such as laptop, PDA, mobile phone, etc.) users to move from one network to another while maintaining their permanent IP (Internet Protocol) address.

Defined in RFC (Request for Comments) 2002, mobile IP is an enhancement of the internet protocol (IP) that adds mechanisms for forwarding internet traffic to mobile devices (known as mobile nodes) when they are connecting through other than their home network.

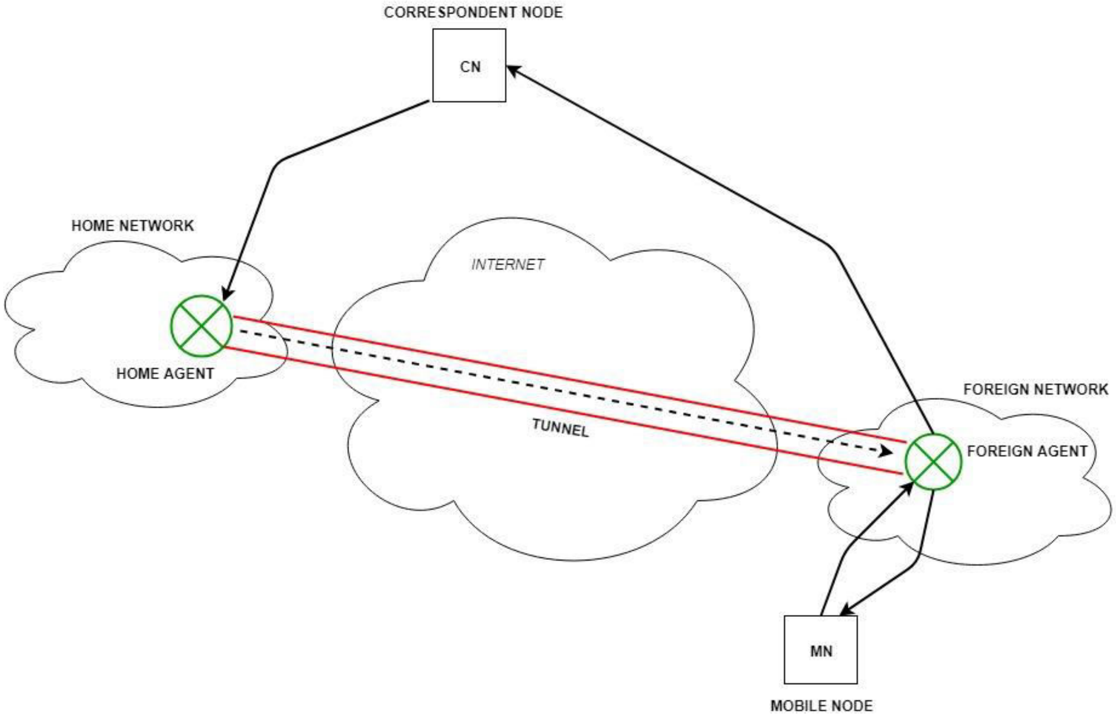


FIGURE 3.1 MOBILE IP FRAMEWORKS

The following case shows how a datagram moves from one point to another within the Mobile IP framework

- First of all, the internet host sends a datagram to the mobile node using the mobile node's home address (normal IP routing process).
- If the mobile node (MN) is on its home network, the datagram is delivered through the normal IP (Internet Protocol) process to the mobile node. Otherwise the home agent picks up the datagram.
- If the mobile node (MN) is on foreign network, the home agent (HA) forwards the datagram to the foreign agent.

- The foreign agent (FA) delivers the datagram to the mobile node.
- Datagrams from the MN to the Internet host are sent using normal IP routing procedures. If the mobile node is on a foreign network, the packets are delivered to the foreign agent. The FA forwards the datagram to the Internet host.

In the case of wireless communications, the above illustrations depict the use of wireless transceivers to transmit the datagrams to the mobile node. Also, all datagrams between the Internet host and the MN use the mobile node's home address regardless of whether the mobile node is on a home or foreign network. The care-of address (COA) is used only for communication with mobility agents and is never seen by the Internet host.

3.1.1 COMPONENTS OF MOBILE IP

The mobile IP has following three components as follows:

1. Mobile Node (MN)

The mobile node is an end system or device such as a cell phone, PDA (Personal Digital assistant), or laptop whose software enables network roaming capabilities.

2. Home Agent (HA)

The home agent provides several services for the mobile node and is located in the home network. The tunnel for packets towards the mobile node starts at home agent. The home agent maintains a location registry, i.e. it is informed of the mobile node's location by the current COA (care of address). Following alternatives for the implementation of an HA exist.

- Home agent can be implemented on a **router** that is responsible for the home network. This is obviously the best position, because without optimization to mobile IP, all packets for the MN have to go through the router anyway.
- If changing the router's software is not possible, the home agent could also be implemented on an **arbitrary node** in the subset. One biggest disadvantage of this solution is the double crossing of the router by the packet if the MN is in a foreign network. A packet for the mobile node comes in via the router; the HA sends it through the tunnel which again crosses the router.

3. Foreign Agent (FA)

The foreign agent can provide several services to the mobile node during its visit to the foreign network. The FA can have the COA (care or address) acting as a tunnel endpoint and forwarding packets to the MN. The foreign agent can be the default router for the MN.

Foreign agent can also provide security services because they belong to the foreign network as opposed to the MN which is only visiting.

In short, FA is a router that may function as the point of attachment for the mobile node when it roams to a foreign network delivers packets from the home agent to the mobile node.

4. Care of Address (COA)

The Care- of- address defines the current location of the mobile node from an IP point of view. All IP packets sent to the MN are delivered to the COA, not directly to the IP address of the MN. Packet delivery toward the mobile node is done using a tunnel. To be more precise, the COA marks the endpoint of the tunnel, i.e. the address where packets exit the tunnel.

There are two different possibilities for the location of the care of address:

1. **Foreign Agent COA:** The COA could be located at the foreign agent, i.e. the COA is an IP address of the foreign agent. The foreign agent is the tunnel endpoint and forwards packets to the MN. Many MN using the FA can share this COA as common COA.
2. **Co-located COA:** The COA is co-located if the MN temporarily acquired an additional IP address which acts as a COA. This address is now topologically correct, and the tunnel endpoint is at the mobile node. Co-located address can be acquired using services such as DHCP. One problem associated with this approach is need for additional addresses if MNs request a COA. This is not always a good idea considering the scarcity of IPv4 addresses.

5. Correspondent Node (CN)

At least one partner is needed for communication. The correspondent node represents this partner for the MN. The correspondent node can be a fixed or mobile node.

6. Home Network

The home network is the subset the MN belongs to with respect to its IP address. No mobile IP support is needed within this network.

7. Foreign network

The foreign network is the current subset the MN visits and which is not the home network.

3.1.2 PROCESS OF MOBILE IP

The mobile IP process has following three main phases, which are:

1. Agent Discovery

During the agent discovery phase the HA and FA advertise their services on the network by using the ICMP router discovery protocol (IROP).

Mobile IP defines two methods: agent advertisement and agent solicitation which are in fact router discovery methods plus extensions.

- **Agent advertisement:** For the first method, FA and HA advertise their presence periodically using special agent advertisement messages. These messages advertisement can be seen as a beacon broadcast into the subnet. For this advertisement internet control message protocol (ICMP) messages according to RFC 1256, are used with some mobility extensions.
- **Agent solicitation:** If no agent advertisements are present or the inter arrival time is too high, and an MN has not received a COA, the mobile node must send agent solicitations. These solicitations are again bases on RFC 1256 for router solicitations.

2. Registration

The main purpose of the registration is to inform the home agent of the current location for correct forwarding of packets.

Registration can be done in two ways depending on the location of the COA. **If the COA is at the FA**, the MN sends its registration request containing the COA to the FA which is forwarding the request to the HA. The HA now set up a **mobility binding** containing the mobile node's home IP address and the current COA.

Additionally, the mobility biding contains the lifetime of the registration which is negotiated during the registration process. Registration expires automatically after the lifetime and is deleted; so a mobile node should register before expiration. After setting up the mobility binding, the HA send a reply message back to the FA which forwards it to the MN.

If the COA is co-located, registration can be very simpler. The mobile node may send the request directly to the HA and vice versa. This by the way is also the registration procedure for MNs returning to their home network.

3. Tunneling

A tunnel is used to establish a virtual pipe for data packets between a tunnel entry and a tunnel endpoint. Packets which are entering in a tunnel are forwarded inside the tunnel and leave the tunnel unchanged. Tunneling, i.e., sending a packet through a tunnel is achieved with the help of encapsulation.

Tunneling is also known as "**port forwarding**" is the transmission and data intended for use only within a private, usually corporate network through a public network.

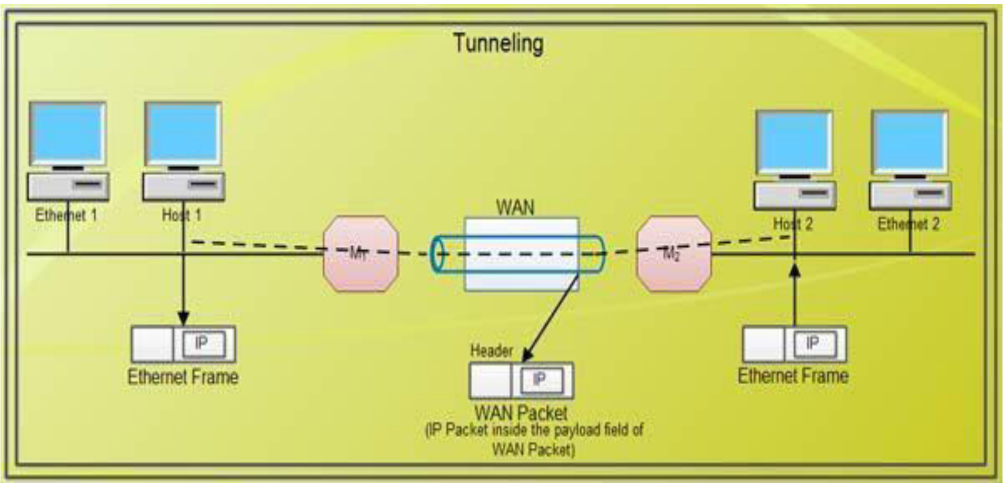


FIGURE 3.2 TUNNELING

- Point-to-Point Tunneling Protocol (PPTP): PPTP keeps proprietary data secure even when it is being communicated over public networks. Authorized users can access a private network called a virtual private network, which is provided by an Internet service provider. This is a private network in the "virtual" sense because it is actually being created in a tunneled environment.
- Layer Two Tunneling Protocol (L2TP): This type of tunneling protocol involves a combination of using PPTP and Layer 2 Forwarding.

- Tunneling is a way for communication to be conducted over a private network but tunneled through a public network. This is particularly useful in a corporate setting and also offers security features such as encryption options

3.2 DYNAMIC HOST CONFIGURATION PROTOCOL

Dynamic Host Configuration Protocol (DHCP) is a network protocol for automatically assigning TCP/IP information to client machines. Each DHCP client connects to the centrally-located DHCP server which returns that client's network configuration, including the IP address, gateway, and DNS servers.

Stands for "Dynamic Host Configuration Protocol." DHCP is a protocol that automatically assigns a unique IP address to each device that connects to a network. With DHCP, there is no need to manually assign IP addresses to new devices. Therefore, no user configuration is necessary to connect to a DCHP-based network. Because of its ease of use and widespread support, DHCP is the default protocol used by most routers and networking equipment.

When you connect to a network, your device is considered a client and the router is the server. In order to successfully connect to a network via DHCP, the following steps must take place.

- When a client detects it has connected to a DHCP server, it sends a DHCPDISCOVER request.
- The router either receives the request or redirects it to the appropriate DHCP server.
- If the server accepts the new device, it will send a DHCPOFFER message back to the client, which contains the client device's MAC address and the IP address being offered.
- The client returns a DHCPREQUEST message to the server, confirming it will use the IP address.
- Finally, the server responds with a DHCPACK acknowledgement message that confirms the client has been given access (or a "lease") for a certain amount of time.

DHCP works in the background when you connect to a network, so you will rarely see any of the above steps happen. The time it takes to connect via DHCP depends on the type of router and the size of the network, but it usually takes around three to ten seconds. DHCP works the same way for both wired and wireless connections, which means desktop computers, tablets, and smartphones can all connect to a DHCP-based network at the same time.

DHCP is useful for automatic configuration of client network interfaces. When configuring the client system, the administrator can choose DHCP and instead of entering an IP address, netmask, gateway, or DNS servers. The client retrieves this information from the DHCP server. DHCP is also useful if an administrator wants to change the IP addresses of a large number of systems. Instead of reconfiguring all the systems, he can just edit one DHCP configuration file on the server for the new set of IP addresses.

If the DNS servers for an organization changes, the changes are made on the DHCP server, not on the DHCP clients. Once the network is restarted on the clients (or the clients are rebooted), the changes take effect. Furthermore, if a laptop or any type of mobile computer is configured for DHCP, it can be moved from office to office without being reconfigured as long as each office has a DHCP server that allows it to connect to the network.

3.2.1 Configuration File

The first step in configuring a DHCP server is to create the configuration file that stores the network information for the clients. Global options can be declared for all clients, while other options can be declared for individual client systems. The configuration file can contain extra tabs or blank lines for easier formatting. Keywords are caseinsensitive and lines beginning with a hash mark (#) are considered comments.

Two DNS update schemes are currently implemented the ad-hoc DNS update mode and the interim DHCP-DNS interaction draft update mode. If and when these two are accepted as part of the Internet Engineering Task Force (IETF) standards process, there will be a third mode the standard DNS update method. The DHCP server must be configured to use one of the two current schemes.

There are two types of statements in the configuration file:

Parameters — State how to perform a task, whether to perform a task, or what network configuration options to send to the client.

Declarations — Describe the topology of the network, describe the clients, provide addresses for the clients, or apply a group of parameters to a group of declarations. Some parameters must start with the option keyword and are referred to as options. Options configure DHCP options; whereas, parameters configure values that are not optional or control how the DHCP server behaves.

In Example the **routers, subnet-mask, domain-name, domain-name-servers, and time-offset** optionsare usedfor any **host** statements declared below it. Additionally, a **subnet** can be declared, a **subnet** declaration must be included for every subnet in the network. If it is not, the DHCP server fails to start.

In this example, there are global options for every DHCP client in the subnet and a range declared.

Clients are assigned an IP address within the range.

```
subnet 192.168.1.0 netmask 255.255.255.0 {
option routers 192.168.1.254;
option subnet-mask 255.255.255.0;
option domain-name "example.com";
option domain-name-servers 192.168.1.1;
option time-offset -18000; # Eastern Standard Time
range 192.168.1.10 192.168.1.100;
```

3.3 ROUTING

Routing is the process of finding the best path for traffic in a network, or across multiple networks. The role of routing is similar to the road map for a hotel. In both cases, we need to deliver messages at proper location and in an appropriate way.

Routing is the process of selecting a path for traffic in a network or between or across multiple networks. Broadly, routing is performed in many types of networks, including circuit-switched networks, such as the public switched telephone network (PSTN), and computer networks, such as the Internet.

In packet switching networks, routing is the higher-level decision making that directs network packets from their source toward their destination through intermediate network nodes by specific packet forwarding mechanisms. Packet forwarding is the transit of network packets from one network interface to another. Intermediate nodes are typically network hardware devices such as routers, gateways, firewalls, or switches. General-purpose computers also forward packets and perform routing, although they have no specially optimized hardware for the task.

The routing process usually directs forwarding on the basis of routing tables, which maintain a record of the routes to various network destinations. Routing tables may be specified by an administrator, learned by observing network traffic or built with the assistance of routing protocols.

Routing, in a narrower sense of the term, often refers to IP routing and is contrasted with bridging. IP routing assumes that network addresses are structured and that similar addresses imply proximity within the network. Structured addresses allow a single routing table entry to represent the route to a group of devices. In large networks, structured addressing (routing, in the narrow sense) outperforms unstructured addressing (bridging). Routing has become the dominant form of addressing on the Internet. Bridging is still widely used within local area networks.

Routing in a mobile ad-hoc network depends on many factors such as:

- Modeling of the topology,
- Selection of routers,
- Initiation of a route request,
- And specific underlying characteristics that could serve as heuristics in finding the path effectively.

In a MANET, each node or device is expected to serve as a router, and each router is indistinguishable from another in the sense that all routers execute the same routing algorithm to compute paths through the entire network.

3.3.1 Need for Routing

There are following needs for routing:

- Since centralized routing in a dynamic and even for small networks is impossible therefore routing computation must be distributed. Route computation should not add many more nodes. If any host demands for the route, they must have quick access. Maintenance of a global state should not involve in the route computation.

- Each node should care about their destination node to its route and should not be involved in frequent topology updates for those portions of the network that have no traffic.
- Since broadcast can be time consuming for MANETs, it must be avoided as much as possible.
- In routing there must have a backup route when the primary route has become stale.

3.3.2 Routing Classification

Routing protocol can be classified as:

1. Proactive Protocol
2. Reactive Protocol
3. Hybrid Protocol

1. Proactive Protocol

Proactive protocols attempt to evaluate continuously the routes within the network. It means proactive protocol continuously maintain the routing information, so that when a packet needs to be forwarded, the path is known already and can be immediately used. The family of distance vector protocols is an example of proactive scheme.

The advantage of the proactive schemes is that whenever a route is needed, there is negligible delay in determining the route.

Unfortunately, it is a big overhead to maintain routing tables in the MANET environment.

Therefore, this type of protocol has following common disadvantages:

- Requires more amounts of data for maintaining routing information.
- Low reaction on re-structuring network and failures of individual nodes.

2. Reactive Protocols

Reactive protocols do not maintain routes but invoke a route determination procedure only on demand or we can say reactive protocols build the routes only on demand. Thus, when a route is required, some sort of global search procedure is initiated. The family of classical flooding algorithms belongs to the reactive protocol group. Examples of reactive ad-hoc network routing protocols include ad hoc on demand distance vector (AODV) and temporally ordered routing algorithm (TORA).

These protocols have the following advantages:

- No large overhead for global routing table maintenance as in proactive protocols.
- Reaction is quick for network restructure and node failure.
- Even though reactive protocols have become the main stream for MANET routing, they still have the following disadvantages:
- Latency time is high in route finding o Excessive flooding can lead to network clogging.

3. Hybrid Protocols

Hybrid protocols attempt to take advantage of best of reactive and proactive schemes. The basic idea behind such protocols is to initiate route discovery on demand but at a limited search cost. One of the popular hybrid protocols is zone routing protocol (ZRP).

3.3.3 CATEGORIZED OF ROUTING PROTOCOLS

Routing protocols may also be categorized as follows:

1. Table-driven protocols
2. Source initiated on -demand protocols

1. Table-driven routing protocol

- These protocols are called table-driven because each node is required to maintain one or more tables containing routing information on every other node in the network.
- They are **proactive** in nature so that the routing information is always consistent and up to date.
- The protocols respond to changes in network topology by propagating the updates throughput the network so that every node has a consistent view of the network.

The table driven routing protocols are categorized as follows:

3.4 DESTINATION - SEQUENCED DISTANCE VECTOR ROUTING

- Destination sequenced distance vector routing (DSDV) is a table driven routing protocol for MANET based on Bellman-Ford algorithm.
- DSDV was developed by C. Perkins and P. Bhagwat in 1994. The main contribution of the algorithm was that the algorithm works correctly, even in the presence of the loops in the routing table.
- As we know, each mobile node maintains a routing table with a route to every possible destination in the network and the number of hops to the destination.
- Each entry in the table contains a sequence number assigned by the destination node.
- The sequence numbers allow the node to distinguish stale routes from new ones, and help avoid formation of routing loops.
- **A new route broadcast contains:**
- The destination address.
- The number of hops required to reach the destination.
- since number of the information received about the destination and a new sequence number unique to the broadcast.
- If there multiple routes are available for the same destination, the route with the most recent sequence number is used. If two updates have the same sequence number, the route with smaller metric is used to optimize the routing.

\

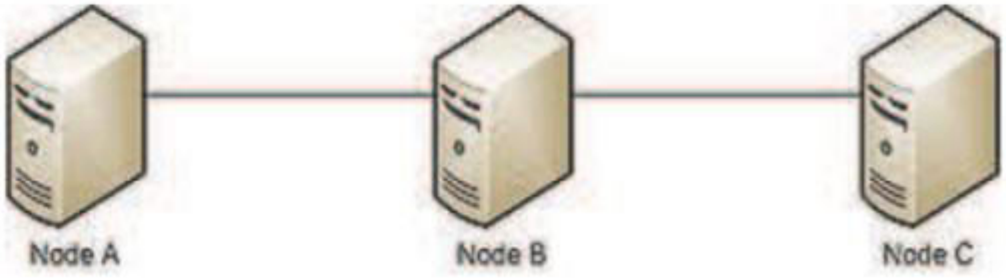


FIGURE 3.3 SEQUENCED DISTANCE VECTOR ROUTING

For example the routing table of Node A from the above network is:

Destination	Next Hop	No. of Hops	Sequence no.	Install time
A	A	0	A46	001000
B	B	1	B36	001200
C	B	2	C28	001500

Basically the table stores description of all possible paths reachable by node A, along with the hop, number of hops, sequence number and install time.

Advantages

- Destination sequenced distance vector routing was one of the early algorithms available.
- It is suitable for creating ad-hoc networks with small no. of nodes.

Disadvantage

- Destination sequenced distance vector routing requires a regular update of its routing tables, which uses more battery power and a small amount of bandwidth even when the network is idle.
- This algorithm is not suitable for highly dynamic networks.

Cluster Head gateway switch Routing

- The cluster head (CH) gateway switch routing (CGSR) protocol is different from the destination sequenced distance vector routing in the type of addressing and the network organization scheme employed.
- Instead of a flat network, CGSR uses cluster heads, which control a group of ad hoc nodes and hence achieve a hierarchical framework for code separation among clusters, routing, channel access, and bandwidth allocation.

- Identification of appropriate clusters and selection of cluster heads is quite complex. Once clusters have been defined, it is desirable to use a distributed algorithm within the cluster to elect a node as the cluster head.
- The disadvantage of using a cluster head scheme is that frequent changes adversely affect performance as nodes spend more time selecting a cluster head rather than relaying packets. Hence, the least cluster change (LCC) clustering algorithm is used rather than CH selection every time the cluster membership changes. Using LCC, CHs change only when two CHs come into contact, or when a node moves out of contact with all other CHs.
- In this scheme, each node must maintain a cluster member table (CMT), which stores the destination CH for each node in the network. The cluster member tables are broadcast periodically by the nodes using the DSDV algorithm.
- When a node receives such a table from a neighbor, it can update its own information. As expected, each node also maintains a routing table to determine the next hop required to reach any destination.

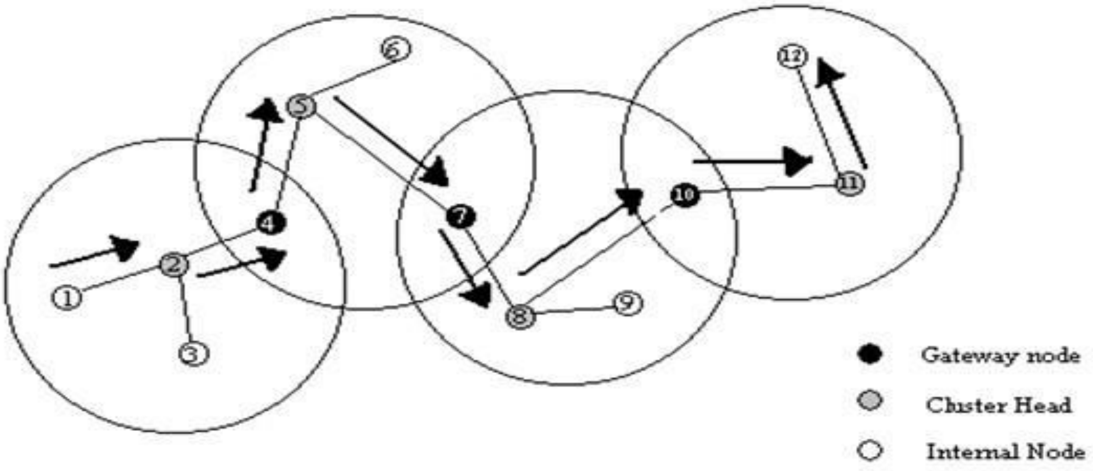


FIGURE 3.4 CLUSTER HEAD GATEWAY SWITCH ROUTING

3.4.1 WIRELESS ROUTING PROTOCOL (WRP)

The wireless routing protocol is a proactive unicast routing protocol for MANETs. It uses an enhanced version of the distance vector routing protocol, which uses the Bellman - Ford algorithm to calculate paths.

For the wireless routing protocol (WRP) each node maintains 4 tables:

- Distance table
- Routing table
- Link cost table
- Message retransmission list (MRL) table

Each entry in the message retransmission list has a sequence number of the update message, a retransmission counter, an acknowledgment required flag vector with one entry per neighbor, and a list of updates sent in the update message.

When any node receives a hello message from a new node, it adds the new node to its routing table and sends the new node a copy of its routing table. A node must send a message to its neighbors within a certain time to ensure connectivity.

The Wireless Routing Protocol (WRP) [Murthy96]is a table-based distance-vector routing protocol. Each node in the network maintains a Distance table, a Routing table, a Link-Cost table and a Message Retransmission list.

The Distance table of a node x contains the distance of each destination node y via each neighbor z of x. It also contains the downstream neighbor of z through which this path is realized. The Routing table of node x contains the distance of each destination node y from node x, the predecessor and the successor of node x on this path. It also contains a tag to identify if the entry is a simple path, a loop or invalid. Storing predecessor and successor in the table is beneficial in detecting loops and avoiding counting-to-infinity problems.

The Link-Cost table contains cost of link to each neighbor of the node and the number of timeouts since an error-free message was received from that neighbor. The Message Retransmission list (MRL) contains information to let a node know which of its neighbor has not acknowledged its update message and to retransmit update message to that neighbor.

Node exchange routing tables with their neighbors using update messages periodically as well as on link changes. The nodes present on the response list of update message (formed using MRL) are required to acknowledge the receipt of update message. If there is no change in routing table since last update, the node is required to send an idle Hello message to ensure connectivity. On receiving an update message, the node modifies its distance table and looks for better paths using new information. Any new path so found is relayed back to the original nodes so that they can update their tables.

The node also updates its routing table if the new path is better than the existing path. On receiving an ACK, the mode updates its MRL. A unique feature of this algorithm is that it checks the consistency of all its neighbors every time it detects a change in link of any of its neighbors. Consistency check in this manner helps eliminate looping situations in a better way and also has fast convergence.

Advantages

- The advantage of WRP is similar to DSDV. In addition, it has faster convergence and adds fewer table updates.

Disadvantage

- The complexity of maintenance of multiple tables demands a large amount of memory and greater processing power from nodes in the MANET.
- Since it suffers from limited scalability therefore WRP is not suitable for highly dynamic and for a very large ad hoc wireless network.

3.4.2 SOURCE INITIATED ON -DEMAND PROTOCOLS

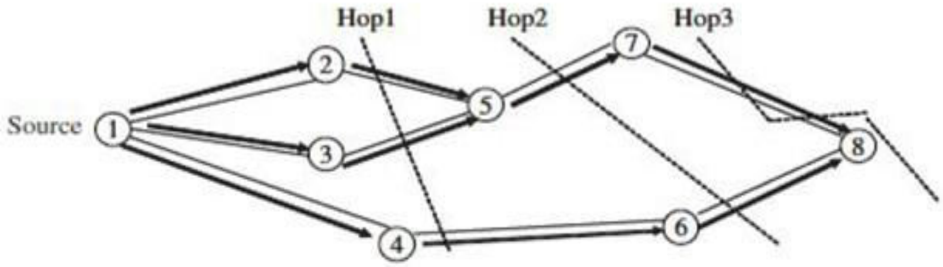
- Source - initiated on demand routing is **reactive** in nature, unlike table driven routing. This type of protocols generates routes only when a source demands it.
- In other words, when a source node requires a route to a destination, the source initiates a route discovery process in the network. This process finishes when a route to the destination has been discovered or all possible routes have been examined without any success.
- The discovered route is maintained by a route maintenance procedure, until it is no longer desired or the destination becomes inaccessible.

The source initiated on demand routing is categorized as follows:

3.4.3 AD HOC ON DEMAND DISTANCE VECTOR ROUTING (AODV)

- AODV is a routing protocol for MANETs (mobile ad hoc networks) and other wireless ad hoc networks.
- It is a reactive routing protocol; it means it establishes a route to a destination only on demand.
- AODV routing is built over the DSDV algorithm. It is a significant improvement over DSDV.
- The devices that are not on a particular path do not maintain routing information, nor do they participate in the routing table exchanges.
- When a source requires sending a message to a destination and does not have a valid route to the latter, the source initiates a route discovery process.
- Source sends a route request (RREQ) packet to all its neighbors, the latter forward the request to all their neighbors, and so on, until either the destination or an intermediate mobile (node) with a "fresh enough" route to the destination is reached.

3.4.4 PROPAGATION OF THE BROADCAST REQUEST(RREQs)



(a) Propagation of route request (RREQ) packet

FIGURE 3.5 PROPAGATION OF THE BROADCAST REQUEST(RREQs)

The above figure illustrates the propagation of the broadcast request (RREQs) across the network. Since in DSDV, destination sequence numbers are used to ensure that all routes are loop free and contain the most recent route information. Each node has a unique sequence number and a broadcast ID, which is incremented each time the node, initiates RREQ.

The broadcast ID, together with the IP address of node, uniquely identifies every RREQ.

Intermediate mobile reply only if they have a route to the destination with a sequence number greater than or at least equal to that contained in the RREQ. To optimize the route performance, intermediate nodes record the address.

From the above figure, since RREP (route reply packet) travels back on the reverse path, the nodes on this path set up their forward route entries to point to the node from which RREP had just been received. These forward route records indicate the active forward route. The RREP continues traveling back along the reverse path till it reaches the initiator of the route discovery. Thus, AODV can support only the use of symmetric links.

3.5 DYNAMIC SOURCE ROUTING (DSR)

- Dynamic source routing is an on-demand routing protocol which is based on source routing.
- It is very similar to AODV in that it forms a route on demand when a transmitting computer requests one. But, it uses source routing instead of relying on the routing

table at each intermediate device. Many successive refinements have been made to dynamic source routing.

This protocol works in two main phases:

- Route discovery
- Route maintenance
- When a node has a message to send, it contacts to the route cache to determine whether is it has a route to the destination. If an active route to the destination exists, it is used to send a message.
- Otherwise a node initiates a route discovery by broadcasting a route request packet. The route request stores the destination address, the source address, and a unique identification number.

- Each device that receives the route request checks whether it has a route to the destination. If it does not, it adds its own address to the route record of the packet and then rebroadcasts the packet on its outgoing links.
- To minimize the no. of broadcasts, a mobile rebroadcasts a packet only if it has not seen the packet before and its own address was not already in the route record.

3.6 ALTERNATIVE METRICS.

- Mobile IP with reverse tunneling
- Router accepts often only "topological correct"addresses (firewall!)
- a packet from the MN encapsulated by the FA is now topological correct
- furthermore multicast and TTL problems solved (TTL in the home network correct, but MN is to far away from the receiver)

Reverse tunneling does not solve

- Problems with firewalls, the reverse tunnel can be abused to circumvent security mechanisms (tunnel hijacking)
- Optimization of data paths, i.e. packets will be forwarded through the tunnel via the HA to a sender (double triangular routing)
- The standard is backwards compatible

- The extensions can be implemented easily and cooperate with current implementations without these extensions
- Agent Advertisements can carry requests for reverse tunneling

World Wide Web and mobility

Protocol (HTTP, Hypertext Transfer Protocol) and language (HTML, Hypertext Markup Language) of the Web have not been designed for mobile applications andmobile devices, thus creating many problems!

Typical transfer sizes

- HTTP request: 100-350 byte
- responsesavg<10 kbyte, header 160 byte, GIF 4.1kByte, JPEG
- 12.8 kbyte, HTML 5.6 kbyte
- but also many large files that cannot be ignored
- The Web is no file system
- Web pages are not simple files to download
- static and dynamic content, interaction with servers via forms, content transformation, push technologies etc.
- many hyperlinks, automatic loading and reloading, redirecting
- a single click might have big consequences!

3.7 TRADITIONAL TCP

TCP is an alternative transport layer protocol over IP.

Traditionally, TCP / IP protocol stack is used for providing connectivity to the stationary devices. To provide support for the mobile devices, lower layers up to network layers are not sufficient. While network layer addresses the host, port, transport (TCP / IP) layer provides dedicated application (lying above them in protocol stack) by way of multiplexing data to and from applications. In addition, while UDP provides a connectionless, TCP can give certain guarantee such as in-order delivery or reliable data transmission using retransmission technique etc. However, these are designed non mobile applications

Based on unique problems associated with the mobile nodes, a set of solutions have been developed. These are : Indirect TCP, Snooping TCP, Mobile TCP, Fast Retransmit/fast recovery, Transmission / time out freezing, selective retransmission, transaction oriented TCP etc Brief description of each is given below:

Traditional TCP: To start with, a bit of under standing of the tradition protocol stack is discussed. Salient features that enhances the TCP performance are:

i. Congestion Control: Once the network system (consisting of routers, bridges, hubs) are established, the hardware and software become matured and they are not likely to drop packets or flip bits (0 to 1 or vice versa). However, temporary overload that occurs when a number of input data (different input links) being addressed to a particular output link This results in a congestion of a node. Congestion may occur from time to time. In this case, the router drops the packets which is observed by the receiver. When the senders does not receive the ACK for the lost packets, each of them assume congestion in the network. As sending the data at full rate is unwise, each of the senders reduce the data rate which removes the congestion over a period of time. So even under heavy load, TCP guarantees at lest sharing of the bandwidth.

ii. Slow Start: An important features of as a response to congestion is Slow Start mechanism. In this once, congestion is indicated, the sender reverts to slow start mechanism. It works as follows:

The sender starts sending one packet and waits for its response. The waiting period is equal to RTT. If ACK is received, he doubles the size of the packet and waits of ACK. This process is repeated till he reaches a threshold limit. That is till he reaches the threshold level, the message size increases exponentially. Once it is reached, the increment changes to linear. Here again, increment is not for ever. Now whenever time out occurs due to missing ACKs, the threshold level is set to half and the congestion is set to one segment and the sender start sending a single segment. Now the exponential growth goes upto new threshold level.

iii Fast Recovery / Fast Retransmit: In TCP, loss in receipt of the data at the destination can be due to two reasons. One is occasional loss due to error. Other may be due to congestion. In case of occasional loss, the receiver sends ACK for the last packet repeatedly for three or four times. This is an indication for the sender that a packet is lost the and the sender now retransmits the same. This is called fast retransmit which takes place without much loss of time.

TCP provides:

- Connection-oriented
- Reliable
- Full-duplex
- Byte-Stream

Connection-Oriented

- Connection oriented means that a virtual connection is established before any user data is transferred.
- If the connection cannot be established - the user program is notified.
- If the connection is ever interrupted - the user program(s) is notified.

Reliable

- Reliable means that every transmission of data is acknowledged by the receiver.
- If the sender does not receive acknowledgement within a specified amount of time, the sender retransmits the data.

Byte Stream

- Stream means that the connection is treated as a stream of bytes.
- The user application does not need to package data in individual datagrams (as with UDP).

Buffering

TCP is responsible for buffering data and determining when it is time to send a datagram.

- It is possible for an application to tell TCP to send the data it has buffered without waiting for a buffer to fill up.

Full Duplex

- TCP provides transfer in both directions.

- To the application program these appear as 2 unrelated data streams, although TCP can piggyback control and data communication by providing control information (such as an ACK) along with user data.

TCP Ports

- Interposes communication via TCP is achieved with the use of ports (just like UDP).
- UDP ports have no relation to TCP ports (different name spaces).

TCP Segments

The chunk of data that TCP asks IP to deliver is called a TCP segment.

Each segment contains:

- data bytes from the byte stream
- control information that identifies the data bytes

TCP Lingo

- When a client requests a connection it sends a "SYN" segment (a special TCP segment) to the server port.
- SYN stands for synchronize. The SYN message includes the client's ISN.
- ISN is Initial Sequence Number.
- Every TCP segment includes a Sequence Number that refers to the first byte of data included in the segment.
- Every TCP segment includes an Acknowledgement Number that indicates the byte number of the next data that is expected to be received.
- All bytes up through this number have already been received.

There are a bunch of control flags:

- URG: urgent data included.
- ACK: this segment is (among other things) an acknowledgement.
- RST: error – connection must be reset.
- SYN: synchronize Sequence Numbers (setup)
- FIN: polite connection termination
- MSS: Maximum segment size (A TCP option)

- Window: Every ACK includes a Window field that tells the sender how many bytes it can send before the receiver will have to toss it away (due to fixed buffer size).

3.8 MOBILE TCP

The delay characteristics when a wireless host switches to a different network is different from when it moves from one cell to another in the same network and the data loses from these two reasons is different from data loss due to congestion in the wired network.

In fixed host interprets these packet losses due to handoffs or interface switching as congestion and invokes the congestion control methods including reducing window size. This is not desirable.

Mobile let the base station tell the sender whether the loss is due to handoff in the same network or if it is due to interface switching

Dropping of packets due to a handover or higher bit error rate is not the only problem occurs

- Special handling of lengthy and/or frequent disconnections
- M-TCP splits as I-TCP does
- unmodified TCP fixed network to supervisory host (SH)
- optimized TCP SH to MH
- Supervisory host
- no caching, no retransmission
- monitors all packets, if disconnection detected
- set sender window size to 0
- sender automatically goes into persistent mode
- old or new SH reopen the window

Advantages

maintains semantics, supports disconnection, no buffer forwarding, no changes to sender's TCP

Disadvantages

- loss on wireless link propagated into fixed network
- adapted TCP on wireless link

3.8.1 INDIRECT TCP

Indirect TCP or I-TCP segments the connection

- no changes to the TCP protocol for hosts connected to the wired Internet, millions of computers use (variants of) this protocol
- optimized TCP protocol for mobile hosts
- splitting of the TCP connection at, e.g., the foreign agent into 2 TCP connections, no real end-to-end connection any longer
- hosts in the fixed part of the net do not notice the characteristics of the wireless part

The two competing insights are

1) TCP performs poorly together with wireless links

2) TCP within the fixed network cannot be changed

Packet delivery (CN to MN)

- If CN sends packet, FA acknowledges packet and forwards packet to MN
- If MN receives packet,it acknowledges
- This acknowledgement only used by CN
- Similarly if MN sends packet, FA acknowledges packet and forwards it to CN

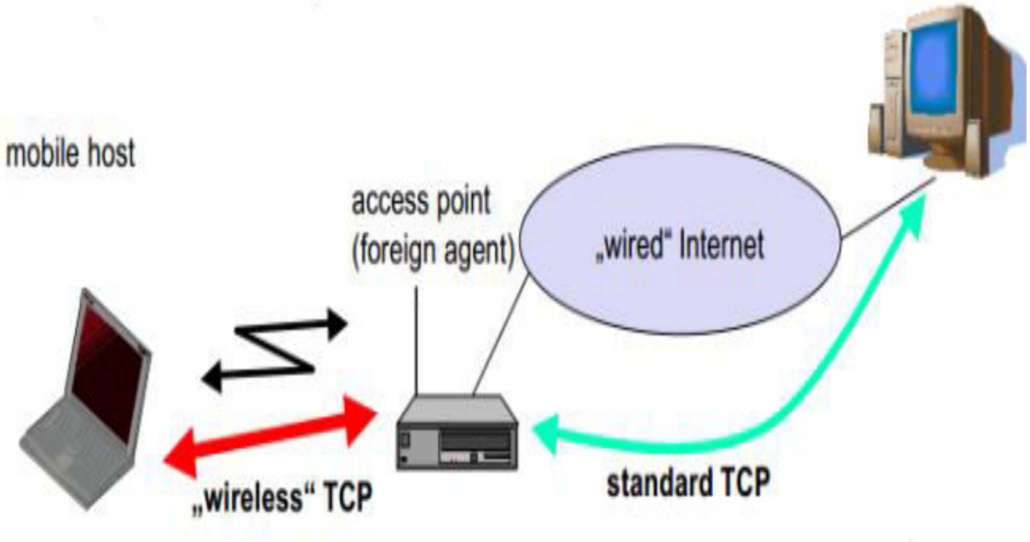


FIGURE 3.6 TCP SEGMENTS A TCP CONNECTION INTO TWO PARTS

I-TCP requires several actions as soon a handover takes place:

- The packets have to be redirected using mobile IP
- The access point acts as a proxy buffering packets for retransmission
- After handover, the old proxy forwards data to new proxy
- The sockets(current state of TCP) of old proxy also migrate to new foreign agent

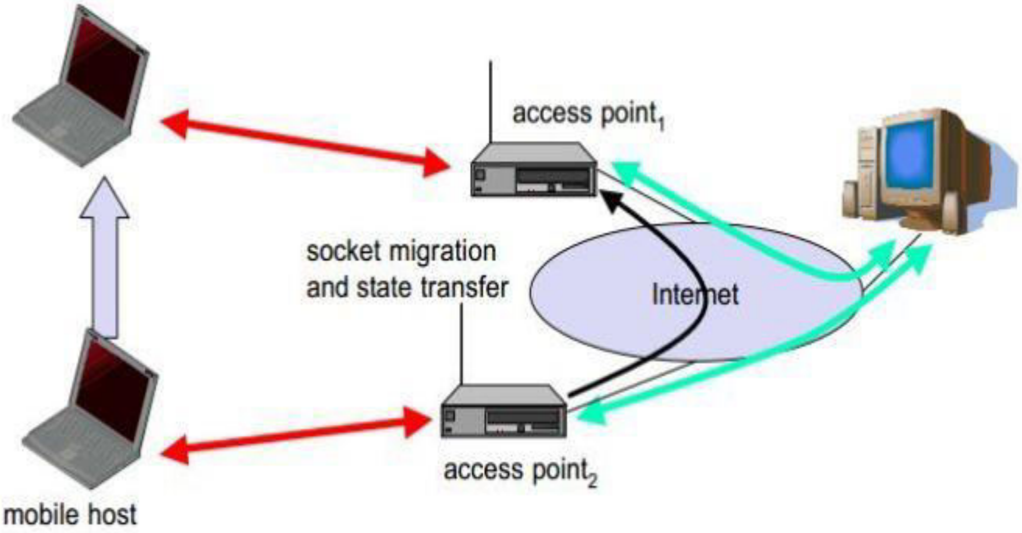


FIGURE 3.7 SOCKET MIGRATION AFTER HANDOVER OF A MOBILE HOST (I-TCP)

Advantages

- no changes in the fixed network necessary, no changes for the hosts (TCP protocol) necessary, all current optimizations to TCP still work
- transmission errors on the wireless link do not propagate into the fixed network
- simple to control, mobile TCP is used only for one hop between, e.g., a foreign agent and mobile host
- therefore, a very fast retransmission of packets is possible, the short delay on the mobile hop
- therefore, a very fast retransmission of packets is possible, the short delay on the mobile hop

Disadvantages

- loss of end-to-end semantics, an acknowledgement to a sender does now not any longer mean that a receiver really got a packet, foreign agents might crash
- higher latency possible due to buffering of data within the foreign agent and forwarding to a new foreign agent

3.8.2 SNOOPING TCP

"Transparent" extension of TCP within the foreign agent

- buffering of packets sent to the mobile host
- lost packets on the wireless link (both directions!) will be retransmitted immediately by the mobile host or foreign agent, respectively (so called "local" retransmission)
- the foreign agent therefore "snoops" the packet flow and recognizes acknowledgements in both directions, it also filters ACKs
- changes of TCP only within the foreign agent

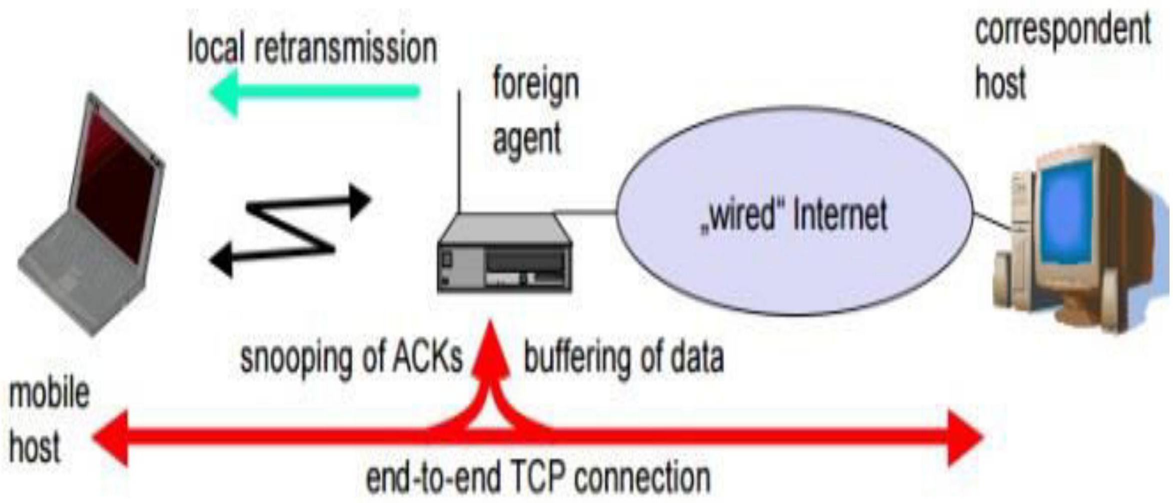


FIGURE 3.8 DATA TRANSFER TO THE MOBILE HOST

Data transfer to the mobile host

- FA buffers data until it receives ACK of the MH, FA detects packet loss via duplicated ACKs or time-out
- fast retransmission possible, transparent for the fixed network

Data transfer from the mobile host

- FA detects packet loss on the wireless link via sequence numbers, FA answers directly with a NACK to the MH
- MH can now retransmit data with only a very short delay

Integration with MAC layer

- MAC layer often has similar mechanisms to those of TCP
- thus, the MAC layer can already detect duplicated packets due to retransmissions and discard them

Problems

- snooping TCP does not isolate the wireless link as good as I-TCP
- snooping might be tough if packets are encrypted

ADVANTAGES

- end-to-end semantics preserves,
- no changes to correspondent host (and few to mobile host)
- no state handover (time-out and retransmission)
- handover: next FA may not use this approach
- Most of the enhancements are done in the foreign agent itself which keeps correspondent host unchanged.
- Handover of state is not required as soon as the mobile host moves to another foreign agent. Even though packets are present in the buffer, time out at the CH occurs and the packets are transmitted to the new COA.
- No problem arises if the new foreign agent uses the enhancement or not. If not, the approach automatically falls back to the standard solution.

DISADVANTAGES OF SNOOPING TCP

- Snooping TCP does not isolate the behavior of the wireless link as well as l-TCP. Transmission errors may propagate till CH.
- Using negative acknowledgements between the foreign agent and the mobile host assumes additional mechanisms on the mobile host. This approach is no longer transparent for arbitrary mobile hosts.
- Snooping and buffering data may be useless if certain encryption schemes are applied end- to-end between the correspondent host and mobile host. If encryption is used above the transport layer, (eg. SSL/TLS), snooping TCP can be used

UNIT IV

APPLICATION LAYER

WIRELESS APPLICATION PROTOCOL(WAP)

4.1INTRODUCTION

- Wireless Application Protocol is a programming model which is made on the concept of World Wide Web(WWW) programming model and the hierarchical design is somehow similar to TCP/IP protocol stack design.
- WAP is a standard which enables the mobile devices to interact, exchange and transmit information over the internet. It is a De-Facto standard.
- As, WAP is based upon the concept of World Wide Web, the backend functioning also remains similar i.e. HTML is used on WWW and Wireless Mark-up Language(WML) is used in WAP for using the WAP services.
- Since the WAP model is developed, it is accepted as a wireless protocol globally that is capable of working on multiple wireless technology such as mobile, printers, pagers etc
- Another reason for opting and making WAP as De-Facto standard was its ability of creating web applications for mobile devices.

4.2 WIRELESS APPLICATION PROTOCOL MODEL : WORKING

- WAP model comprises of 3-Levels that are : Client, Gateway and Origin Server.
- The WAP user agent sends a request via mobile to WAP gateway by using encoded WAP protocol i.e. called as encoding request.
- The encoding request is translated through WAP gateway and is further forwarded in the form of HTTP request to the server side where scripts are available.
- Response from the scripts and content is picked up as requested, through HTTP and is forwarded to the WAP gateway once again.
- The required HTTP response is then forwarded in decode format to the client protocol stack as the final response for the initial request made by client.

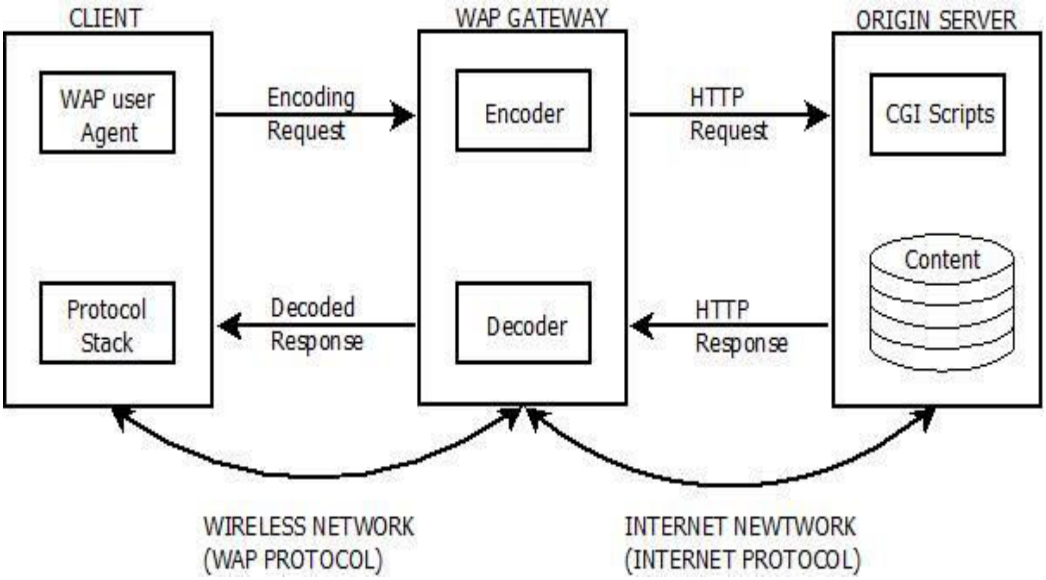


FIGURE 4.1 WIRELESS APPLICATION PROTOCOL

ADVANTAGES OF WIRELESS APPLICATION PROTOCOL

- Fast paced technology.
- Open source-Free.
- Can be implemented on multiple platform.
- Independent of network standard.
- Higher controlling options.

DISADVANTAGES OF WIRELESS APPLICATION PROTOCOL

- Fast Paced Technology
- Less Secured.
- User interface(UI) is small.
- Less availability.

APPLICATIONS OF WIRELESS APPLICATION PROTOCOL

- E-mails access.
- Weather forecasting.
- Flight information.

- Movie & cinema information.
- Traffic updates.

WAP is the de facto worldwide standard for providing Internet communications and advanced telephony services on digital mobile phones, pagers, personal digital assistants, and other wireless terminals.

WAP stands for **W**ireless **A**pplication **P**rotocol. These terms are as follows −

- **Wireless** − Lacking or not requiring a wire or wires pertaining to radio transmission.
- **Application** − A computer program or piece of computer software that is designed to do a specific task.
- **Protocol** − A set of technical rules about how information should be transmitted and received using computers.

WAP is the set of rules governing the transmission and reception of data by computer applications on or via wireless devices like mobile phones.

WAP allows wireless devices to view specifically designed pages from the Internet using only plain text and very simple black-and-white pictures.

WAP is a standardized technology for cross-platform, distributed computing very similar to the Internet's combination of Hypertext Markup Language (HTML) and Hypertext

Transfer Protocol (HTTP), except that it is optimized for:

- low-display capability
- low-memory
- low-bandwidth devices, such as personal digital assistants (PDAs), wireless phones, and pagers.

WAP is designed to scale across a broad range of wireless networks like GSM, IS-95, IS-136, and PDC.

4.3 WAP MODEL

WAP Gateway/Proxy is the entity that connects the wireless domain with the Internet.

- Note that the request that is sent from the wireless client to the WAP Gateway/Proxy uses the Wireless Session Protocol (WSP). In its essence, WSP is a binary version of HTTP.

- A **markup language** − the Wireless Markup Language (WML) has been adapted to develop optimized WAP applications.
- In order to save valuable bandwidth in the wireless network, WML can be encoded into a compact binary format.
- Encoding WML is one of the tasks performed by the WAP Gateway/Proxy.

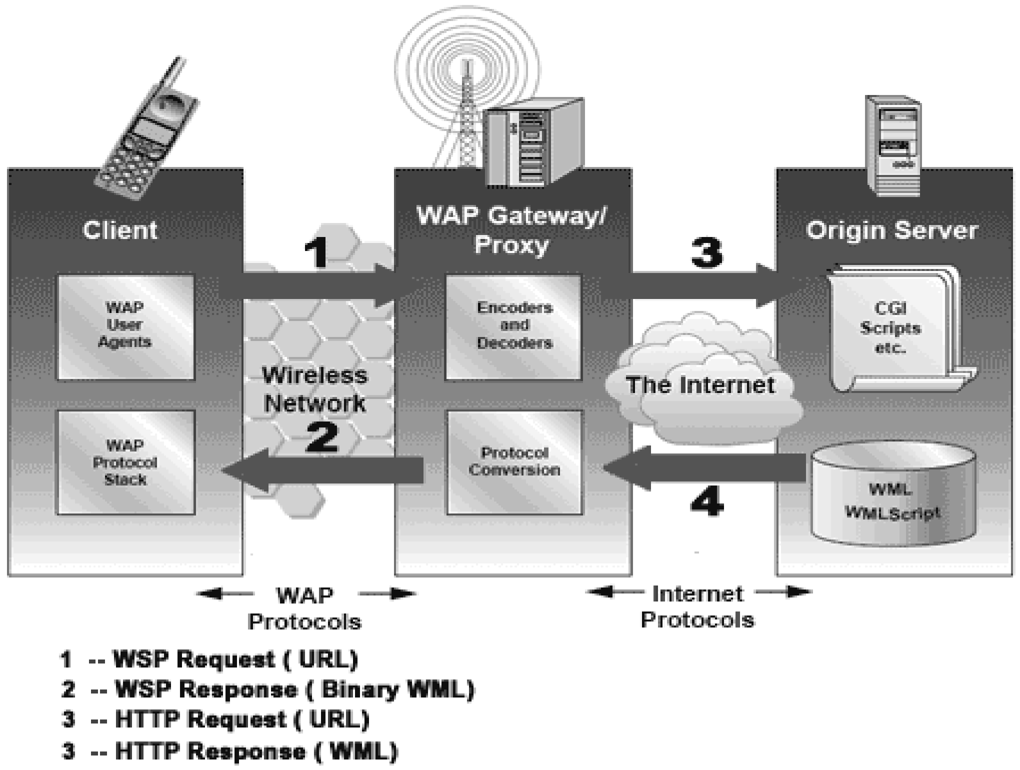


FIGURE 4.2 WAP AND INTERNET PROTOCOL

4.3.1 How WAP Model Works?

When it comes to actual use, 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.

4.3.2 The Internet Model

The Internet model makes it possible for a client to reach services on a large number of origin servers, each addressed by a **unique Uniform Resource Locator** (URL).

The content stored on the servers is of various formats, but HTML is the predominant.

- HTML provides the content developer with a means to describe the appearance of a service in a flat document structure.
- If more advanced features like procedural logic are needed, then scripting languages such as JavaScript or VB Script may be utilized.
- The figure4.4 below shows how a WWW client request a resource stored on a web server.
- On the Internet standard communication protocols, like HTTP and Transmission Control Protocol/Internet Protocol (TCP/IP) are used.

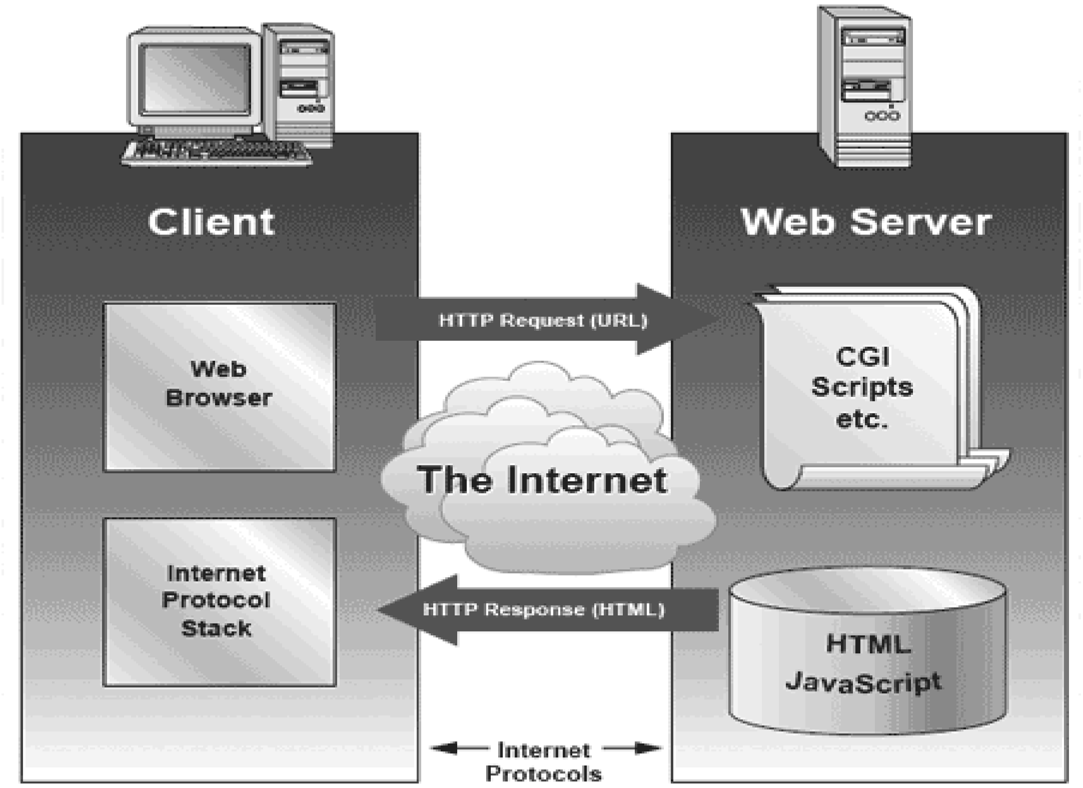


FIGURE 4.3 INTERNET MODEL

The web server may be static or dynamic.

- Static content is produced once and not changed or updated very often; for example, a company presentation.
- Dynamic content is needed when the information provided by the service changes more often; for example, timetables, news, stock quotes, and account information.
- Technologies such as Active Server Pages (ASP), Common Gateway Interface (CGI), and Servlets allow content to be generated dynamically.

4.3.3 LOCATION-BASED SERVICES

Location-based services (LBS) have languished on the back burner for many years, hobbled by global positioning system (GPS) support and technical challenges. However, E911 legislation and related mobile handset upgrades are now dismantling these roadblocks. Today, a growing number of 3G phones and PDAs incorporate GPS chips that can be used to determine and map geographic location. As a result, wireless carriers are finally getting serious about LBS mobile applications for individuals and businesses.

A location-based service (LBS) is a software application for a IP-capable mobile device that requires knowledge about where the mobile device is located. Location-based services can be query-based and provide the end user with useful information such as "Where is the nearest ATM?" or they can be push-based and deliver coupons or other marketing information to customers who are in a specific geographical area.

An LBS requires five basic components:

- the service provider's software application,
- a mobile network to transmit data and requests for service,
- a content provider to supply the end user with geo-specific information,
- a positioning component (see GPS) and the end user's mobile device.
- By law, location-based services must be permission-based.

That means that the end user must opt-in to the service in order to use it. In most cases, this means installing the LBS application and accepting a request to allow the service to know the device's location.

Mobile phone-based LBS services were initially offered in the Asia-Pacific market, tracking the early 3G handset deployment in that region. This year, several North American carriers with CDMA 3G networks launched LBS services, including Verizon and Sprint/Nextel. UMTS carriers such as Cingular and T-Mobile have now followed suit.

New mobile devices that incorporate built-in GPS chips -- the Motorola KRZR K1m and RAZR V3m, for example, or the BlackBerry 7130e and 8703e, and the HP iPAQ 6920 and 6925 -- are natural targets for these new LBS applications. Many popular smartphones that lack GPS, such as the Palm Treo 650/700w and the Nokia E62, can still tap into LBS applications by using an external Bluetooth GPS fob.

Emerging LBS applications

One good example of an LBS application is VZ Navigator, offered by Verizon Wireless. This subscription-based service uses LBS technology developed by Networks in Motion to provide Verizon Wireless customers with directions, maps and local search functions on any supported handset. Simply download VZ Navigator client software to your phone or PDA, enable that handset's GPS position location function, and start mapping

4.4 WAP gateway

A WAP gateway sits between mobile devices using the Wireless Application Protocol (WAP) and the World Wide Web, passing pages from one to the other much like a proxy. This translates pages into a form suitable for the mobiles, for instance using the Wireless Markup Language (WML). This process is hidden from the phone, so it may access the page in the same way as a browser accesses HTML, using a URL (for example, http://example.com/foo.wml), provided the mobile phone operator has not specifically prevented this.

WAP gateway software that encodes and decodes request and response between the smartphones, microbrowser and internet. It decodes the encoded WAP requests from the microbrowser and send the HTTP requests to the internet or to a local application server. It also encodes the WML and HDML data returning from the web for transmission to the microbrowser in the handset.

Typically, the WAP gateway is a server that acts as an intermediary in an access request. The server gets data from the requested web site by HTTP and coverts it into an encrypted form that goes out to the client endpoint.

The protocol used is called Wireless Markup Language (WML). WML has its roots in Extensible Markup Language (XML), a language developed with a specific syntax to address 'plans' or 'schemas' for complex documents.

In addition to WML, a Wireless or WAP Protocol Stack determines how data are sent between the gateway and the user's device. This type of networking provides a more capable environment for Internet use as the Internet grows and expands.

WAP adopts a client-server approach.

- It specifies a proxy server that acts as an interface between the wireless domain and core wired network.

- This proxy server, also known as a **WAP gateway**, is responsible for a wide variety of functions such as protocol translation and optimizing data transfer over the wireless medium.

Wireless network parts consist of

- Content provider (Application or origin server)
- Mobile device (WAP client)
- WAP gateway
- WAP proxy

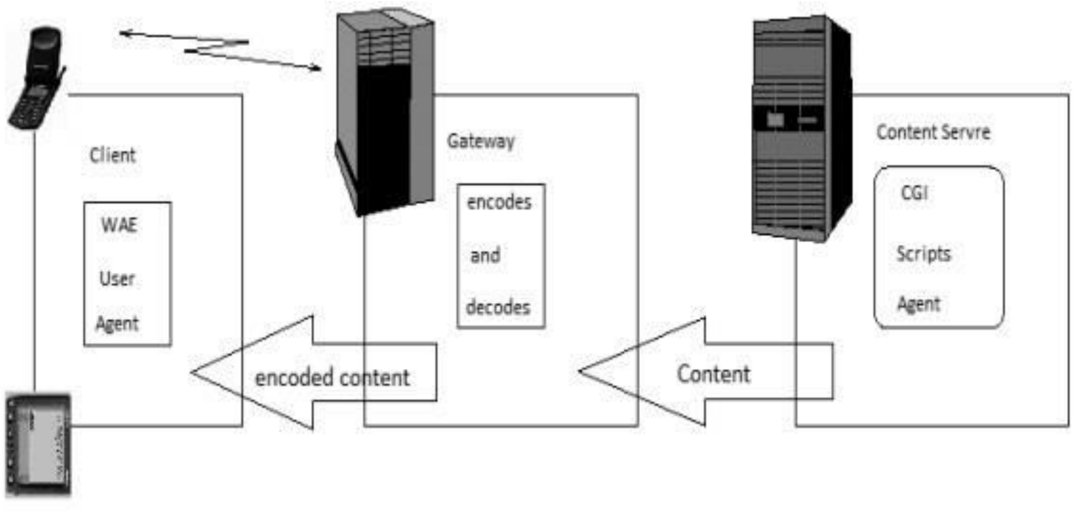


FIGURE 4.4 WAP GATEWAY

The WAP Architecture has been designed to closely follow the web. The only difference is the presence of the WAP gateway is translating between HTTP and WAP.

4.4.1.WAP Client

The three sections to be mentioned regarding WAP client are WAE user agent, WTA user agent and WAP stack.

- **WAE user agent** − Wireless application environment user agent is the browser that renders the content for display.
- **WTA user agent** − Wireless telephony application agent receives compiled WTA files from WTA server and executes them.
- **WAP stack** − WAP stack allows the phone to connect to the WAP gateway using the WAP Protocols

4.4.2 Key features offered by WAP –

A programming model similar to the Internet's

- Wireless Markup Language (WML)
- WMLScript
- Optimized protocol stack

4.5 WAP PROTOCOL STACK

The WAP protocol stack has undergone significant change from WAP 1.x to WAP 2.x.

The basis for the change is the support for Internet Protocols (IPs) when IP connectivity is supported by the mobile device and network.

The WAP 2.x protocol stack is backward-compatible. Support for the legacy WAP 1.x stack has been maintained for non-IP and low-bandwidth IP networks that can benefit from the optimizations in the WAP 1.x protocol stack.

4.5.1. WAP 1.x

The protocols in the WAP 1.x protocol stack have been optimized for low-bandwidth, high-latency networks, which are prevalent in pre-3G wireless networks. The protocols are as follows:

1. Wireless Session Protocol (WSP).

- WSP provides capabilities similar to HTTP/1.1
- while incorporating features designed for low-bandwidth, high-latency wireless networks such as long-lived sessions and session suspend/resume.
- The communication from a WAP gateway to the microbrowser client is over WSP.

2. Wireless Transaction Protocol (WTP).

- WTP provides a reliable transport mechanism for the WAP datagram service. It offers similar reliability as Transmission Control Protocol/Internet Protocol (TCP/IP).
- The result is that WTP requires less than half of the number of packets of a standard HTTP-TCP/IP request.

- WTP means that a TCP stack is not required on the wireless device, reducing the processing power and memory required.

3. Wireless Transport Layer Security (WTLS).

- WTLS is the wireless version of the Transport Security Layer (TLS), which was formerly known as Secure Sockets Layer (SSL).
- It provides privacy, data integrity, and authentication between the client and the wireless server.
- Using WTLS, WAP gateways can automatically provide wireless security for Web applications that use TLS.
- In addition, WTLS incorporates features designed for wireless networks, such as datagram support, optimized handshakes, and dynamic key refreshing.

4. Wireless Datagram Protocol (WDP).

- WDP is a datagram service that brings a common interface to wireless transportation bearers.
- It can provide this consistent layer by using a set of adapters designed for specific features of these bearers.
- It supports CDPD, GSM, CDMA, TDMA, SMS, FLEX (a wireless technology developed by Motorola), and Integrated Digital Enhanced Network (iDEN) protocols.

4.5.2. WAP 2.x

One of the main new features in WAP 2.x is the use of Internet protocols in the WAP protocol stack. This change was precipitated by the rollout of 2.5G and 3G networks that provide IP support directly to wireless devices.

WAP 2.x has the following new protocol layers:

1. Wireless Profiled HTTP (WP-HTTP).

- WP-HTTP is a profile of HTTP designed for the wireless environment.
- It is fully interoperable with HTTP/1.1 and allows the usage of the HTTP request/response model for interaction between the wireless device and the wireless server.

2. Transport Layer Security (TLS).

- WAP 2.0 includes a wireless profile of TLS, which allows secure transactions.
- The TLS profile includes cipher suites, certificate formats, signing algorithms, and the use of session resume, providing robust wireless security.
- There is also support for TLS tunneling, providing end-to-end security at the transport level.
- The support for TLS removes the WAP security gap that was present in WAP 1.x.

3. Wireless Profiled TCP (WP-TCP)

- WP-TCP is fully interoperable with standard Internet-based TCP implementations, while being optimized for wireless environments.
- These optimizations result in lower overhead for the communication stream.

4.5.3. Other WAP 2.x Services

- WAP Push.
- User Agent Profile (UAProf).
- External Functionality Interface (EFI).
- Wireless Telephony Application (WTA).
- Persistent storage interface.
- Data synchronization.
- Multimedia Messaging Service (MMS).

4.6 WAP architecture

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

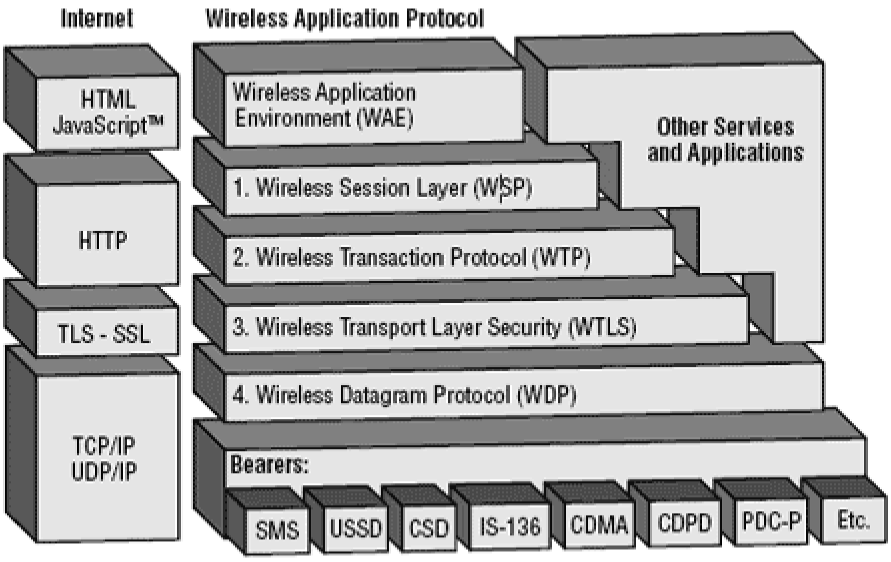

Internet
Wireless Application Protocol
HTML
JavaScript™
HTTP
TLS - SSL
TCP/IP
UDP/IP
Wireless Application Environment (WAE)
Other Services and Applications
1. Wireless Session Layer (WSP)
2. Wireless Transaction Protocol (WTP)
3. Wireless Transport Layer Security (WTLS)
4. Wireless Datagram Protocol (WDP)
Bearers:
SMS
USSD
CSD
IS-136
CDMA
CDPD
PDC-P
Etc.

FIGURE 4.5 WAPPROTOCOL ARCHITECTURE

4.6.1. Wireless Application Environment (WAE)

The Wireless Application Environment (WAE) is the application layer of the OSI model. It provides the required elements for interaction between Web applications and wireless clients using a WAP micro browser. These elements are as follows:

- A specification for a micro browser that controls the user interface and interprets WML and WMLScript.
- The foundation for the micro browser in the form of the Wireless Markup Language (WML). WML has been designed to accommodate the unique characteristics of wireless devices, by incorporating a user interface model that is suitable for small form-factor devices that do not have a QWERTY keyboard.
- A complete scripting language called WMLScript that extends the functionality of WML, enabling more capabilities on the client for business and presentation logic.
- Support for other content types such as wireless bitmap images (WBMP), vCard, and vCalendar.

WAP 2.x extends WAE by adding the following elements:

- A new markup language specification called WML2 that is based on XHTML-Basic. Backward compatibility with WML1 has been maintained.

- Support for stylesheets to enhance presentation capabilities. Stylesheet support is based on the Mobile Profile of Cascading Style Sheets (CSS) from the W3C, and supports both inline and external style sheets.

4.6.2. Layers of WAP Protocol

WAP is designed in a layered fashion ,so that it can be extensible, flexible, and scalable. As a result, the WAP protocol stack is divided into five layers−

1. Application Layer

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.

2. Session Layer

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

3. 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.

4. 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.

5. 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.

- The layered architecture allows other applications and services to utilise the features provided by the WAP-stack as well.
- The WAP-stack for services and applications that currently are not specified by WAP.

6. Bearer

The bearers that are used by the WAP protocol stack form the lower interface of the datagram service and allow the WAP to be used for various network types with specific bearer functions.

Thus, WDP is defined for a variety of bearers. For an IP bearer, the transport protocol (WDP) is implemented by User Datagram Protocol (UDP)..

4.7. WML

WML Script complements to WML and provides a general scripting capability in the WAP architecture (WAP Forum, 2000h). While all WML content is static (after loading on the client),

WML

The topmost layer in the WAP (Wireless Application Protocol) architecture is made up of WAE (Wireless Application Environment), which consists of WML and WML scripting language.

- WML stands for **W**ireless **M**arkup **L**anguage
- WML is an application of XML, which is defined in a document-type definition.
- WML is based on HDML and is modified so that it can be compared with HTML.
- WML takes care of the small screen and the low bandwidth of transmission.
- WML is the markup language defined in the WAP specification.
- WAP sites are written in WML, while web sites are written in HTML.
- WML is very similar to HTML. Both of them use tags and are written in plain text format.
- WML files have the extension ".wml". The MIME type of WML is "text/vnd.wap.wml".
- WML supports client-side scripting. The scripting language supported is called WMLScript.

WML Versions:

WAP Forum has released a latest version WAP 2.0. The markup language defined in WAP 2.0 is XHTML Mobile Profile (MP).

The WML MP is a subset of the XHTML. A style sheet called WCSS (WAP CSS) has been introduced along with XHTML MP. The WCSS is a subset of the CSS2.

Most of the new mobile phone models released are WAP 2.0-enabled. Because WAP 2.0 is backward compatible to WAP 1.x, WAP 2.0-enabled mobile devices can display both XHTML MP and WML documents.

WML 1.x is an earlier technology. However, that does not mean it is of no use, since a lot of wireless devices that only supports WML 1.x are still being used.

Latest version of WML is 2.0 and it is created for backward compatibility purposes.

So WAP site developers need not to worry about WML 2.0.

WML Document Body:

The body is enclosed within a <wml> </wml> tag pair. The body of a WML document can consist of one or more of the following:

- Deck
- Card
- Content to be shown
- Navigation instructions

WML Decks and Cards:

A main difference between HTML and WML is that the basic unit of navigation in HTML is a page, while that in WML is a card. A WML file can contain multiple cards and they form a deck.

When a WML page is accessed from a mobile phone, all the cards in the page are downloaded from the WAP server.

So if the user goes to another card of the same deck, the mobile browser does not have to send any requests to the server since the file that contains the deck is already stored in the wireless device.We can put links, text, images, input fields, option boxes and many other elements in a card.

WML Program Structure:

Following is the basic structure of a WML program:

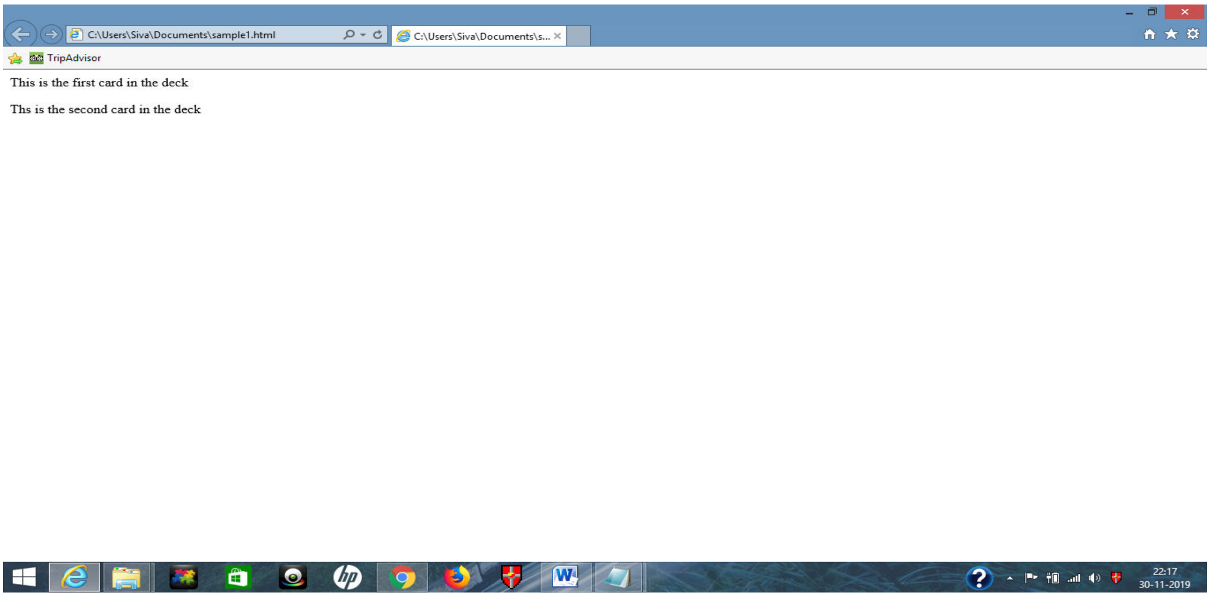
```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.2//EN"
"http://www.wapforum.org/DTD/wml12.dtd">

<wml>

<card id="one" title="First Card">
<p>
This is the first card in the deck
</p>
</card>

<card id="two" title="Second Card">
<p>
Ths is the second card in the deck
</p>
</card>

</wml>
```

The first line of this text says that this is an XML document and the version is 1.0. The second line selects the document type and gives the URL of the document type definition (DTD).

One WML deck (i.e. page) can have one or more cards as shown above. We will see complete details on WML document structure in subsequent chapter.

Unlike HTML 4.01 Transitional, text cannot be enclosed directly in the <card>...</card> tag pair. So you need to put a content inside <p>...</p> as shown above.

OUTPUT


C:\Users\Siva\Documents\sample1.html
C:\Users\Siva\Documents\s...
TripAdvisor
22:17
30-11-2019

This is the first card in the deck

Ths is the second card in the deck

Elements have one of the following two structures:

- **<tag> content </tag>** : This form is identical to HTML.
- **<tag />:** This is used when an element cannot contain visible content or is empty, such as a line break. WML document's prolog part does not have any element which has closing element.

Following table lists the majority of valid elements

DECK & CARD ELEMENTS

WML Elements	Purpose
<!-->	Defines a WML comment
<wml>	Defines a WML deck (WML root)
<head>	Defines head information
<meta>	Defines meta information
<card>	Defines a card in a deck

<access>	Defines information about the access control of a deck
<template>	Defines a code template for all the cards in a deck

TEXT ELEMENTS

WML Elements	Purpose
<br>	Defines a line break
<p>	Defines a paragraph
<table>	Defines a table
<td>	Defines a table cell (table data)
<tr>	Defines a table row
<pre>	Defines preformatted text

TEXT FORMATTING TAGS

WML Elements	Purpose
<b>	Defines bold text
<big>	Defines big text
<em>	Defines emphasized text
<i>	Defines italic text
<small>	Defines small text
<strong>	Defines strong text
<u>	Defines underlined text

IMAGE ELEMENTS

WML Elements	Purpose
<img>	Defines an image

ANCHOR ELEMENTS

WML Elements	Purpose
<a>	Defines an anchor
<anchor>	Defines an anchor

EVENT ELEMENTS

WML Elements	Purpose
<do>	Defines a do event handler
<onevent>	Defines an onevent event handler
<postfield>	Defines a postfield event handler
<ontimer>	Defines an ontimer event handler
<onenterforward>	Defines an onenterforward handler
<onenterbackward>	Defines an onenterbackward handler
<onpick>	Defines an onpick event handler

TASK ELEMENTS

WML Elements	Purpose
<go>	Represents the action of switching to a new card
<noop>	Says that nothing should be done
<prev>	Represents the action of going back to the previous card
<refresh>	Refreshes some specified card variables.

INPUT ELEMENTS

WML Elements	Purpose
<input>	Defines an input field
<select>	Defines a select group
<option>	Defines an option in a selectable list
<fieldset>	Defines a set of input fields
<optgroup>	Defines an option group in a selectable list

VARIABLE ELEMENTS

WML Elements	Purpose
<setvar>	Defines and sets a variable
<timer>	Defines a timer

WAP Site Design Considerations:

Wireless devices are limited by the size of their displays and keypads. It's therefore very important to take this into account when designing a WAP Site.

While designing a WAP site you must ensure that you keep things simple and easy to use.

We should always keep in mind that there are no standard microbrowser behaviors and that the data link may be relatively slow, at around 10Kbps.

However, with GPRS, EDGE, and UMTS, this may not be the case for long, depending on where you are located.

The following are general design tips that you should keep in mind when designing a service:

- Keep the WML decks and images to less than 1.5KB.
- Keep text brief and meaningful, and as far as possible try to precode options to minimize the rather painful experience of user data entry.
- Keep URLs brief and easy to recall.
- Minimize menu levels to prevent users from getting lost and the system from slowing down.
- Use standard layout tags such as <big> and <b>, and logically structure your information.
- Don't go overboard with the use of graphics, as many target devices may not support them.

4.7.1WMLScript

WirelessMarkupLanguageScript is the client-side scripting language of WML.

A scripting language is similar to a programming language, but is of lighter weight. With WMLScript, the wireless device can do some of the processing and computation. This reduces the number of requests and responses to/from the server.

4.7.1.1 WML Script Components

1. WML Script Operators

WML Script supports following type of operators.

- Arithmetic Operators
- Comparison Operators
- Logical or Relational Operators
- Assignment Operators
- Conditional or ternary

2. WML Script Control Statements:

- Control statements are used for controlling the sequence and iterations in a program.
- Statement Description if-else Conditional branching for Making self-incremented fixed iteration loop while Making variable iteration loop break Terminates a loop continue Quit the current iteration of a loop Check for complete detail of WML Script Control Statements.

3. WML Script Functions:

The user-defined functions are declared in a separate file having the extension .wmls.

Functions are declared as follows:

- function name (parameters) { control statements; return var; }
- The functions used are stored in a separate file with the extension .wmls.
- The functions are called as the filename followed by a hash, followed by the function name: maths.wmls#squar()

4. WML Scripts Standard Libraries:

There are six standard libraries totally. Here is an overview of them: Lang: The Lang library provides functions related to the WMLScript language core.

Example Function:

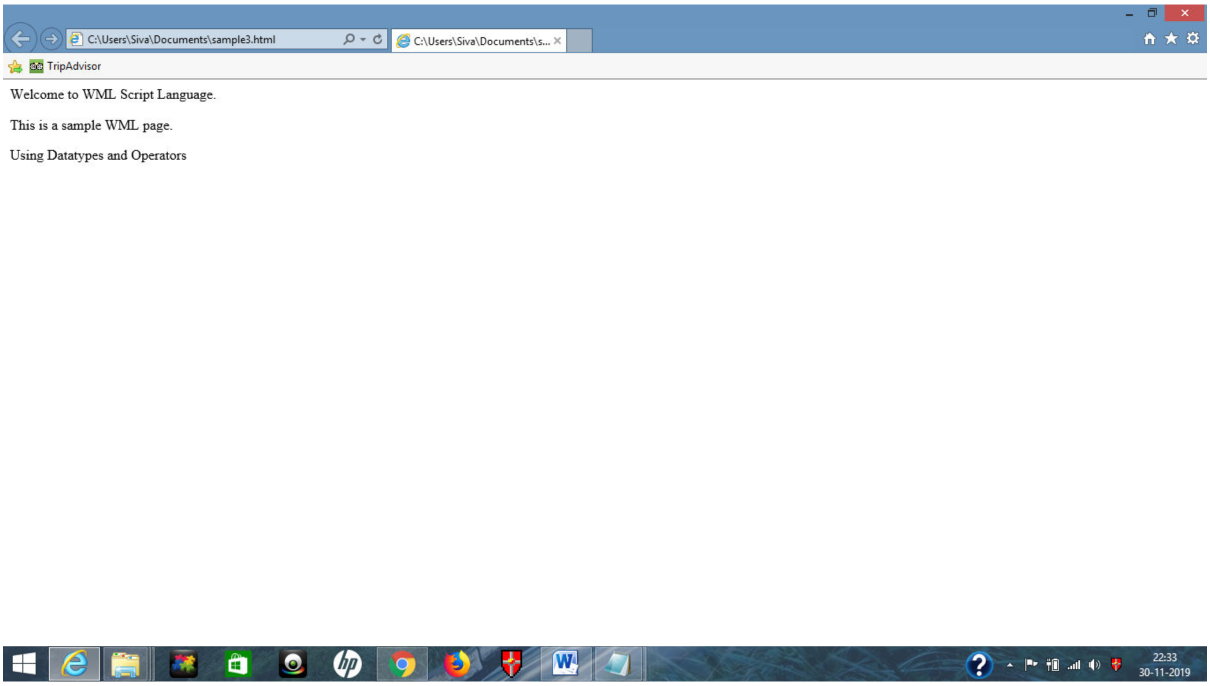
- abs

- abort
- characterSet
- float
- is
- Float
- isInt
- max
- isMax
- min
- minInt
- maxInt
- parseFloat
- parseInt
- random

SAMPLE PROGRAM

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
  "http://www.wapforum.org/DTD/wml_1.1.xml" >
<wml>
 <card id="main" title="First Card">
<p mode="wrap">Welcome to WML Script Language.</p>
  <p mode="wrap">This is a sample WML page.</p>
<p mode="wrap">Using  Datatypes and Operators</p>
 </card>
</wml>
```

OUTPUT



Welcome to WML Script Language.

This is a sample WML page.

Using Datatypes and Operators

FLOAT:

The Float library contains functions that help us perform floating-point arithmetic operations.

Example Function:

- sqrt
- round
- pow
- ceil
- floor
- int
- maxFloat
- minFloat

STRING:

The String library provides a number of functions that help us manipulate strings.

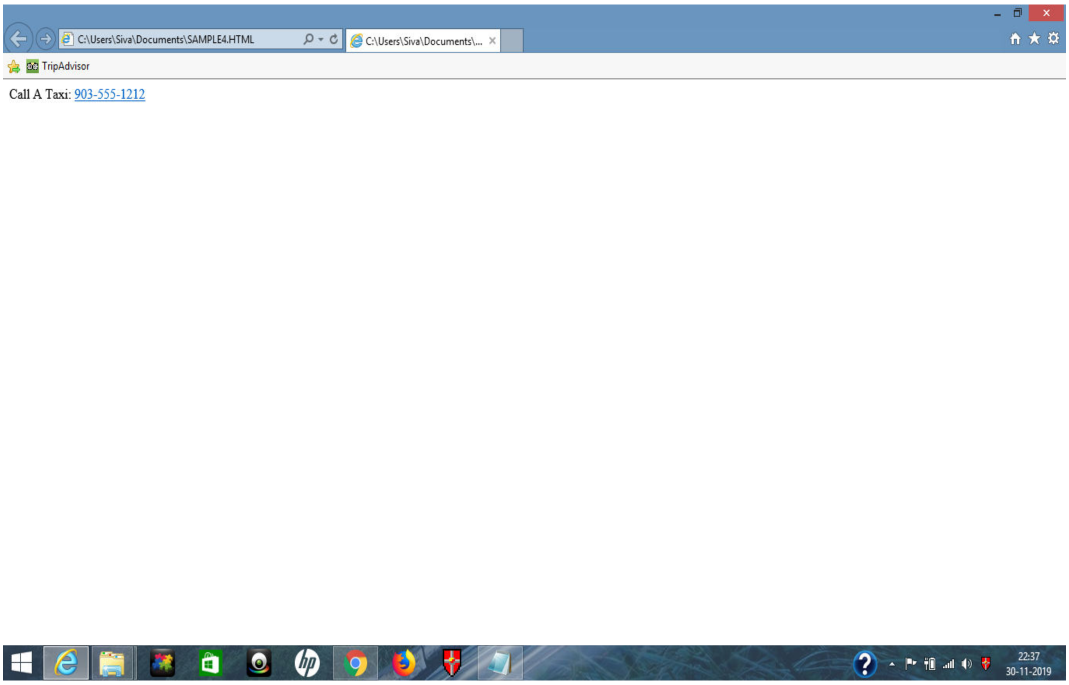
Example Function:

- length
- charAt
- find
- replace
- trim
- compare
- format
- isEmpty
- squeeze
- toString
- elementAt
- elements
- insertAt
- removeAt
- replaceAt

SAMPLE PROGRAM

```
<card id="cM" title="MY_DOMAIN.com">
<p>
Call A Taxi:
<a href="wtai://wp/mc;%2B19035551212">903-555-1212</a>
</p>
</card>
```

OUTPUT


C:\Users\Siva\Documents\SAMPLE4.HTML
C:\Users\Siva\Documents\...
TripAdvisor
22:37
30-11-2019

Call A Taxi: 903-555-1212

5. URL:

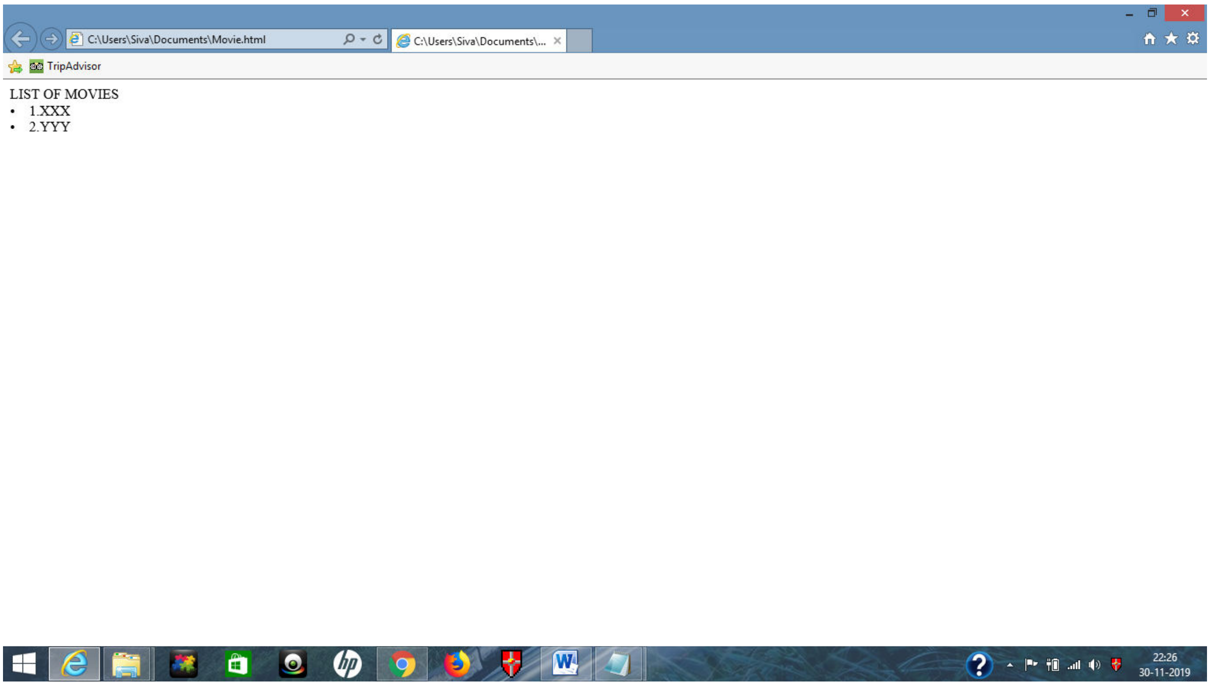
The URL library contains functions that help us manipulate URLs

Example Function:

- getPath
- getReferer
- getHost
- getBase
- escapeString
- isValid
- loadString
- resolve
- unescapeString
- getFragment

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.2//EN"
"http://www.wapforum.org/DTD/wml12.dtd">
<!-- WML prolog.declaration of file type and version>

<wml>
<!-- Declaration of the WML deck>
<card id="info" newcontext="true">
<!-- declaration of a card in deck>
<p align="center"><b>Information Center</b></p>
<!--paragraph declaration to display heading>
<p>
<!--paragraph declaration to display links>
<a href="Movie.wml">1. Movies info.</a>
<a href="Weather.wml">2. Weather Info.</a>
<!--declaration of links for weather and movies>
</p>
</card>
<!-- card end>
</wml>
<!-- program end>
```

OUTPUT


C:\Users\Siva\Documents\Movie.html
C:\Users\Siva\Documents\...
TripAdvisor
22:26
30-11-2019

LIST OF MOVIES

- 1.XXX
- 2.YYY

WMLBrowser:

The WMLBrowser library provides a group of functions to control the WML browser or to get information from it. Example Function: go, prev, next, getCurrentCard, refresh, getVar, setVar Dialogs: The Dialogs library Contains the user interface functions.

Example Function:

- Prompt
- confirm
- alert

WML Scripts Comments:

There are two types of comments in WMLScript:

1. Single-line comment: To add a single-line comment, begin a line of text with the // characters.
2. Multi-line comment: To add a multi-line comment, enclose the text within /* and */. These rules are the same in WMLScript, JavaScript, Java, and C++.

UNIT – V

5. DATABASE ISSUES

5. 1 INTRODUCTION

A database is a collection of systematically stored records or information. Databases store data in a particular logical manner.

A mobile device is not always connected to the server or network; neither does the device retrieve data from a server or a network for each computation.

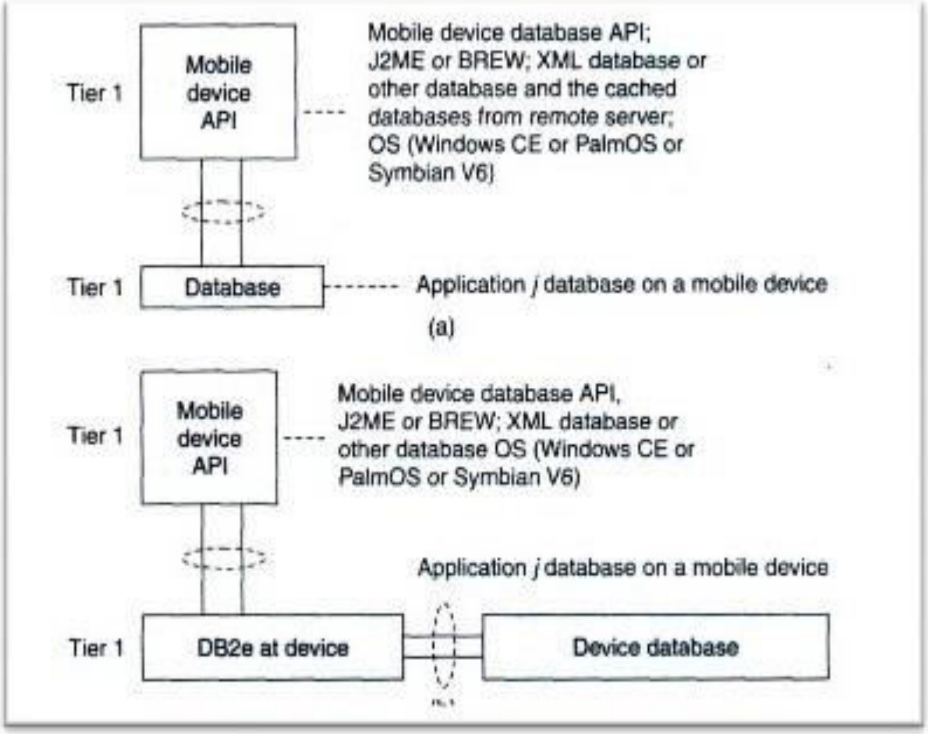
Rather, the device caches some specific data, which may be required for future computations, during the interval in which the device is connected to the server or network.

Caching entails saving a copy of select data or a part of a database from a connected system with a large database.

The cached data is hoarded in the mobile device database. Hoarding of the cached data in the database ensures that even when the device is not connected to the network, the data required from the database is available for computing.

5.2 DATABASE HOARDING

Database hoarding may be done at the application tier itself. The following figure shows a simple architecture in which a mobile device API directly retrieves the data from a database. It also shows another simple architecture in which a mobile device API directly retrieves the data from a database through a program, for ex: IBM DB2 Everyplace (DB2e)


Tier 1
Mobile device API
Mobile device database API; J2ME or BREW; XML database or other database and the cached databases from remote server; OS (Windows CE or PalmOS or Symbian V6)
Tier 1
Database
Application / database on a mobile device
(a)
Tier 1
Mobile device API
Mobile device database API, J2ME or BREW; XML database or other database OS (Windows CE or PalmOS or Symbian V6)
Application / database on a mobile device
Tier 1
DB2e at device
Device database

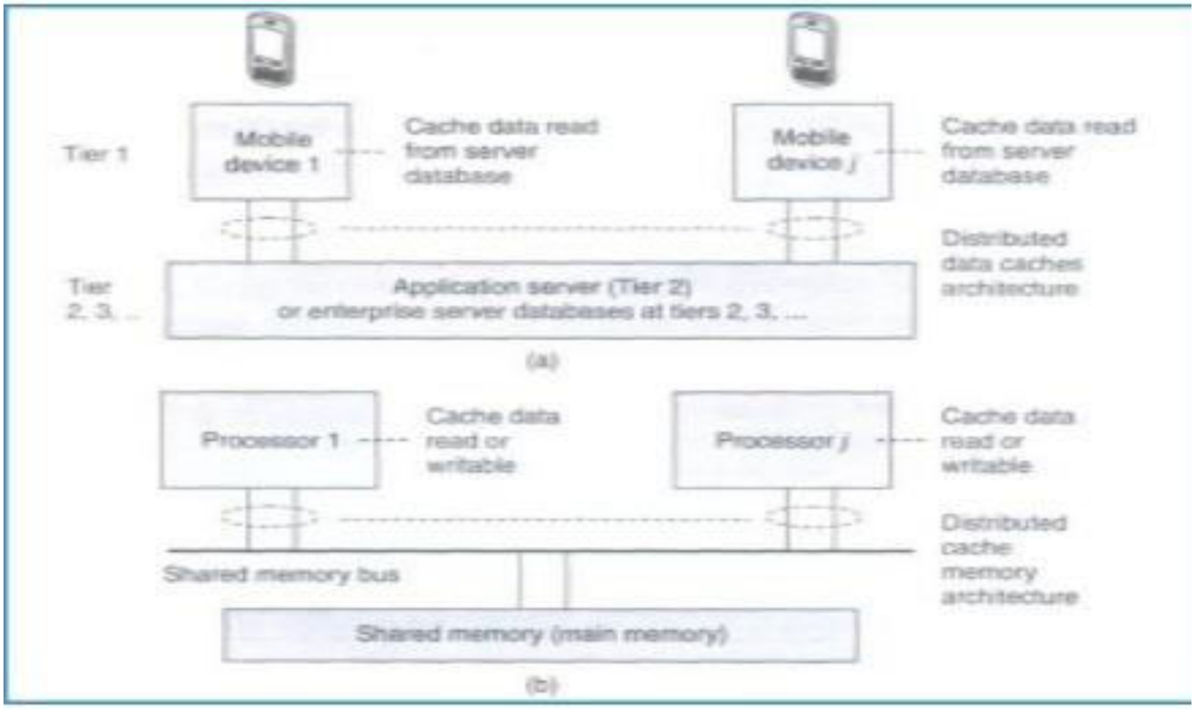
(a) API at mobile device sending queries and retrieving data from local database (Tier 1)
(b) API at mobile device retrieving data from database using DB2e (Tier 1)

FIGURE 5.1 DATABASE HOARDING

Both the two architectures belong to the class of one-tier database architecture because the databases are specific to a mobile device, not meant to be distributed to multiple devices, not synchronized with the new updates, are stored at the device itself.

Some examples are downloaded ringtones, music etc. IBM DB2 Everyplace (DB2e) is a relational database engine which has been designed to reside at the device. It supports J2ME and most mobile device operating systems.

DB2e synchronizes with DB2 databases at the synchronization, application, or enterprise server The database architecture shown below is for two-tier or multi-tier databases. Here, the databases reside at the remote servers and the copies of these databases are cached at the client tiers. This is known as client-server computing architecture.


Tier 1
Mobile device 1
Cache data read from server database
Mobile device j
Cache data read from server database
Distributed data caches architecture
Tier 2, 3, ...
Application server (Tier 2) or enterprise server databases at tiers 2, 3, ...
(a)
Processor 1
Cache data read or writable
Processor j
Cache data read or writable
Shared memory bus
Distributed cache memory architecture
Shared memory (main memory)
(b)

(a) Distributed data caches in mobile devices
(b) Similar architecture for a distributed cache memory in multiprocessor systems

FIGURE 5.2 DISTRIUTED DATA CACHES IN MOBILE DEVICES

A cache is a list or database of items or records stored at the device.

Databases are hoarded at the application or enterprise tier, where the database server uses business logic and connectivity for retrieving the data and then transmitting it to the device.

The server provides and updates local copies of the database at each mobile device connected to it.

The computing API at the mobile device (first tier) uses the cached local copy.

At first tier (tier 1), the API uses the cached data records using the computing architecture as explained above. From tier 2 or tier 3, the server retrieves and transmits the data records to tier 1 using business logic and synchronizes the local copies at the device. These local copies function as device caches.

The advantage of hoarding is that there is no access latency (delay in retrieving the queried record from the server over wireless mobile networks). The client device API has instantaneous data access to hoarded or cached data. After a device caches the data distributed by the server, the data is hoarded at the device. The disadvantage of hoarding is that the consistency of the cached data with the database at the server needs to be maintained.

Data Caching Hoarded copies of the databases at the servers are distributed or transmitted to the mobile devices from the enterprise servers or application databases. The copies cached at the devices are equivalent to the cache memories at the processors in a multiprocessor system with a shared main memory and copies of the main memory data stored at different locations.

5.2.1 CACHE ACCESS PROTOCOLS

A client device caches the pushed (disseminated) data records from a server.

Caching of the pushed data leads to a reduced access interval as compared to the pull (on demand) mode of data fetching.

Caching of data records can be-based on pushed 'hot records' (the most needed database records at the client device).

Also, caching can be based on the ratio of two parameters—access probability (at the device) and pushing rates (from the server) for each record. This method is called cost-based data replacement or caching.

Pre-fetching: Pre-fetching is another alternative to caching of disseminated data.

The process of perfecting entails requesting for and pulling records that may be required later.

The client device can pre-fetch instead of caching from the pushed records keeping future needs in view. Pre- fetching reduces server load. Further, the cost of cache-misses can thus be reduced.

The term 'cost of cache misses' refers to the time taken in accessing a record at the server in case that record is not found in the device database when required by the device API.

Caching Invalidation Mechanisms A cached record at the client device may be invalidated.

This may be due to expiry or modification of the record at the database server.

5.3 CACHE INVALIDATION MECHANISMS

Cache invalidation is a process by which a cached data item or record becomes invalid and thus unusable because of modification, expiry, or invalidation at another computing system or server.

Cache invalidation mechanisms are used to synchronize the data at other processors whenever the cache-data is written (modified) by a processor in a multiprocessor system, cache invalidation mechanisms are also active in the case of mobile devices having distributed copies from the server.

A cache consists of several records. Each record is called a cache-line, copies of which can be stored at other devices or servers.

The cache at the mobile devices or server databases at any 74 given time can be assigned one of four possible tags indicating its state—modified (after rewriting), exclusive, shared, and invalidated (after expiry or when new data becomes available) at any given instance.

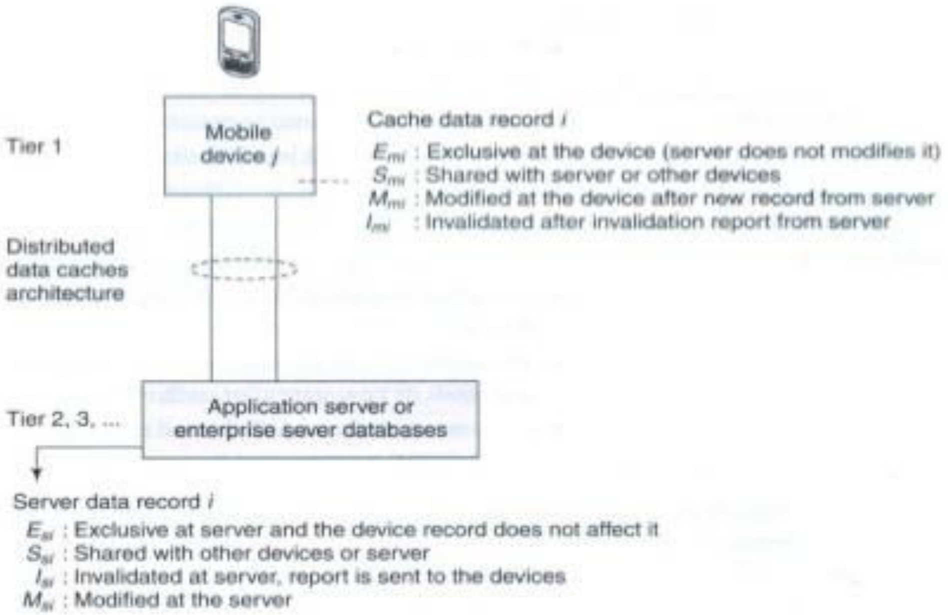
These four states are indicated by the letters M, E, S, and I, respectively (MESI). The states indicated by the various tags are as follows:

a) The E tag indicates the exclusive state which means that the data record is for internal use and cannot be used by any other device or server.

b) The S tag indicates the shared state which indicates that the data record can be used by others.

c) The M tag indicates the modified state which means that the device cache

d) The I tag indicates the invalidated state which means that the server database no longer has a copy of the record which was shared and used for computations earlier. The following figure shows the four possible states of a data record i at any instant in the server database and its copy at the cache of the mobile device j.


Tier 1
Mobile device j
Cache data record i
E_{mi} : Exclusive at the device (server does not modifies it)
S_{mi} : Shared with server or other devices
M_{mi} : Modified at the device after new record from server
I_{mi} : Invalidated after invalidation report from server
Distributed data caches architecture
Tier 2, 3, ...
Application server or enterprise sever databases
Server data record i
E_{si} : Exclusive at server and the device record does not affect it
S_{si} : Shared with other devices or server
I_{si} : Invalidated at server, report is sent to the devices
M_{si} : Modified at the server

Four possible states *(M, E, S,* or *I*) of a data record *I* at any instance at the server database and device *j* cache

FIGURE 5.3 CACHE INVALIDATION MECHANISMS

Another important factor for cache maintenance in a mobile environment is cache consistency (also called cache coherence).

This requires a mechanism to ensure that a database record is identical at the server as well as at the device caches and that only the valid cache records are used for computations.

Cache invalidation mechanisms in mobile devices are triggered or initiated by the server.

There are four possible invalidation mechanisms – Stateless asynchronous, stateless synchronous, stateful asynchronous and stateful synchronous.

5.3.1 STATELESS ASYNCHRONOUS:

A stateless mechanism entails broadcasting of the invalidation of the cache to all the clients of the server. The server does not keep track of the records stored at the device caches.

It just uniformly broadcasts invalidation reports to all clients irrespective o f whether the device cache holds that particular record or not.

The term 'asynchronous' indicates that the invalidation information for an item is sent as soon as its value changes.

The server does not keep the information of the present state (whether Emi, Mmi, Smi, or Imi) of a data-record in cache for broadcasting later. The server advertises the invalidation information only.

The client can either request for a modified copy of the record or cache the relevant record when data is pushed from the server.

The server advertises as and when the corresponding data-record at the server is invalidated and modified (deleted orreplaced).

The advantage of the asynchronous approach is that there are no frequent, unnecessary transfers of data reports, thus making the mechanism more bandwidth efficient.

The disadvantages of this approach are—

(a) every client device gets an invalidation report, whether thatclient requires that copy or not and

(b) client devices presume that as long as there is no invalidation report, the copy is valid for use in computations.

Therefore, even when there is link failure, the devices may be using the invalidated data and the server is unaware of state changes at the clients after it sends the invalidation report.

Stateless Synchronous This is also a stateless mode, i.e., the server has no information regarding the present state of data records at the device caches and broadcasts to all client devices.

However, unlike the asynchronous mechanism, here the server advertises invalidation information at periodic intervals as well as whenever the corresponding data-record at server is invalidated or modified.

This method ensures synchronization because even if the in-between period report is not detected by the device due to a link failure, the device expects the period end report of invalidation and if that is not received at the end of the period, then the device sends a request for the same (deleted or replaced). In case the client device does not get the periodic report due to link failure, it requests the server to send the report.

The advantage of the synchronous approach is that the client devices receive periodic information regarding invalidity (and thus validity) of the data caches. The periodic invalidation reports lead to greater reliability of cached data as update requests for invalid data can be sent to the server by the device-client. This also helps the server and devices maintain cache consistency through periodical exchanges.

The disadvantages of this mode of cache invalidation are—

(a) unnecessary transfers of data invalidation reports take place,

(b) every client device gets an advertised invalidation report periodically, irrespective of whether that client has a copy of the invalidated data or not, and

(c) during the period between two invalidation reports, the client .

Devices assume that, as long as there is no invalidation report, the copy is valid for use in computations. Therefore, when there are link failures, the devices use data which has been invalidated in the in-between period and the server is unaware of state changes at the clients after it sends the invalidation report.

5.3.2 STATEFUL ASYNCHRONOUS

The stateful asynchronous mechanism is also referred to as the AS (asynchronous stateful) scheme.

The term 'stateful' indicates that the cache invalidation reports are sent only to the affected client devices and not broadcasted to all.

The server stores the information regarding the present state (a record I can have its state as Emi, Mmi, Smi, or Imi) of each data-record at the client device caches.

This state information is stored in the home location cache (HLC) at the server. The HLC is maintained by an HA (home agent) software. This is similar to the HLR at the MSC in a mobile network.

The client device informs the HA of the state of each record to enable storage of the same at the HLC. The server transmits the invalidation information as and when the records are invalidated and it transmits only to the device-clients which are affected by the invalidation of data.

Based on the invalidation information, these device-clients then request the server for new or modified data to replace the invalidated data.

After the data records transmitted by the server modify the client device cache, the device sends information about the new state to the server so that the record of the cache-states at the server is also modified.

The advantage of the stateful asynchronous approach is that the server keeps track of the state of cached data at the client device. This enables the server to synchronize with the state of records at the device cache and keep the HLC updated. The stateful asynchronous mode is also advantageous in that only the affected clients receive the invalidation reports and other devices are not flooded with irrelevant reports.

The disadvantage of the AS scheme is that the client devices presume that, as long as there is no invalidation report, the copy is valid for use in computations.

Therefore, when there is a link failure, then the devices use invalidated data.

Stateful Synchronous: The server keeps the information of the present state (Emi, Mmi, Smi, or Imi) of data-records at the client-caches.

The server stores the cache record state at the home location cache (HLC) using the home agent (HA).

The server transmits the invalidation information at periodic intervals to the clients and whenever the data-record relevant to the client is invalidated or modified (deleted or replaced) at the server.

This method ensures synchronization because even if the in-between period report is not detected by the device due to a link failure, the device expects the period-end report of invalidation and if it is not received at the end of the period, then the device requests for the same.

The advantage of the stateful synchronous approach is that there are reports identifying invalidity (and thus, indirectly, of validity) of data caches at periodic intervals and that the server also periodically updates the client-cache states stored in the HLC.

This enables to synchronize with the client device when invalid data gets modified and becomes valid. Moreover, since the invalidation report is sent periodically, if a device does not receive an invalidation report after the specified period of time, it can request the server to send the report.

Each client can thus be periodically updated of any modifications at the server.

When the invalidation report is not received after the designated period and a link failure is found at the device, the device does not use the invalidated data.

Instead it requests the server for an invalidation update.

The disadvantage ofthe stateful synchronous approach is the high bandwidth requirement to enable periodic transmission of invalidation reportsto each device and updating requests from each client device.

Data Cache Maintenance in Mobile Environments Assume that a device needs a data-record during an application.

A request must be sent to the server for the data record (this mechanism is called pulling).

The time taken for the application software to access a particular record is known as access latency. Caching and hoarding the record at the device reduces access latency to zero.

Therefore, data cache maintenance is necessary in a mobile environment to overcome accesslatency. Data cache inconsistency means that data records cached for applications are not invalidated at the device when modified at the server but not modified at the device.

Data cache consistency can be maintained by the three methods given below:

I. Cache invalidation mechanism (server-initiated case): the server sends invalidation reports on invalidation of records (asynchronous) or at regular intervals (synchronous).

II. Polling mechanism (client-initiated case): Polling means checking from the server, the state of data record whether the record is in the valid, invalid, modified, or exclusive state.

Each cached record copy is polled whenever required by the application software during computation. If the record is found to be modified or invalidated, then the device requests for the modified data and replaces the earlier cached record copy.

III. Time-to-live mechanism (client-initiated case): Each cached record is assigned a TTL (time-to live).

- The TTL assignment is adaptive (adjustable) previous update intervals of that record. After the end of the TTL, the cached record copy is polled. If it is modified, then the device requests the server to replace the invalid cached record with the modified data.
- When TTL is set to 0, the TTL mechanism is equivalent to the polling mechanism. Web Cache Maintenance in Mobile Environments The mobile devices or their servers can be connected to a web server (e.g., traffic information server or train information server).
- Web cache at the device stores the web server data and maintains it in a manner similar to the cache maintenance for server data described above. If an application running at the device needs a data record from the web which is not at the web cache, then there is access latency. Web cache maintenance is necessary in a mobile environment to overcome access latency in downloading from websites due to disconnections.
- Web cache consistency can be maintained by two methods.

These are:

- Time-to-live (TTL) mechanism (client-initiated case): The method is identical to the one discussed for data cache maintenance.
- Power-aware computing mechanism (client-initiated case): Each web cache maintained at the device can also store the CRC (cyclic redundancy check) bits.

Assume that there are N cached bits and n CRC bits. N is much greater than n. Similarly at the server, n CRC bits are stored.

As long as there is consistency between the server and device records, the CRC bits at both are identical.

Whenever any of the records cached at the server is modified, the corresponding CRC bits at the server are also modified.

After the TTL expires or on- demand for the web cache records by the client API, the cached record CRC is polled and obtained from the website server.

If the n CRC bits at server are found to be modified and the change is found to be much higher than a given threshold (i.e., a significant change), then the modified part of the website hypertext or database is retrieved by t he client device for use by the API. However, if the change is minor, then the API uses the previous cache. Since N » n, the power dissipated in the web cache maintenance method (in which invalidation reports and all invalidated record bits are transmitted) is much greater than that in the present method (in which the device polls for the significant change in the CRC bits at server and the records are transmitted only when there is a significant change in the CRC bits).

5.4 CLIENT-SERVER COMPUTING

Client-server computing is a distributed computing architecture, in which there are two types of nodes, i.e., the clients and the servers.

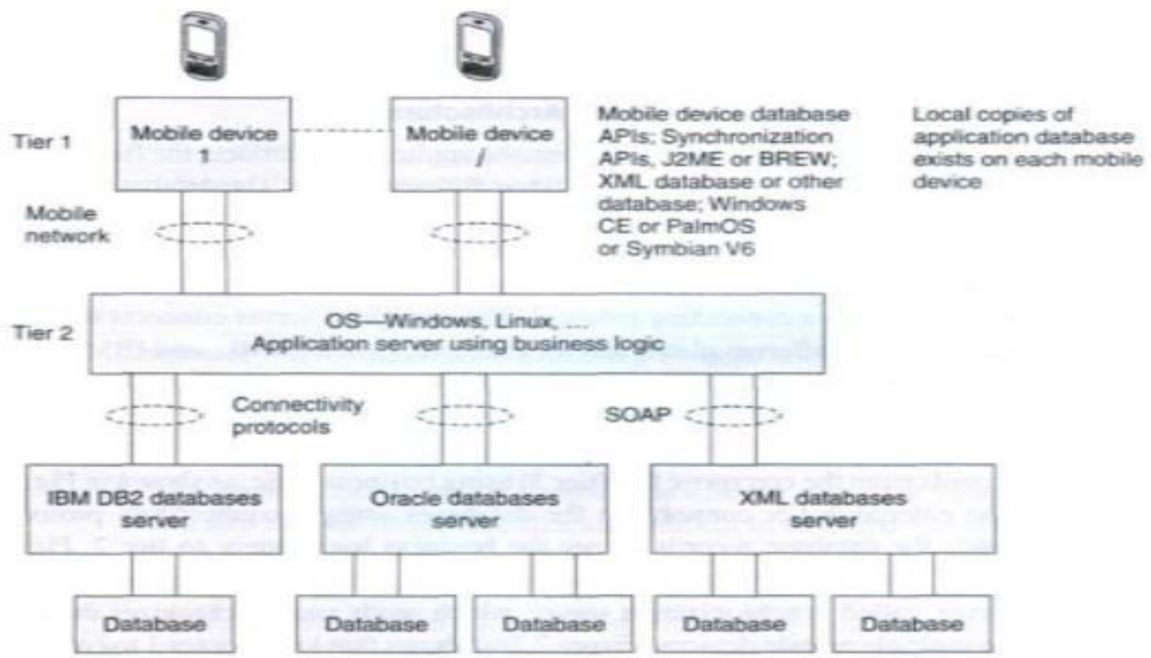
A server is defined as a computing system, which responds to requests from one or more clients.

A client is defined as a computing system, which requests the server for a resource or for executing a task.

The client can either access the data records at the server or it can cache these records at the client device.

The data can be accessed either on client request or through broadcasts or distribution from the server. The client and the server can be on the same computing system or on different computing systems. Client-server computing can have N-tier architecture (N= 1, 2 ...). When the client and the server are on the same computing system then the number of tiers,

N =1. When the client and the server are on different computing systems on the network, then N = 2. A command interchange protocol (e.g., HTTP) is used for obtaining the client requests at the server or the server responses at the client. The following subsections describe client-server computing in 2, 3, or N-tier architectures. Each tier connects to the other with a connecting, synchronizing, data, or command interchange protocol. The following figure shows the application server at the second tier.


Tier 1
Mobile device 1
Mobile device j
Mobile device database APIs: Synchronization APIs, J2ME or BREW; XML database or other database; Windows CE or PalmOS or Symbian V6
Local copies of application database exists on each mobile device
Mobile network
Tier 2
OS—Windows, Linux, ...
Application server using business logic
Connectivity protocols
SOAP
IBM DB2 databases server
Oracle databases server
XML databases server
Database
Database
Database
Database
Database

Multimedia file server in two-tier client-server computing architecture (local copies 1 to j of image and voice hoarding at the mobile devices)

FIGURE 5.4 CLIENT - SERVER COMPUTING – TWO TIER

The data records are retrieved using business logic and a synchronization server in the application server synchronizes with the local copies at the mobile devices.

Synchronization means that when copies of records at the server-end are modified, the copies cached at the client devices should also be accordingly modified.

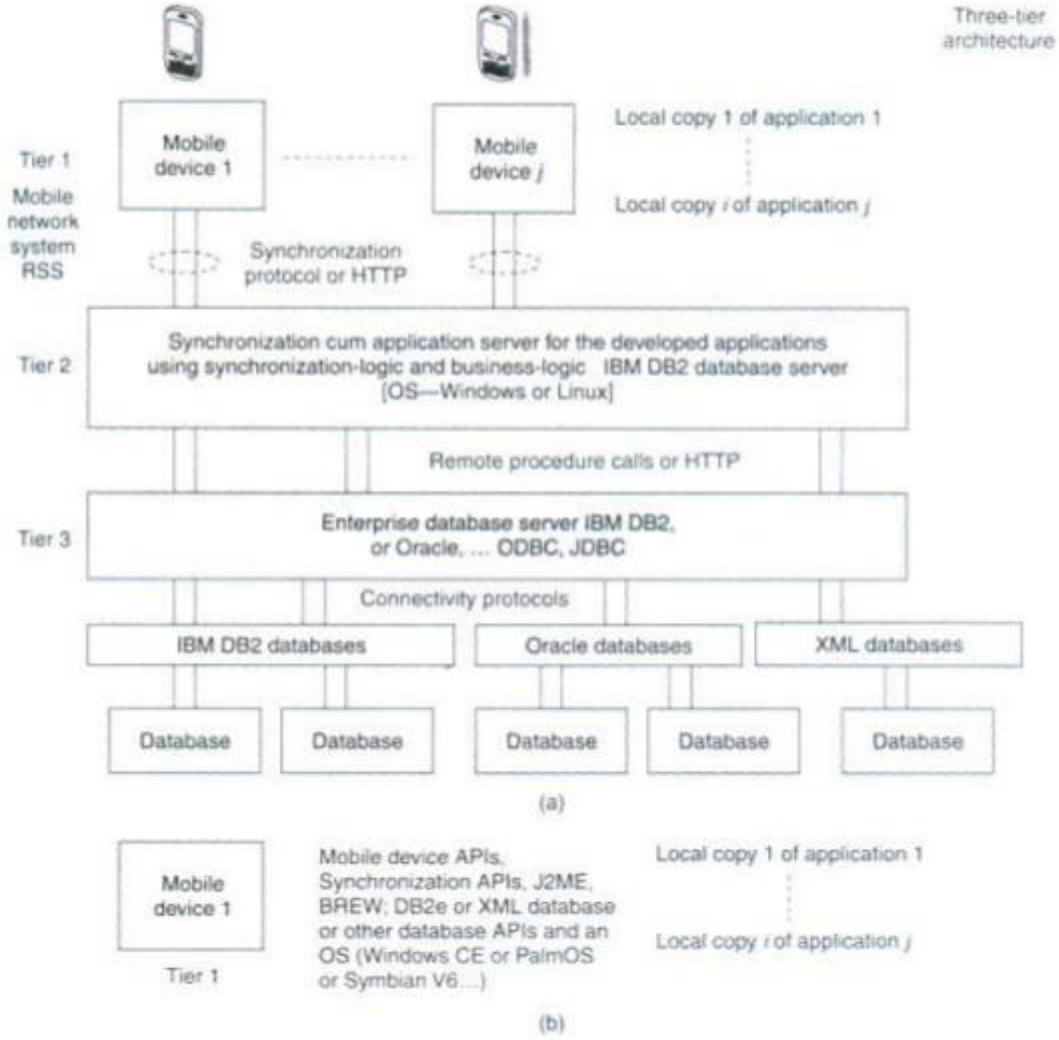
The APIs are designed independent of hardware and software platforms as far as possible as different devices may have different platforms.

5.4.1 Three-tier Client-Server Architecture

In a three-tier computing architecture, the application interface, the functional logic, and the database are maintained at three different layers.

The database is associated with the enterprise server tier (tier 3) and only local copies of the database exist at mobile devices.

The database connects to the enterprise server through a connecting protocol. The enterprise server connects the complete databases on different platforms, for example, Oracle, XML, and IBM DB2.


Three-tier architecture
Tier 1
Mobile network system RSS
Mobile device 1
Mobile device j
Local copy 1 of application 1
Local copy i of application j
Synchronization protocol or HTTP
Tier 2
Synchronization cum application server for the developed applications using synchronization-logic and business-logic IBM DB2 database server [OS—Windows or Linux]
Remote procedure calls or HTTP
Tier 3
Enterprise database server IBM DB2, or Oracle, ... ODBC, JDBC
Connectivity protocols
IBM DB2 databases
Oracle databases
XML databases
Database
Database
Database
Database
Database
(a)
Mobile device 1
Tier 1
Mobile device APIs, Synchronization APIs, J2ME, BREW; DB2e or XML database or other database APIs and an OS (Windows CE or PalmOS or Symbian V6...)
Local copy 1 of application 1
Local copy i of application j
(b)

(a) Local copies 1 to j of database hoarded at the mobile devices using an enterprise database connection synchronization server, which synchronizes the required local copies for application with the enterprise database server (b) Mobile device with J2ME or BREW platform, APIs an OS and database having local copies

FIGURE 5.5 THREE-TIER CLIENT-SERVER ARCHITECTURE

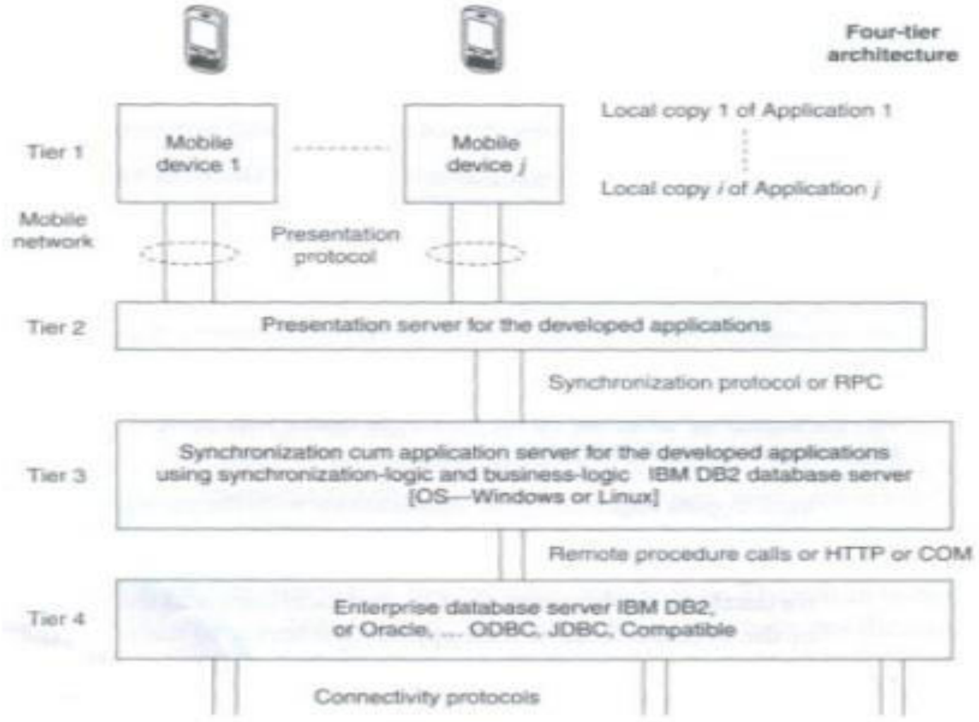
Data records at tier 3 are sent to tier 1 as shown in the figure through a synchronization-cum application server at tier 2.

The synchronization-cum-application server has synchronization and server programs, which retrieves data records from the enterprise tier (tier 3) using business logic.

There is an in-between server, called synchronization server, which sends and synchronizes the copies at the multiple mobile devices.

The figure shows that local copies 1 to j of databases are hoarded at the mobile devices for the applications 1 to j. 81 N-tier Client-Server Architecture When N is greater than 3, then the database is presented at the client through in-between layers.

For example, the following figure shows a four-tier architecture in which a client device connects to a data-presentation server at tier 2.


Four-tier architecture
Tier 1
Mobile device 1
Mobile device j
Local copy 1 of Application 1
Local copy j of Application j
Mobile network
Presentation protocol
Tier 2
Presentation server for the developed applications
Synchronization protocol or RPC
Tier 3
Synchronization cum application server for the developed applications using synchronization-logic and business-logic IBM DB2 database server [OS—Windows or Linux]
Remote procedure calls or HTTP or COM
Tier 4
Enterprise database server IBM DB2, or Oracle, ... ODBC, JDBC, Compatible
Connectivity protocols

4-tier architecture in which a client device connects to a data-presentation server

FIGURE 5.6 FOUR-TIER CLIENT-SERVER ARCHITECTURE

The presentation server then connects to the application server tier 3.

The application server can connect to the database using the connectivity protocol and to the multimedia server using Java or XML API at tier 4.

The total number of tiers can be counted by adding 2 to the number ofin-between servers between the database and the client device.

The presentation, application, and enterprise servers can establish connectivity using RPC, Java RMI, JNDI, or HOP. These servers may also use HTTP or HTTPS in case the server at a tier j connects to tier j+1 using the Internet.

5.5 CLIENT-SERVER COMPUTING WITH ADAPTATION

The data formats of data transmitted from the synchronization server and those required for the device database and device APIs are different in different cases, there are two adapters at a mobile device an adapter for standard data format for synchronization at the mobile device and another adapter for the backend database copy, which is in a different data format for the API at the mobile device.

An adapter is software to get data in one format or data governed by one protocol and convert it to another format or to data governed by another protocol.

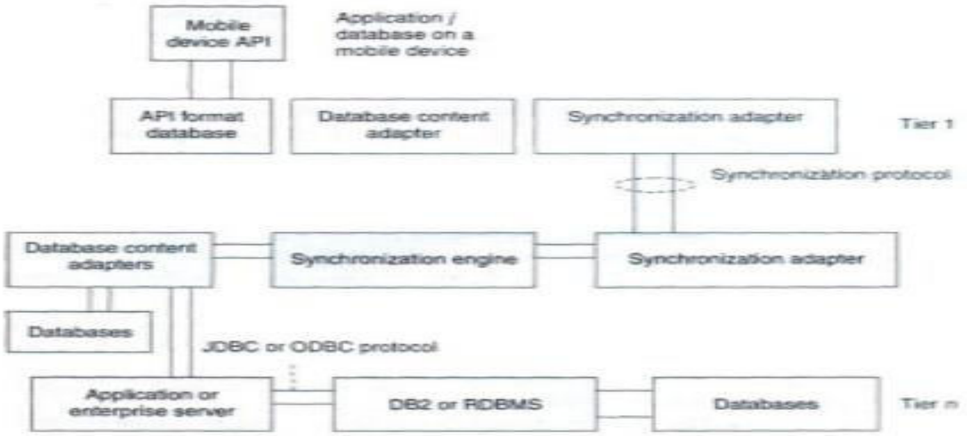


Figure shows an API, database, and adapters at a mobile device and the adapters at the synchronization, application, or enterprise servers. Here the adapters are an addition used for interchange between standard data formats and data formats for the API.

FIGURE 5.7 CLIENT-SERVER COMPUTING WITH ADAPTATION

5.6 CONTEXT-AWARE COMPUTING

The context of a mobile device represents the circumstances, situations, applications, or physical environment under which the device is being used. For example, let us assume that a mobile phone is operating in a busy, congested area. If the device is aware of the surrounding noises, then during the conversation, it can raise the speaker volume by itself and when the user leaves that area, the device can again reduce the volume.

Also, if there is intermittent loss of connectivity during the conversation, the device can introduce background noises by itself so that the user does not feel discomfort due to intermittent periods of silence.

This is one example in which the computing system is aware of the surrounding physical context in which the conversation is taking place.

A context-aware computing system is one which has user, device, and application interfaces such that, using these, the system remains aware of the past and present surrounding situations, circumstances, or actions such as the present mobile network, surrounding devices or systems, changes in the state of the connecting network, physical parameters such as present time of the day, presently remaining memory and battery power, presently available nearest connectivity, past sequence of actions of the device user, past sequence of application or applications, and previously cached data records, and takes these into account during computations.

Context The term 'context' refers to the interrelated conditions in which a collection of elements, records, components, or entities exists or occurs.

Each message, data record, element, or entity has a meaning. But when these are considered along with the conditions that relate them to each other and to the environment, then they have a wider meaning.

Understanding of the context in which a device is meant to operate, results in better, more efficient computing strategies.

5.6.1 STRUCTURAL CONTEXT

To explain what is meant by structural context let us consider a few examples of records with structural arrangement.

The fields name, address, experience, and achievements of a person have an individual meaning. However, when put together to form a resume, these fields acquire a significance beyond their individual meanings.

This significance comes from the fact that they are now arranged in a structure which indicates an interrelationship between them. The structure of the resume includes the records and their interrelationship and thus defines a context for these records. Whereby, the records have a new meaning in the context of the resume (which is a structure).

Contexts such as the context of the resume of an individual are called structural contexts.

The context in such cases comes from the structure or format in which the records in a database are organized.

- Consider another example, this time that of a line in a telephone directory.
- It has a sequence of records including a name, an address, and a 10-digit number.
- Each record has an individual meaning. But a collection of these records shows an interrelationship and thus defines a context, i.e., a telephone directory.

5.6.2 IMPLICIT AND EXPLICIT CONTEXTS CONTEXT

Implicit context provides for omissions by leaving out unimportant details, takes independent world-views, and performs alterations in order to cope with incompatible protocols, interfaces, or APIs by transparently changing the messages.

Implicit context uses history to examine call history, to manage omissions, or to determine recipients and performs contextual message alterations.

Consider the context 'Contacts' which has a set of contacts. The name, e-mail ID, and telephone number are implicit in a contact in the context Contacts.

When a computing device uses a contact to call a number using a name record, the system takes independent view and uses the telephone number implicitly and deploys CDMA or GSM protocols for connecting to the mobile network implicitly.

Context CDMA is implicit in defining the records 'Contact'. When a computing system uses a contact to send an e-mail using a name record, the use of the e-mail ID record is implicit to the system and the use of SMTP (simple mail transfer protocol) or other mail sending protocol is also implicit.

Name gets automatically altered to e-mail ID when the context is sending of e-mail.

The implicit context also copes with incompatible interfaces, for example, mail sending and receiving software handling data in different formats. Consider the context document.

In document context, the contact or personal information is an extrinsic context. In context to processing of a Document, the existence of document author contact information is extrinsic.

The contacts context is imported into the document context to establish interrelationship between document and contact.

5.7 CONTEXT-AWARE COMPUTING

Context-aware computing leads to application-aware computing.

This is so because the APIs are part of the context (implicit or explicit contexts). For example, if context is a contact, the phone talk application will adapt itself to use of the telephone number from the 'contact' and to the use of GSM or CDMA communication.

- Use of context in computing helps in reducing possibility of errors. It helps in reducing the ambiguity in the action(s).
- It helps in deciding the expected system response on computations.
- For example, if name is input in personal biodata context, then the address, experience, and achievements, which correspond to that name, are also required for computations.
- This is because all four are related and needed in biodata context.
- When name is input in telephone directory context, then the address and phone number, which correspond to that name, are also required for computations.
- This is because all three are related in context to telephone directory.

The name in two different contexts (personal biodata and telephone directory) during computations needs computations to perform different actions.

Context Types in Context-aware Computing

The five types of contexts that are important in context-aware computing are

- Physical context
- Computing context
- User context
- Temporal context
- Structural context

5.7.1 PHYSICAL CONTEXT

The context can be that of the physical environment. The parameters for defining a physical context are service disconnection, light level, noise level, and signal strength. For example, if there is service disconnection during a conversation, the mobile device can sense the change in the physical conditions and it interleaves background noise so that the listener does not feel the effects of the disconnection.

Also, the mobile device can sense the light levels, so during daytime the display brightness is increased and during night time or in poor light conditions, the device display brightness is reduced.

The physical context changes and the device display is adjusted accordingly.

5.7.2 COMPUTING CONTEXT

The context in a context-aware computing environment may also be computing context.

Computing context is defined by interrelationships and conditions of the network connectivity protocol in use (Bluetooth, ZigBee, GSM, GPRS, or CDMA), bandwidth, and available resources. Examples of resources are keypad, display unit, printer, and cradle.

A cradle is the unit on which the mobile device lies in order to connect to a computer in the vicinity. Consider a mobile device lying on a cradle.

It discovers the computing context and uses ActiveSync to synchronize and download from the computer.

When a mobile device lies in the vicinity of a computer with a Bluetooth interface, it discovers another computing context resource and uses wireless Bluetooth for connecting to the computer.

When it functions independently and connects to a mobile network, it discovers another computing context and uses a GSM, CDMA, GPRS, or EDGE connection.

The response of the system is as per the computing context, i.e., the network connectivity protocol.

5.7.3 USER CONTEXT

The user context is defined user location, user profiles, and persons near the user. Reza B 'Far defines user-interfaces context states as follows—'within the realm of user interfaces, we can define context as the sum of the relationships between the user interface components, the condition of the user, the primary intent of the system, and all of the other elements that allow users and computing systems to communicate.

5.7.4TEMPORAL CONTEXT

Temporal context defines the interrelation between time and the occurrence of an event or action. A group of interface components have an intrinsic or extrinsic temporal context. For example, assume that at an instant the user presses the switch for dial in a mobile device.

At the next instant the device seeks a number as an input. Then user will consider it in the context of dialing and input the number to be dialed. Now, assume that at another time the user presses the switch to add a contact in the mobile device.

- The device again prompts the user to enter a number as an input.
- The user will consider it in context of the number to be added in the contacts and stored in the device for future use.
- The device then seeks the name of the contact as the input. Response of the system in such cases is as per the temporal context.
- The context for the VUI (voice user interface) elements also defines a temporal context (depending upon the instances and sequences in which these occur).

5.7.5 STRUCTURAL CONTEXT

Structural context defines a sequence and structure formed by the elements or records. Graphic user interface (GUI) elements have structural context. Structural context may also be extrinsic for some other type of context.

Interrelation among the GUI elements depends on structural positions on the display screen. When time is the context, then the hour and minute elements.

Transaction Models

A transaction is the execution of interrelated instructions in a sequence for a specific operation on a database.

Database transaction models must maintain data integrity and must enforce a set of rules called ACID rules.

These rules are as follows:

Atomicity: All operations of a transaction must be complete. In case, a transaction cannotϖ be completed; it must be undone (rolled back).

Operations in a transaction are assumed to be one indivisible unit (atomic unit).

Consistency: A transaction must be such that it preserves the integrity constraints andϖ follows the declared consistency rules for a given database.

Consistency means the data is not in a contradictory state after the transaction.

Isolation: If two transactions are carried out simultaneously, there should not be anyϖ interference between the two. Further, any intermediate results in a transaction should be invisible to any other transaction.

Durability: After a transaction is completed, it must persist and cannot be aborted orϖ discarded. For example, in a transaction entailing transfer of a balance from account A to account B, once the transfer is completed and finished there should be no roll back. Consider a base class library included in Microsoft.NET.

It has a set of computer software components called ADO.NET (ActiveX Data Objects in .NET).

These can be used to access the data and data services including for access and modifying the data stored in relational database systems. The ADO.NET transaction model permits three transaction commands:

1**. Begin Transaction**: It is used to begin a transaction. Any operation after Begin Transaction is assumed to be a part of the transaction till the Commit Transaction command or the Rollback Transaction command.

An example of a command is as follows:

connectionA.open();

transA = connectionA.BeginTransaction();

Here connectionA and transA are two distinct objects.

2. **Commit:** It is used to commit the transaction operations that were carried out after the BeginTransaction command and up to this command.

An example of this is transA.Commit();

All statements between BeginTransaction and commit must execute automatically.

3**. Rollback**: It is used to rollback the transaction in case an exception is generated after the BeginTransactioncommand is executed.

A DBMS may provide for auto-commit mode. Auto-commit mode means the transaction finished automatically even if an error occurs in between.

5.7.5.1 QUERY PROCESSING

It is the step by step process of breaking the high level language into low level language which machine can understand and perform the requested action for user.

Query processor in the DBMS performs this task.

Above diagram depicts how a query is processed in the database to show the result.

When a query is submitted to the database, it is received by the query compiler.

It then scans the query and divides it into individual tokens.

Once the tokens are generated, they are verified for their correctness by the parser.

Then the tokenized queries are transformed into different possible relational expressions, relational trees and relational graphs (Query Plans).

Query optimizer then picks them to identify the best query plan to process.

It checks in the system catalog for the constraints and indexes and decides the best query plan. It generates different execution plans for the query plan.

The query execution plan then decides the best and optimized execution plan for execution.

The command processor then uses this execution plan to retrieve the data from the database and returns the result. This is an overview of how a query processing works. Let us see in detail in below.

There are four phases in a typical query processing .

- Parsing and Translation
- Query Optimization
- Evaluation or query code generation
- Execution in DB's runtime processor.

Parsing and Translation

- This is the first step of any query processing.
- The user typically writes his requests in SQL language.
- In order to process and execute this request, DBMS has to convert it into low level – machine understandable language.
- Any query issued to the database is first picked by query processor.
- It scans and parses the query into individual tokens and examines for the correctness of query.
- It checks for the validity of tables / views used and the syntax of the query.
- Once it is passed, then it converts each tokens into relational expressions, trees and graphs. These are easily processed by the other parsers in the DBMS.

Let us try to understand these steps using an example. Suppose user wants to see the student details who are studying in DESIGN_01 class.

If the users say 'Retrieve Student details who are in DESIGN_01 class', the DBMS will not understand.

Hence DBMS provides a language - SQL which both user and DBMS can understand and communicate with each other.

. So the user would write his request in SQL as below:

```
SELECT STD_ID, STD_NAME, ADDRESS, DOB
   FROM STUDENT s, CLASS c
 WHERE s.CLASS_ID = c.CLASS_ID
    AND c.CLASS_NAME = 'DESIGN_01';
```

The query processor scans the SQL query submitted and divides into individual meaningful tokens.

In our example, 'SELECT * FROM', 'STUDENT s', 'CLASS c', 'WHERE', 's.CLASS_ID = c.CLASS_ID', 'AND' and 'c.CLASS_NAME = 'DESIGN_01'' are the different tokens.

These tokenized forms of query are easily used by the processor to further processing. It fires query on the data dictionary tables to verify if the tables and columns in these tokens exists or not. If they are not present in the data dictionary, then the submitted query will be failed at this stage itself.

Else it proceeds to find if the syntax used in the query are correct.

Note that it does not validate if DESIGN_01 exists in the table or not, it verifies if 'SELECT * FROM', 'WHERE', 's.CLASS_ID = c.CLASS_ID', 'AND' etc have SQL defined syntaxes. Once it validates the syntaxes, it converts them into a relational algebra, relational tree and graph representations.

These are easily understood and handled by the optimizer for further processing.

Above query can be converted into any of the two forms of relation algebra as below.

First query identifies the students in DESIGN_01 class first and then selects only the requested columns from it.

Another query first selects requested columns from the STUDENT table and then filters it for DESIGN_01. Both of them results in same result.

∏ STD_ID, STD_NAME, ADDRESS, DOB (σ CLASS_NAME = 'DESIGN_01' (STUDENT ∞CLASS))

or

σ CLASS_NAME = 'DESIGN_01' (∏ STD_ID, STD_NAME, ADDRESS, DOB (STUDENT ∞CLASS))

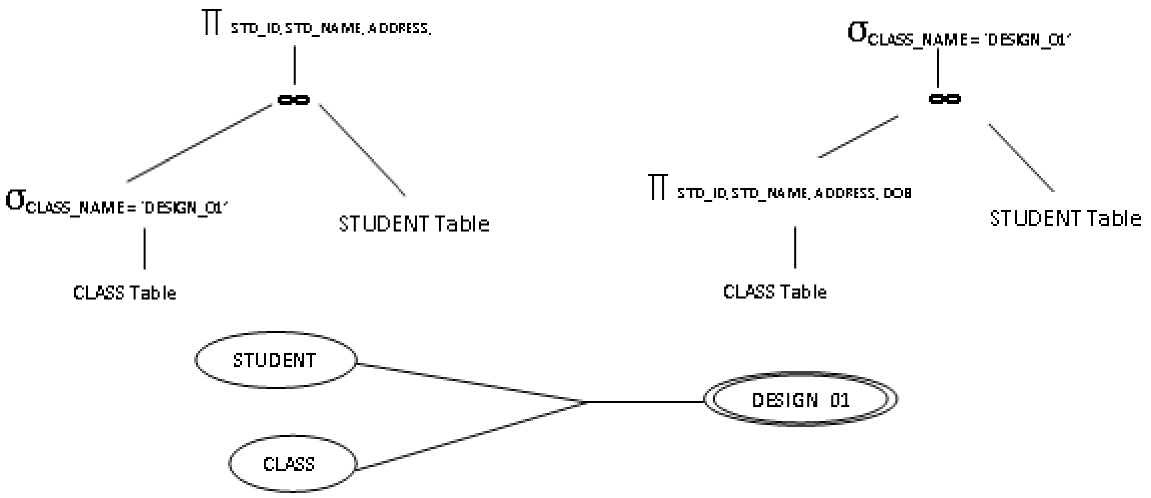

∏ STD_ID, STD_NAME, ADDRESS,
∞
σ CLASS_NAME = 'DESIGN_01'
STUDENT Table
CLASS Table
σ CLASS_NAME = 'DESIGN_01'
∞
∏ STD_ID, STD_NAME, ADDRESS, DOB
STUDENT Table
CLASS Table
STUDENT
CLASS
DESIGN_01

FIGURE 5.7 QUERY PROCESSOR

Query processor then applies the rules and algorithms on these relational structures to represent more efficient and powerful structures which are used only by the DBMS.

These structures are based on the mappings between the tables, joins used, cost of execution algorithm of these queries.

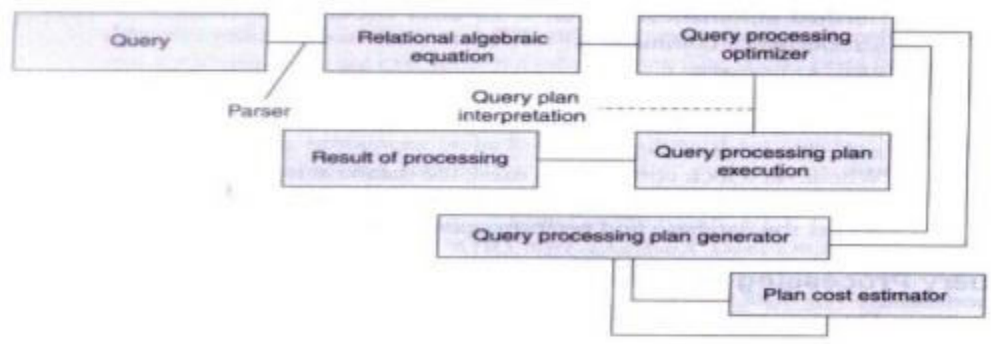
It determines which structure – selecting and then projecting or projecting and then selecting – is the efficient way of processing, when to apply filters etc.

In the third step of query processing, the best structure and plan selected by the optimizer is selected and executed.

It digs into the database memory to retrieve the records based on the plan. Sometimes it process and compiles the query and keeps it in DB to use it in the runtime DB processor.

The result is then returned to the user. This is the overall step processed by the DBMS when a simple to complex query is fired.

The time taken by all these process will be in fraction of seconds. But ideal optimization and selection of execution path will make the query even faster


Query
Relational algebraic equation
Query processing optimizer
Parser
Query plan interpretation
Result of processing
Query processing plan execution
Query processing plan generator
Plan cost estimator

Query processing architecture

FIGURE 5.8 STRUCTURAL CONTEXT

Π represents the projection operation, σ the selection operation, and Λ, the AND operation. It is clear that the second set of operations in query processing is less efficient than the first.

5.7.5 Query decomposition of the first set gives efficiency.

Decomposition is done by

(i) analysis,

(ii) conjunctive and disjunctive normalization, and

(iii) semantic analysis.

Efficient processing of queries needs optimization of steps for query processing. Optimization can be based on cost (number of micro-operations in processing) by evaluating the costs of sets of equivalent expressions.

Optimization can also be based on a heuristic approach consisting of the following steps: perform the selection steps and projection steps as early as possible and eliminate duplicate operations.

The query optimizer employs

- query processing plan generator and
- query processing cost estimator to provide an efficient plan for query processing.

Data Recovery Process Data is non-recoverable in case of media failure, intentional attack on the database and transactions logging data, or physical media destruction.

However, data recovery is possible in other cases. Figure below shows recovery management architecture.

It uses a recovery manager, which ensures atomicity and durability. Atomicity ensures that an uncommitted but started transaction aborts on failure and aborted transactions are logged in log file.

Durability ensures that a committed transaction is not affected by failure and is recovered.

Stable state databases at the start and at the end of transactions reside in secondary storage.

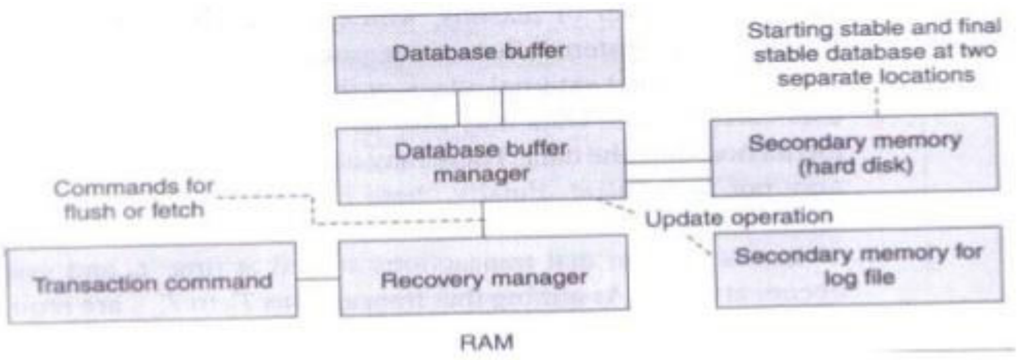
Transaction commands are sent to the recovery manager, which sends fetch commands to the database manager.

The database manager processes the queries during the transaction and uses a database buffer.

The recovery manager also sends the flush commands to transfer the committed transactions and database buffer data to the secondary storage.

The recovery manager detects the results of operations.

It recovers lost operations from the secondary storage. Recovery is by detecting the data lost during the transaction.


Database buffer
Starting stable and final stable database at two separate locations
Database buffer manager
Secondary memory (hard disk)
Commands for flush or fetch
Update operation
Secondary memory for log file
Transaction command
Recovery manager
RAM

Recovery Management Architecture

FIGURE 5.9 Query Decomposition Of The First Set Gives Efficiency

The recovery manager uses a log file, which logs actions in the following manner:

- Each instruction for a transaction for update (insertion, deletion, replacement, and addition) must be logged.
- Database read instructions are not logged
- Log files are stored at a different storage medium.
- Log entries are flushed out after the final stable state database is stored.

Each logged entry contains the following fields. transaction type (begin, commit, or rollback transaction)¬ transaction ID¬ operation-type¬ object on which the operation is performed¬ Pre-operation and post-operation values of the object.¬ A procedure called the Aries algorithm is also used for recovering lost data.

The basic steps of the algorithm are:

- Analyze from last checkpoint and identify all dirty records (written again after operation restarted) in the buffer.
- Redo all buffered operations logged in the update log to finish and make finalpage.
- Undo all write operations and restore pre-transaction values.

The recovery models used in data recovery processes are as follows:

- The full recovery model creates back up of the database and incremental backup of the changes. All transactions are logged from the last backup taken for the database.

- The bulk logged recovery model entails logging and taking backup of bulk data record operations but not the full logging and backup. Size of bulk logging is kept to the minimum required.
- This improves performance. We can recover the database to the point of failure by restoring the database with the bulk transaction log file backup.
- This is unlike the full recovery model in which all operations are logged.
- The simple recovery model prepares full backups but the incremental changes are not logged.

We can recover the database to the most recent backup of the given database.

Ongoing advances in communications including the proliferation of internet, development of mobile and wireless networks, high bandwidth availability to homes have led to development of a wide range of new-information centered applications.

Many of these applications involve data dissemination, i.e. delivery of data from a set of producers to a larger set of consumers.

Data dissemination entails distributing and pushing data generated by a set of computing systems or broadcasting data from audio, video, and data services.

The output data is sent to the mobile devices.

- A mobile device can select, tune and cache the required data items, which can be used for application programs.
- Efficient utilization of wireless bandwidth and battery power are two of the most important problems facing software designed for mobile computing.
- Broadcast channels are attractive in tackling these two problems in wireless data dissemination.
- Data disseminated through broadcast channels can be simultaneously accessed by an arbitrary number of mobile users, thus increasing the efficiency of bandwidth usage.

5.8 QUALITY OF SERVICE

Quality of service (**QoS**) is the description or measurement of the overall performance of a service, such as a telephony or computer network or a cloud computing service, particularly the performance seen by the users of the network. To quantitatively measure quality of service, several related aspects of the network service are often considered, such as packet loss, bit rate, throughput, transmission delay, availability, jitter, etc.

In the field of computer networking and other packet-switched telecommunication networks, quality of service refers to traffic prioritization and resource reservation control mechanisms rather than the achieved service quality. Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

Quality of service is particularly important for the transport of traffic with special requirements. In particular, developers have introduced Voice over IP technology to allow computer networks to become as useful as telephone networks for audio conversations, as well as supporting new applications with even stricter network performance requirements.

In the field of telephony, quality of service was defined by the ITU in 1994. Quality of service comprises requirements on all the aspects of a connection, such as service response time, loss, signal-to-noise ratio, crosstalk, echo, interrupts, frequency response, loudness levels, and so on.

A subset of telephony QoS is grade of service (GoS) requirements, which comprises aspects of a connection relating to capacity and coverage of a network, for example guaranteed maximum blocking probability and outage probability.

In the field of computer networking and other packet-switched telecommunication networks, teletraffic engineering refers to traffic prioritization and resource reservation control mechanisms rather than the achieved service quality. Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

For example, a required bit rate, delay, delay variation, packet loss or bit error rates may be guaranteed. Quality of service is important for real-time streaming multimedia applications such as voice over IP, multiplayer online games and IPTV, since these often require fixed bit rate and are delay sensitive. Quality of service is especially important in networks where the capacity is a limited resource, for example in cellular data communication.

A network or protocol that supports QoS may agree on a traffic contract with the application software and reserve capacity in the network nodes, for example during a session establishment phase. During the session it may monitor the achieved level of performance, for example the data rate and delay, and dynamically control scheduling priorities in the network nodes. It may release the reserved capacity during a tear down phase.

A best-effort network or service does not support quality of service. An alternative to complex QoS control mechanisms is to provide high quality communication over a best-effort network by over-provisioning the capacity so that it is sufficient for the expected peak traffic load. The resulting absence of network congestion reduces or eliminates the need for QoS mechanisms.

QoS is sometimes used as a quality measure, with many alternative definitions, rather than referring to the ability to reserve resources. Quality of service sometimes refers to the level of quality of service, i.e. the guaranteed service quality. High QoS is often confused with a high level of performance, for example high bit rate, low latency and low bit error rate.

QoS is sometimes used in application layer services such as telephony and streaming video to describe a metric that reflects or predicts the subjectively experienced quality. In this context, QoS is the acceptable cumulative effect on subscriber satisfaction of all imperfections affecting the service. Other terms with similar meaning are the quality of experience(QoE), mean opinion score (MOS), perceptual speech quality measure (PSQM) and perceptual evaluation of video quality (PEVQ).

TWO MARKS QUESTIONS AND ANSWERS

UNIT-I

1. What is mobility?

- Between different geographical locations
- Between different networks
- Between different communication devices
- Between different applications
- A device that moves Between different geographical locations
- Between different networks

2. What are two different kinds of mobility?

User Mobility: It refers to a user who has access to the same or similar telecommunication Services as different places.

Device portability: Many mechanisms in the network and inside the device have to make sure that Communication is still possible while the device is moving.

3. Find out the characteristics while device can thus exhibit during communication.

- Fixed and Wired
- Mobile and Wired
- Fixed and Wireless
- Mobile and Wireless

4. What are applications of mobile computing?

- Vehicles
- Business
- Replacement of wired networks
- Infotainment
- Location dependents services
- Mobile and wireless devices

5. What are the obstacles in mobile communications?

- Interference

- Regulations and spectrum
- Low Bandwidth
- High delays, large delay variation
- Lower security, simpler to attack
- Shared Medium
- Adhoc-networks

6. Give the information in SLM?

- Card type serial no list of subscribed services
- Personal Identity Number(PIN)
- pin Unlocking key(PUK)
- An Authentication key(KI)

7. What are the Advantages of wireless LAN?

- Flexibility
- planning
- Design
- Robustness

8. Mention some of the disadvantages of WLANS?

- Quality of service
- Proprietary solutions
- Restrictions
- safety and security

9. Describe about MAC layer in DECT architecture?

The medium access control (MAC) layer establishes, maintains and releases channels for higher layers by activating and deactivating physical channels. MAC multiplexes several logical Channels onto physical channels. Logical channels exist for signaling network control, user data Transmission, paging or sending broadcast messages. Additional services offered include Segmentation/reassembly of packets and error control/error correction.

10. What are the basic tasks of the MAC layer?

Medium access Fragmentation of user data Encryption

11. What are the basic services provided by the MAC layer?

Asynchronous data service data service (mandatory) time-bounded service (optional)

12. What are the techniques used for MAC management?

- Synchronization
- Power
- Management
- Roaming
- Management information base(MIB)

13. Describe about MAC layer in DECses.6Tarchitecture?

The medium access control (MAC) layer establishes, maintains and releases channels for higher layers by activating and deactivating physical channels. MAC multiplexes several Logical channels onto physical channels. Logical channels exist for signaling network control, User data transmission, paging or sending broadcast messages. Additional services offered Include segmentation/reassembly of packets and error control/error correction.

14. Define hidden terminal?

The transmission range of A reaches B but not C. The transmission range of C reaches B but not A. B reaches A and C. A cannot detect C and vice versa. A starts sending to B, but C does not receive this transmission. C also wants to send something to B and sense the medium. The medium appears to be free, the carrier sense fails. C also Starts sending, causing a collision at B. But A can't detect this collision at B and continues with its Transmission. A is hidden for C and vice versa.

15. What is Mobile Computing and the applications?

Mobile computing is the process of computation on a mobile device. In such computing, A set of distributed computing systems or services provider servers participate, connect, and Synchronize through mobile communication protocols.

APPLICATION:

Mobile computing offers mobility with computer power. It provides decentralized computations on diversified devices, system, and Networks, which are mobile synchronized, and interconnected via mobile communication Standards and protocols.

16. List the Limitations of Mobile Computing?

- Resource
- Constraints
- Interface
- Bandwidth
- Dynamic changes in communication
- Environment
- Network issues.
- Interoperability issues.
- Security constrains.

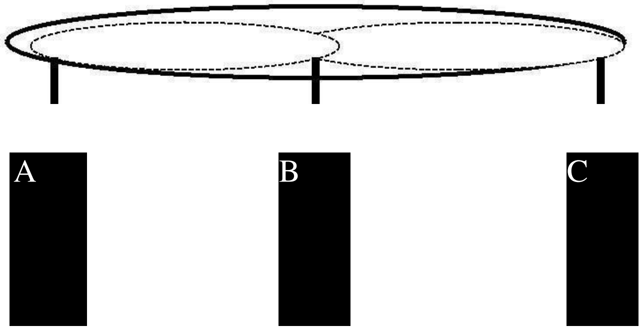
17. Give the difference between the network 1G, 2G, 3G, 5G mobile communications?

- 1G-Voice-only communication.
- 2G-Communicate voice as well as data signals.
- 2.5G-Enhancements of the second generations and sport data rates up to 100 kbs.
- 3G-Mobile devices communicate at even higher data rates and support voice, data and
- Multimedia streams. High data rates in 3G devices enable transfer of video clips and faster
- Multimedia communication.

18. Difference between Hidden and Exposed Terminal Near and Far Terminals?

Hidden and Exposed Terminals

Let us consider another scenario where ‘B’ sends something to ’A’ and ‘c’ wants to transmit data to some other mobile phones outside the interface ranges pf A and B. C senses the carrier and detects that the carrier is busy; C postpones range of C, waiting is It detects the medium is free; but as A is outside the interference range of C, waiting is Not necessary. i.e. collision at B does not matter because the collision is too weak to Propagate to A.



19. What is MAC?

Message authentication codes (MAC) are also used to authenticate message during transmission. MAC of a message is created using a cryptographic MAC function which is similar to the hash function but has different security requirement.

20. Define Mobile Binding?

A binding created for providing mobility to a mobile node after registration at a foreign network.

21. Define Agent-based computing?

An agent is any program that acts on behalf of a (human) user. A software mobile agent is a process capable of migrating from one computer node to another.

22. Define Ubiquitous computing?

Ubiquitous computing enhances computer use by making many computers available throughout the physical environment, while making the effectively invisible to Users.

23. Define Client-server computing?

An architecture in which the client is the requesting machine and the server is the supplying machine. The client contains the user interface and may perform some or all of the application Processing.

24. Define the term wireless?

Wireless telecommunications refers to the transfer of information between two or more points that are not physically connected. Distances can be short, such as a few meters for television Remote control, or as far as thousand or even millions of kilometers for deep-space radio Communications. It encompasses various types of fixed, mobile, and portable applications, including Two-way radios, cellular telephones, personal digital assistant (PDAs), and wireless networking.

25. What are the different types of mobile Middleware?

- Adaptation
- Agent

26. What are the logical channels in GSM?

- Traffic channel(TCH)
- Control channel(CCH)

27. Define the term wireless?

Wireless telecommunication refers to the transfer of information between two Points that are not physically connected. Distance can be short, such as a few meters for space radio Remote controls, or as far as thousands or even millions of kilometer for deep-space radio Communication. It encompasses various types of fixed, mobile, and portable, applications, including two-way radios, cellular telephones, personal digital assistants (PDAs),and wireless networking.

28. Define GPRS?

General packet Radio service (GPRS)is a packet oriented service for mobile devices data communication which utilizes the unused channels in TDMA mode in a GSM network and also sends and receive packet data through the internet.

29. What is communication?

- Communication is a two-way transmission and reception and reception of data streams.
- Transmission are of two types,
- Guided Transmission
- Unguided Transmission

30. Explain difference between wired and wireless networks

Wired Networks	Mobile Networks
high bandwidth	low bandwidth
low bandwidth variability	high bandwidth variability

can listen on wire	hidden terminal problem
high power machines	low power machines
high resource machines	low resource machines
need physical access(security)	need proximity
low delay	higher delay

31. List out the Types of Wireless Devices.

- Laptops
- Palmtops
- PDAs
- Cell
- Phones
- Pagers
- Sensors

32. Why we need Mobile computing?

- Enable anywhere/anytime connectivity
- Bring Computer communications to areas without preexisting
- Infrastructure enable mobility
- Enable new applications
- An exciting new research area

33. What are the New Forms of Computing available?

- Wireless computing
- Nomadic computing
- Ubiquitous Computing
- Pervasive Computing
- Invisible Computing

34. Write Mobile Communication Networks with Examples

- GSM(Global System for mobile Communications):worldwide standard for digital cellular Mobile Radio Networks

- UMTS(Universal Mobile Telecommunications System):European Standard for future digital Mobile Radio Networks
- AMPS (Advanced Mobile Phone System):analog mobile Radio Networks in USA
- DECT (Digital Enhanced Cordless Telecommunications): European standard for circuit switched radio networks
- ERMES(European Radio Message System):European standard for radio paging systems (pager)802.11: International standard for Wireless Local Networks
- Bluetooth: wireless networking in close/local area
- Inmarsat: geostationary satellite systems
- Teledesic: planned satellite system on non-geostationary orbit

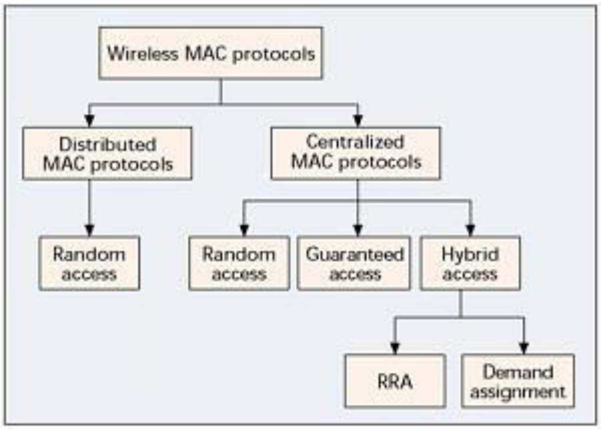
35. Write all the Components of a wireless communications system

- Transmitter,
- receiver,
- filter,
- antenna,
- amplifier,
- mixers

36. Write the Wireless Networking Standards

ITU, IEEE and ISO IEEE 802.11 standards.

37. Draw the Classification of Wireless MAC protocol.



38. What are the disadvantages of Small cells?

a)Infrastructure

b)Handover

c)Frequency

39. What are the benefits of Reservation Schemes?

a)Increased no other station is allowed to transit during this slot

b)Avoidance of congestion.

c) Waiting time in clearly known.

40. Define hidden terminal?

The transmission range of A reaches B but not C. The transmission range of C reaches B but not A. B reaches A and C. A cannot detect C and vice versa. A starts sending to B, but C does not receive this transmission. C also wants to send something to B and sense the medium the medium appears to be free, the carrier sense fails also starts sending, causing a collision at B. But A can't detect this collision at B and continues with its transmission. A is hidden for C and vice versa.

41. Write down the Characteristics of Mobile computing.

- Mobile devices
- Laptops
- Palmtops
- Smart cell phones
- Requirements
- Data access:
- Anywhere
- Anytime
- Nomadic users
- Constraints
- Limited resources
- Variable connectivity:
- Performance
- Reliability

42. What are the different types of Modulation?

The Modulation types are:

i) Amplitude modulation

ii)Frequency modulation

iii)Phase Modulation

43. What are the multiplexing techniques?

The Multiplexing techniques are:

i)Space division multiplexing .

ii)Time division multiplexing.

iii)Frequency division multiplexing

iv)Code division multiplexing

44. Define Space Division Multiplexing Access?

Space division multiple access(SDMA)means division of the available space so that multiple sources can access the medium at the same time. SDMA is the technique in which a wireless transmitter transmit the modulated signals and accesses a space slot and another transmitter accesses another space slot such that signals from both can propagated in two separate spaces in the medium without affecting each other.

45. Define Code division multiplexing Access?

CDMA(Code Division Multiple Access) is an access method in which multiple users are allotted different codes (sequences of symbols) to access the same channel(set of frequencies).

46. Define Time division multiplexing Access?

Time division multiplexing (TDMA) is an access method in which multiple users, data services, or sources are allotted different time-slices to access the same channel. The available time-slice is divided among multiple modulated-signal sources. These sources use the same medium, the same set of frequencies, and the same channel for transmission of data.

47. Define frequency division multiplexing Access?

Frequency division multiple access (FDMA) is an access method in which entails assignments of different frequency users for accessing the same carrier.

48. Difference between Circuit Switching and Packet Switching?

CIRCUIT SWITCHING:

Circuit switching is a method of data transmission in which a circuit (Communication channel or path) once established continues to be used till the transmission is complete.

PACKET SWITCHING:

Packet switching is a means of establishing connection and transmitting data in which the message consists of packets containing the data frames . A Packet is a formatted series of data, which follows a distinct path directed by a router from among a number of paths, available at that instant.

49. What is CSMA?

The capacity of ALOHA or slotted ALOHA is limited by the large vulnerability period of a packet. By listening before transmitting, stations try to reduce the vulnerability period to one propagation delay. This is the basis of CSMA(Kleinrock and Tobagi,UCLA,1975)The capacity of ALOHA or slotted ALOHA is limited by the large vulnerability period of a packet. By listening before transmitting, stations try to reduce the vulnerability period to one propagation delay. This is the basis of CSMA (Kleinrock and Tobagi, UCLA, 1975).Station that wants to transmit first listens to check if another transmission is in progress (carrier sense).If medium is in use, station waits; else, it transmits. Collisions can still occur. Transmitter waits for ACK; if no ACKs, retransmits.

50. What is the aim of Ubiquitous computing?

The aim of ubiquitous computing is to design computing infrastructures in such a manner that they integrate seamlessly with the environment and become almost invisible. Present Everywhere Bringing mobile, wireless and sensor Ubiquitous computing (ubicomp) integrates computation into the environment, rather than having computers which are distinct objects

51. What are the characteristics of Mobile computing devices?

- Adaptation Data dissemination and Management

- Heterogeneity Interoperability Context awareness

52. What are the key Constraints of Mobile computing?

- unpredictable variation in network quality
- lowered trust and robustness of mobile elements

53. List out the N-tier Client Server Frame Work and Tools

- N-Tier Any number of Tier-No Limits
- 3-Tier (Client, Application server, Database)

54. Define FDMA?

Frequency division multiple access (FDMA)

This comprises all algorithms allocating frequencies to transmission channels according to the frequency division multiplexing (FDM).Frequency can be fixed or dynamic.

55. Define CDMA?

An access method in which multiple carriers, channels, or sources are allotted different codes (Sequences and Symbols) to access the same channel (set of frequencies at the same time in same space).

56. What is ALOHA?

ALOHA net used a new method of medium access (ALOHA random access) and experimental UHF frequencies for its operation, since frequency assignments for communications to and from a computer were not available for commercial applications in the 1970s. But even before such frequencies were assigned there were two other media available for the application of an ALOHA channel – cables and satellites. In the 1970s ALOHA random access was employed in the widely used Ethernet cable based network and then in the Marisat (now Inmarsat) satellite network.

In the early 1980s frequencies for mobile networks became available, and in 1985 frequencies suitable for what became known as Wi-Fi were allocated in the US. These regulatory developments made it possible to use the ALOHA random access techniques in both Wi-Fi and in mobile telephone networks.

UNIT –II

1. What are the requirements of mobile IP?

- Compatibility
- Transparency
- Scalability and efficiency
- Security

2. Mention the different entities in a mobile IP.

- Mobile Node
- Correspondent Node
- Home Network
- Foreign Agent
- Home Agent
- Care- Of address
- Foreign agent COA
- Co-located COA

3. Define Mobile Node.

A Mobile node is an end system or router that can change its point of attachment to the Internet using mobile IP. The MN keeps its IP address and can continuously with any other system in the Internet as long as link layer connectivity is given.

4. Explain cellular IP.

Cellular IP provides local handovers without renewed registration by installing a single cellular IP gateway for each domain, which acts to the outside world as a foreign agent.

5. What do you mean by Mobility binding?

The Mobile Node sends its registration request to the Home agent. The HA now sets up a mobility binding containing the mobile node's home IP address and the current COA.

6. Define COA.

The COA (care if address) defines the current location of the MN from an IP point of view. All IP packets sent to the MN are delivered to the COA, not directly to the IP address of the

MN. Packets delivery toward the MN is done using the tunnel. DHCP is a good candidate us a good candidate for supporting the acquisition of care of addresses.

7. Define a tunnel.

A tunnel establishes a virtual pipe for data packets between a tunnel entry and a tunnel endpoint. Packets entering a tunnel are forwarded inside the tunnel and leave the tunnel unchanged.

8. What is encapsulation?

Encapsulation is the mechanism of taking a packet consisting of packet header and data putting it into the data part of a new packet.

9. What is decapsulation?

The reverse operation, taking a packet out of the data part of another packet is called decapsulation.

10. What is MOT? Give its primary goal.

DAB faces a broad range of different receiver capabilities. So to solve this problem it defines a common standard for data transmission, the multi-media object transfer (MOT) protocol. The primary goal of mot is the support of data formats used in other multi-media systems,

11. What is SUMR?

An important register in satellite networks is the satellite user mapping register (SUMR). This stores the current position of satellites and a mapping of each other user to the current satellite through which communication with a user is possible.

12. Give the two basic reasons for a handover in GSM.

The mobile station moves out the range of a BTS or a certain antenna of a BTS. The received signal level decreases continuously until it fall below the minimal requirements for communication. The error rate may grow due to interference. All these effects may diminish the quality of the radio link.

The wired infrastructure may decide that the traffic in one cell is one cell is too high and shift some MS to other cell with a lower lead. Handover may be due to load balancing.

13. Give the security services offered by GSM.

- Access control and authentication
- Confidentiality
- Anonymity.

14. What is the primary goal of GSM?

The primary goal of GSM was to provide a mobile phone system that allows users to roam throughout Europe and provides voice services compatible to ISDN and other PSTN system.

15. Differentiate GSM and DECT.

- GSMDECT
- Global system for mobile communication
- Digital enhanced cordless telecommunication
- Range is up to 70km
- Range is limited to about 300km.

16. What are the two new network elements in GPRS architecture?

Gateway GPRS support node (GGSN). It is the inter-working unit between the GPRS network and external packet data networks (PDN). Serving GPRS supportable node (SGSN). It supports the MS.

17. Describe about MAC layer in DECT architecture.

The medium access control (MAC) layer establishes, maintains and release channel for higher layers by activating and deactivating physical channels. MAC multiplexes several logical channels onto physical channels. Logical channel exist for signaling network control, user data transmission, paging or sending broadcast messages. Additional services offered include segmentation/reassembly of packets and error control/error correction.

18. Give the full form for the following:

a)CKSN b)EIR c)DTMF d)MOC

a)CKSN-ciphering key sequence number b) EIR-Equipment Identify Register

c)DTMF-Dual Tone multiple frequency d)MOC-Mobile originated call.

19. Define snooping TCP?

A protocol in which an agent buffers the packet from the fixed connection layer for transmission to the mobile node on a wireless transceiver, the agent also buffer the packets on the wireless transmission and reception in place in place of acknowledgement-or-timeout-based TCP method in the mobile part of the network.

20. Define Mobile TCP?

A method of splitting the TCP layer into two TCP sub-layers using a mechanism that reduce window size to zero. The split is asymmetric; The window is set to zero prevent transmission form the TCP transport layer at the mobile node (MN) or at the fixed node when disconnection is noticed. The window opens again on getting the packet, there is no slow start by the base transceiver and it is presumed that packet loss is due to disconnection and not due to congestion or interference.

21. Explain the concept "Fast Retransmit/Fast Transmission?

A method in which there are four or more phase of fast retransmit and fast recovery-first phase as slow start and beginning (exponential), then fast retransmit/recovery phase1(FRR1) on three duplicate acknowledgement, fast retransmit/fast recovery phase2(FRR2), and wait(Constant time out and window size).

22. Define T-TCP?

A protocol which is efficient and is used in situations where short messages are to be sent in sequence and a packet is delivered after the SYN and SYN_ACK packet exchanges and the connection closes after the packet exchanges of FIN, FIN_ACK, and CLOSING.

23. Define ISR?

Interrupt Service Routine (ISR):A program unit (function, method, or subroutine) which runs when a hardware or software event occurs and running of which can be masked and can be prioritized by assigning a priority.

24. Define IST?

Interrupt Service Thread (IST): A special type of ISR or ISR unit (function, method , or subroutine) which initiates and runs on an event and which can be prioritized by assigning a priority.

25. Features of TCP?

The main features of TCP are:

1)Transmission as data Streams

2)Buffering and retransmission

3)Session-start, data transfer, and session-finish fully acknowledged end to end.

4)In-order delivery

5) Congestion Control and avoidance

26. What is explicit notification?

A method of congestion control by explicit notification of congestion, for example, when a base transceiver at the receiver end is not able to transmit a packet to the mobile node then it sends an ESBN (explicit bad state notification) to the sender (on fixed line) at the other end.

27. What is selective re transmission?

A method in which there is an additional acknowledgement, known as selective acknowledgement; a timeout is set at transmitting end for receiving SACKs. Only the lost packet corresponding ta a SACK needs to be retransmitted.

28. What are all he Methods of Congestion Control.

The methods of congestion control:

1)Slow start and congestion avoidance

2)Fast recovery after packet loss

3)Fast retransmit and fast recovery

4)Selective acknowledgement

5) Explicit congestion notification

29. Define TCP header.

A header used in the TCP protocol; it consists of fields in five 32-bit words followed by words for the option fields and padding.

30. Describe the three subsystems of GSM.

- Radio subsystem (RSS): It comprises all radio specific entities i.e. the mobile stations (MS) and the base station subsystem (BSS).
- Networking and switching subsystem (NSS): The heart of the GSM system is formed by the NSS. This connects the wireless network with standard public networks.
- Operating subsystem (OSS): It monitors and controls all other network entities.

31. What are the applications of satellites?

- Weather forecasting
- Radio and TV broadcast satellites Military satellites
- Satellites for navigation

32. List out the Application Layer protocols

- File Transfer Protocol (FTP)
- Trivial File Transfer Protocol (TFTP) Network File System (NFS)
- Simple Mail Transfer Protocol (SMTP) Terminal emulation protocol (telnet) Remote login application (rlogin)
- Simple Network Management Protocol (SNMP) Domain Name System (DNS)
- Hypertext Transfer Protocol (HTTP)

33. What are Advantage and Disadvantage of Mobile TCP?

Advantages: i. M-TCP maintains the TCP end-to-end semantic. The SH does not send any ACK itself but forwards the ACKs from the MH. ii. If the MH is disconnected, M_TCP avoids useless retransmissions, slow starts or breaking connections by simply shrinking the sender's window to 0; iii. Since M-TCP does not buffer data in the SH as I-TCP does, it is not necessary to forward buffers to a new SH. Lost packets will be automatically retransmitted to the new SH.

Disadvantages: i. As the SH does not act as proxy as in I-TCP, packet loss on the wireless link due to bit errors is propagated to the sender. M-TCP assumes low bit error rates, which is not always a valid assumption. ii. A modified TCP on the wireless link not only requires modification to the MH protocol software but also new network elements like the bandwidth manager

34. What is Mobile routing?

Even if the location of a terminal is known to the system, it still has to route the traffic through the network to the access point currently responsible for the wireless terminal. Each time a user moves to a new access point, the system must reroute traffic. This is known as mobile routing.

35. What are the functions which support service and connection control?

- Access point control function
- Call control and connection control function

- Network security agent
- Service control function
- Mobility management function

36. What are the examples for service scenarios identified in WATM?

- Office environments
- Universities, schools, training, centers
- Industry
- Hospitals
- Home
- Networked vehicles

37. What is slow start?

TCP's reaction to a missing acknowledgement is necessary to get rid of congestion quickly. The behavior TCP shows after the detection of congestion is called slow start.

38. What is the use of congestion threshold?

The exponential growth of the congestion window in the slow start mechanism is dangerous as it doubles the congestion window at each step. So a congestion threshold is set at which the exponential growth stops.

39. What led to the development of Indirect TCP?

TCP performs poorly together with wireless links.TCP within the fixed network cannot be changed. This led to the development of I-TCP which segments a TCP connection into a fixed part and a wireless part.

40. What is the goal of M-TCP?

The goal of M-TCP is to prevent the sender window from shrinking if bit errors or disconnection but not congestion cause current problems.

It wants

- To provide overall throughput
- To lower the delay
- To maintain end-to-end semantics of TCP
- To provide a more efficient handover.

41. What do you mean by persistent mode?

Persistent mode is the state of the sender will not change no matter how long the receiver is disconnected. This means that the sender will not try to retransmit the data.

42. What are the characteristics of 2.5G/3.5G wireless networks?

- Data rates
- Latency Jitter
- Packet loss

43. What are the configuration parameters to adapt TCP to wireless environments?

- Large Windows Limited Transmit Large MTU
- Selective Acknowledgement Explicit Congestion Notification Timestamp
- No header compression

44. Mobile IP Terminology

- Mobile Node (MN)
- system (node) that can change the point of connection to the network without changing its IP address
- Home Agent (HA)
- system in the home network of the MN, typically a router registers the location of the MN, tunnels IP datagrams to the
- COA Foreign Agent (FA)
- system in the current foreign network of the MN, typically a router
- forwards the tunneled datagrams to the MN, typically also the default router for the MN
- Care-of Address (COA)
- address of the current tunnel end-point for the MN (at FA or MN) actual location of the MN from an IP point of view can be chosen, e.g., via DHCP Correspondent Node (CN) communication partner

45. What Mobile IP

Mobile IP solves the following problems:

- if a node moves without changing its IP address it will be unable to receive its packets,
- if a node changes its IP address it will have to terminate and restart its ongoing

connections every time it moves to a new network area (new network prefix).

- Mobile IP is a routing protocol with a very specific purpose.
- Mobile IP is a network layer solution to node mobility in the Internet.
- Mobile IP is not a complete solution to mobility, changes to the transport protocols need to be made for a better solution (i.e., the transport layers are unaware of the mobile node's point of attachment and it might be useful if, e.g., TCP knew that a wireless link was being used!).

UNIT III

1. Define GSM?

The global system for mobile communication (GSM) was developed by Group Special Mobile (GSM) which was founded in Europe in 1992. The GSM is a standard for mobile telecommunication through a cellular network at data rates if up to 14.4 kbps. Now a days it consist of a set of standards and protocols for mobile telecommunication.

2. Define GPRS?

General Packet Radio Service (GPRS) is a packet oriented service for mobile devices data communication which utilizes the unused channels in TDMA mode in a GSM network and also sends and receives packet of data through the internet.

3. What are subsystems in GSM system?

Radio Subsystem (RSS)

- Network & Switching subsystem (NSS)
- Operation subsystem (OSS)

4. What are the control channel groups in GSM?

- Broadcast control channel (BCCH)
- Common control channel (CCCH
- Dedicated control channel (DCCH)

5. What are the four types of handover available in GSM?

- Intra cell Handover
- Inter cell Intra BSC Handover Inter BSC Intra MSC handover

- Inter MSC Handover

6. What is the frequency range of uplink and downlink in GSM network?

- The frequency range of uplink in GSM network is 890-960 MHz
- The frequency range of downlink in GSM network is 935-960 MHz

7. What are the security services offered by GSM?

- The security services offered by GSM are:
- Access control and authentication
- Confidentiality.
- Anonymity.

8. What are the reasons for delays in GSM for packet data traffic?

Collisions only are possible in GSM with a connection establishment. A slotted ALOHA mechanism is used to get access to the control channel by which the base station is told about the connection establishment attempt. After connection establishment, a designated channel is installed for the transmission.

9. What is meant by beacon?

A beacon contains a timestamp and other management information used for power management and roaming. e.g., identification of the base station subsystem (BSS)

10. List out the numbers needed to locate an MS and to address the MS.

The numbers needed to locate an MS and to address the MS are:

- Mobile station international ISDN number (MSISDN)
- International mobile subscriber identity (IMSI)
- Temporary mobile subscriber identity(TMSI)
- Mobile station roaming number (MSRN)

11. What is meant by GPRS?

The General Packet Radio Service provides packet mode transfer for applications that exhibit traffic patterns such as frequent transmission of small volumes.

12. What is meant by GGSN?

GGSN is Gateway GPRS Support Node. It is the inter-working unit between the GPRS network and external packet data networks. The GGSN is connected to external networks via the GI interface and transfers packets to the SGSN via an IP based GPRS backbone network.

13. What is meant by SGSN?

SGSN is Serving GPRS Support Node. It supports the MS via the Gb interface. The GSN is connected to a BSC via frame relay.

14. What is meant by BSSGP?

BSSGP is Base Station Subsystem GPRS Protocol. It is used to convey routing and QoS-related information between the BSS and SGSN.BSSGP does not perform error correction and works on top of a frame relay network.

15. Expand GSM, GPRS and UMTS.

- Global System for Mobile Communication(GSM)
- General Packet Radio Service(GPRS)
- Universal Mobile Telecommunication System (UMTS)

16. Mention the types of Interface in GSM system and its use.

- A interface
- Makes the connection between the RSS and the NSS
- Based on circuit-switched PCM-30 systems (2.048 Mbit/s), carrying up to 30 64 kbit/s connections
- 0interface
- Makes the connection between the RSS and the OSS
- Uses the Signaling System No.7 (SS7) based on X.25 carrying management data to/from the RSS
- Uinterface
- Makes the connection between the BTS and MS
- Contains all the mechanisms necessary for wireless transmission
- Ab. interface
- IS
- Makes the connection between the BTS and BSC Consists of 16 or 64 kbits connections

17. What is RSS?

- RSS stands for Radio subsystem(RSS)
- RSS comprises all radio specific entities

18. Name the entities of RSS.

- Base Station Subsystem(BSS)
- Base Transceiver Station(BTS)
- Base Station Controller (BSC)
- Mobile Station(MS)

19. Mention the advantages of GSM.

- Communication
- Total mobility
- Worldwide connectivity
- High capacity
- High transmission quality'
- Security functions

20. What does SIM card contain?

- a personal identity number(PIN)
- a PIN unblocking key(PUK)
- an authentication key Ki
- the international mobile subscriber identity(IMSI)

21. Mention the disadvantages of GSM.

- No end-to-end encryption of user data
- Reduced concentration while moving
- Electromagnetic radiation
- High complexity of system
- Several incompatibilities within the GSM standards
- Card-type
- Serial number

- A list of subscribed services

22. Mention the use of SS7.

Used for handling all signaling needed for connection setup, connection release and handover of connections to other MSCs

UNIT IV

1. Define MANET.

- MANET - Mobile Adhoc NETworks
- Continuously self-configuring, infrastructure-less network of mobile devices connected without wires

2. List the advantages of MANET.

- Independence from central network administration
- Self-configuring, nodes are also routers
- Self-healing through continuous re-configuration
- Scalable-accommodates the addition of more nodes
- Flexible-similar to being able to access 'the Internet from many different locations
- Ease of deployment
- Speed of deployment
- Decreased dependence on infrastructure
- Reduced administrative cost
- Supports anytime and anywhere computing

3. What are the limitations of MANET?

- Each node must have full performance
- Throughput is affected by system loading
- Reliability requires a sufficient number of available nodes
- Large networks can have excessive latency (time delay), which affects some applications
- Limited wireless range
- Hidden terminals
- Packet losses due to transmission errors
- Routes changes

- Devices heterogeneity
- Battery power constraints
- Link changes are happening quite often
- Routing loop may exist

4. Difference between cellular and Ad-Hoc Networks

CELLULAR	Ad-Hoc NETWORKS
Infrastructure Networks	Infrastructure less Networks
Fixed, pre-located cell sites and base stations	No base station, and rapid deployment
Static backbone network topology	Highly dynamic network topologies
Relatively caring environment and stable connectivity	Hostile environment and irregular connectivity
Detailed planning before base station can be installed	Ad-Hoc network automatically forms and adapts to changes
High setup costs	Cost-effective
Large setup time	Less setup time

5. What are the functions of each node in MANET?

- Forward the packet to the next hop
- Before forwarding, Sender has to ensure that:
- the packet moves towards its destination
- the number of hops(path length) to destination is minimum
- Delay is minimized
- Packet loss is minimum through the path
- Path does not have a loop

6. Comparison of Link state and Distance vector.

Routing protocol	Building Topological map	Router can Independently determine the shortest path to every network	Conver-gence	Event driven routing up-dates (instead of periodic updates)	Use of LSP
Link State	Yes	Yes	Fast	Generally Yes	Yes
Distance Vector	No	No	Slow	Generally No	No

7. List the Types of Communications.

- **Unicast**
- Message is sent to a single destination node
- **Multicast**
- Message is sent to a selected subset of network nodes
- **Broadcast**
- Broadcasting is a special case of multicasting
- Message is sent to all the nodes in the network

8. Define Proactive (table-driven) protocols.

Also known as table-driven routing protocols

Each node in the routing table maintains information about routes, to every other node in the network. Tables are updates frequently due to Changes in network topology. Node Movements N odes shutting down. Nodes can determine the best route to a destination. Generates a large number of control messages to keep. The routing tables up-to-date Generates overhead which consumes large part of available bandwidth

9. Define Reactive protocols.

- Also called as On-demand routing protocol
- Nodes do not maintain up-to-date routing information
- New routes are discovered only when required
- Uses flooding technique to determine the route
- Flooding technique is used when the node does not have routing knowledge

10. Compare MANET Vs VANET.

MANET	VANET
MANET - Mobile Adhoc NETwork	VANET- Vehicular Adhoc NETworks
Nodes moves randomly	Nodes moves regularly
Mobility is low	Mobility is high
Reliability is medium	Reliability is high
Node lifetime depends on power source	N ode lifetime depends on vehicle life time
Network topology is sluggish and slow	Network topology is frequent and fast

UNIT V

1. **Define Operating System.**
    - Interface between hardware and user
    - Manages hardware and software
    - Provides set of services to application program.
2. **Name of the feature of operating system.**
    - Multitasking
    - Scheduling
    - Memory Allocation
    - File System interface
    - Keypad interface
    - I/O Interface

- Protection and security
- Multimedia features.

3. **How is the operating system structured?**
   - Kernel Layer
   - Shell Layer
4. **Give the types of Operating system.**
   - Monolithic Kernel
   - Micro Kernel
5. **Specify the motivation of Monolithic kernel OS design.**
   - Kernel contains the entire OS operations except shell code.
   - Motivation
   - OS Services can run more securely and efficiently in supervisor mode.
6. **Mention the examples of Monolithic kernel OS design.**
   - Windows
   - UNIX.
7. **List the Advantages of Monolithic kernel OS design.**
   - Provides good performance
   - Always runs in supervisor mode
   - More efficient and secure.
8. **List the disadvantages of Monolithic kernel OS design.**
   - Makes kernel
   - Massive
   - Non Modular
   - Hard two tailer
   - Maintain
   - Extend
   - Configure
9. **List the disadvantages of Microkernel OS design.**
   - Flexible

- Modular
- Easier to port
- Easy to extend and implement

10. List the disadvantages of microkernel OS design

- Difficult to debug compared to application program
- Bog in the kernel crashes the system and the debugger.
- Non –reliable

11. What is Mobile OS.

- Facilitate third party development of application software
- Allow manufactures of different brands of mobile devices to build their choice set of functionalities for the users.

12. Give some examples of Mobile OS.

- Window Mobile
- Palm Os
- Symbian Os
- iOS
- Android
- Blackberry

13. What are the parts in Android architecture or Android Software stack?

- Application Layer
- Application Framework
- Android Runtime
- Native libraries(Middleware)
- Linux Kernel.

14. What are the Key services provided in Application Framework?

- Activity Manager
- Content Providers
- Resource Manager

- Notifications Manager
- View System

15. List the Native libraries in Android architecture.

- WebKit - web browser engine OpenGL
- FreeType - font support
- SQLite - SQLdatabase
- Media - playing and recording audio and video formats MP3
- MPEG-4,
- C runtime library (libc)etc

16. Mention the responsibilities of Linux Kernel.

- Device drivers
- Power management
- Networking Functionalities.
- Memory management
- Device management
- Resource access

17. What is M-Commerce?

- M-Commerce stands for Mobile Commerce
- Buying and selling of goods and services through mobile handheld devices

18. Compare B2C andB2B.

B2C	B2B
B2C stands for Business- to-Consumer	B2B stands for Business- to- Business
Form of commerce in which products or services are sold by a business firm to a consumer	Form of commerce in which products or services are sold from a company to its dealers

19. What is the function of transport layer in WAP?

The transport layer offers a bearer independent, consistent datagram-oriented service to the higher layers of the WAP architecture. Communication is done transparently over one of the available bearer services.

20. What is the use of WCMP?

The wireless control message protocol provides error handling mechanisms for WDP. WCMP is used for diagnostic and informational purposes. It is used by WDP nodes and gateways to report errors.

21. What are the advantages of WTP?

WTP offers several advantages to higher layers, including an improved reliability over datagram services, improved efficiency over connection-oriented services and support for transaction-oriented services such as web browsing.

22. How is reliability achieved in WTP?

WTP achieves reliability using duplicate removal, retransmission, acknowledgements and unique transaction identifiers.

23. What are the service primitives offered by WTP?

The three service primitives offered by WTP are o TR-Invoke to initiate a new transaction

- TR-Result to send back the result of a previously initiated transaction
- TR-Abort to abort an existing transaction.

24. What are the features offered by WSP?

WSP offers certain features for content exchange between cooperating clients and servers: Session management, Capability, negotiation, content encoding.

25. What is meant by WML?

The wireless markup language (WML) is based on the standard HTML known from the www and on HDML. WML is specified as an XML document type. WML follows a deck and card metaphor.

26. What are the capabilities of WML Script?

WML Script offer several capabilities:

- Validity check of user input
- Access to device facilities
- Local user interaction
- Extension to the device software.

26. Define WTA

Wireless telephony application (WTA) is a collection of telephony specific extensions for call and feature control mechanisms, merging data networks and voice networks.

27. What do you mean by MMS?

The multimedia messaging service (MMS) transfers asynchronous multi-media content. MMS supports different media types such as JPEG, GIF, text and AMR coded audio. There is no fixed upper bound for the message size. Depending on the network operator and device capabilities typical sizes are 30- 100 Kbytes.

28. What are the two functions of transport layer in the internet?

1) Check summing over user data.

2) Multiplexing / Demultiplexing from / to applications device software

29. Distinguish TCP&UDP?

TCP	**UDP**
Connection oriented protocol	Connection less protocol
TCP is network friendly	UDP is not network friendly
TCP guarantees in-order delivery or reliable data transmission using Retransmission techniques	Does not pull back in case of congestion to send packets in to an already congested network

Question bank – Detailed Questions

UNIT –I

1. Discuss the advantage and disadvantage of cellular system with small cells (06)

2. Briefly explain the Frequency Division Multiplexing (06)

3. Write short notes on DHSS(04)

4. Write short note on FHSS (04)

5. Explain the GSM system architecture with a neat diagram.(16)

6. Describe the security services provided by GSM. (08)

7. Explain the protocol architecture of GSM for signaling.(16)

8. Explain the architecture of GPRS with a neat diagram. (10)

9. What are typical steps for handover on GSM network? (08)

10. Explain the steps involved in the call delivery procedure in GSM network in the following cases:

(i)GSM mobile terminated call (08)

(ii)GSM mobile originated call (08)

11. Why are so many different identifiers/addresses needed in GSM? Give reasons and distinguish between user-related and system related identifiers.(08)

12. Explain the services provided by GSM? (08)

13. Write short notes on

(i)Mobile management. (08)

(ii)Connection Establishment.(08)

UNIT-II

1. Compare Hiper LAN and Blue tooth in terms of ad-hoc capabilities, power saving mode, solving hidden terminal problem, providing reliability fairness problem regarding channel access.(16)
2. Write short notes on wireless PAN?(04)
3. Explain the operation of DFWMAC_DCF with a neat timing diagram.(8)
4. Draw the MAC frame of 802.11 and list the use of the fields. (8)
5. Describe HiperLAN architectural components and their interactions. (16)
6. Explain the architecture of Wi-Fi in detail.(16)
7. Explain the system architecture of IEEE802.11 (16)
8. Describe the architecture of WiMAX in detail. (16)
9. Compare and Contrast Wi-Fi and WiMax.(06)
10. Briefly explain about BRAN.(04)
11. Explain in detail about Wireless ATM. (10)

12. Explain the information bases and networking of adhoc HIPERLAN.(8)
13. Discuss MAC layer Bluetooth system (08)

UNIT – III

1. Show the steps required for a handover from one FA to another FA including layer-2 andlayer-3.Assume 802.11aslayer-2.(08)
2. Name the inefficacies of Mobile IP regarding data forwarding from CN to MN. W hat are the optimizations possible?(08)
3. What are the differences between wired networks and ad-hoc networks related to routing? (06)
4. What is the need for DHCP? With a state chart explain the operation of DHCP? (10)
5. List the entities involved in mobile IP and describe the process of data transfer from a mobile node to a fixed node and vice versa.(08)
6. Why is conventional routing in wired networks not suitable for wireless networks? Substantiate your answers with suitable examples.(08)
7. Discuss DSDV routing in detail. (16)
8. Describe how the multicast routing is done in ad-hoc networks.(08)
9. Explain how tunneling works in general and especially for mobile IP using IP-in-IP, MINIMAL, and generic routing encapsulation, respectively. Discuss the advantages and disadvantages of these three methods.(16)
10. How does dynamic source routing handle routing? What is the motivation between dynamic source routing compared to other routing algorithms from fixed networks?(16)
11. Briefly explain about CGSR.(06)
12. Compare and Contrast about Pro Active and Reactive routing protocol(4)

UNIT IV

1. Explain the mechanisms of TCP that influence the efficiency in mobile environment.(08)
2. Explain the operation of Mobile TCP.(08)
3. Compare and Contrast Traditional and Mobile TCP.(04)

4. Why has a scripting language been added to WML? How can this language help saving bandwidth and reducing delay? (08)
5. Which WTP class reflects the typical web access best?
6. How is unnecessary overhead avoided when using WSP on top of this class of web browsing? (10)
7. State the requirements of WAP. Explain its architectural components. (16)
8. Explain WML and WML scripts with an example. (16)
9. What is WTP? Discuss about its classes.(08)
10. Explain the architecture of WTA. (08)

UNITV

1. What are the design and implementation issues in device connectivity aspect of pervasive computing? Explain.(08)
2. Explain the operating system issues related to miniature devices.(08)
3. Explain the various soft surface and semi-soft-surface-based display system and technologies. (16)
4. Describe the various hardware components involved in pervasive computing devices. (08)
5. Explain how a pervasive web application can be secured using an 'Authentication Proxy'. (08)
6. What are the applications of pervasive computing? Discuss any two of them.(08)
7. Explain how pervasive web applications can be accessed via WAP. (10)