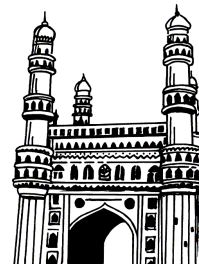


Rahul's ✓
Topper's Voice

**NEW
SYLLABUS**



M.Sc.




(COMPUTER SCIENCE)

II Year IV Sem

(Osmania University)

**LATEST
EDITION**

MOBILE COMPUTING

-  **Study Manual**
-  **Important Questions**
-  **Solved Model Papers**

- by -

WELL EXPERIENCED LECTURER

Price
~~249-00~~
199-00



Rahul Publications™

Hyderabad. Cell : 9391018098, 9505799122

All disputes are subjects to Hyderabad Jurisdiction only

M.Sc.

II Year IV Sem

MOBILE COMPUTING

Inspite of many efforts taken to present this book without errors, some errors might have crept in. Therefore we do not take any legal responsibility for such errors and omissions. However, if they are brought to our notice, they will be corrected in the next edition.

© No part of this publications should be reporduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording and/or otherwise without the prior written permission of the publisher



Sole Distributors :

Cell : 9391018098, 9505799122

VASU BOOK CENTRE

Shop No. 2, Beside Gokul Chat, Koti, Hyderabad.

Maternity Hospital Opp. Lane, Narayan Naik Complex, Koti, Hyderabad.

Near Andhra Bank, Subway, Sultan Bazar, Koti, Hyderabad -195.

MOBILE COMPUTING

CONTENTS

Important Questions	III - V
Model Paper - I	VI - VI
Model Paper - II	VII - VII
Model Paper - III	VIII - VIII
Unit - I	1 - 38
Unit - II	39 - 76
Unit - III	77 - 100
Unit - IV	101 - 119

SYLLABUS

UNIT - I

Introduction to Mobile Computing: applications, a simplified reference model, Wireless Transmission: frequencies of radio transmission, signals, antennas, signal propagation, multiplexing, modulation, spread spectrum, cellular system. Media Access Control: motivation for a specialized MAC, SDMA, FDMA, TDMA, CDMA, and Comparisons.

UNIT - II

GSM, DECT, Wireless LAN: Infrared vs. radio transmission, Infrastructure and ad-hoc networks, IEEE 802.11, HPERLAN, Bluetooth.

UNIT - III

Mobile Network Layer: mobile IP, dynamic host configuration protocol, ad-hoc networks. Mobile Transport Layer: Traditional TCP, classical TCP improvements, TCP over 2.5/3G wireless networks.

UNIT - IV

File Systems, World Wide Web, Wireless Application Protocol (WAP) and WAP 2.0.

Contents

Topic No.		Page No.
UNIT - I		
1.1	Introduction to Mobile Computing	1
1.1.1	Applications	1
1.1.2	A Simplified Reference Model	3
1.2	Wireless Transmission	4
1.2.1	Frequencies Of Radio Transmission	4
1.2.2	Signals	5
1.2.3	Antenas	6
1.2.4	Signal Propagation	8
1.2.5	Multiplexing	10
1.2.5.1	Time division multiplexing	12
1.2.6	Modulation	14
1.2.7	Spread Spectrum	20
1.2.8	Cellular System	25
1.3	Media Access Control	27
1.3.1	Motivation for a Specialized mac	27
1.3.2	SDMA	29
1.3.3	FDMA	29
1.3.4	TDMA	30
1.3.5	CDMA	35
1.3.6	Comparisons	38
UNIT - II		
2.1	GSM	39
2.2	DECT	51
2.3	Wireless lan	54
2.3.1	Infrared vs. Radio Transmission	55
2.3.2	Infrastructure And ad-hoc Networks	55
2.3.4	IEEE 802.11	56
2.3.5	Hiperlan	63
2.3.6	Bluetooth	70

UNIT - III

3.1	Mobile Network Layer	77
3.1.1	Mobile IP	77
3.1.2	Dynamic Host Configuration Protocol	89
3.1.3	AD-HOC Networks	90
3.2	Mobile Transport Layer	93
3.2.1	Traditional TCP	93
3.2.2	Classical TCP Improvements	97
3.2.3	TCP Over 2.5/3G Wireless Networks	100

UNIT - IV

4.1	File Systems	101
4.2	World Wide Web	103
4.3	Wireless Application Protocol (WAP) and WAP 2.0	110

IMPORTANT QUESTIONS

UNIT - I

Short Questions

1. Write the characteristics of mobile communication.
2. What are the limitations of mobile computing.
3. Explain about signal propagation.
4. What is quadrature amplitude modulation.
5. What is spread spectrum.
6. Write a note on cell structure.
7. What is frequency reuse or frequency planning.
8. What is cell breathing.
9. Write a note on media access control.
10. What is SDMA.

Long Questions

1. Explain the layers of the mobile reference model.
2. What are Antennas? Explain about various antennas used in communication.
3. What is multiplexing? Explain about various multiplexing techniques.
4. What is Modulation? Explain various modulation techniques.
5. Explain various types of spread spectrum signals.
6. Explain Hidden and Exposed Terminals.
7. Explain near and far terminals.
8. Discuss briefly about FDMA.
9. What is TDMA. Explain different schemes of TDMA.
10. What is CDMA? Explain about it.

UNIT - II

Short Questions

1. Write about Localization and calling GSM.
2. What is Handover in GSM. Write shortly about it.
3. Write the advantages and disadvantages of WLAN.
4. Differentiate between Infrared and radio transmission.
5. Write a note on Infrastructure and ad-hoc networks.
6. Write a short note about HIPER LAN.
7. What is the need of WATM.
8. What is BRAN? Explain about it.
9. Write a note on Bluetooth?
10. What are the security services in blue tooth.

Long Questions

1. Write about the services provided by GSM.
2. Explain GSM architecture with neat diagram.
3. Write about GSM TDMA frame . 4. Explain GSM Frame Hierarchy.
4. Explain about GSM protocols.
5. Write about DECT.
6. Explain about IEEE 802.11.
7. Explain the protocol architecture of IEEE 802.11. Explain the Frame Format of 802.11.
8. Explain about HIPER LAN1.
9. Explain the network topology of blue tooth.
10. Explain Bluetooth protocol stack.

UNIT - III**Short Questions**

1. Define the terms used in mobile IP.
Mobile Node (MN) Correspondent node (CN).
2. Define the terms used in mobile IP.
Foreign agent (FA).
Care-of address (COA).
3. Write a note on agent discovery.
4. Write a short note on agent registration.
5. Define tunnelling.
6. What is reverse tunnelling?
7. Write short note on IPv6.
8. What are the characteristics of MANETs.
9. Write a short note on TCP.
10. Write about slow start and fast transmission congestion technique.

Long Questions

1. Explain the need for mobile IP.
2. Explain briefly about Mobile IP.
3. Why is mobile IP packet required to be forwarded through a tunnel.
4. What is Encapsulation ? Explain about various encapsulation techniques.
5. Explain DHCP.
6. Explain various routing protocols used in MANET.
7. How congestion is controlled in TCP?
8. Explain I- TCP.
9. Explain Snooping TCP.
10. Explain Mobile TCP.

Unit - IV
Short Questions

1. What is file system? What are the goals of file systems.
2. What is little work file system ? write a note on it.
3. Write a not on Ficus File system.
4. Write about Mio-NFS file system.
5. What is HTTP protocol?
6. Write any two components of HTTP protocol.
7. List any three features of HTTP.
8. What is HTML?
9. What are the approaches of www for a mobile devices.
10. What is the use of Wireless Session Protocol.

Long Questions

1. Describe about Coda File sytem.
2. What are the components of HTTP protocol.
3. Explain about HTTP Flow.
4. Write about the mobility in HTTP.
5. Describe WWW system architecture.
6. Explain about WAP architecture.
7. Explain Wireless Datagram Protocol.
8. Write about Wireless Transport Layer Security.
9. Explain about wireless transaction protocol.
10. Explain Wireless Session Protocol.

FACULTY OF SCIENCE
M.Sc. II Year IV Semester Examination
MOBILE COMPUTING

Time : 3 Hours]

ANSWERS TO MODEL PAPER - I

[Max. Marks : 80

PART - A (8 × 4 = 32)

Answer all questions

Each Question Carries Equal Marks

ANSWERS :

- | | |
|---|----------------------|
| 1. Explain about signal propagation. | (Unit - I, Q.No.8) |
| 2. Write a note on cell structure | (Unit - I, Q.No.18) |
| 3. Write a short note on HIPER LAN | (Unit - II, Q.No.16) |
| 4. Write a note on Bluetooth | (Unit - II, Q.No.21) |
| 5. What is reverse tunnelling ? | (Unit - III, Q.No.8) |
| 6. Define tunnelling | (Unit - III, Q.No.5) |
| 7. What is little work file system? Write a note on it. | (Unit - IV, Q.No.3) |
| 8. What is HTTP Protocol ? | (Unit - IV, Q.No.6) |

PART - B (4 × 12 = 48)

Answer all the questions

- | | |
|--|-----------------------|
| 9. a) What is multiplexing? Explain about various multiplexing techniques. | (Unit - I, Q.No.10) |
| (OR) | |
| b) Discuss briefly about FDMA. | (Unit - I, Q.No.25) |
| 10. a) Explain GSM architecture with neat diagram. | (Unit - II, Q.No.2) |
| (OR) | |
| b) Explain about IEEE 802.11 | (Unit - II, Q.No.13) |
| 11. a) What is Encapsulation ? Explain about various encapsulation techniques. | (Unit - III, Q.No.7) |
| (OR) | |
| b) Explain I- TCP | (Unit - III, Q.No.15) |
| 12. a) Describe about Coda File system. | (Unit - IV, Q.No.2) |
| (OR) | |
| b) Describe WWW system architecture. | (Unit - IV, Q.No.13) |

FACULTY OF SCIENCE
M.Sc. II Year IV Semester Examination
MOBILE COMPUTING

Time : 3 Hours]

ANSWERS TO MODEL PAPER - II

[Max. Marks : 80

PART - A (8 × 4 = 32)*Answer all questions**Each Question Carries Equal Marks*

- | | |
|--|-----------------------------|
| 1. What is spread spectrum ? | (Unit - I, Q.No.14) |
| 2. What is SDMA ? | (Unit - I, Q.No.24) |
| 3. Write about Localization and calling GSM. | (Unit - II, Q.No.6) |
| 4. What is Handover in GSM ? Write shortly about it. | (Unit - II, Q.No.7) |
| 5. Explain the need for mobile IP. | (Unit - III, Q.No.1) |
| 6. Write short note on IPv6. | (Unit - III, Q.No.9) |
| 7. Write about Mio-NFS file system. | (Unit - IV, Q.No.5) |
| 8. What is the use of Wireless Session Protocol ? | (Unit - IV, Q.No.18) |

PART - B (4 × 12 = 48)*Answer all the questions*

- | | |
|--|--------------------------------|
| 9. a) Explain near and far terminals. | (Unit - I, Q.No.23) |
| (OR) | |
| b) What is TDMA. Explain different schemes of TDMA. | (Unit - I, Q.No.26) |
| 10. a) Explain the protocol architecture of IEEE 802.11. Explain the Frame Format of 802.11. | (Unit - II, Q.No.14,15) |
| (OR) | |
| b) Explain Bluetooth protocol stack. | (Unit - II, Q.No.23) |
| 11. a) Explain various routing protocols used in MANET. | (Unit - III, Q.No.12) |
| (OR) | |
| b) Explain Snooping TCP. | (Unit - III, Q.No.16) |
| 12. a) Explain about WAP architecture. | (Unit - IV, Q.No.14) |
| (OR) | |
| b) Explain about wireless transaction protocol. | (Unit - IV, Q.No.17) |

FACULTY OF SCIENCE
M.Sc. II Year IV Semester Examination
MOBILE COMPUTING

Time : 3 Hours]

ANSWERS TO MODEL PAPER - III

[Max. Marks : 80

PART - A (8 × 4 = 32)*Answer all questions**Each Question Carries Equal Marks*

- | | |
|---|------------------------------|
| 1. What is quadrature amplitude modulation ? | (Unit - I, Q.No.13) |
| 2. What is cell breathing ? | (Unit - I, Q.No.20) |
| 3. Write the advantages and disadvantages of WLAN. | (Unit - II, Q.No.10) |
| 4. What is BRAN? Explain about it. | (Unit - II, Q.No.19) |
| 5. What is reverse tunnelling ? | (Unit - III, Q.No.8) |
| 6. Write a short note on TCP. | (Unit - III, Q.No.13) |
| 7. What is file system? What are the goals of file systems. | (Unit - IV, Q.No.1) |
| 8. Write any two components of HTTP protocol. | (Unit - IV, Q.No.7) |

PART - B (4 × 12 = 48)*Answer all the questions*

- | | |
|--|------------------------------|
| 9. a) What is Modulation? Explain the various modulation techniques. | (Unit - I, Q.No.11) |
| (OR) | |
| b) What is CDMA? Explain about it. | (Unit - I, Q.No.27) |
| 10. a) Explain about GSM protocols. | (Unit - II, Q.No.5) |
| (OR) | |
| b) Explain about HIPER LAN1 | (Unit - II, Q.No.17) |
| 11. a) Explain DHCP. | (Unit - III, Q.No.10) |
| (OR) | |
| b) Explain Mobile TCP. | (Unit - III, Q.No.17) |
| 12. a) Explain Wireless Datagram Protocol. | (Unit - IV, Q.No.15) |
| (OR) | |
| b) Explain Wireless Session Protocol. | (Unit - IV, Q.No.18) |

UNIT I

Introduction to Mobile Computing: applications, a simplified reference model, Wireless Transmission: frequencies of radio transmission, signals, antennas, signal propagation, multiplexing, modulation, spread spectrum, cellular system. Media Access Control: motivation for a specialized MAC, SDMA, FDMA, TDMA, CDMA, and Comparisons.

1.1 INTRODUCTION TO MOBILE COMPUTING

Q1. Define Communication, mobile communication and describe its characteristics.

Ans :

Communication

Communication is a two-way transmission and reception of data streams. Signals for Voice, data, or multimedia streams are transmitted. Signals are received by a receiver.

Signals from a system transmit through a fiber, wire, or wireless medium, according to

defined regulations, recommended standards and protocols.

Mobile Communication entails transmission of data to and from handheld devices. Two or more communicating devices at least one is handheld or mobile. Location of the device can vary either locally or globally. Communication takes place through a wireless, distributed, or diversified network.

Mobile Computing is an umbrella term used to describe technologies that enable people to access network services anyplace, anytime, and anywhere.

A communication device can exhibit any one of the following characteristics :

- ▶ **Fixed and wired:** This configuration describes the typical desktop computer in an office. Neither weight nor power consumption of the devices allow for mobile usage. The devices use fixed networks for performance reasons.
- ▶ **Mobile and wired:** Many of today's laptops fall into this category; users carry the laptop from one hotel to the next, reconnecting to

the company's network via the telephone network and a modem.

- ▶ **Fixed and wireless:** This mode is used for installing networks, e.g., in historical buildings to avoid damage by installing wires, or at trade shows to ensure fast network setup.
- ▶ **Mobile and wireless :** This is the most interesting case. No cable restricts the user, who can roam between different wireless networks. With this type of device and the networks supporting them. Today's most successful example for this category is GSM with more than 800 million users.

1.1.1 Applications

Q2. Explain about various applications of Mobile Communications.

Ans :

In many fields of work, the ability to keep on the move is vital in order to utilise time efficiently. The importance of Mobile Computers has been highlighted in many fields of which a few are described below :

a) Vehicles

Music, news, road conditions, weather reports, and other broadcast information are received via digital audio broadcasting (DAB) with 1.5 Mbit/s. For personal communication, a universal mobile telecommunications system (UMTS) phone might be available offering voice and data connectivity with 384 kbit/s.

The current position of the car is determined via the global positioning system (GPS). Cars driving in the same area build a local ad-hoc network for the fast exchange of information in emergency situations or to help each other keep a safe distance. In case of an accident, not only will the air bag be triggered, but the police and ambulance service will be informed via an emergency call to a service provider. Buses, trucks, and trains are already transmitting maintenance and logistic information to their home base, which helps to improve organization and saves time and money.

b. Emergencies

An ambulance with a high-quality wireless connection to a hospital can carry vital information about injured persons to the hospital from the scene of the accident. All the necessary steps for this particular type of accident can be prepared and specialists can be consulted for an early diagnosis. Wireless networks are the only means of communication in the case of natural disasters such as hurricanes or earthquakes. In the worst cases, only decentralized, wireless ad-hoc networks survive.

c. Business

Managers can use mobile computers say, critical presentations to major customers. They can access the latest market share information. At a small recess, they can revise the presentation to take advantage of this information. They can communicate with the office about possible new offers and call meetings for discussing responds to the new proposals. Therefore, mobile computers can leverage competitive advantages.

A travelling salesman today needs instant access to the company's database: to ensure that files on his other laptop reflect the current situation, to enable the company to keep track of all activities of their travelling employees, to keep databases consistent etc.

With wireless access, the laptop can be turned into a true mobile office, but efficient and powerful synchronization mechanisms are needed to ensure data consistency.

d. Credit Card Verification

At Point of Sale (POS) terminals in shops and supermarkets, when customers use credit cards for transactions, the intercommunication required between the bank central computer and the POS terminal, in order to effect verification of the card usage, can take place quickly and securely over cellular channels using a mobile computer unit. This can speed up the transaction process and relieve congestion at the POS terminals.

e. Replacement of Wired Networks

wireless networks can also be used to replace wired networks, e.g., remote sensors, for trade shows, or in historic buildings. Due to economic reasons, it is often impossible to wire remote sensors for weather forecasts, earthquake detection, or to provide environmental information. Wireless connections, e.g., via satellite, can help in this situation. Other examples for wireless networks are computers, sensors, or information displays in historical buildings, where excess cabling may destroy valuable walls or floors.

f. Infotainment

Wireless networks can provide up-to-date information at any appropriate location. The Travel guide might tell you something about the history of a building (knowing via GPS, contact to a local base station, or triangulation where you are) downloading information about a concert in the building at the same evening via a local wireless network. Another growing field of wireless network applications lies in entertainment and games to enable, e.g., ad-hoc gaming networks as soon as people meet to play together.

Q3. What are the limitations of mobile computing ?

Ans :

Limitations of Mobile Computing

- ▶ **Resource constraints :** Battery
- ▶ **Interference :** Radio transmission cannot be protected against interference using shielding and result in higher loss rates for transmitted data or higher bit error rates respectively.

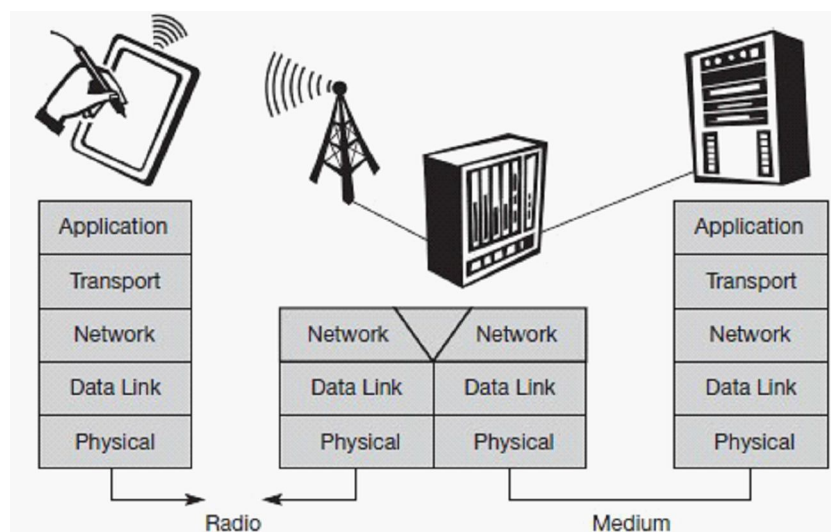
- ▶ **Bandwidth:** Although they are continuously increasing, transmission rates are still very low for wireless devices compared to desktop systems. Researchers look for more efficient communication protocols with low overhead.
- ▶ **Dynamic changes in communication environment:** variations in signal power within a region, thus link delays and connection losses.
- ▶ **Network Issues:** discovery of the connection-service to destination and connection stability
- ▶ **Interoperability issues:** the varying protocol standards
- ▶ **Security constraints:** Not only can portable devices be stolen more easily, but the radio interface is also prone to the dangers of eavesdropping. Wireless access must always include encryption, authentication, and other security mechanisms that must be efficient and simple to use.

1.1.2 A Simplified Reference Model

Q4. Explain the layers of the mobile reference model.

Ans :

The figure shows the **protocol stack** implemented in the system according to the reference model. **End-systems**, such as the PDA and computer in the example, need a full protocol stack comprising the application layer, transport layer, network layer, data link layer, and physical layer. Applications on the end-systems communicate with each other using the lower layer services. **Intermediate systems**, such as the interworking unit, do not necessarily need all of the layers.



Physical Layer : This is the lowest layer in a communication system and is responsible for the conversion of a stream of bits into signals that can be transmitted on the sender side. The physical layer of the receiver then transforms the signals back into a bit stream. For wireless communication, the physical layer is responsible for frequency selection, generation of the carrier frequency, signal detection, modulation of data onto a carrier frequency and encryption.

- ▶ **Data link layer:** The main tasks of this layer include accessing the medium, multiplexing of different data streams, correction of transmission errors, and synchronization (i.e., detection of a data frame). Altogether, the data link layer is responsible for a reliable point-to-point connection between two devices or a point to-multipoint connection between one sender and several receivers.

- **Network layer:** This third layer is responsible for routing packets through a network or establishing a connection between two entities over many other intermediate systems. Important functions are addressing, routing, device location, and handover between different networks.
- **Transport layer:** This layer is used in the reference model to establish an end-to-end connection
- **Application layer:** Finally, the applications (complemented by additional layers that can support applications) are situated on top of all transmission oriented layers. Functions are service location, support for multimedia applications, adaptive applications that can handle the large variations in transmission characteristics, and wireless access to the world-wide web using a portable device.

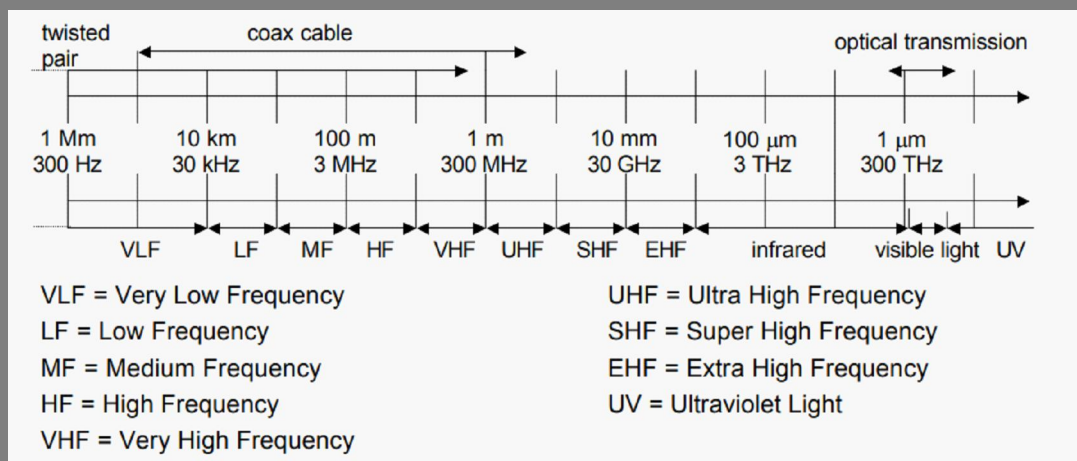
1.2 WIRELESS TRANSMISSION

1.2.1 Frequencies Of Radio Transmission

Q5. Give the overview of frequency spectrum that can be used for data communication.

Ans :

Radio transmission can take place using many different frequency bands. Each frequency band exhibits certain advantages and disadvantages. The following Figure gives a rough overview of the frequency spectrum that can be used for data transmission.



Frequency and wave length : $\lambda = c/f$ wave length λ , speed of light $c \cong 3 \times 10^8 \text{ m/s}$, frequency f .

- For traditional wired networks, frequencies of up to several hundred kHz are used for distances up to some km with twisted pair copper wires, while frequencies of several hundred MHz are used with coaxial cable.
- Fiber optics are used for frequency ranges of several hundred THz, but here one typically refers to the wavelength which is, e.g., 1500 nm, 1350 nm etc. (infra red).
- Radio transmission starts at several kHz, the **very low frequency (VLF)** range. These are very long waves. Waves in the **low frequency (LF)** range are used by submarines, because they can penetrate water and can follow the earth's surface.
- The **medium frequency (MF)** and **high frequency (HF)** ranges are typical for transmission of hundreds of radio stations either as amplitude modulation (**AM**) between 520 kHz and 1605.5

kHz, as short wave (**SW**) between 5.9 MHz and 26.1 MHz, or as frequency modulation (**FM**) between 87.5 MHz and 108 MHz..

- ▶ TV stations follow higher frequencies, Conventional analog TV is transmitted in ranges of 174–230 MHz and 470–790 MHz using the very high frequency (**VHF**) and ultra high frequency (**UHF**) bands.
- ▶ **Super high frequencies (SHF)** are typically used for directed microwave links (approx. 2–40 GHz).
- ▶ The **extremely high frequency (EHF)** range which comes close to infra red.. **Infra red (IR)** transmission is used for directed links, e.g., to connect different buildings via laser links. The most widespread IR technology, infra red data association (IrDA), uses wavelengths of approximately 850–900 nm to connect laptops, PDAs etc.
- ▶ Finally, visible light has been used for wireless transmission for thousands of years.

1.2.2 Signals

Q6. Write a note on signals.

Ans :

- ▶ Signals are the physical representation of data. Users of a communication system can only exchange data through the transmission of signals.
- ▶ Layer 1 of the ISO/OSI basic reference model is responsible for the conversion of data, i.e., bits, into signals and vice versa.
- ▶ Signals are functions of time and location. Signal parameters represent the data values. The most interesting types of signals for radio transmission are **periodic signals, especially sine waves as carriers**.
- ▶ The general function of a sine wave is :
- ▶ $g(t) = A \sin(2\pi f t + \phi)$

- ▶ Signal parameters are the **amplitude A, the frequency f, and the phase shift ϕ** . The amplitude as a factor of the function g may also change overtime, thus $A(t)$,

- ▶ The frequency f expresses the periodicity of the signal with the period $T = 1/f$.

- ▶ Finally, the phase shift determines the shift of the signal relative to the same signal without a shift.

- ▶ Sine waves are of special interest, as it is possible to construct every periodic signal g by using only sine and cosine functions according to a fundamental equation of **Fourier** :

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n \sin(2\pi n f t) + \sum_{n=1}^{\infty} b_n \cos(2\pi n f t)$$

- ▶ In this equation the parameter c determines the **Direct Current (DC) component** of the signal, the coefficients a_n and b_n are the amplitudes of the nth sine and cosine function.

- ▶ The equation shows that an infinite number of sine and cosine functions is needed to construct arbitrary periodic functions.

- ▶ the frequencies of these functions (the so-called **harmonics**) **increase** with a growing parameter n and are a multiple of the **fundamental frequency f**.

- ▶ The bandwidth of any medium, air, cable, transmitter etc. is limited and, there is an upper limit for the frequencies. A typical way to represent signals is the time domain

- ▶ Representations in the time domain are problematic if a signal consists of many different frequencies

- ▶ In this case, a better representation of a signal is the **frequency domain**

Fourier Representation of Periodic Signals

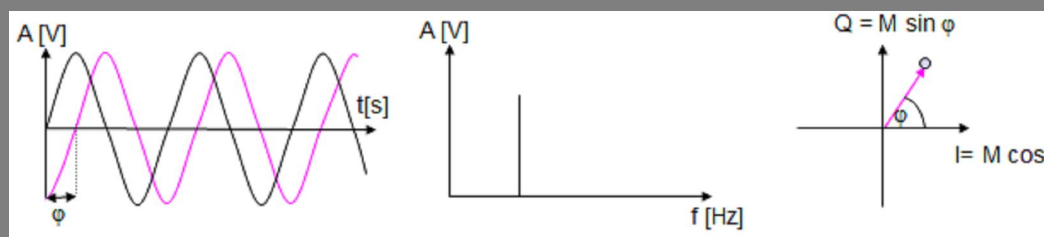
Fourier transformations are a mathematical tool for translating from the time domain into the frequency domain and vice versa.

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n \sin(2\pi n f t) + \sum_{n=1}^{\infty} b_n \cos(2\pi n f t)$$



Different Representations of Signals

- ▶ amplitude (amplitude domain)
- ▶ frequency spectrum (frequency domain)
- ▶ phase state diagram (amplitude M and phase ϕ in polar coordinates)



- ▶ Composed signals transferred into frequency domain using Fourier transformation
- ▶ Digital signals need
 - o infinite frequencies for perfect transmission
 - o modulation with a carrier frequency for transmission (analog signal)

1.2.3 Antennas

Q7. What are Antennas ? Explain about various antennas used in communication.

Ans :

Antennae are devices that transmit and receive electromagnetic signals. Most function efficiently for relatively narrow frequency ranges. If not properly tuned to the frequency band in which the transmitting system connected to it operates, the transmitted or received signals may be impaired. The forms of antennae are mainly determined by the frequency ranges they operate in and can vary from a single piece of wire to a parabolic dish.

isotropic radiator

A theoretical reference antenna is the **isotropic radiator**, a point in space radiating equal power in all directions, i.e., all points with equal power are located on a sphere with the antenna as its center. The **radiation pattern** is symmetric in all directions

Radiation Pattern of Antenna:

The important feature of an antenna is

- ▶ Signal amplitude at an instant is identical along the pattern.
- ▶ Circular pattern means that radiated energy, and thus signal strength, is equally distributed in all directions in the plane.
- ▶ A pattern in which the signal strength is directed along a specific direction in the plane.

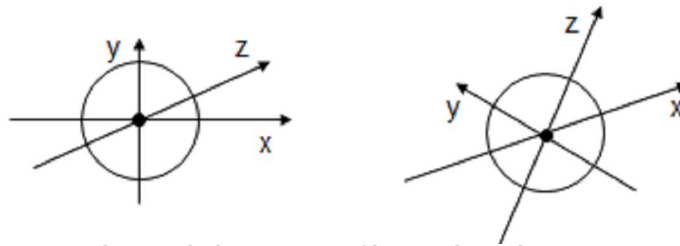


Fig. : radiation pattern of isotropic radiator

Types of Antennas

1. Simple dipole antenna

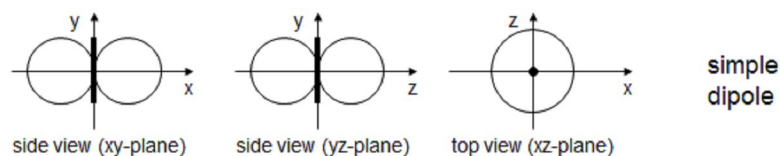
However, such an antenna does not exist in reality. Real antennas all exhibit **directive effects**, i.e., the intensity of radiation is not the same in all directions from the antenna. The simplest real antenna is a thin, center-fed **dipole**, also called Hertzian dipole, as shown in Figure.



The dipole consists of two collinear conductors of equal length, separated by a small feeding gap. The length of the dipole is not arbitrary. If mounted on the roof of a car, the length of $\lambda/4$ is efficient. This is also known as Marconi antenna.

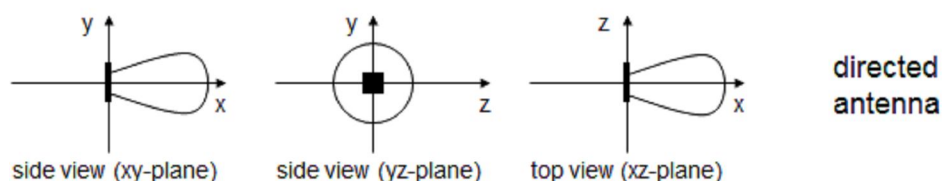
A $\lambda/2$ dipole has a uniform or **omni-directional** radiation pattern in one plane and a figure eight pattern in the other two planes as shown in figure.

Example: Radiation pattern of a simple Hertzian dipole



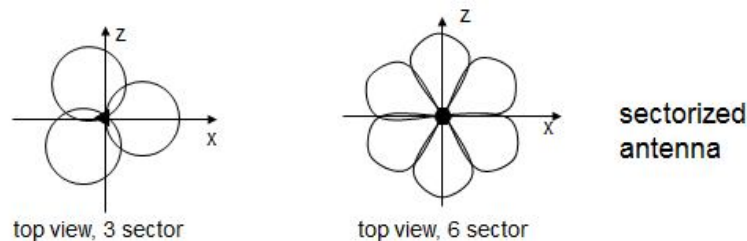
2. Directed Antennas

If an antenna is positioned, e.g., in a valley or between buildings, an omnidirectional radiation pattern is not very useful. In this case, **directional antennas** with certain fixed preferential transmission and reception directions can be used. Figure shows the radiation pattern of a directional antenna with the main lobe in the direction of the x-axis. A special example of directional antennas is constituted by satellite dishes.



3. sectorized Antennas

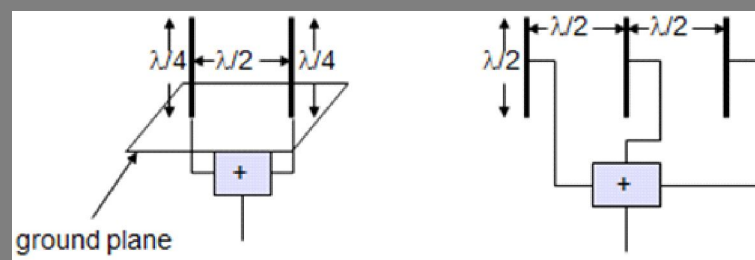
Directed antennas are typically applied in cellular systems. Several directed antennas can be combined on a single pole to construct a **sectorized antenna**. A cell can be sectorized into, for example, three or six sectors, thus enabling frequency can be reused Figure shows the radiation patterns of these sectorized antennas.



4. Multi element or Diversity Antennas

Two or more antennas can also be combined to improve reception by counteracting the negative effects of multi-path propagation. These antennas, also called **multi-element antenna arrays**, allow different diversity schemes.

Diversity combining constitutes a combination of the power of all signals to produce gain. As shown in Figure different schemes are possible. On the left, two $\lambda/4$ antennas are combined with a distance of $\lambda/2$ between them on top of a ground plane. On the right, three standard $\lambda/2$ dipoles are combined with a distance of $\lambda/2$ between them. Spacing could also be in multiples of $\lambda/2$.



1.2.4 Signal Propagation

Q8. Explain about signal propagation.

Ans :

The Wireless propagation of signals faces many complications. Mobile communication renders reliable wireless transmission much more difficult than communication between fixed antennae. The antenna height and size at mobile terminals are generally quite small. The obstacles in the vicinity of the antenna have a significant influence on the propagated signal. The propagation properties vary with place and, for a mobile terminal, with time. **Attenuation** is the gradual loss in intensity of any kind of flux through a medium. For instance, sunlight is attenuated by dark glasses, X-rays are attenuated by lead, and light and sound are attenuated by water.

Ranges for Transmission, Detection, and Interference of Signals

1. Transmission Range

Within a certain radius of the sender transmission is possible, i.e., a receiver receives the signals with an error rate low enough to be able to communicate and can also act as sender.

2. Detection Range

Within a second radius, detection of the transmission is possible, i.e., the transmitted power is large enough to differ from background noise. However, the error rate is too high to establish communication.

Interference range:

Within a third even larger radius, the sender may interfere with other transmission by adding to the background noise. A receiver will not be able to detect the signals, but the signals may disturb other signals.

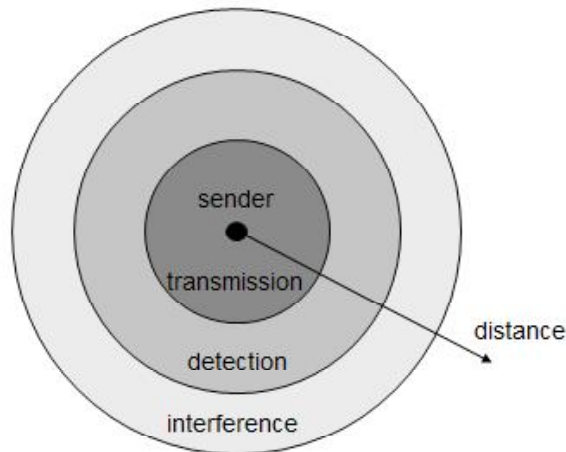


Fig. : Ranges for transmission, detection, and interference of signals

The Signal strength

1. Decrease due to attenuation
2. When obstacles in the path of the signal greater in size than the wavelength of the signal.

The propagation of signals is

- ▶ Line of Sight is the transmission of signals without refraction, diffraction, or scattering inbetween the transmitter and receiver.
- ▶ Shadowing
- ▶ Reflection at large obstacles
- ▶ Refraction depending on the density of a medium
- ▶ Scattering at small obstacles
- ▶ Diffraction at edges

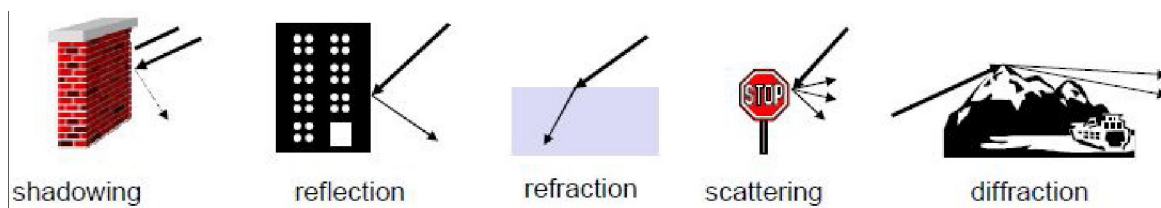


Fig. : Propagation of signals

Q9. Write a short note on multi path propagation.

Ans :

Multi-path Propagation

Signal can take many different paths between sender and receiver due to Reflection, scattering, and diffraction.

Time dispersion: signal is dispersed over time

Interference with "neighbor" symbols, Inter Symbol Interference (ISI)

The signal reaches a receiver directly and phase shifted.

Distorted signal depending on the phases of the different parts.

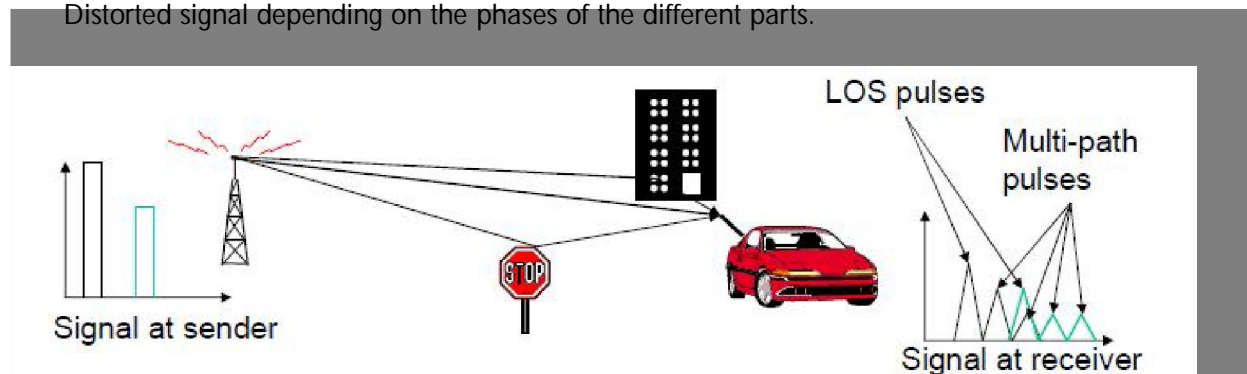


Fig. : Multi-path Propagation

1.2.5 Multiplexing

Q10. What is multiplexing ? Explain about various multiplexing techniques.

Ans :

Multiplexing is not only a fundamental mechanism in communication systems but also in everyday life. Multiplexing describes how several users can share a medium with minimum or no interference. One example is highways with several lanes. Many users (car drivers) use the same medium (the highways) with hopefully no interference (i.e., accidents). This is possible due to the provision of several lanes (space division multiplexing) separating the traffic.

Space Division Multiplexing

For wireless communication, multiplexing can be carried out in four dimensions: **space**, **time**, **frequency**, and **code**. In this field, the task of multiplexing is to assign space, time,

frequency, and code to each communication channel with a minimum of interference and a maximum of medium utilization. The term communication channel here only refers to an association of sender(s) and receiver(s) who want to exchange data.

The figure 1.5 shows six channels k_i and introduces a three dimensional coordinates system. This system shows the dimensions of code c , time t and frequency f . For this first type of multiplexing, **space division multiplexing (SDM)**, the (three dimensional) space is also shown. Here space is represented via circles indicating the interference range as introduced in figure.

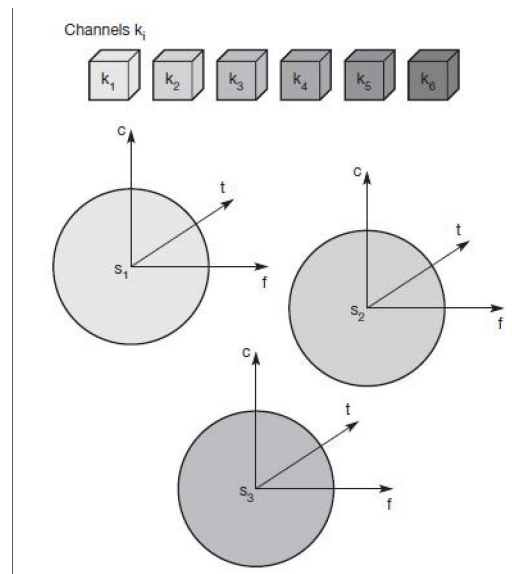


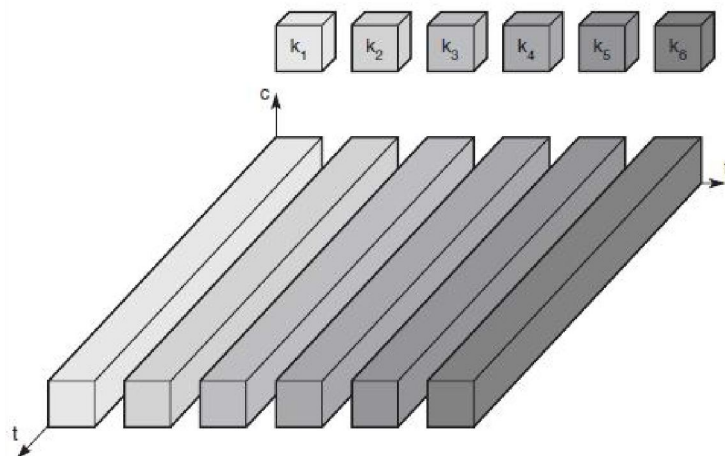
Fig. : Space division multiplexing (SDM)

The channels k_1 to k_3 can be mapped onto the three 'spaces' s_1 to s_3 which clearly separate the channels and prevent the interference ranges from overlapping. The space between the interference ranges is sometimes called **guard space**. Such a guard space is needed in all four multiplexing schemes presented.

For the remaining channels (k_4 to k_6) three additional spaces would be needed.

Frequency Division Multiplexing

Frequency division multiplexing (FDM) describes schemes to subdivide the frequency dimension into several non-overlapping frequency bands as shown in **figure**. Each channel k_i is now allotted its own frequency band as indicated. Senders using a certain frequency band can use this band continuously. Again, **guard spaces** are needed to avoid frequency band overlapping (also called **adjacent channel interference**). This scheme is used for radio stations within the same region, where each radio station has its own frequency. This very simple multiplexing scheme does not need complex coordination between sender and receiver: the receiver only has to tune in to the specific sender.



1.2.5.1 Time division multiplexing

A more flexible multiplexing scheme for typical mobile communications is **time division multiplexing (TDM)**. Here a channel k_i is given the whole bandwidth for a certain amount of time, i.e., all senders use the same frequency but at different points in time.

Again, **guard spaces**, which now represent time gaps, have to separate the different periods when the senders use the medium. If two transmissions overlap in time, this is called **co-channel interference**. To avoid this type of interference, precise synchronization between different senders is necessary. This is clearly a disadvantage, as all senders need precise clocks or, alternatively, a way has to be found to distribute a synchronization signal to all senders. For a receiver tuning in to a sender this does not just involve adjusting the frequency, but involves listening at exactly the right point in time. However, this scheme is quite flexible as one can assign more sending time to senders with a heavy load and less to those with a light load.

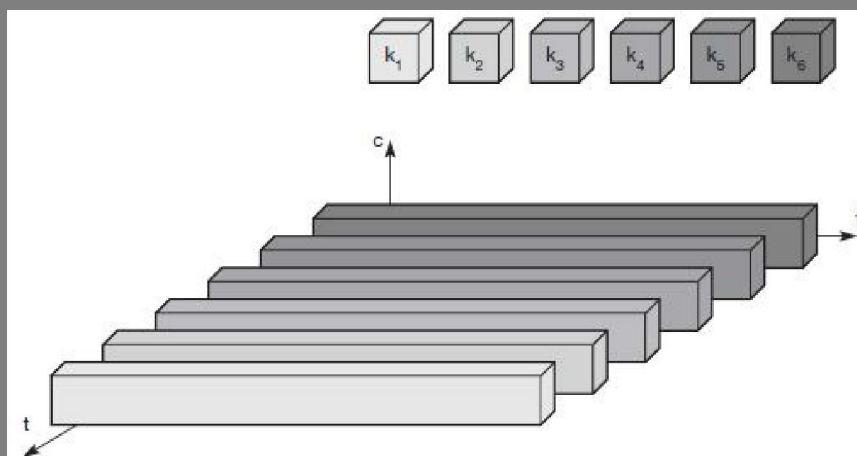


Fig. : Time division multiplexing (TDM)

Frequency and time division multiplexing can be combined, i.e., a channel k_i can use a certain frequency band for a certain amount of time as shown in figure 1.8. Now guard spaces are needed both in the time and in the frequency dimension. This scheme is more robust against frequency selective interference, i.e., interference in a certain small frequency band.

A channel may use this band only for a short period of time. Additionally, this scheme provides some (weak) protection against tapping, as in this case the sequence of frequencies a sender must be known to listen in to a channel. The mobile phone standard GSM uses this combination of frequency and time division multiplexing for transmission between a mobile phone and a so-called base station.

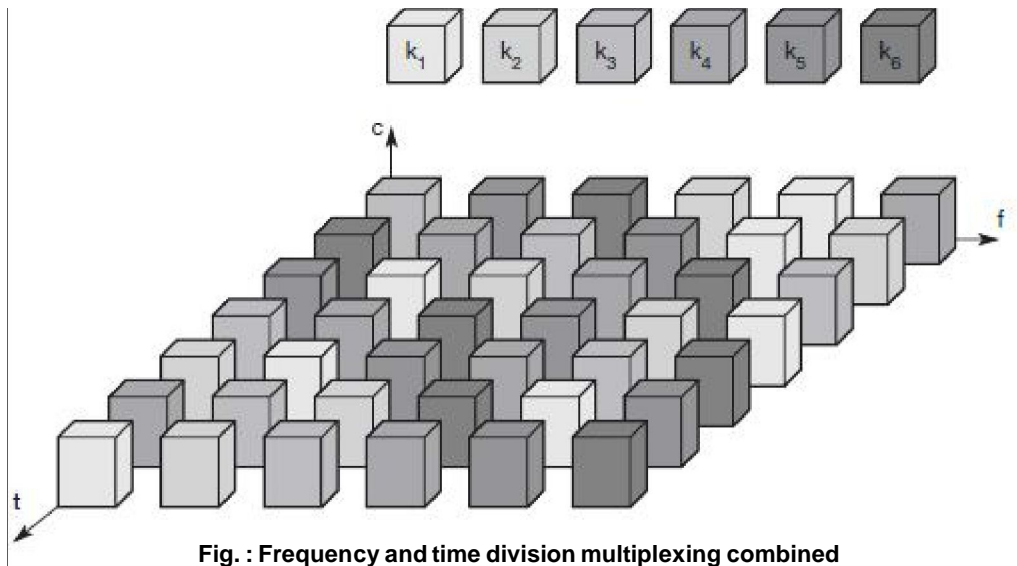


Fig. : Frequency and time division multiplexing combined

A disadvantage of this scheme is again the necessary coordination between different senders. One has to control the sequence of frequencies and the time of changing to another frequency. Two senders will interfere as soon as they select the same frequency at the same time.

However, if the frequency change (also called frequency hopping) is fast enough, the periods of interference may be so small that, depending on the coding of data into signals, a receiver can still recover the original data.

Code division multiplexing (CDM)

Code division multiplexing is by using a wide range of frequencies, called spread spectrum. Spread spectrum has distinct set of equally separated frequencies. Different source transmitting signals along identical path in the same time slices transmits using spread spectrum frequencies using distinct codes.

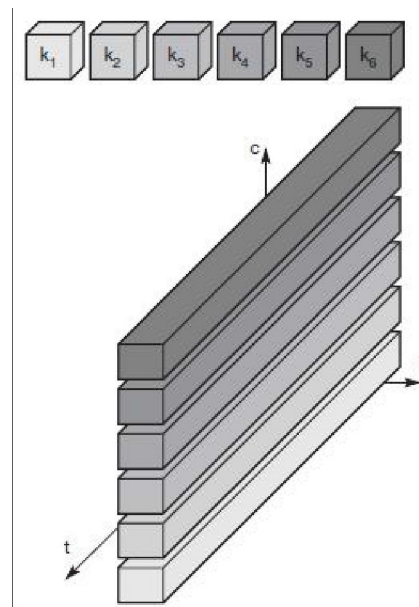


Fig. : Code division multiplexing (CDM)

Figure shows how all channels k_i use the same frequency at the same time for transmission. Separation is now achieved by assigning each channel its own 'code', **guard spaces** are realized by using codes with the necessary 'distance' in code space, e.g., **orthogonal codes**. The typical everyday example of CDM is a party with many participants from different countries around the world, who establish communication channels, i.e., they talk to each other, using the same frequency range at the same time. If everybody speaks the same language, SDM is needed to be able to communicate. But as soon as another code, i.e., another language, is used, one can tune in to this language and clearly separate communication in this language from all the other languages.

The main **advantage** of CDM for wireless transmission is that it gives good protection against interference and tapping. Different codes have to be assigned, but code space is huge compared to the frequency space.

The main **disadvantage** of this scheme is the relatively high complexity of the receiver.

A receiver has to know the code and must separate the channel with user data from the background noise composed of other signals and environmental noise. Additionally, a receiver must be precisely synchronized with the transmitter to apply the decoding correctly. The voice example also gives a hint to another problem of CDM receivers. All signals should reach a receiver with almost equal strength; otherwise some signals could drain others.

1.2.6 Modulation

Q11. What is Modulation? Explain various modulation techniques.

Ans :

Modulation is nothing but, a carrier signal that varies in accordance with the message signal. Modulation technique is used to change the signal characteristics. Basically, the modulation is of following two types:

Modulation Techniques

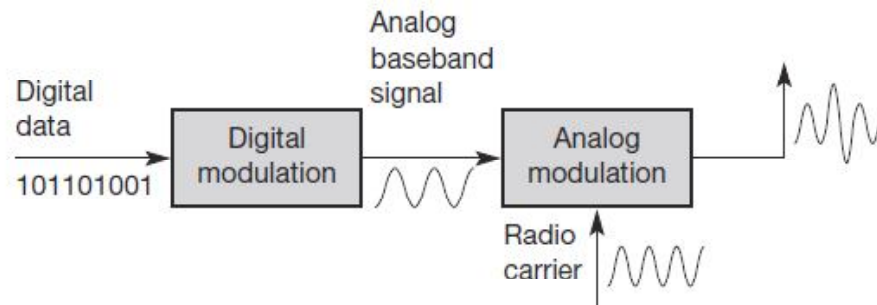
- ▶ Analog Modulation
- ▶ Digital Modulation

1. Analog Modulation

In analog modulation, analog signal (sinusoidal signal) is used as a carrier signal that modulates the message signal or data signal. The general function Sin wave's is shown in the figure below, in which, three parameters can be altered to get modulation – they are amplitude, frequency and phase; so, the types of analog modulation are :

$$A_c \cos(2\pi f_c t + \phi)$$

(Frequency = Rate of change of Angle)



Analog Modulation

- ▶ Amplitude Modulation (AM)
- ▶ Frequency Modulation (FM)
- ▶ Phase Modulation (PM)

1. Amplitude Modulation

Amplitude modulation was developed in the beginning of the 20th century. It was the earliest modulation technique used to transmit voice by radio. This type of modulation technique is used in electronic communication. In this modulation, the amplitude of the carrier signal varies in accordance with the message signal, and other factors like phase and frequency remain constant.

The modulated signal is shown in the below figure, and its spectrum consists of the lower frequency band, upper frequency band and carrier frequency components. This type of modulation requires more power and greater bandwidth; filtering is very difficult. Amplitude modulation is used in computer modems, VHF aircraft radio, and in portable two-way radio

2. Frequency Modulation

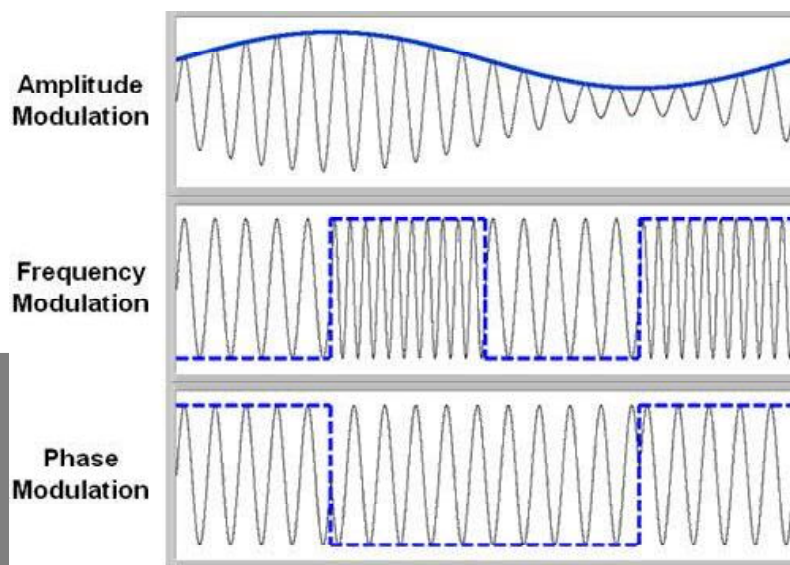
In this type of modulation, the frequency of the carrier signal varies in accordance with the message signal, and other parameters like amplitude and phase remain constant. Frequency modulation is used in different applications like radar, radio and telemetry, seismic prospecting and monitoring newborns for seizures via EEG, etc.

This type of modulation is commonly used for broadcasting music and speech, magnetic tape recording systems, two way radio systems and video transmission systems. When noise occurs naturally in radio systems, frequency modulation with sufficient bandwidth provides an advantage in cancelling the noise.

3. Phase Modulation

In this type of modulation, the phase of the carrier signal varies in accordance with the message signal. When the phase of the signal is changed, then it affects the frequency. So, for this reason, this modulation is also comes under the frequency modulation.

Generally, phase modulation is used for transmitting waves. It is an essential part of many digital transmission coding schemes that underlie a wide range of technologies like GSM, WiFi, and satellite television. This type of modulation is used for signal generation in all synthesizers, such as the Yamaha DX7 to implement FM synthesis.

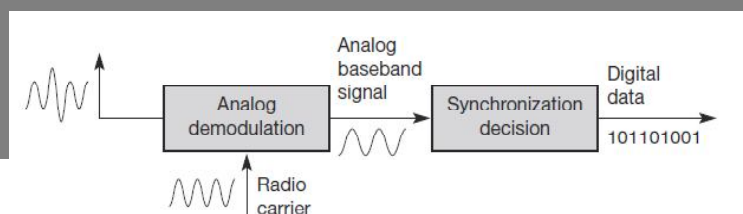


Types of Analog Modulation

Therefore, Analog modulation includes AM, FM and PM and these are more sensitive to noise. If noise enters into a system, it persists and gets carried up to the end receiver. So, this drawback can be overcome by the digital modulation technique.

Digital Modulation

For a better quality and efficient communication, digital modulation technique is employed. The main advantages of the digital modulation over analog modulation include available bandwidth, high noise immunity and permissible power. In digital modulation, a message signal is converted from analog to digital message, and then modulated by using a carrier wave.



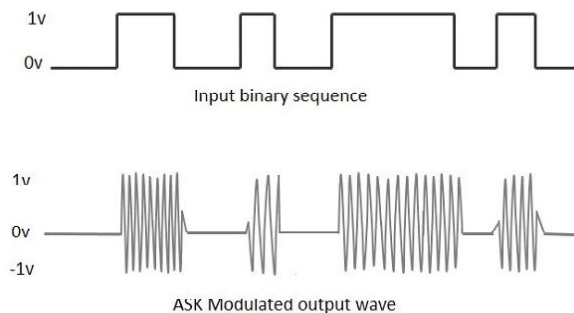
There are three basic ways to modulate a sine wave radio carrier: modifying the amplitude, frequency, or phase.

Amplitude Shift Keying

Amplitude Shift Keying (ASK) is a type of Amplitude Modulation which represents the binary data in the form of variations in the amplitude of a signal.

Any modulated signal has a high frequency carrier. The binary signal when ASK modulated, gives a **zero** value for **Low** input while it gives the **carrier output** for **High** input.

The following figure represents ASK modulated waveform along with its input.



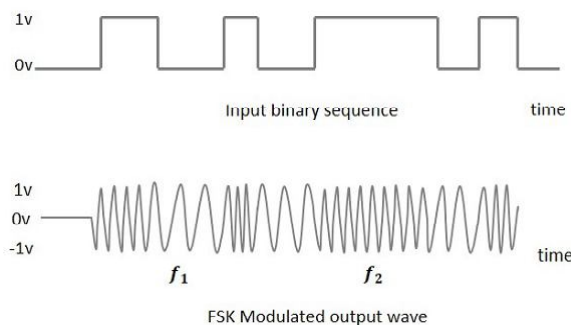
To find the process of obtaining this ASK modulated wave, let us learn about the working of the ASK modulator.

Frequency Shift Keying

Frequency Shift Keying (FSK) is the digital modulation technique in which the frequency of the carrier signal varies according to the digital signal changes. FSK is a scheme of frequency modulation.

The output of a FSK modulated wave is high in frequency for a binary High input and is low in frequency for a binary Low input. The binary **1s** and **0s** are called Mark and Space frequencies.

The following image is the diagrammatic representation of FSK modulated waveform along with its input.



To find the process of obtaining this FSK modulated wave, let us know about the working of a FSK modulator.

Phase Shift Keying

Phase Shift Keying (PSK) is the digital modulation technique in which the phase of the carrier signal is changed by varying the sine and cosine inputs at a particular time. PSK technique is

widely used for wireless LANs, bio-metric, contactless operations, along with RFID and Bluetooth communications.

PSK is of two types, depending upon the phases the signal gets shifted. They are :

► Binary Phase Shift Keying (BPSK)

This is also called as 2-phase PSK or Phase Reversal Keying. In this technique, the sine wave carrier takes two phase reversals such as 0° and 180° .

BPSK is basically a Double Side Band Suppressed Carrier (DSBSC) modulation scheme, for message being the digital information.

► Quadrature Phase Shift Keying (QPSK)

This is the phase shift keying technique, in which the sine wave carrier takes four phase reversals such as 0° , 90° , 180° , and 270° .

If this kind of techniques are further extended, PSK can be done by eight or sixteen values also, depending upon the requirement.

Q12. Explain about advanced shift keying techniques.

Ans :

Advanced frequency shift keying (AFSK)

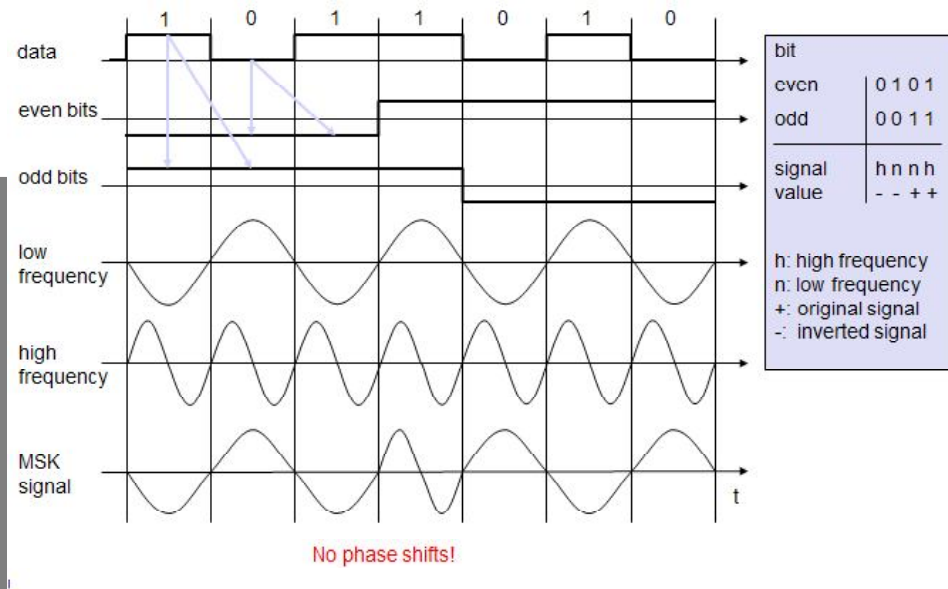
A famous scheme used in many wireless systems is **minimum shift keying (MSK)**. MSK is basically BFSK without **abrupt phase changes** i.e it belongs to CPM schemes. In this data bits are first separated into even and odd bits, the duration of each bit being doubled. This scheme also uses two frequencies : f_1 - lower frequency and f_2 — higher frequency, the higher frequency is twice that of lower frequency, $f_2 = 2 f_1$.

According to this scheme, the lower or higher frequency is chosen to generate the MSK signal:

1. If the even and the odd bit are both 0, then higher frequencies f_2 is inverted. (i.e f_2 is used with phase shift of 180°).
2. If the even bit is 1, odd bit is 0 then the lower frequency f_1 is inverted. This is the case, eg, in the fifth to seventh columns.

3. If the even bit is 0 and the odd bit is 1, f_1 is taken without changing the phase.
4. If both bits are 1 then original f_2 is taken.

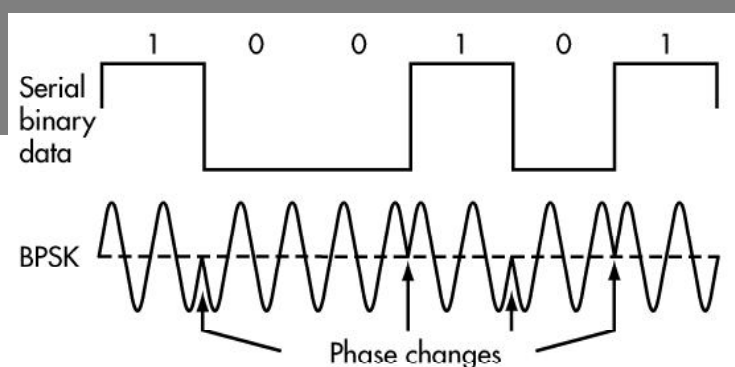
A high frequency is always chosen if even and odd bits are equal. The signal is inverted if odd bit equals 0. This scheme avoids all phase shift in resulting MSK signal.



Advanced Phase Shift Keying

BPSK (Binary Phase Shift Keying):

A very popular digital modulation scheme, binary phase shift keying (BPSK), shifts the carrier sine wave 180° for each change in binary state (Fig. 2). BPSK is coherent as the phase transitions occur at the zero crossing points.



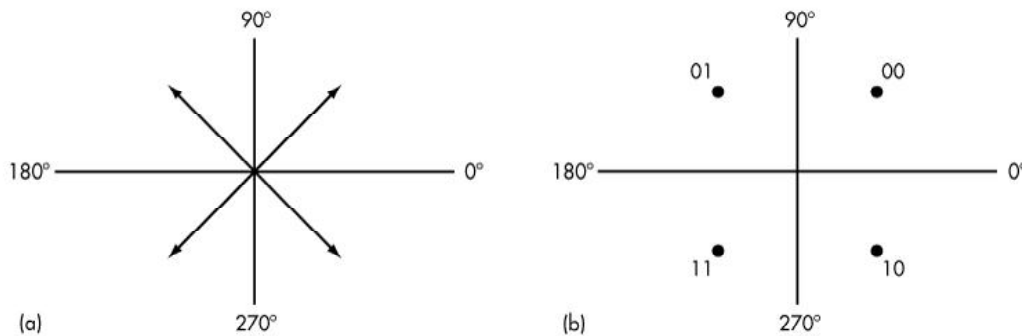
QPSK (Quadrature Phase Shift Keying):

In a popular variation of BPSK, quadrature PSK (QPSK), the modulator produces two sine carriers 90° apart. The binary data modulates each phase, producing four unique sine signals shifted by 45° from one another. The two phases are added together to produce the final signal. Each unique pair of bits generates a carrier with a different phase (Table 1).

TABLE 1: CARRIER PHASE SHIFT FOR EACH PAIR OF BITS REPRESENTED

Bit pairs	Phase (degrees)
0 0	45
0 1	135
1 1	225
1 0	315

Figure a illustrates QPSK with a phasor diagram where the phasor represents the carrier sine amplitude peak and its position indicates the phase. A constellation diagram in Figure b shows the same information. QPSK is very spectrally efficient since each carrier phase represents two bits of data. The spectral efficiency is 2 bits/Hz, meaning twice the data rate can be achieved in the same bandwidth as BPSK.



Multiple Phase Shift Keying (M-PSK)

QPSK produces two bits per symbol, making it very spectrally efficient. QPSK can be referred to as 4-PSK because there are four amplitude-phase combinations. By using smaller phase shifts, more bits can be transmitted per symbol. Some popular variations are 8-PSK and 16-PSK.

8-PSK uses eight symbols with constant carrier amplitude 45° shifts between them, enabling three bits to be transmitted for each symbol. 16-PSK uses 22.5° shifts of constant amplitude carrier signals. This arrangement results in a transmission of 4 bits per symbol.

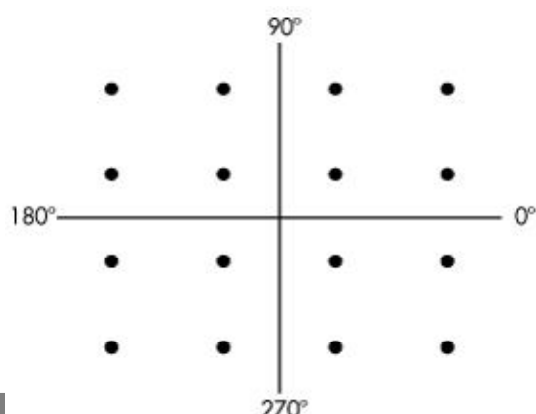
While Multiple Phase Shift Keying (M-PSK) is much more spectrally efficient, the greater the number of smaller phase shifts, the more difficult the signal is to demodulate in the presence of noise. The benefit of M-PSK is that the constant carrier amplitude means that more efficient nonlinear power amplification can be used.

Q13. What is quadrature amplitude modulation.

Ans :

Quadrature Amplitude Modulation (QAM)

The creation of symbols that are some combination of amplitude and phase can carry the concept of transmitting more bits per symbol further. This method is called quadrature amplitude modulation (QAM). For example, 8QAM uses four carrier phases plus two amplitude levels to transmit 3 bits per symbol. Other popular variations are 16QAM, 64QAM, and 256QAM, which transmit 4, 6, and 8 bits per symbol respectively (Fig. 4).



4. 16QAM uses a mix of amplitudes and phases to achieve 4 bits/Hz. In this example, there are three amplitudes and 12 phase shifts.

While QAM is enormously efficient of spectrum, it is more difficult to demodulate in the presence of noise, which is mostly random amplitude variations. Linear power amplification is also required. QAM is very widely used in cable TV, Wi-Fi wireless local-area networks (LANs), satellites, and cellular telephone systems to produce maximum data rate in limited bandwidths.

1.2.7 Spread Spectrum

Q14. What is spread spectrum ?

Ans :

A collective class of signalling techniques are employed before transmitting a signal to provide a secure communication, known as the **Spread Spectrum Modulation**. The main advantage of spread spectrum communication technique is to prevent "interference" whether it is intentional or unintentional.

The signals modulated with these techniques are hard to interfere and cannot be jammed. An intruder with no official access is never allowed to crack them. Hence, these techniques are used for military purposes. These spread spectrum signals transmit at low power density and has a wide spread of signals.

Pseudo-Noise Sequence

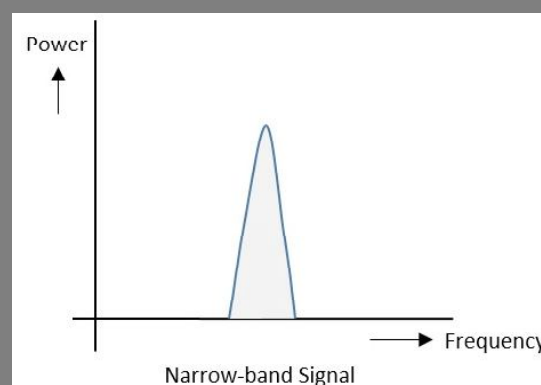
A coded sequence of **1s** and **0s** with certain auto-correlation properties, called as **Pseudo-Noise coding sequence** is used in spread spectrum techniques. It is a maximum-length sequence, which is a type of cyclic code.

Narrow-band and Spread-spectrum Signals

Both the Narrow band and Spread spectrum signals can be understood easily by observing their frequency spectrum as shown in the following figures.

Narrow-band Signals

The Narrow-band signals have the signal strength concentrated as shown in the following frequency spectrum figure.



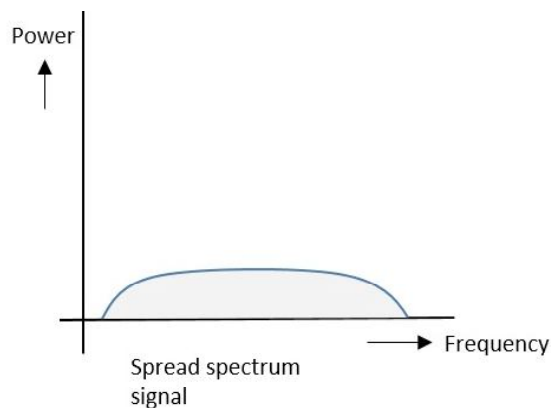
Following are some of its features "

- ▶ Band of signals occupy a narrow range of frequencies.
- ▶ Power density is high.
- ▶ Spread of energy is low and concentrated.

Though the features are good, these signals are prone to interference.

Spread Spectrum Signals

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



Following are some of its features “

- ▶ Band of signals occupy a wide range of frequencies.
- ▶ Power density is very low.
- ▶ Energy is wide spread.

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

Q15. Explain various types of spread spectrum signals.

Ans :

Spread spectrum multiple access techniques uses signals which have a transmission bandwidth of a magnitude greater than the minimum required RF bandwidth.

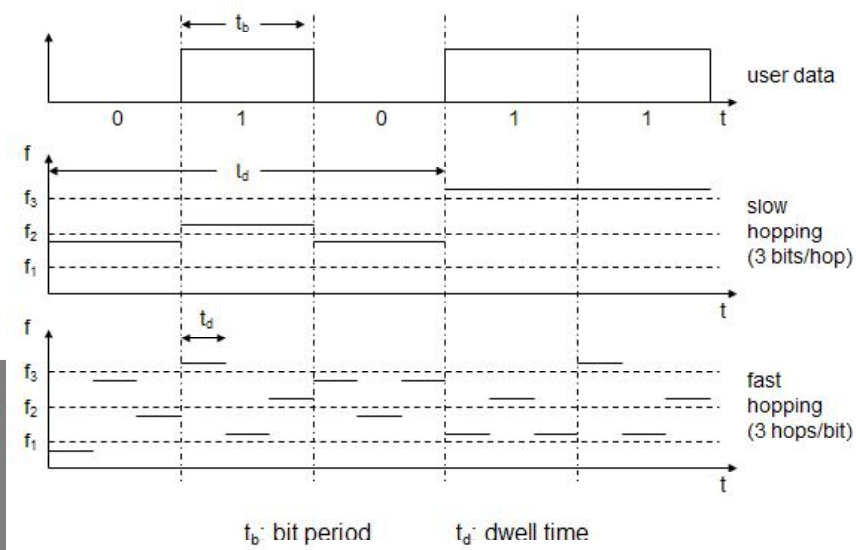
These are of two types.

- ▶ Frequency Hopped Spread Spectrum (FHSS)
- ▶ Direct Sequence Spread Spectrum (DSSS)

Frequency Hopped Spread Spectrum (FHSS)

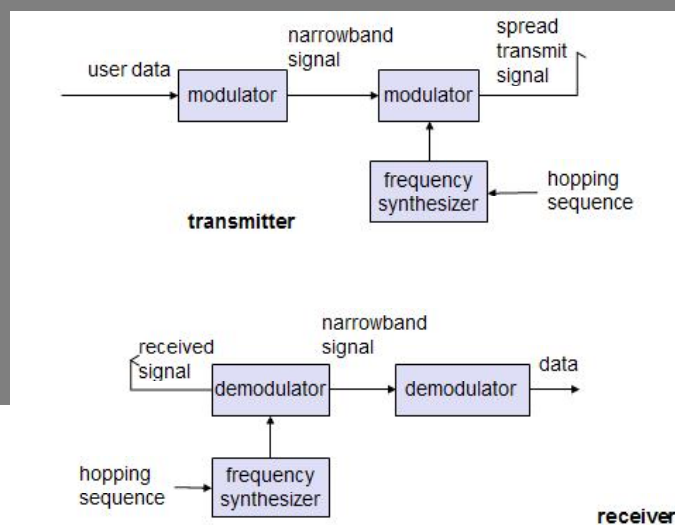
This is frequency hopping technique, where the users are made to change the frequencies of usage, from one to another in a specified time interval, hence called as **frequency hopping**. For example, a frequency was allotted to sender 1 for a particular period of time. Now, after a while, sender 1 hops to the other frequency and sender 2 uses the first frequency, which was previously used by sender 1. This is called as **frequency reuse**.

The frequencies of the data are hopped from one to another in order to provide a secure transmission. The amount of time spent on each frequency hop is called as **Dwell time**.



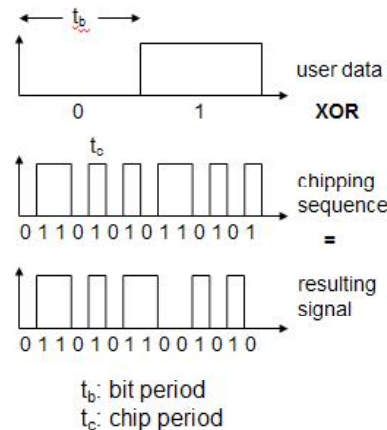
FSSS Receiver and Transmitter

The receiver of an FHSS system has to know the hopping sequence and must stay synchronized. It then performs the inverse operations of the modulation to reconstruct user data.



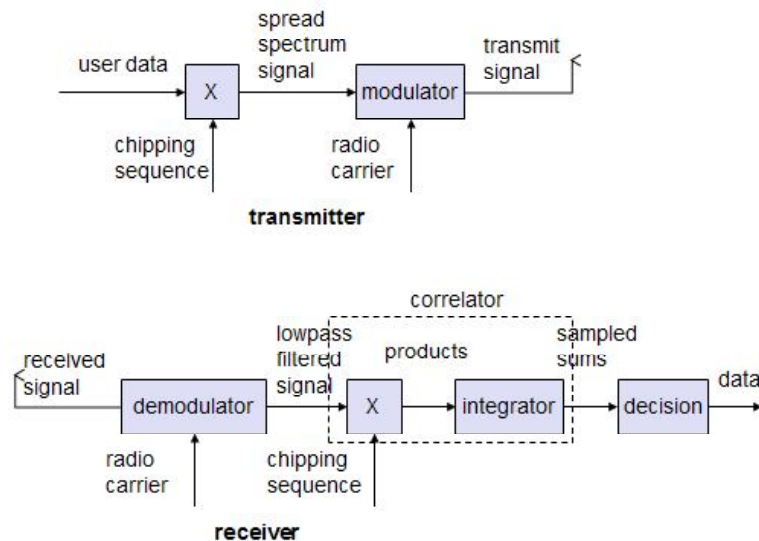
Direct Sequence Spread Spectrum (DSSS)

Whenever a user wants to send data using this DSSS technique, each and every bit of the user data is multiplied by a secret code, called as **chipping code**. This chipping code is nothing but the spreading code which is multiplied with the original message and transmitted. The receiver uses the same code to retrieve the original message.



DSSS receiver and Transmitter

The DSSS receiver is more complex than the transmitter. The receiver only has to perform the inverse functions of the two transmitter modulation steps. However, noise and multi-path propagation require additional mechanisms to reconstruct the original data. The first step in the receiver involves demodulating the received signal. This is achieved using the same carrier as the transmitter reversing the modulation and results in a signal with approximately the same bandwidth as the original spread spectrum signal.



Q16. Differentiate between FHSS and DSSS/CDMA.

Ans :

Comparison between FHSS and DSSS/CDMA

Both the spread spectrum techniques are popular for their characteristics. To have a clear understanding, let us take a look at their comparisons.

FHSS	DSSS / CDMA
Multiple frequencies are used	Single frequency is used
Hard to find the user's frequency at any instant of time between them	User frequency, once allotted is always the same
Frequency reuse is allowed	Frequency reuse is not allowed
Sender need not wait	Sender has to wait if the spectrum is busy
Power strength of the signal is high	Power strength of the signal is low
Stronger and penetrates through the obstacles	It is weaker compared to FHSS
It is never affected by interference	It can be affected by interference
It is cheaper	It is expensive
This is the commonly used technique	This technique is not frequently used

Q17. What are the advantages of spread spectrum ?

Ans :

Advantages of Spread Spectrum

Following are the advantages of spread spectrum "

- ▶ Cross-talk elimination
- ▶ Better output with data integrity
- ▶ Reduced effect of multipath fading
- ▶ Better security
- ▶ Reduction in noise
- ▶ Co-existence with other systems
- ▶ Longer operative distances
- ▶ Hard to detect
- ▶ Not easy to demodulate/decode
- ▶ Difficult to jam the signals

Although spread spectrum techniques were originally designed for military uses, they are now being used widely for commercial purpose.

1.2.8 Cellular System

Q18. Write a note on cell structure.

Ans :

Geographic region is subdivided in radio cells. Base Station provides radio connectivity to Mobile Station within cell. Handover to neighboring base station when necessary. Base Stations connected by some networking infrastructure.

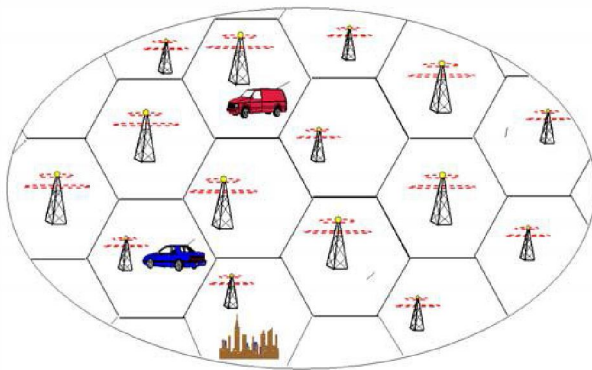


Fig. : Cellular Networks

Cell Structure

Each transmitter, typically called a **base station**, covers a certain area, a **cell**. Cell radii can vary from tens of meters in buildings, and hundreds of meters in cities, up to tens of kilometers in the countryside. The shape of cells are never perfect circles or hexagons.

Advantages of cellular systems with small cells are the following :

- ▶ **Higher capacity:** Implementing SDM allows frequency reuse. If one transmitter is far away from another, i.e., outside the interference range, it can reuse the same frequencies.
- ▶ **Less transmission power:** A receiver far away from a base station would need much more transmit power than the current few Watts. With small cells receiver is not far away from the base station.
- ▶ **Local interference only:** Having long distances between sender and receiver results

in even more interference problems. With small cells, mobile stations and base stations only have to deal with 'local' interference.

- ▶ **Robustness:** Cellular systems are decentralized and so, more robust against the failure of single components. If one antenna fails, this only influences communication within a small area.

Small cells also have some **disadvantages**:

- ▶ **Infrastructure needed:** Cellular systems need a complex infrastructure to connect all base stations. This includes many antennas, switches for call forwarding, location registers to find a mobile station etc, which makes the whole system quite expensive.
- ▶ **Handover needed:** The mobile station has to perform a handover when changing from one cell to another. Depending on the cell size and the speed of movement, this can happen quite often.
- ▶ **Frequency planning:** To avoid interference between transmitters using the same frequencies, frequencies have to be distributed carefully. On the one hand, interference should be avoided, on the other, only a limited number of frequencies is available.

Q19. What is frequency reuse or frequency planning ?

Ans :

Frequency reuse or frequency planning

To avoid interference, different transmitters within each other's interference range use FDM. Two possible models to create cell patterns with minimal interference are shown in Figure. Cells are combined in **clusters** – on the left side three cells form a cluster, on the right side seven cells form a cluster.

All cells within a cluster use disjointed sets of frequencies. On the left side, one cell in the cluster uses set f1, another cell f2, and the third cell f3.

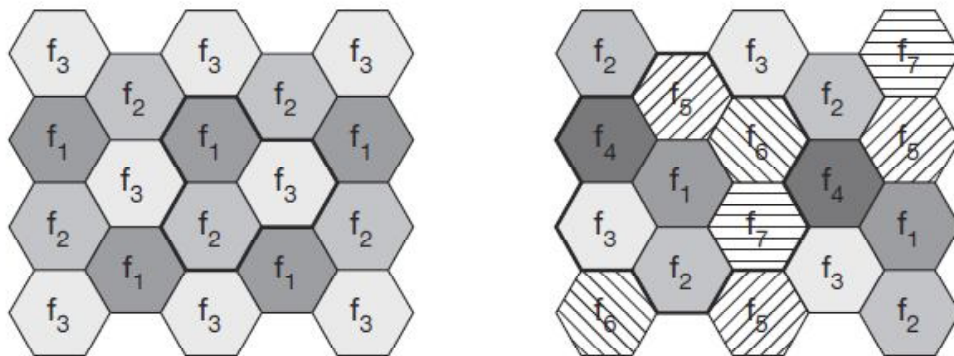
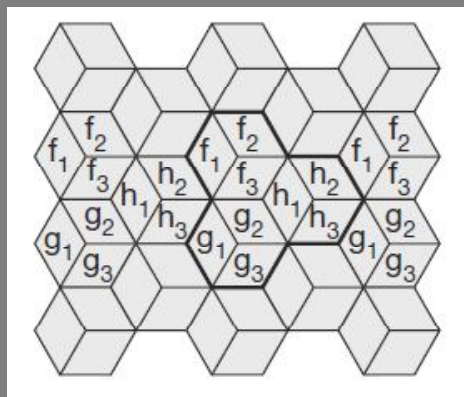


Fig. : Cellular system with three and seven cell clusters

To reduce interference even further (and under certain traffic conditions, i.e., number of users per km²) **sectorized antennas** can be used. Figure shows the use of three sectors per cell in a cluster with three cells.



For instance, in the case of a heavy load in one cell and a light load in a neighboring cell, it could make sense to 'borrow' frequencies. Cells with more traffic are dynamically allotted more frequencies. This scheme is known as **borrowing channel allocation (BCA)**, while the first fixed scheme is called **fixed channel allocation (FCA)**. In **dynamic channel allocation (DCA)** scheme frequencies can only be borrowed, but it is also possible to freely assign frequencies to cells.

20. What is cell breathing ?

Ans :

Cell breathing

Cell planning faces another problem – the cell size depends on the current load. Accordingly, **CDM cells** are commonly said to '**breathe**'. While a cell can cover a larger area under a light load, it shrinks if the load increases. The reason for this is the growing noise level if more users are in a cell.

The higher the noise, the higher the path loss and the higher the transmission errors. Finally, mobile stations further away from the base station drop out of the cell.

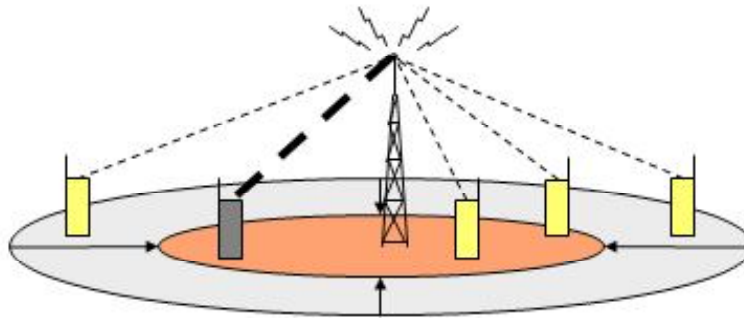


Fig. : cell breathing depending on the current load

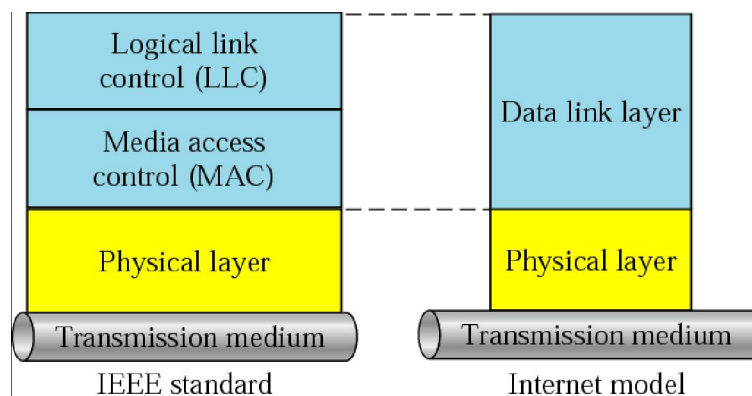
1.3 MEDIA ACCESS CONTROL

1.3.1 Motivation for a Specialized MAC

Q21. Write a note on media access control.

Ans :

The **Media Access Control (MAC)** data communication protocol sub-layer, also known as the Medium Access Control, is a sublayer of the Data Link Layer specified in the seven-layer OSI model (layer 2). The hardware that implements the MAC is referred to as a **Medium Access Controller**. The MAC sub-layer acts as an interface between the Logical Link Control (LLC) sublayer and the network's physical layer. The MAC layer emulates a full-duplex logical communication channel in a multi-point network. This channel may provide unicast, multicast or broadcast communication service.



LLC and MAC Sublayers

One of the most commonly used MAC schemes for wired networks is carrier sense multiple access with collision detection (CSMA/CD). In this scheme, a sender senses the medium (a wire or coaxial cable) to see if it is free. If the medium is busy, the sender waits until it is free. If the medium is free, the sender starts transmitting data and continues to listen into the medium. If the sender detects a collision while sending, it stops at once and sends a jamming signal. But this scheme does not work well with wireless networks. The problems are :

- Signal strength decreases proportional to the square of the distance.

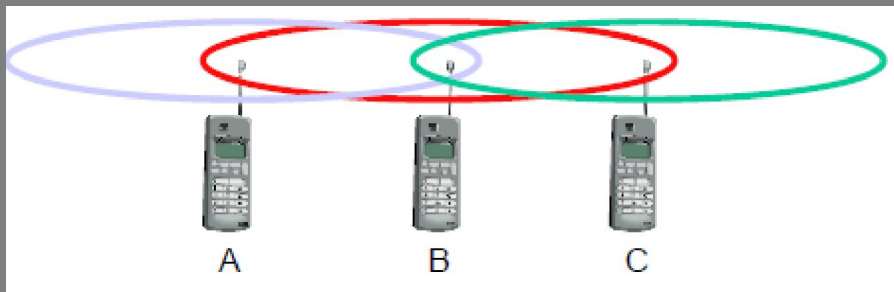
- ▶ The sender would apply CS and CD, but the collisions happen at the receiver.
- ▶ It might be a case that a sender cannot "hear" the collision, i.e., CD does not work.
- ▶ Furthermore, CS might not work, if for e.g., a terminal is "hidden".

Q22. Explain Hidden and Exposed Terminals.

Ans :

Hidden and Exposed Terminals

Consider the scenario with three mobile phones as shown below. The transmission range of A reaches B, but not C (the detection range does not reach C either). The transmission range of C reaches B, but not A. Finally, the transmission range of B reaches A and C, i.e., A cannot detect C and vice versa.



Hidden Terminals

- ▶ A sends to B, C cannot hear A
- ▶ C wants to send to B, C senses a "free" medium (CS fails) and starts transmitting
- ▶ Collision at B occurs, A cannot detect this collision (CD fails) and continues with its transmission to B
- ▶ A is "hidden" from C and vice versa

Exposed Terminals

- ▶ B sends to A, C wants to send to another terminal (not A or B) outside the range
- ▶ C senses the carrier and detects that the carrier is busy.
- ▶ C postpones its transmission until it detects the medium as being idle again
- ▶ but A is outside radio range of C, waiting is **not** necessary
- ▶ C is "exposed" to B

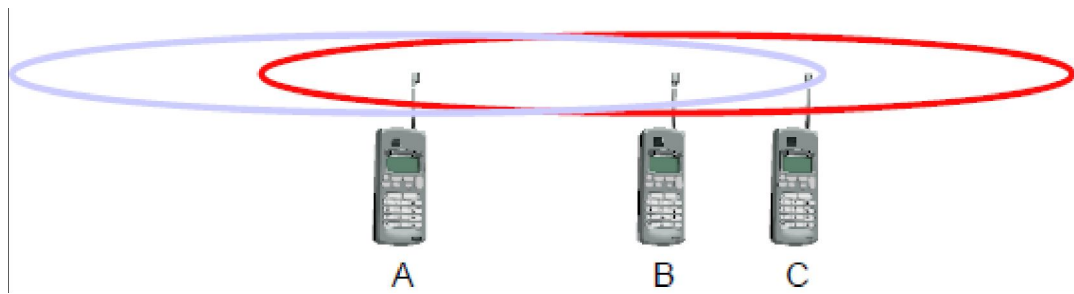
Hidden terminals cause collisions, whereas Exposed terminals cause unnecessary delay.

Q23. Explain near and far terminals.

Ans :

Near and Far Terminals

Consider the situation shown below. A and B are both sending with the same transmission power.



- ▶ Signal strength decreases proportional to the square of the distance
- ▶ So, B's signal drowns out A's signal making C unable to receive A's transmission
- ▶ If C is an arbiter for sending rights, B drowns out A's signal on the physical layer making C unable to hear out A.

The **near/far effect** is a severe problem of wireless networks using CDM. All signals should arrive at the receiver with more or less the same strength for which Precise power control is to be implemented.

1.3.2 SDMA

Q24. What is SDMA ?

Ans :

Space Division Multiple Access (SDMA) is used for allocating a separated space to users in wireless networks. A typical application involves assigning an optimal base station to a mobile phone user. The mobile phone may receive several base stations with different quality. A MAC algorithm could now decide which base station is best, taking into account which frequencies (FDM), time slots (TDM) or code (CDM) are still available.

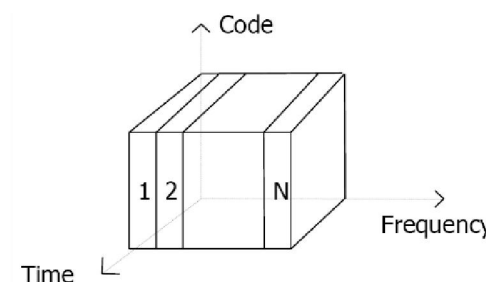
The basis for the SDMA algorithm is formed by cells and sectorized antennas which constitute the infrastructure implementing **space division multiplexing (SDM)**. SDM has the unique advantage of not requiring any multiplexing equipment. It is usually combined with other multiplexing techniques to better utilize the individual physical channels.

1.3.3 FDMA

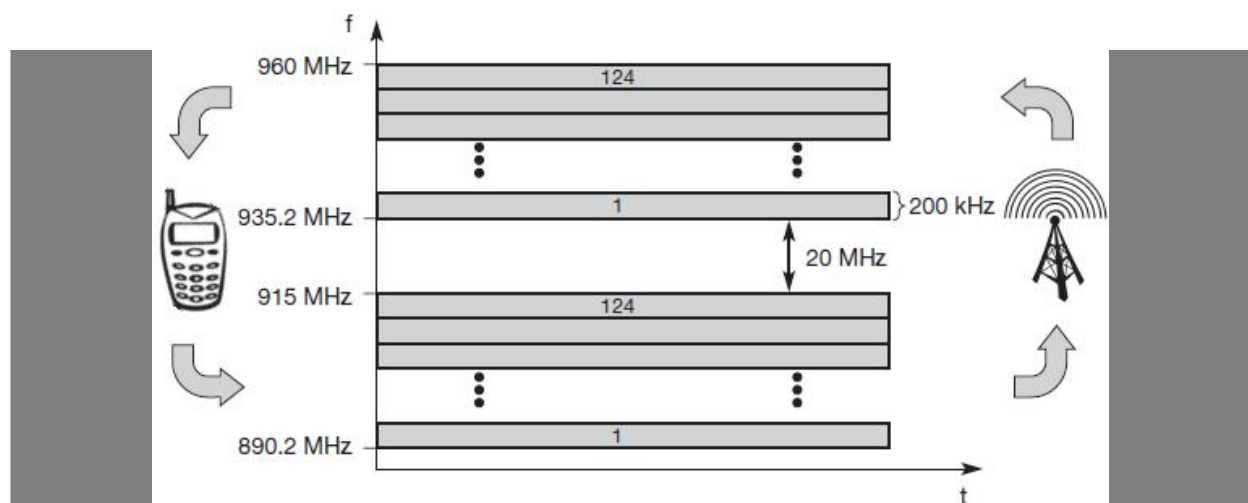
Q25. Discuss briefly about FDMA.

Ans :

Frequency division multiplexing (FDM) describes schemes to subdivide the frequency dimension into several non-overlapping frequency bands.



Frequency Division Multiple Access is a method employed to permit several users to transmit simultaneously on one satellite transponder by assigning a specific frequency within the channel to each user. Each conversation gets its own, unique, radio channel. The channels are relatively narrow, usually 30 KHz or less and are defined as either transmit or receive channels. A full duplex conversation requires a transmit & receive channel pair. FDM is often used for simultaneous access to the medium by base station and mobile station in cellular networks establishing a duplex channel. A scheme called **frequency division duplexing (FDD)** in which the two directions, mobile station to base station and vice versa are now separated using different frequencies.



FDMA for Multiple Access and Duplex

The two frequencies are also known as **uplink**, i.e., from mobile station to base station or from ground control to satellite, and as **downlink**, i.e., from base station to mobile station or from satellite to ground control. The basic frequency allocation scheme for GSM is fixed and regulated by national authorities. All uplinks use the band between 890.2 and 915 MHz, all downlinks use 935.2 to 960 MHz. According to FDMA, the base station, shown on the right side, allocates a certain frequency for up- and downlink to establish a duplex channel with a mobile phone. Up- and downlink have a fixed relation. If the uplink frequency is $f_u = 890 \text{ MHz} + n \cdot 0.2 \text{ MHz}$, the downlink frequency is $f_d = f_u + 45 \text{ MHz}$, i.e., **$f_d = 935 \text{ MHz} + n \cdot 0.2 \text{ MHz}$** for a certain channel n . The base station selects the channel. Each channel (uplink and downlink) has a bandwidth of 200 kHz.

This scheme also has disadvantages. While radio stations broadcast 24 hours a day, mobile communication typically takes place for only a few minutes at a time. Assigning a separate frequency for each possible communication scenario would be a tremendous waste of (scarce) frequency resources. Additionally, the fixed assignment of a frequency to a sender makes the scheme very inflexible and limits the number of senders.

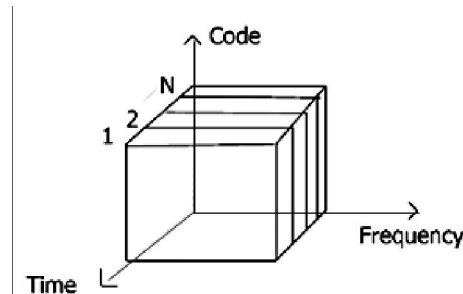
1.3.4 TDMA

Q26. What is TDMA. Explain different schemes of TDMA ?

Ans :

Compared to FDMA, time division multiple access (TDMA) offers a much more flexible scheme, which comprises all technologies that allocate certain time slots for communication. Now synchronization

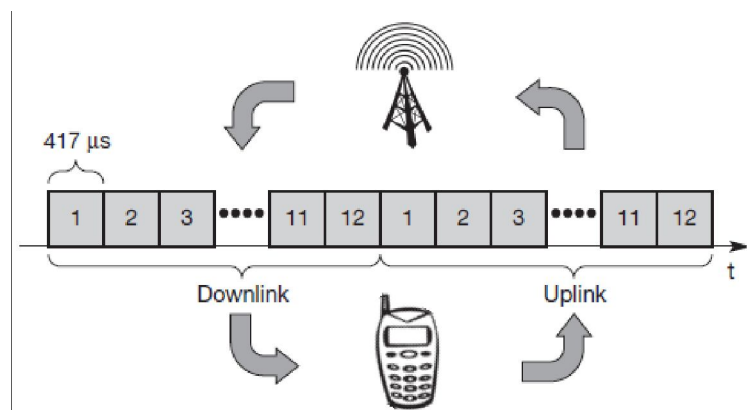
between sender and receiver has to be achieved in the time domain. Again this can be done by using a fixed pattern similar to FDMA techniques, i.e., allocating a certain time slot for a channel, or by using a dynamic allocation scheme.



Listening to different frequencies at the same time is quite difficult, but listening to many channels separated in time at the same frequency is simple. Fixed schemes do not need identification, but are not as flexible considering varying bandwidth requirements.

Fixed TDM

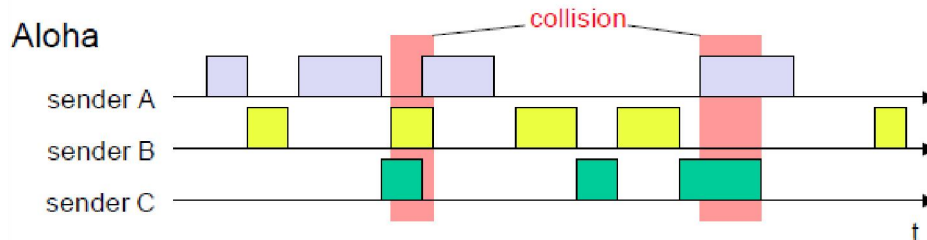
The simplest algorithm for using TDM is allocating time slots for channels in a fixed pattern. This results in a fixed bandwidth and is the typical solution for wireless phone systems. MAC is quite simple, as the only crucial factor is accessing the reserved time slot at the right moment. If this synchronization is assured, each mobile station knows its turn and no interference will happen. The fixed pattern can be assigned by the base station, where competition between different mobile stations that want to access the medium is solved.



The above figure shows how these fixed TDM patterns are used to implement multiple access and a duplex channel between a base station and mobile station. Assigning different slots for uplink and downlink using the same frequency is called **time division duplex (TDD)**. As shown in the figure, the base station uses one out of 12 slots for the downlink, whereas the mobile station uses one out of 12 different slots for the uplink. Uplink and downlink are separated in time. Up to 12 different mobile stations can use the same frequency without interference using this scheme. Each connection is allotted its own up- and downlink pair. This general scheme still wastes a lot of bandwidth. It is too static, too inflexible for data communication. In this case, connectionless, demand-oriented TDMA schemes can be used.

Classical Aloha

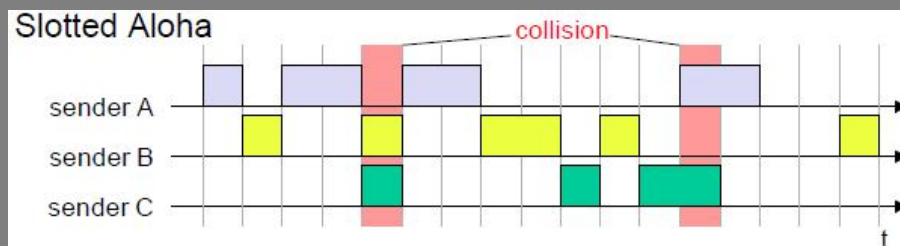
In this scheme, TDM is applied without controlling medium access. Here each station can access the medium at any time as shown below:



This is a random access scheme, without a central arbiter controlling access and without coordination among the stations. If two or more stations access the medium at the same time, a **collision** occurs and the transmitted data is destroyed. Resolving this problem is left to higher layers (e.g., retransmission of data). The simple Aloha works fine for a light load and does not require any complicated access mechanisms.

Slotted Aloha

The first refinement of the classical Aloha scheme is provided by the introduction of time slots (**slotted Aloha**). In this case, all senders have to be **synchronized**, transmission can only start at the beginning of a **time slot** as shown below.



The introduction of slots raises the throughput from 18 per cent to 36 per cent, i.e., slotting doubles the throughput. Both basic Aloha principles occur in many systems that implement distributed access to a medium. Aloha systems work perfectly well under a light load, but they cannot give any hard transmission guarantees, such as maximum delay before accessing the medium or minimum throughput.

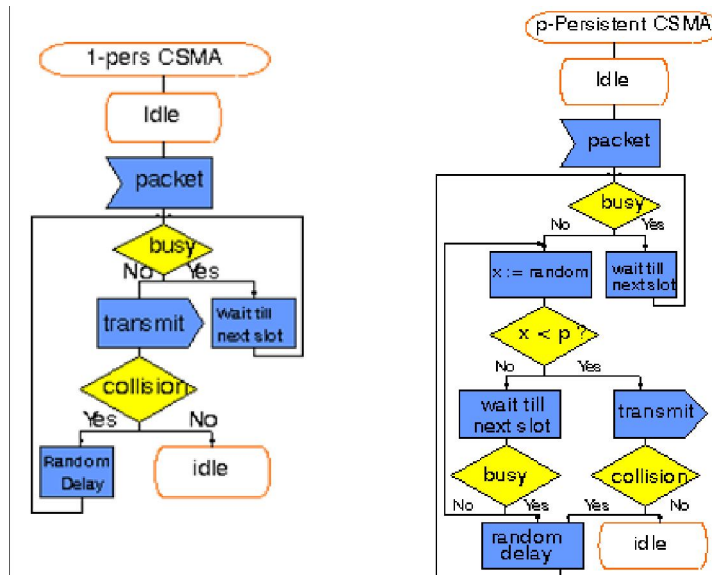
Carrier sense multiple access

One improvement to the basic Aloha is sensing the carrier before accessing the medium. Sensing the carrier and accessing the medium only if the carrier is idle decreases the probability of a collision. But, as already mentioned in the introduction, hidden terminals cannot be detected, so, if a hidden terminal transmits at the same time as another sender, a collision might occur at the receiver. This basic scheme is still used in most wireless LANs. The different versions of CSMA are:

- ▶ **1-persistent CSMA:** Stations sense the channel and listens if its busy and transmit immediately, when the channel becomes idle. It's called 1-persistent CSMA because the host transmits with a probability of 1 whenever it finds the channel idle.
- ▶ **non-persistent CSMA:** stations sense the carrier and start sending immediately if the medium is idle. If the medium is busy, the station pauses a random amount of time before sensing the medium again and repeating this pattern.

- **p-persistent CSMA:** systems nodes also sense the medium, but only transmit with a probability of p , with the station deferring to the next slot with the probability $1-p$, i.e., access is slotted in addition

CSMA with collision avoidance (**CSMA/CA**) is one of the access schemes used in wireless LANs following the standard IEEE 802.11. Here sensing the carrier is combined with a back-off scheme in case of a busy medium to achieve some fairness among competing stations.

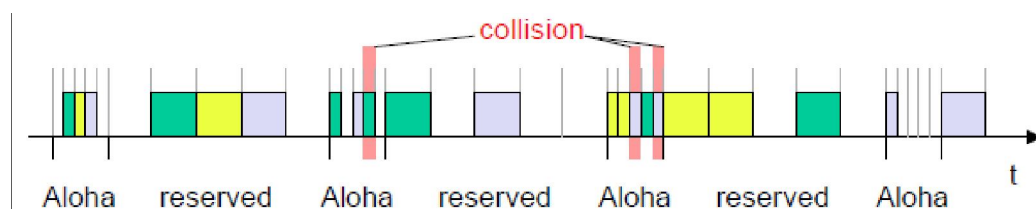


Demand Assigned Multiple Access

Channel efficiency for Aloha is 18% and for slotted Aloha is 36%. It can be increased to 80% by implementing reservation mechanisms and combinations with some (fixed) TDM patterns. These schemes typically have a reservation period followed by a transmission period. During the reservation period, stations can reserve future slots in the transmission period. While, depending on the scheme, collisions may occur during the reservation period, the transmission period can then be accessed without collision.

One basic scheme is **demand assigned multiple access (DAMA)** also called **reservation Aloha**, a scheme typical for satellite systems. It increases the amount of users in a pool of satellite channels that are available for use by any station in a network. It is assumed that not all users will need simultaneous access to the same communication channels. So that a call can be established, DAMA assigns a pair of available channels based on requests issued from a user. Once the call is completed, the channels are returned to the pool for an assignment to another call. Since the resources of the satellite are being used only in proportion to the occupied channels for the time in which they are being held, it is a perfect environment for voice traffic and data traffic in batch mode.

It has two modes as shown below.

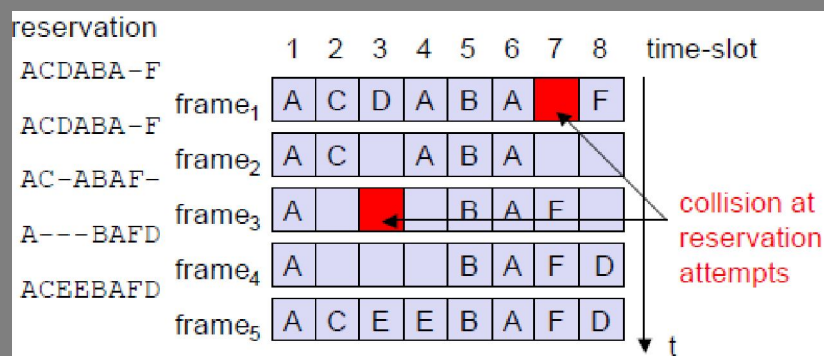


During a contention phase following the slotted Aloha scheme; all stations can try to reserve future slots. Collisions during the reservation phase do not destroy data transmission, but only the short requests for

data transmission. If successful, a time slot in the future is reserved, and no other station is allowed to transmit during this slot. Therefore, the satellite collects all successful requests (the others are destroyed) and sends back a reservation list indicating access rights for future slots. All ground stations have to obey this list. To maintain the fixed TDM pattern of reservation and transmission, the stations have to be synchronized from time to time. DAMA is an **explicit reservation** scheme. Each transmission slot has to be reserved explicitly.

PRMA packet reservation multiple access

It is a kind of implicit reservation scheme where, slots can be reserved implicitly. A certain number of slots form a frame. The frame is repeated in time i.e., a fixed TDM pattern is applied. A base station, which could be a satellite, now broadcasts the status of each slot to all mobile stations. All stations receiving this vector will then know which slot is occupied and which slot is currently free.



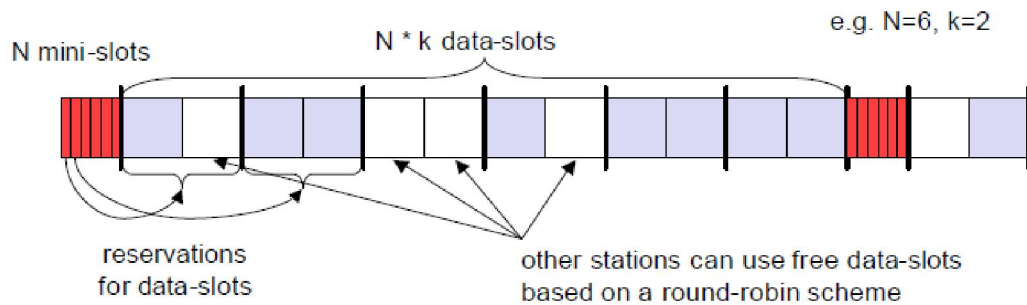
The base station broadcasts the reservation status 'ACDABA-F' to all stations, here A to F. This means that slots one to six and eight are occupied, but slot seven is free in the following transmission. All stations wishing to transmit can now compete for this free slot in Aloha fashion. The already occupied slots are not touched. In the example shown, more than one station wants to access this slot, so a collision occurs.

The base station returns the reservation status 'ACDABA-F', indicating that the reservation of slot seven failed (still indicated as free) and that nothing has changed for the other slots. Again, stations can compete for this slot. Additionally, station D has stopped sending in slot three and station F in slot eight. This is noticed by the base station after the second frame. Before the third frame starts, the base station indicates that slots three and eight are now idle. Station F has succeeded in reserving slot seven as also indicated by the base station.

As soon as a station has succeeded with a reservation, all future slots are implicitly reserved for this station. This ensures transmission with a guaranteed data rate. The slotted aloha scheme is used for idle slots only; data transmission is not destroyed by collision.

Reservation TDMA

In a fixed TDM scheme N mini-slots followed by $N \cdot k$ data-slots form a frame that is repeated. Each station is allotted its own mini-slot and can use it to reserve up to k data-slots.



This guarantees each station a certain bandwidth and a fixed delay. Other stations can now send data in unused data-slots as shown. Using these free slots can be based on a simple round-robin scheme or can be uncoordinated using an Aloha scheme. This scheme allows for the combination of, e.g., isochronous traffic with fixed bitrates and best-effort traffic without any guarantees.

1.3.5 CDMA

Q27. What is CDMA ? Explain about it.

Ans :

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.

Code Division Multiple Access system is very different from time and frequency multiplexing. In this system, a user has access to the whole bandwidth for the entire duration. The basic principle is that different CDMA codes are used to distinguish among the different users.

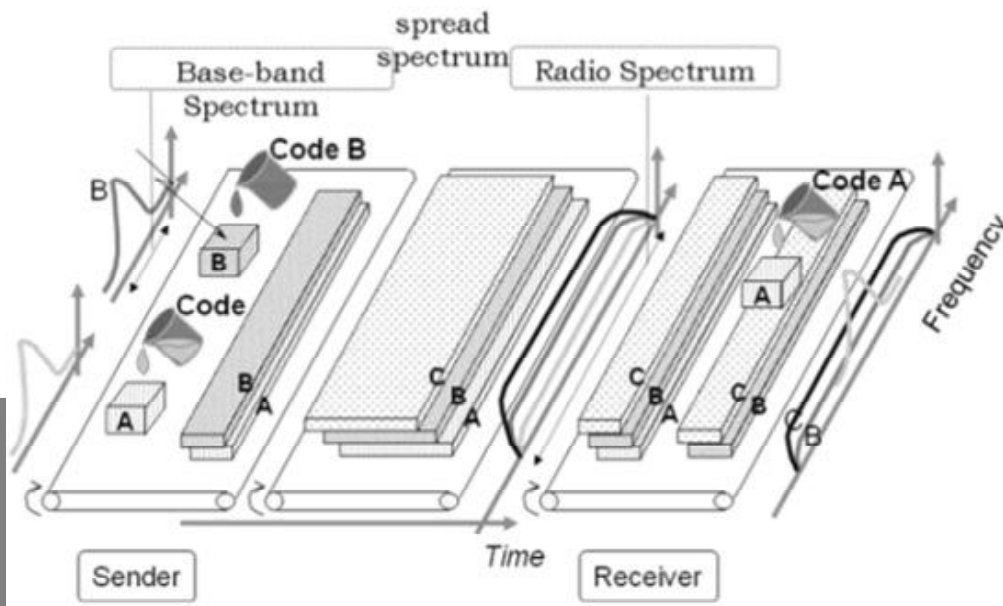
Techniques generally used are direct sequence spread spectrum modulation (DS-CDMA), frequency hopping or mixed CDMA detection (JDCDMA). Here, a signal is generated which extends over a wide bandwidth. A code called **spreading code** is used to perform this action. Using a group of codes, which are orthogonal to each other, it is possible to select a signal with a given code in the presence of many other signals with different orthogonal codes.

How Does CDMA Work?

CDMA allows up to 61 concurrent users in a 1.2288 MHz channel by processing each voice packet with two PN codes. There are 64 Walsh codes available to differentiate between calls and theoretical limits. Operational limits and quality issues will reduce the maximum number of calls somewhat lower than this value.

In fact, many different "signals" baseband with different spreading codes can be modulated on the same carrier to allow many different users to be supported. Using different orthogonal codes, interference between the signals is minimal. Conversely, when signals are received from several mobile stations, the base station is capable of isolating each as they have different orthogonal spreading codes.

The following figure shows the technicality of the CDMA system. During the propagation, we mixed the signals of all users, but by that you use the same code as the code that was used at the time of sending the receiving side. You can take out only the signal of each user.



CDMA Capacity

The factors deciding the CDMA capacity are :

- ▶ Processing Gain
- ▶ Signal to Noise Ratio
- ▶ Voice Activity Factor
- ▶ Frequency Reuse Efficiency

Capacity in CDMA is soft, CDMA has all users on each frequency and users are separated by code. This means, CDMA operates in the presence of noise and interference.

In addition, neighboring cells use the same frequencies, which means no re-use. So, CDMA capacity calculations should be very simple. No code channel in a cell, multiplied by no cell. But it is not that simple. Although not available code channels are 64, it may not be possible to use a single time, since the CDMA frequency is the same.

Centralized Methods

- ▶ The band used in CDMA is 824 MHz to 894 MHz (50 MHz + 20 MHz separation).
- ▶ Frequency channel is divided into code channels.
- ▶ 1.25 MHz of FDMA channel is divided into 64 code channels.

Processing Gain

CDMA is a spread spectrum technique. Each data bit is spread by a code sequence. This means, energy per bit is also increased. This means that we get a gain of this.

$$P(\text{gain}) = 10 \log (W/R)$$

W is Spread Rate

R is Data Rate

$$\text{For CDMA } P(\text{gain}) = 10 \log (1228800/9600) = 21\text{dB}$$

This is a gain factor and the actual data propagation rate. On an average, a typical transmission condition requires a signal to the noise ratio of 7 dB for the adequate quality of voice.

Translated into a ratio, signal must be five times stronger than noise.

$$\text{Actual processing gain} = P(\text{gain}) - \text{SNR}$$

$$= 21 - 7 = 14\text{dB}$$

CDMA uses variable rate coder

The Voice Activity Factor of 0.4 is considered = -4dB.

Hence, CDMA has 100% frequency reuse. Use of same frequency in surrounding cells causes some additional interference.

$$\text{In CDMA frequency, reuse efficiency is } 0.67 \text{ (70\% eff.)} = -1.73\text{dB}$$

Advantages of CDMA

CDMA has a soft capacity. The greater the number of codes, the more the number of users. It has the following advantages :

- ▶ CDMA requires a tight power control, as it suffers from near-far effect. In other words, a user near the base station transmitting with the same power will drown the signal latter. All signals must have more or less equal power at the receiver
- ▶ Rake receivers can be used to improve signal reception. Delayed versions of time (a chip or later) of the signal (multipath signals) can be collected and used to make decisions at the bit level.
- ▶ Flexible transfer may be used. Mobile base stations can switch without changing operator. Two base stations receive mobile signal and the mobile receives signals from the two base stations.
- ▶ Transmission Burst " reduces interference.

Disadvantages of CDMA

The disadvantages of using CDMA are as follows :

- ▶ The code length must be carefully selected. A large code length can induce delay or may cause interference.
- ▶ Time synchronization is required.
- ▶ Gradual transfer increases the use of radio resources and may reduce capacity.
- ▶ As the sum of the power received and transmitted from a base station needs constant tight power control. This can result in several handovers.

1.3.6 Comparisons

Q28. Compare among SDMA, TDMA, FDMA and CDMA.

Ans :

Approach	SDMA	TDMA	FDMA	CDMA
Idea	segment space into cells/sectors	segment sending time into disjoint time-slots, demand driven or fixed patterns	segment the frequency band into disjoint sub-bands	spread the spectrum using orthogonal codes
Terminals	only one terminal can be active in one cell/one sector	all terminals are active for short periods of time on the same frequency	every terminal has its own frequency, uninterrupted	all terminals can be active at the same place at the same moment, uninterrupted
Signal separation	cell structure, directed antennas	synchronization in the time domain	filtering in the frequency domain	code plus special receivers
Advantages	very simple, increases capacity per km ²	established, fully digital, flexible	simple, established, robust	flexible, less frequency planning needed, soft handover
Dis-advantages	inflexible, antennas typically fixed	guard space needed (multipath propagation). synchronization difficult	inflexible, frequencies are a scarce resource	complex receivers, needs more complicated power control for senders
Comment	only in combination with TDMA, FDMA or CDMA useful	standard in fixed networks, together with FDMA/SDMA used in many mobile networks	typically combined with TDMA (frequency hopping patterns) and SDMA (frequency reuse)	still faces some problems, higher complexity, lowered expectations; will be integrated with TDMA/FDMA

UNIT II

GSM, DECT, Wireless LAN : Infrared vs. Radio Transmission, Infrastructure and ad-hoc Networks, IEEE 802.11, HPERLAN, Bluetooth.

2.1 GSM

GSM Services

Q1. Write about the services provided by GSM.

Ans :

GSM is the most successful digital mobile telecommunication system in the world today. GSM permits the integration of different voice and data services and the interworking with existing networks. Services make a network interesting for customers.

GSM has defined three different categories of services: **bearer, tele and supplementary services.**

Bearer Services

GSM specifies different mechanisms for data transmission, the original GSM allowing for data rates of up to 9600 bit/s for non-voice services.

Bearer services permit transparent and non-transparent, synchronous or asynchronous data transmission.

Transparent bearer services only use the functions of the physical layer (layer 1) to transmit data. Data transmission has a constant delay and throughput if no transmission errors occur. Transmission quality can be improved with the use of **forward error correction (FEC)**, which codes redundancy into the data stream and helps to reconstruct the original data in case of transmission errors.

Transparent bearer services do not try to recover lost data in case of, for example, shadowing or interruptions due to handover.

Non-transparent bearer services use protocols of layers two and three to implement error correction and flow control.

These services use the transparent bearer services, adding a **radio link protocol (RLP)**. This protocol comprises mechanisms of **high-level data link control (HDLC)**, And special selective-reject mechanisms to trigger retransmission of erroneous data. Using transparent and non-transparent services, GSM specifies several bearer services for interworking with PSTN, ISDN, and packet switched public data networks (PSPDN) like X.25, which is available worldwide.

Tele Services

GSM mainly focuses on voice-oriented tele services. These comprise encrypted voice transmission, message services, and basic data communication with terminals as known from the PSTN or ISDN (e.g., fax). The primary goal of GSM was the provision of high-quality digital voice transmission.

Special codecs (coder/decoder) are used for voice transmission, while other codecs are used for the transmission of analog data for communication with traditional computer modems used in, e.g., fax machines. Another service offered by GSM is the **emergency number**. This service is mandatory for all providers and free of charge. This connection also has the highest priority, possibly pre-empting other connections, and will automatically be set up with the closest emergency center.

A useful service for very simple message transfer is the **short message service (SMS)**, which offers transmission of messages of up to 160 characters. Sending and receiving of SMS is possible during data or voice transmission.

The successor of SMS, the **enhanced message service (EMS)**, offers a larger message size, formatted text, and the transmission of animated pictures, small images and ring tones in a standardized way. But with MMS, EMS was hardly used.

Another non-voice tele service is **group 3 fax**, which is available worldwide. In this service, fax data is transmitted as digital data over the analog telephone network according to the ITU-T standards T.4 and T.30 using modems.

Supplementary Services

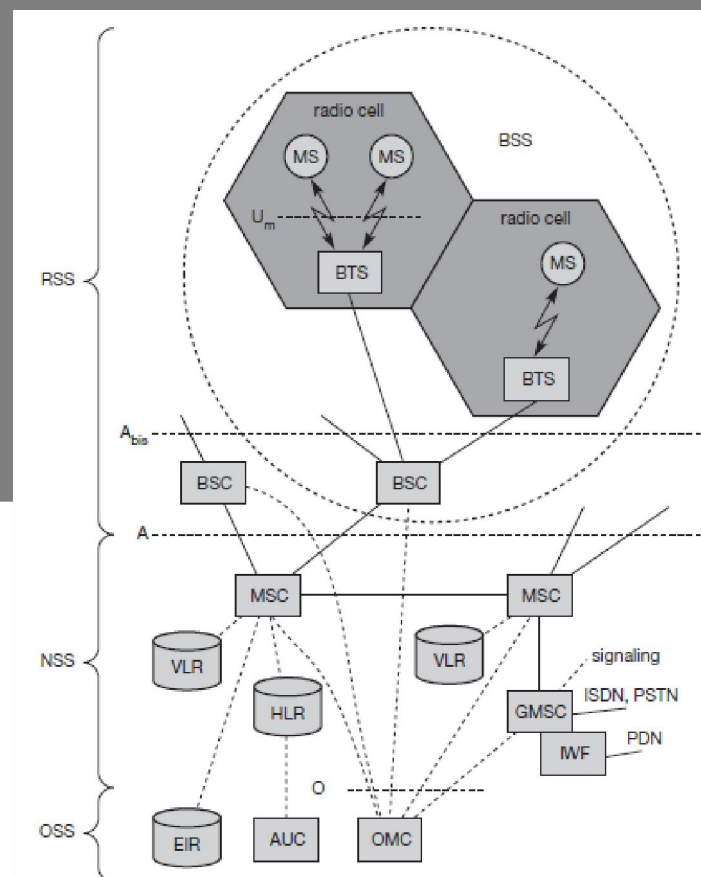
In addition to tele and bearer services, GSM providers can offer **supplementary services**. These services offer various enhancements for the standard telephony service, and may vary from provider to provider. Typical services are user **identification**, call **redirection**, or **forwarding** of ongoing calls, barring of incoming/outgoing calls, Advice of Charge (AoC) etc. Standard ISDN features such as **closed user groups** and **multiparty** communication may be available.

Q2. Explain GSM architecture with neat diagram.

Ans :

GSM Architecture

A GSM system consists of three subsystems, the radio sub system (RSS), the network and switching subsystem (NSS), and the operation subsystem (OSS).



Functional Architecture of a GSM System

Net work Switching Sub System

The NSS is responsible for performing call processing and subscriber related functions. The switching system includes the following functional units:

Home Location Register (HLR)

It is a database used for storage and management of subscriptions. HLR stores permanent data about subscribers, including a subscribers service profile, location information and activity status.

When an individual buys a subscription from the PCS provider, he or she is registered in the HLR of that operator.

Visitor Location Register (VLR)

It is a database that contains temporary information about subscribers that is needed by the MSC in order to service visiting subscribers. VLR is always integrated with the MSC. When a MS roams into a new MSC area, the VLR connected to that MSC will request data about the mobile station from the HLR. Later if the mobile station needs to make a call, VLR will be having all the information needed for call setup.

Authentication center (AUC)

A unit called the AUC provides authentication And encryption parameters that verify the users identity and ensure the confidentiality of each call.

Equipment Identity Register (EIR)

It is a database that contains information about the identity of mobile equipment that prevents calls from stolen, unauthorized or defective mobile stations.

Mobile Switching Center (MSC)

The MSC performs the telephony switching functions of the system. It controls calls to and from other telephone and data systems.

Radio Sub system(RSS) : the radio subsystem (RSS) comprises all radio specific entities, i.e., the mobile **stations (MS)** and the **base station subsystem (BSS)**. The figure shows the connection between the RSS and the NSS via the **A interface** (solid lines) and the connection to the OSS via the **O interface** (dashed lines).

Base Station Sub system (BSS)

A GSM network comprises many BSSs, each controlled by a base station controller (BSC). The BSS performs all functions necessary to maintain radio connections to an MS, coding/decoding of voice, and rate adaptation to/from the wireless network part. Besides a BSC, the BSS contains several BTSs.

Base Station Controllers (BSC)

The BSC provides all the control functions and physical links between the MSC and BTS. It is a high capacity switch that provides functions such as handover, cell configuration data, and control of radio frequency (RF) power levels in BTS. A number of BSC's are served by and MSC.

Base Transceiver Station (BTS)

The BTS handles the radio interface to the Mobile station. A BTS can form a radio cell or, using sectorized antennas, several and is connected to MS via the **Um interface**, and to the BSC via the **Abis interface**. The Um interface contains all the mechanisms necessary for wireless transmission (TDMA, FDMA etc.) The BTS is the radio equipment (transceivers and antennas) needed to service each cell in the network. A group of BTS's are controlled by an BSC.

Operation and Support System

The operations and maintenance center (OMC) is connected to all equipment in the switching system and to the BSC. Implementation of OMC is called operation and support system (OSS). The OSS is the functional entity from which the network operator monitors and controls the system. The purpose of OSS is to offer the customer cost-effective support for centralized, regional and local operational and maintenance activities that are required for a GSM network. OSS provides a network overview and allows engineers to monitor, diagnose and troubleshoot every aspect of the GSM network.

The mobile station (MS) consists of the mobile equipment and a smart card called the Subscriber Identity Module (SIM). The SIM provides personal mobility, so that the user can have access to subscribed services irrespective of a specific terminal. By inserting the SIM card into another GSM

terminal, the user is able to receive calls at that terminal, make calls from that terminal, and receive other subscribed services.

The mobile equipment is uniquely identified by the International Mobile Equipment Identity (IMEI). The SIM card contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication, and other information. The IMEI and the IMSI are independent, thereby allowing personal mobility. The SIM card may be protected against unauthorized use by a password or personal identity number.

Radio Interface

The most interesting interface in a GSM system is Um, the radio interface, as it comprises various multiplexing and media access mechanisms. GSM implements SDMA using cells with BTS and assigns an MS to a BTS.

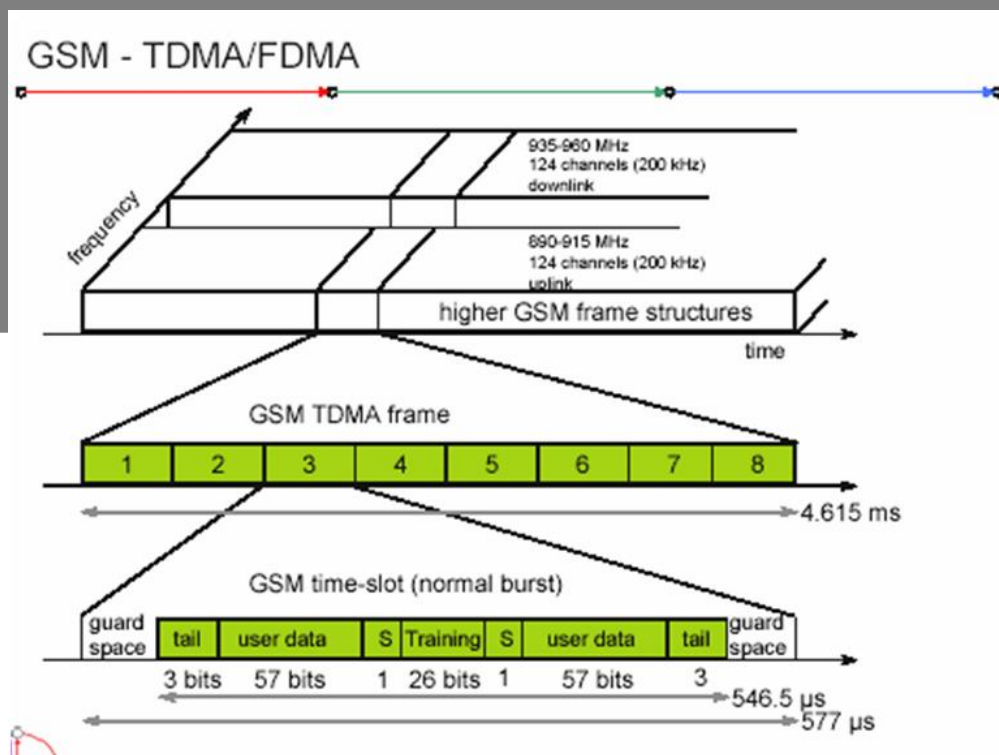
Q3. Write about GSM TDMA frame.

Ans :

GSM TDMA Frame, Slots and Bursts

Each of the 248 channels is additionally separated in time via a **GSM TDMA frame**, i.e., each 200 kHz carrier is subdivided into frames that are repeated continuously. The duration of a frame is 4.615 ms. A frame is again subdivided into 8 **GSM time slots**, where each slot represents a physical TDM channel and lasts for 577 μ s. Each TDM channel occupies the 200 kHz carrier for 577 μ s every 4.615 ms.

Data is transmitted in small portions, called **bursts**. The following figure shows a so called **normal burst** as used for data transmission inside a time slot. As shown, the burst is only 546.5 μ s long and contains 148 bits. The remaining 30.5 μ s are used as **guard space** to avoid overlapping with other bursts due to different path delays and to give the transmitter time to turn on and off.



The first and last three bits of a normal burst (**tail**) are all set to 0 and can be used to enhance the receiver performance. The **training** sequence in the middle of a slot is used to adapt the parameters of the receiver to the current path propagation characteristics and to select the strongest signal in case of multi-path propagation.

A flag **S** indicates whether the **data** field contains user or network control data. Apart from the normal burst, defines four more bursts for data transmission: a **frequency correction** burst allows the MS to correct the local oscillator to avoid interference with neighbouring channels, a **synchronization burst** with an extended training sequence synchronizes the MS with the BTS in time, an **access burst** is used for the initial connection setup between MS and BTS, and finally a **dummy burst** is used if no data is available for a slot.

Q4. Explain GSM Frame Hierarchy.

Ans :

Logical Channels and Frame Hierarchy

Two types of channels, namely physical channels and logical channels are present. **Physical channel:** channel defined by specifying both, a carrier frequency and a TDMA timeslot number.

Logic Channel

Logical channels are multiplexed into the physical channels. Each logic channel performs a specific task. Consequently the data of a logical channel is transmitted in the corresponding timeslots of the physical channel. During this process, logical channels can occupy a part of the physical channel or even the entire channel.

Each of the frequency carriers is divided into frames of 8 timeslots. The duration of a TDMA frame is 4.615ms. The bits per timeslot and frame duration yield a gross bit rate of about 271 kbps per TDMA frame. TDMA frames are grouped into two types of multiframes:

- 26-frame multiframe comprising of 26 TDMA frames. This multiframe is used to carry traffic channels and their associated control channels.
- 51-frame multiframe comprising 51 TDMA frames. This multiframe is exclusively used for control channels. The multiframe structure is further multiplexed into a single superframe of duration of 6.12sec. This means a superframe consists of 51 multiframes of 26 frames and 26 multiframes of 51 frames.
- The last multiplexing level of the frame hierarchy, consisting of 2048 superframes is a hyperframe. This long time period is needed to support the GSM data encryption mechanisms. The frame hierarchy is shown below:

GSM Frame Hierarchy

There are two different types of logical channel within the GSM system : Traffic Channels (TCHs), Control channels (CCHs).

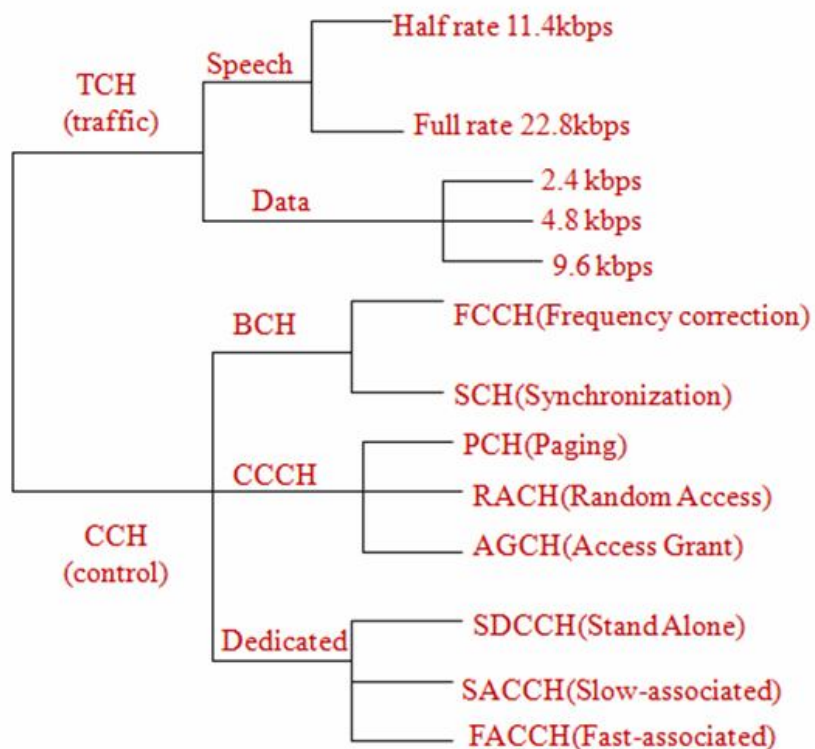
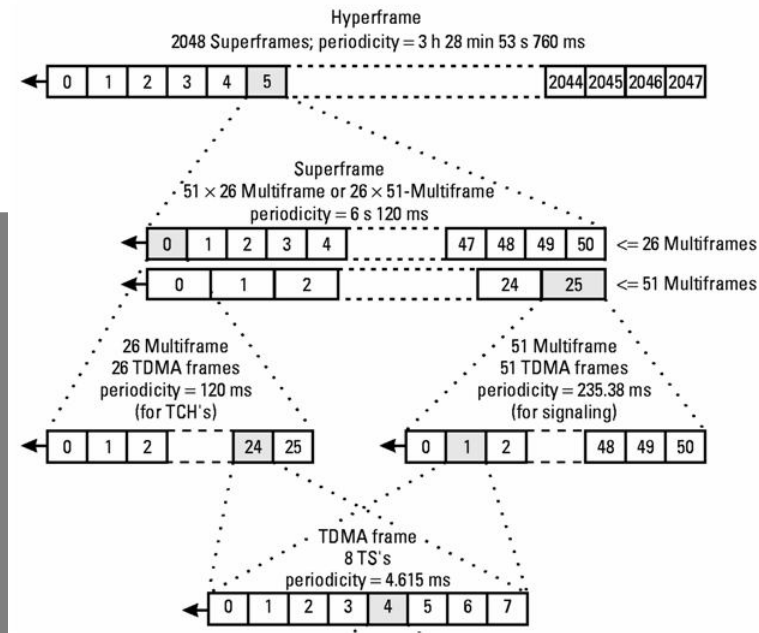
Traffic Channels

Traffic channels carry user information such as encoded speech or user data. Traffic channels are defined by using a 26-frame multiframe. Two general forms are defined:

- i) Full rate traffic channels (TCH/F), at a gross bit rate of 22.8 kbps.
- ii) Half rate traffic channels (TCH/H), at a gross bit rate of 11.4 kbps.

Uplink and downlink are separated by three slots (bursts) in the 26-multi frame structure. This simplifies the duplexing function in mobile terminals design, as mobiles will not need to transmit and receive at the same time. The 26-frame multiframe structure, shown below multiplexes two types of logical channels, a TCH and a Slow.

Associated Control Channel (SACCH)



Control Channels

Control channels carry system signalling and synchronisation data for control procedures such as location registration, mobile station synchronisation, paging, random access etc. between base station and mobile station. Three categories of control channel are defined: Broadcast, Common and Dedicated. Control channels are multiplexed into the 51-frame multiframe.

Broadcast Control Channel (BCCH)

A BTS uses this channel to signal information to all MSs within a cell. Information transmitted in this channel, and frequencies available inside the cell and in neighboring cells. The BTS sends information for frequency correction via the **frequency correction channel (FCCH)** and information about time synchronization via the **synchronization channel (SCH)**, where both channels are subchannels of the BCCH.

Common Control Channel (CCCH)

All information regarding connection setup between MS and BS is exchanged via the CCCH. For calls toward an MS, the BTS uses the **paging channel (PCH)** for paging the appropriate MS. If an MS wants to set up a call, it uses the **random access channel (RACH)** to send data to the BTS. The BTS uses the **access grant channel (AGCH)** to signal an MS that it can use a TCH or SDCCH for further connection setup.

Dedicated Control Channel (DCCH)

While the previous channels have all been unidirectional, the following channels are bidirectional. As long as an MS has not established a TCH with the BTS, it uses the **stand-alone dedicated control channel (SDCCH)** with a low data rate (782 bit/s) for signaling. This can comprise authentication, registration or other data needed for setting up a TCH.

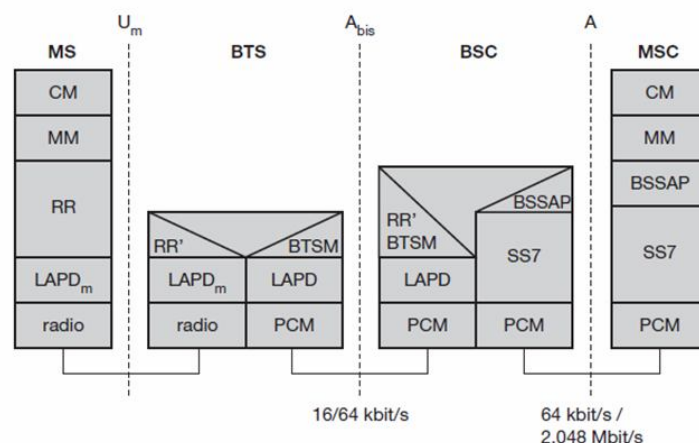
Q5. Explain about GSM protocols.

Ans. :

GSM Protocols

The signalling protocol in GSM is structured into three general layers depending on the interface, as shown below.

Layer 1 is the physical layer that handles all **radio**-specific functions. This includes the creation of bursts according to the five different formats, **multiplexing** of bursts into a TDMA frame, **synchronization** with the BTS, detection of idle channels, and measurement of the **channel quality** on the downlink. The physical layer at Um uses GMSK for digital **modulation** and performs **encryption/decryption** of data, i.e., encryption is not performed end-to-end, but only between MS and BSS over the air interface.



The main tasks of the physical layer comprise **channel coding** and **error detection/correction**, which is directly combined with the coding mechanisms. Channel coding makes extensive use of different **forward error correction (FEC)** schemes. Signalling between entities in a GSM network requires higher layers. For this purpose, the **LAPDm** protocol has been defined at the Um interface for **layer two**. LAPDm has been derived from link access procedure for the Dchannel (**LAPD**) in ISDN systems, which is a version of HDLC. LAPDm is a light weight LAPD because it does not need synchronization flags or check summing for error detection. LAPD offers reliable data transfer over connections, re-sequencing of data frames, and flow control.

The network layer in GSM, layer three, comprises several sublayers. The lowest sublayer is the radio resource management (RR). Only a part of this layer, RR', is implemented in the BTS, the remainder is situated in the BSC. The functions of RR' are supported by the BSC via the BTS management (BTSM). The main tasks of RR are setup, maintenance, and release of radio channels. Mobility management (MM) contains functions for registration, authentication, identification, location updating, and the provision of a temporary mobile subscriber identity (TMSI).

Finally, the call management (CM) layer contains three entities: call control (CC), short message service (SMS) and supplementary service (SS). SMS allows for message transfer using the control channels SDCCH and SACCH, while SS offers the services like user identification, call redirection, or forwarding of ongoing calls. CC provides a point-to-point connection between two terminals and is used by higher layers for call establishment, call clearing and change of call parameters. This layer also provides functions to send in-band tones, called dual tone multiple frequency (DTMF), over the GSM network. These tones are used, e.g., for the remote control of answering machines or the entry of PINs in electronic banking and are, also used for dialing in traditional analog telephone systems.

Additional protocols are used at the A_{bis} and A interfaces. Data transmission at the physical layer typically uses **pulse code modulation (PCM)**

systems. LAPD is used for layer two at Abis, BTSM for BTS management. **Signaling system No. 7 (SS7)** is used for signaling between an MSC and a BSC. This protocol also transfers all management information between MSCs, HLR, VLRs, AuC, EIR, and OMC. An MSC can also control a BSS via a **BSS application part (BSSAP)**.

Q6. Write about Localization and calling GSM.

Ans :

Localization and Calling

The fundamental feature of the GSM system is the automatic, world wide localization of users for which, the system performs periodic location updates. The HLR always contains information about the current location and the VLR currently responsible for the MS informs the HLR about the location changes. Changing VLRs with uninterrupted availability is called roaming. Roaming can take place within a network of one provider, between two providers in a country and also between different providers in different countries. To locate and address an MS, several numbers are needed :

Mobile Station International ISDN Number (MSISDN)

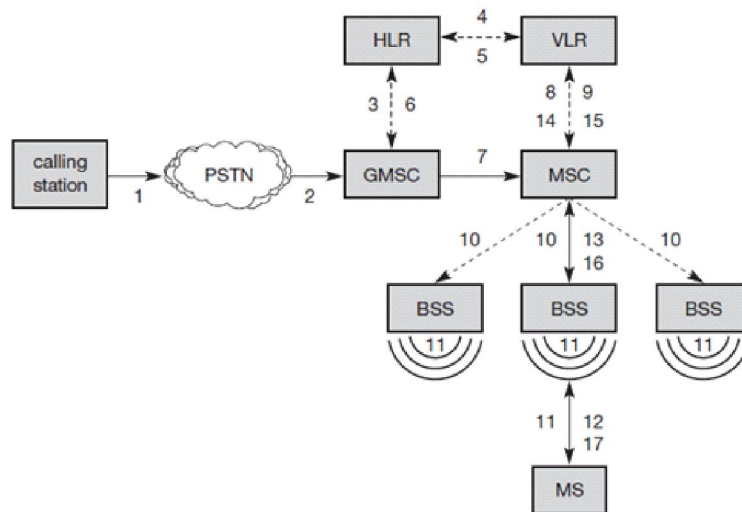
The only important number for a user of GSM is the phone number. This number consists of the country code (CC), the national destination code (NDC) and the subscriber number (SN).

International Mobile Subscriber Identity (IMSI)

GSM uses the IMSI for internal unique identification of a subscriber. IMSI consists of a mobile country code (MCC), the mobile network code (MNC), and finally the mobile subscriber identification number (MSIN).

Temporary Mobile Subscriber Identity (TMSI)

To hide the IMSI, which would give away the exact identity of the user signalling over the air interface, GSM uses the 4 byte TMSI for local subscriber identification. For a mobile terminated call (MTC), the following figure shows the different steps that take place.



Step 1: User dials the phone number of a GSM subscriber.

Step 2: The fixed network (PSTN) identifies the number belongs to a user in GSM network and forwards the call setup to the Gateway MSC (GMSC).

Step 3: The GMSC identifies the HLR for the subscriber and signals the call setup to HLR

Step 4: The HLR checks for number existence and its subscribed services and requests MSRN from the current VLR.

Step 5: VLR sends the MSRN to HLR

Step 6: Upon receiving MSRN, the HLR determines the MSC responsible for MS and forwards the information to the GMSC

Step 7: The GMSC can now forward the call setup request to the MSC indicated

Step 8: The MSC requests the VLR for the current status of the MS

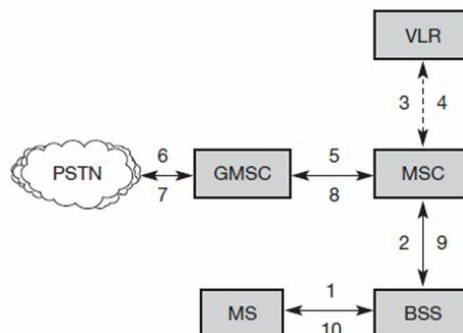
Step 9: VLR sends the requested information

Step 10: If MS is available, the MSC initiates paging in all cells it is responsible for.

Step 11: The BTSs of all BSSs transmit the paging signal to the MS

Step 12: Step 13: If MS answers, VLR performs security checks

Step 15: Till step 17: Then the VLR signals to the MSC to setup a connection to the MS For a mobile originated call (MOC), the following steps take place.

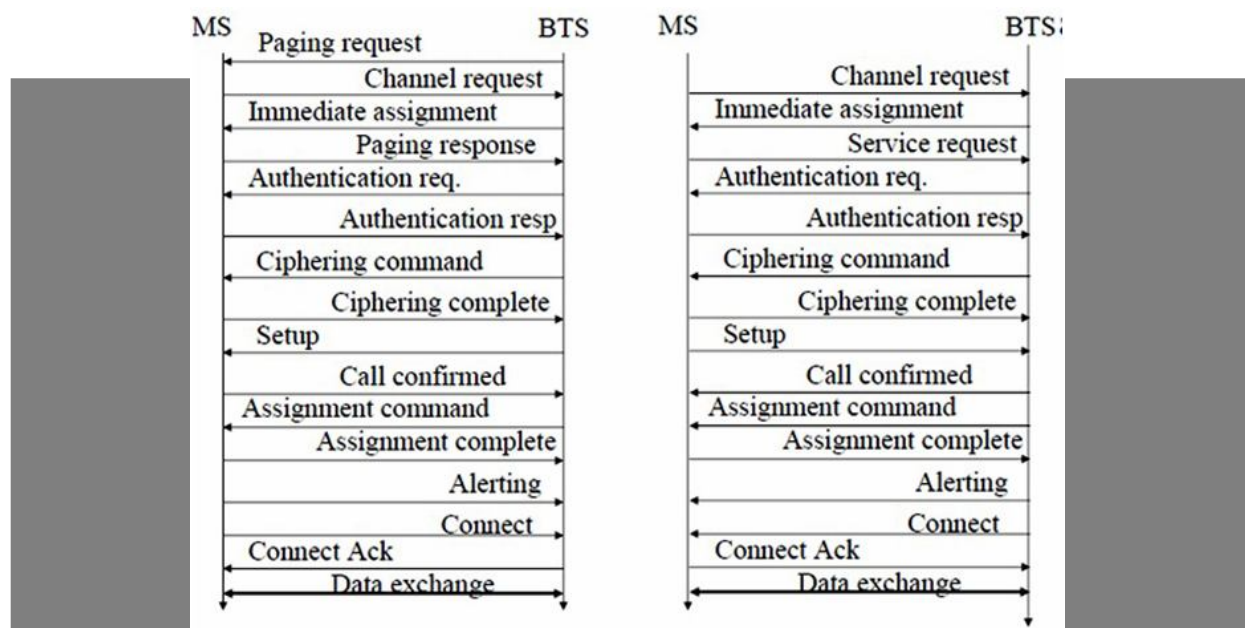


Step 1: The MS transmits a request for a new connection.

Step 2: The BSS forwards this request to the MSC

Step 3: Step 4: The MSC then checks if this user is allowed to set up a call with the requested and checks the availability of resources through the GSM network and into the PSTN. If all resources are available, the MSC sets up a connection between the MS and the fixed network.

In addition to the steps mentioned above, other messages are exchanged between an MS and BTS during connection setup (in either direction).



Q7. What is Handover in GSM. Describe briefly

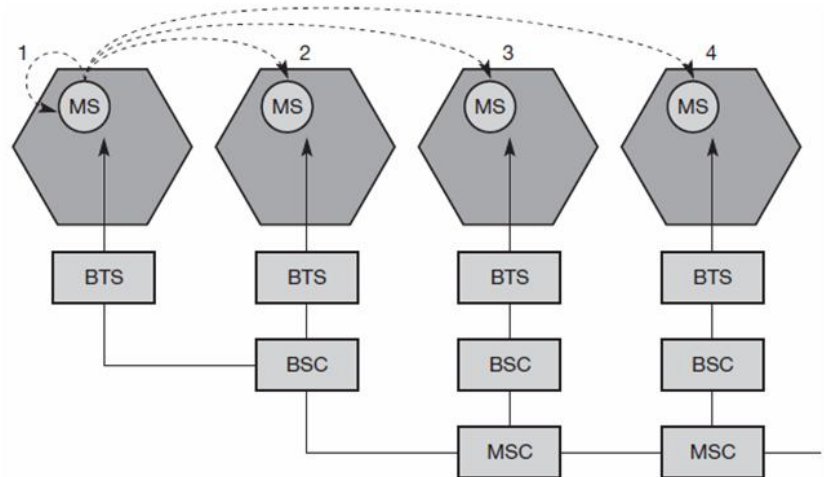
Ans :

Handover

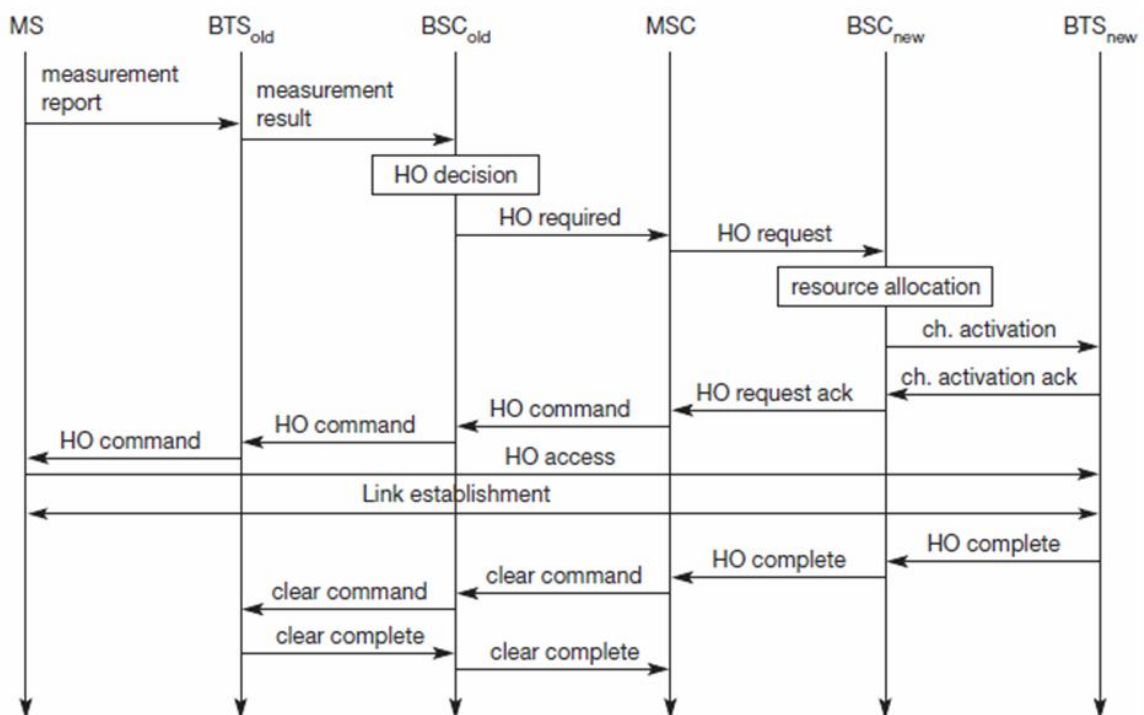
Cellular systems require **handover** procedures, as single cells do not cover the whole service area. However, a handover should not cause a cut-off, also called **call drop**. GSM aims at maximum handover duration of 60 ms. There are two basic reasons for a handover:

1. The mobile station **moves out of the range** of a BTS, decreasing the received **Signal level** increasing the **error rate** there by diminishing the **quality of the radiolink**.
2. Handover may be due to **load balancing**, when an MSC/BSC decides the traffic is too high in one cell and shifts some MS to other cells with a lower load. The four possible handover scenarios of GSM are shown below:
 - **Intra-cell handover:** Within a cell, narrow-band interference could make transmission at a certain frequency impossible. The BSC could then decide to change the carrier frequency (scenario 1).
 - **Inter-cell, intra-BSC handover:** This is a typical handover scenario. The mobile station moves from one cell to another, but stays within the control of the same BSC. The BSC then performs a handover, assigns a new radio channel in the new cell and releases the old one (scenario 2).

- **Inter-BSC, intra-MSC handover:** As a BSC only controls a limited number of cells; GSM also has to perform handovers between cells controlled by different BSCs. This handover then has to be controlled by the MSC (scenario 3).
- **Inter MSC handover:** A handover could be required between two cells belonging to different MSCs. Now both MSCs perform the handover together (scenario 4).



Handover Decision Depending on Receive Level



Intra-MSC handover

More sophisticated handover mechanisms are needed for seamless handovers between different systems.

Q8. Write about the security services offered at GSM.

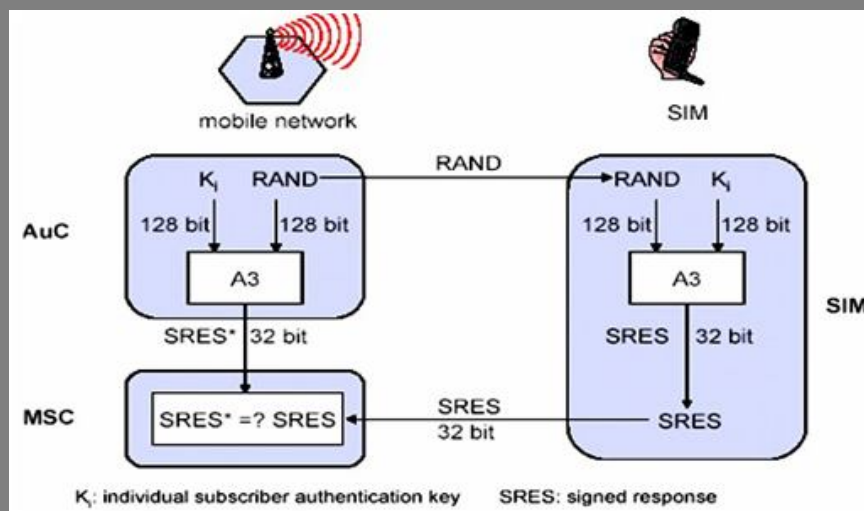
Ans :

Security

GSM offers several security services using confidential information stored in the AuC and in the individual SIM. The SIM stores personal, secret data and is protected with a PIN against unauthorized use. Three algorithms have been specified to provide security services in GSM. **Algorithm A3** is used for **authentication**, **A5** for **encryption**, and **A8** for the **generation of a cipher key**. The various security services offered by GSM are:

1. Access Control and Authentication

The first step includes the authentication of a valid user for the SIM. The user needs a secret PIN to access the SIM. The next step is the subscriber authentication. This step is based on a challenge-response scheme as shown below:

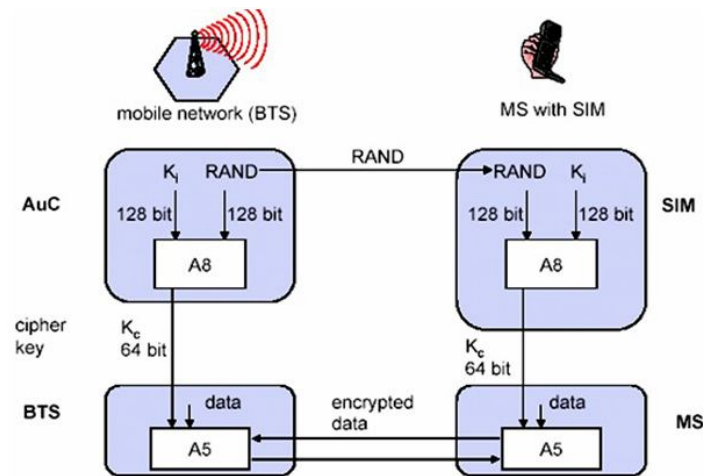


2. Subscriber Authentication

Authentication is based on the SIM, which stores the **individual authentication key Ki**, the **user identification IMSI**, and the algorithm used for authentication **A3**. The AuC performs the basic generation of random values RAND, signed responses SRES, and cipher keys Kc for each IMSI, and then forwards this information to the HLR. The current VLR requests the appropriate values for RAND, SRES, and Kc from the HLR. For authentication, the VLR sends the random value RAND to the SIM. Both sides, network and subscriber module, perform the same operation with RAND and the key Ki, called **A3**. The MS sends back the SRES generated by the SIM; the VLR can now compare both values. If they are the same, the VLR accepts the subscriber, otherwise the subscriber is rejected.

3. Confidentiality

All user-related data is encrypted. After authentication, BTS and MS apply encryption to voice, data, and signalling as shown below.



To ensure privacy, all messages containing user-related information are encrypted in GSM over the air interface. After authentication, MS and BSS can start using encryption by applying the cipher key **K_c**, which is generated using the individual key **K_i** and a random value by applying the algorithm A8. Note that the SIM in the MS and the network both calculate the same **K_c** based on the random value RAND. The key **K_c** itself is not transmitted over the air interface. MS and BTS can now encrypt and decrypt data using the algorithm A5 and the cipherkey **K_c**.

4. Anonymity

To provide user anonymity, all data is encrypted before transmission, and user identifiers are not used over the air. Instead, GSM transmits a temporary identifier (TMSI), which is newly assigned by the VLR after each location update. Additionally, the VLR can change the TMSI at any time.

2.2 DECT

Q9. Write about DECT.

Ans :

Another fully digital cellular network is the **digital enhanced cordless telecommunications** (DECT) system specified by ETSI. Formerly also called **digital European cordless telephone and digital European cordless telecommunications**, DECT replace older analog cordless phone systems such as CT1 and CT1+.

These **analog systems** only ensured security to a limited extent as they did **not use encryption** for data transmission and only offered a relatively low capacity.

DECT is mainly used in offices, on campus, at trade shows, or in the home. Furthermore, access points to the PSTN can be established within, e.g., railway stations, large government buildings and hospitals, offering a much cheaper telephone service compared to a GSM system.

A big difference between DECT and GSM exists in terms of **cell diameter** and **cell capacity**. While GSM is designed for outdoor use with a cell diameter of up to 70 km, the range of DECT is limited to about **300 m** from the base station. DECT can also handle handover, but it was not designed to work at a higher speed. DECT works at a frequency range of 1880–1990 MHz offering **120 full duplex channels**. Time division duplex (TDD) is applied using **10 ms frames**.

The frequency range is subdivided into **10 carrier frequencies** using FDMA, each frame being divided into **24 slots** using TDMA. For the TDD mechanism, 12 slots are used as uplink, 12 slots as downlink. The digital modulation scheme is GMSK – each station has an average transmission power of only 10 mW with a maximum of 250 mW.

System Architecture

A DECT system, may have various different physical implementation depending on its actual use. Different DECT entities can be integrated into one physical unit; entities can be distributed, replicated etc. However, all implementations are based on the same logical reference model of the system architecture. A global network connects the local communication structure to the outside world and offers its services via the interface D1. Global networks could be integrated services digital networks (ISDN), public switched telephone networks (PSTN), public landmobile networks (PLMN), e.g., GSM, or packet switched public data network (PSPDN). The services offered by these networks include transportation of data and the translation of addresses and routing of data between the local networks.

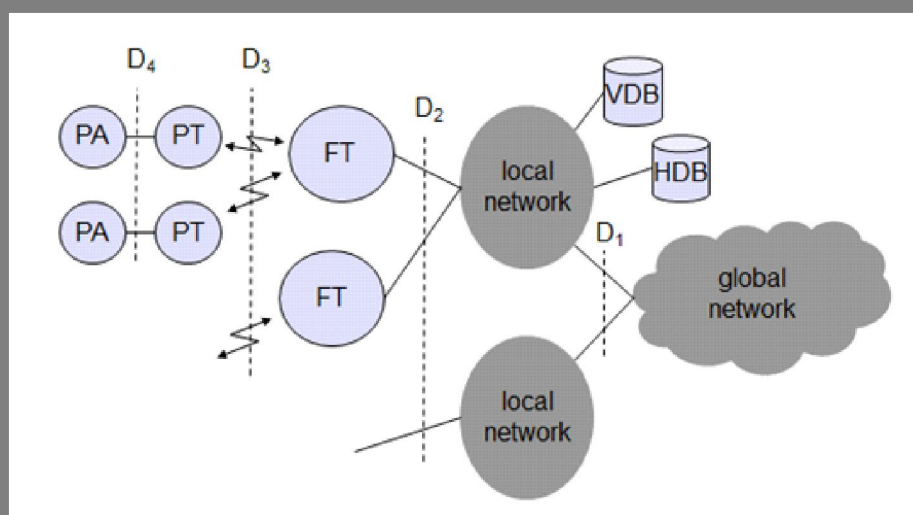


Fig. : DECT System Architecture

Local networks in the DECT context offer local telecommunications services that can include everything from simple switching to intelligent call forwarding, address translation etc.

Examples for such networks are analog or digital **private branch exchanges** (PBXs) or LANs, e.g., those following the IEEE 802.x family of LANs. As the core of the DECT system itself is quite simple, all typical network functions have to be integrated in the local or global network, where the databases **home data base** (HDB) and **visitor data base** (VDB) are also located. Both databases support mobility with functions that are similar to those in the HLR and VLR in GSM systems. Incoming calls are automatically forwarded to the current subsystem responsible for the DECT user, and the current VDB informs the HDB about changes in location.

The DECT core network consists of the **fixed radio termination** (FT) and the **portable radio termination** (PT), and basically only provides a multiplexing service. FT and PT cover layers one to three at the fixed network side and mobile network side respectively. Additionally, several **portable applications** (PA) can be implemented on a device.

Protocol Architecture

The DECT protocol reference architecture follows the OSI reference model. Figure shows the layers covered by the standard: the physical layer, medium access control, and data link control for both the **control plane** (C-Plane) and the **user plane** (U-Plane). An additional **network layer** has been specified for the C-Plane, so that user data from layer two is directly forwarded to the U-Plane. A **management plane** vertically covers all lower layers of a DECT system.

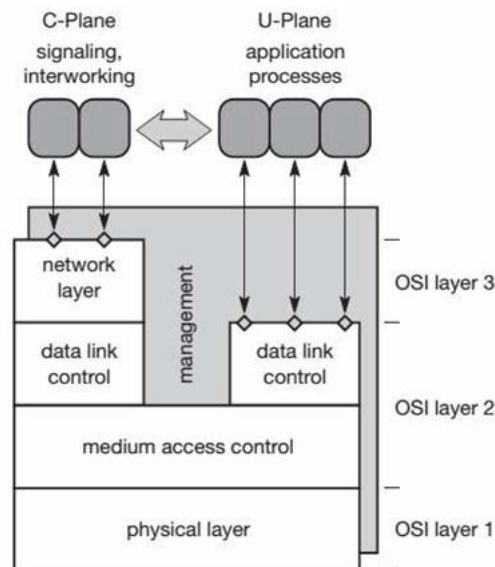


Fig. : DECT Protocol Layers

Physical Layer

As in all wireless networks, the physical layer comprises all functions for modulation/demodulation, incoming signal detection, sender/receiver synchronization, and collection of status information for the management plane. This layer generates the physical channel structure with a certain, guaranteed throughput. On request from the MAC layer, the physical layer assigns a channel for data transmission.

Figure shows the standard TDMA frame structure used in DECT and some typical data packets.

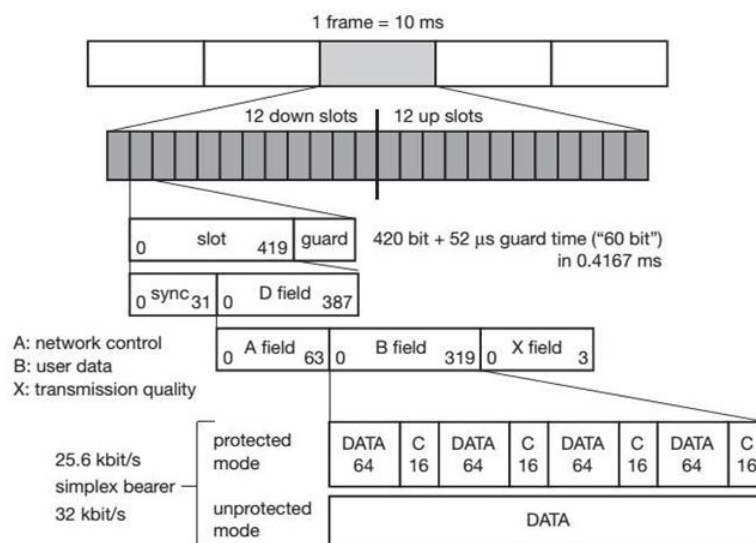


Fig. : DECT Multiplex and Frame Structure

Each frame has a duration of 10 ms and contains 12 slots for the downlink and 12 slots for the uplink in the basic connection mode. If a mobile node receives data in slot s , it returns data in slot $s+12$. An advanced connection mode allows different allocation schemes. Each slot has a duration of 0.4167 ms and can contain several different physical packets. Typically, 420 bits are used for data; the remaining 52 is left as guard space. The 420 data bits are again divided into a 32 bit synchronization pattern followed by the data field D.

The fields for data transmission now use these remaining 388 bits for **network control** (A field), **user data** (B field), and the transfer of the **transmission quality** (X field).

While network control is transmitted with a data rate of 6.4 kbit/s (64 bit each 10 ms), the user data rate depends on additional error correction mechanisms.

The **simplex bearer** provides a data rate of 32 kbit/s in an unprotected mode, while using a 16 bit CRC checksum C for a data block of 64 bit in the protected mode reduces the data rate to 25.6 kbit/s.

A duplex bearer service is produced by combining two simplex bearers.

DECT also defines bearer types with higher throughputs by combining slots, e.g., the double duplex bearer offers 80 kbit/s full duplex.

Medium Access Control Layer

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 on to physical channels. Logical channels exist for signalling network control, user data transmission, paging, or sending broadcast messages. Additional services offered include segmentation/reassembly of packets and error control/error correction.

Data Link Control Layer

The data link control (DLC) layer creates and maintains reliable connections between the mobile terminal and the base station.

Two services have been defined for the C-Plane: a **connectionless broadcast service** for paging (called **Lb**) and a **point-to-point protocol** similar to LAPD in ISDN, but adapted to the underlying MAC (called **LAPC+Lc**).

Several services exist for the U-Plane, e.g., a transparent unprotected service (basically a null service), a forward error correction service, rate adaptation services, and services for future enhancements.

Network Layer

The network layer of DECT is similar to those in ISDN and GSM and only exists for the C-Plane. This layer provides services to request, check, reserve, control, and release resources at the fixed station and the mobile terminal.

The **mobility management** (MM) within the network layer is responsible for identity management, authentication, and the management of the location data bases. **Call control** (CC) handles connection setup, release, and negotiation.

Two message services, the **connection oriented message service** (COMS) and the **connectionless message service** (CLMS) transfer data to and from the interworking unit that connects the DECT system with the outside world.

2.3 WIRELESS LAN

Q10. Write the advantages and disadvantages of WLAN.

Ans :

WLANs are typically restricted in their diameter to buildings, a campus, single rooms etc. and are operated by individuals, not by large-scale network providers.

Advantages

1. Very flexible within the reception area
2. Ad-hoc networks without previous planning possible (almost) no wiring difficulties (e.g. historic buildings, firewalls)
3. More robust against disasters like, e.g., earthquakes, fire - or users pulling a plug.

Disadvantages

1. Typically very low bandwidth compared to wired networks (1-10 Mbit/s)
2. Many proprietary solutions, especially for higher bit-rates, standards take their time (e.g. IEEE 802.11)
3. Products have to follow many national restrictions if working wireless, it takes a very long time to establish global solutions like, e.g., IMT-2000 global, seamless operation
4. Low power for battery use
5. No special permissions or licenses needed to use the LAN
6. Robust transmission technology
7. Simplified spontaneous cooperation at meetings
8. Easy to use for everyone, simple management
9. Protection of investment in wired networks
10. Security (no one should be able to read my data), privacy (no one should be able to collect user profiles), safety (low radiation).
11. Transparency concerning applications and higher layer protocols, but also location awareness if necessary.

2.3.1 Infrared vs. Radio Transmission**Q11. Differentiate between Infrared and radio transmission.***Ans :***Infrared**

Uses IR diodes, diffuse light, multiple reflections (walls, furniture etc.)

Advantages

- i) Simple, cheap, available in many mobile devices.
- ii) No licenses needed.
- iii) Simple shielding possible.

Disadvantages

- i) Interference by sunlight, heat sources etc.
- ii) Many things shield or absorb IR light
- iii) Low bandwidth

Example

IrDA (Infrared Data Association) interface available everywhere

Radio

Typically using the license free ISM band at 2.4 GHz.

Advantages

- i) Experience from wireless WAN and mobile phones can be used
- ii) Coverage of larger areas possible (radio can penetrate walls, furniture etc.)

Disadvantages

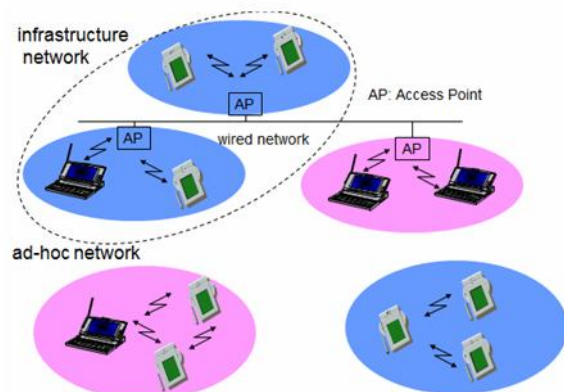
- i) Very limited license free frequency bands
- ii) Shielding more difficult, interference with other electrical devices.

Example:

WaveLAN, HIPERLAN, Bluetooth

2.3.2 Infrastructure And AD-HOC Networks**Q12. Write about Infrastructure and ad-hoc networks.***Ans :*

Infrastructure networks not only provide access to other networks, but also include forwarding functions, medium access control etc. In these infrastructure-based wireless networks, communication typically takes place only between the wireless nodes and the access point, but not directly between the wireless nodes.



The access point does not just control medium access, but also acts as a bridge to other wireless or wired networks. Figure shows three access points with their three wireless networks and a wired network. Several wireless networks may form one logical wireless network, so the access points together with the fixed network in between can connect several wireless networks to form a larger network beyond actual radio coverage.

Typically, the design of infrastructure-based wireless networks is simpler because most of the network functionality lies within the access point, whereas the wireless clients can remain quite simple. This structure is reminiscent of switched Ethernet or other star-based networks, where a central element (e.g., a switch) controls network flow. This type of network can use different access schemes with or without collision. Collisions may occur if medium access of the wireless nodes and the access point is not coordinated. However, if only the access point controls medium access, no collisions are possible.

Infrastructure-based networks lose some of the flexibility wireless networks can offer, e.g., they cannot be used for disaster relief in cases where no infrastructure is left.

Ad-hoc wireless networks, however, do not need any infrastructure to work. Each node can communicate directly with other nodes, so no access point controlling medium access is necessary.

Ad-hoc wireless networks, however, do not need any infrastructure to work. Each node can communicate directly with other nodes, so no access point controlling medium access is necessary. Figure shows two ad-hoc networks with three nodes each. Nodes within an ad-hoc network can only communicate if they can reach each other physically.

In ad-hoc networks, the complexity of each node is higher because every node has to implement medium access mechanisms, mechanisms to handle hidden or exposed terminal problems.

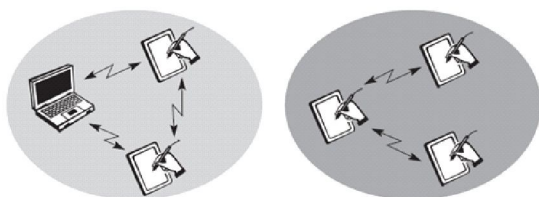


Fig. : Example of two ad-hoc Wireless Networks

2.3.4 IEEE 802.11

Q13. Explain about IEEE 802.11 system architecture.

Ans :

System Architecture

The 802.11 architecture defines two types of services and three different types of stations

802.11 Services

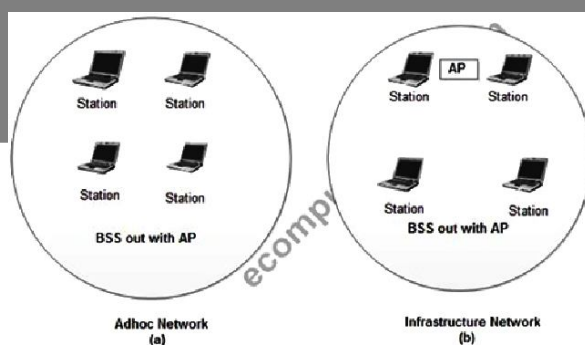
The two types of services are

1. Basic services set (BSS)
2. Extended Service Set (ESS)

1. Basic Services Set (BSS)

The basic services set contain stationary or mobile wireless stations and a central base station called access point (AP).

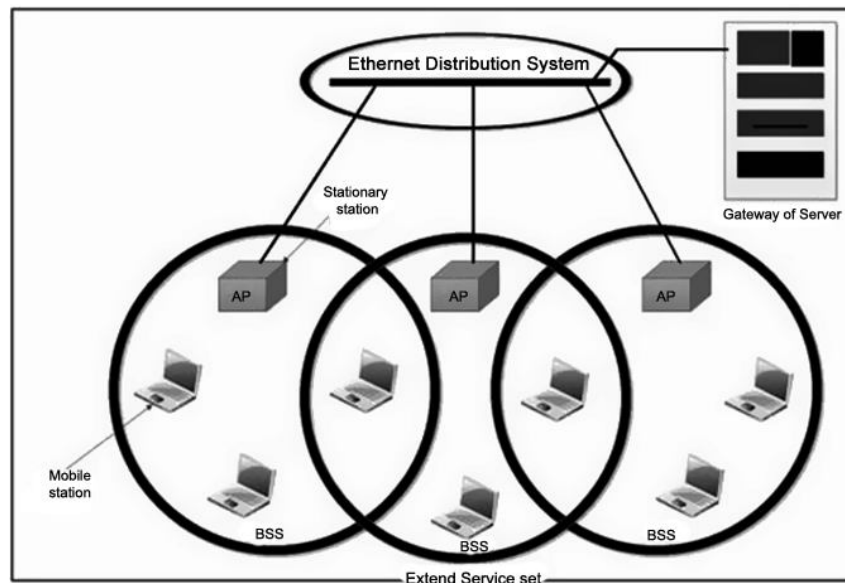
- The use of access point is optional.
- If the access point is not present, it is known as stand-alone network. Such a BSS cannot send data to other BSSs. This type of architecture is known as adhoc architecture.
- The BSS in which an access point is present is known as an infrastructure network.



Basic Service Sets

2. Extend Service Set (ESS)

An extended service set is created by joining two or more basic service sets (BSS) having access points (APs).



These extended networks are created by joining the access points of basic services sets through a wired LAN known as distribution system.

- The distribution system can be any IEEE LAN.
- There are two types of stations in ESS:
 - i) **Mobile stations:** These are normal stations inside a BSS.
 - ii) **Stationary stations:** These are AP stations that are part of a wired LAN.
- Communication between two stations in two different BSS usually occurs via two APs.
- A mobile station can belong to more than one BSS at the same time.

802.11 Station Types

IEEE 802.11 defines three types of stations on the basis of their mobility in wireless LAN. These are:

1. No-transition Mobility
2. BSS-transition Mobility
3. ESS-transition Mobility

1. No-transition Mobility

These types of stations are either stationary *i.e.* immovable or move only inside a BSS.

2. BSS-transition Mobility

These types of stations can move from one BSS to another but the movement is limited inside an ESS.

3. ESS-transition Mobility

These types of stations can move from one ESS to another. The communication may or may not be continuous when a station moves from one ESS to another ESS.

Protocol Architecture

Q14. Explain the protocol architecture of IEEE 802.11.

Ans :

The IEEE 802.11 standard only covers the physical layer **PHY** and medium access layer **MAC**. The physical layer is subdivided into the **physical layer convergence protocol (PLCP)** and the **physical medium dependent** sublayer **PMD**.

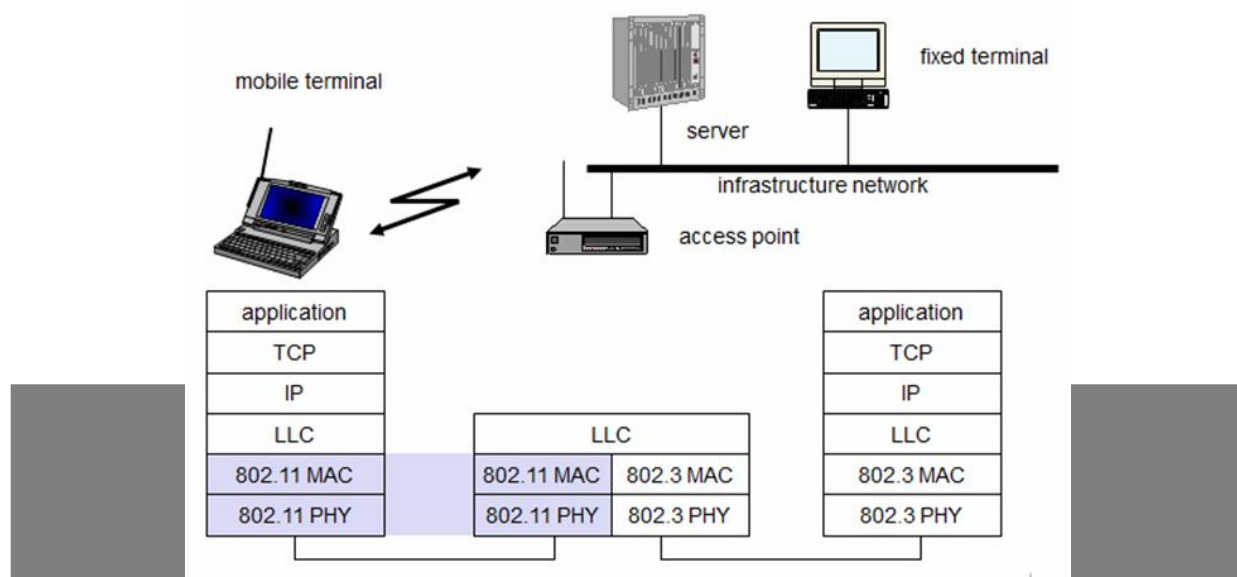


Fig. : IEEE 802.11 Protocol Architecture and Bridging

Physical Layer Functions

1. As we know that physical layer is responsible for converting data stream into signals, the bits of 802.11 networks can be converted to radio waves or infrared waves.
2. These are six different specifications of IEEE 802.11. These implementations, except the first one, operate in industrial, scientific and medical (ISM) band. These three bands are unlicensed and their ranges are
 1. 902-928 MHz
 2. 2.400-4.835 GHz
 3. 5.725-5.850 GHz
3. The different implementations of IEEE 802.11 are given below.
 1. **IEEE 802.11 Infrared**
 - It uses diffused (not line of sight) infrared light in the range of 800 to 950 nm.
 - It allows two different speeds: 1 Mbps and 2Mbps.
 - For a 1-Mbps data rate, 4 bits of data are encoded into 16 bit code. This 16 bit code contains fifteen 0s and a single 1.
 - For a 2-Mbps data rate, a 2 bit code is encoded into 4 bit code. This 4 bit code contains three 0s and a single 1.
 - The modulation technique used is pulse position modulation (PPM) i.e. for converting digital signal to analog.
 2. **IEEE 802.11 FHSS**
 - IEEE 802.11 uses Frequency Hopping Spread Spectrum (FHSS) method for signal generation.
 - This method uses 2.4 GHz ISM band. This band is divided into 79 subbands of 1MHz with some guard bands.

- In this method, at one moment data is sent by using one carrier frequency and then by some other carrier frequency at next moment. After this, an idle time is there in communication. This cycle is repeated after regular intervals.

- A pseudo random number generator selects the hopping sequence.

- The allowed data rates are 1 or 2 Mbps.

- This method uses frequency shift keying (two level or four level) for modulation i.e. for converting digital signal to analogy.

3. IEEE 802.11 DSSS

- This method uses Direct Sequence Spread Spectrum (DSSS) method for signal generation. Each bit is transmitted as 11 chips using a Barker sequence.

- DSSS uses the 2.4-GHz ISM band.

- It also allows the data rates of 1 or 2 Mbps.

- It uses phase shift keying (PSK) technique at 1 M baud for converting digital signal to analog signal.

4. IEEE 802.11a OFDM

- This method uses Orthogonal Frequency Division Multiplexing (OFDM) for signal generation.

- This method is capable of delivering data upto 18 or 54 Mbps.

- In OFDM all the subbands are used by one source at a given time.

- It uses 5 GHz ISM band.

- This band is divided into 52 subbands, with 48 subbands for data and 4 subbands for control information.

- If phase shift keying (PSK) is used for modulation then data rate is 18 Mbps. If quadrature amplitude modulation (QAM) is used, the data rate can be 54 Mbps.

5. IEEE 802.11b HR-OSSS

- It uses High Rate Direct Sequence Spread Spectrum method for signal generation.

- HR-DSSS is similar to DSSS except for encoding method.

- Here, 4 or 8 bits are encoded into a special symbol called complementary code key (CCK).

- It uses 2.4 GHz ISM band.

- It supports four data rates: 1, 2, 5.5 and 11 Mbps.

- 1 Mbps and 2 Mbps data rates uses phase shift modulation.

- The 5.5 Mbps version uses BPSK and transmits at 1.375 Mbaud/s with 4-bit CCK encoding.

- The 11 Mbps version uses QPSK and transmits at 1.375 Mbps with 8-bit CCK encoding.

6. IEEE 802.11g OFDM

- It uses OFDM modulation technique.

- It uses 2.4 GHz ISM band.

- It supports the data rates of 22 or 54 Mbps.

- It is backward compatible with 802.11 b.

MAC sublayer Functions

802.11 support two different modes of operations. These are:

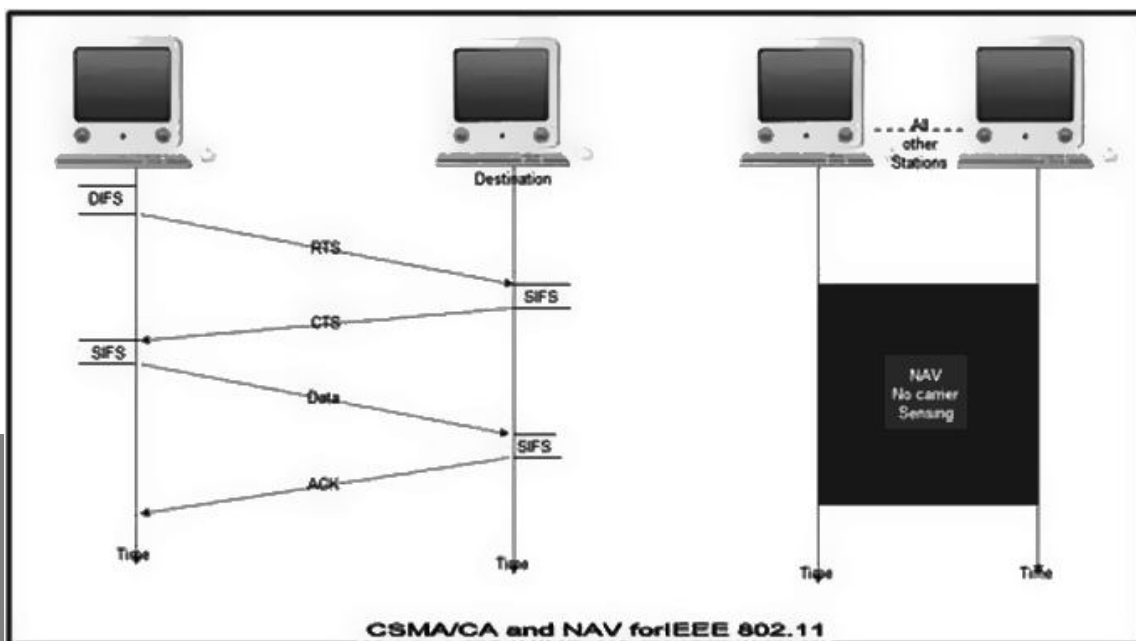
1. Distributed Coordination Function (DCF)
2. Point Coordination Function (PCF)

1. Distributed Coordination Function

- The DCF is used in BSS having no access point.

- DCF uses CSMA/CA protocol for transmission.

- The following steps are followed in this method.



1. When a station wants to transmit, it senses the channel to see whether it is free or not.
2. If the channel is not free the station waits for back off time.
3. If the station finds a channel to be idle, the station waits for a period of time called distributed interframe space (DIFS).
4. The station then sends control frame called request to send (RTS) as shown in figure.
5. The destination station receives the frame and waits for a short period of time called short interframe space (SIFS).
6. The destination station then sends a control frame called clear to send (CTS) to the source station. This frame indicates that the destination station is ready to receive data.
7. The sender then waits for SIFS time and sends data.
8. The destination waits for SIFS time and sends acknowledgement for the received frame.

Collision Avoidance

- 802.11 standard uses Network Allocation Vector (NAV) for collision avoidance.
- The procedure used in NAV is explained below:
 1. Whenever a station sends an RTS frame, it includes the duration of time for which the station will occupy the channel.
 2. All other stations that are affected by the transmission creates a timer called network allocation vector (NAV).
 3. This NAV (created by other stations) specifies for how much time these stations must not check the channel.
 4. Each station before sensing the channel, check its NAV to see if has expired or not.
 5. If its NAV has expired, the station can send data, otherwise it has to wait.
- There can also be a collision during handshaking i.e. when RTS or CTS control frames are exchanged between the sender and receiver. In this case following procedure is used for collision avoidance:

1. When two or more stations send RTS to a station at same time, their control frames collide.
2. If CTS frame is not received by the sender, it assumes that there has been a collision.
3. In such a case sender, waits for back off time and retransmits RTS.

2. Point Coordination Function

- PCF method is used in infrastructure network. In this Access point is used to control the network activity.
- It is implemented on top of the DCF and IS used for time sensitive transmissions.
- PCF uses centralized, contention free polling access method.
- The AP performs polling for stations that wants to transmit data. The various stations are polled one after the other.
- To give priority to PCF over DCF, another interframe space called PIFS is defined. PIFS (PCF IFS) is shorter than DIFS.
- If at the same time, a station is using DCF and AP is using PCF, then AP is given priority over the station.
- Due to this priority of PCF over DCF, stations that only use DCF may not gain access to the channel.
- To overcome this problem, a repetition interval is defined that is repeated continuously. This repetition interval starts with a special control frame called beacon frame.
- When a station hears beacon frame, it start their NAV for the duration of the period of the repetition interval.

Q15. Explain the Frame Format of 802.11.

Ans :

Frame Format **of 802.11**

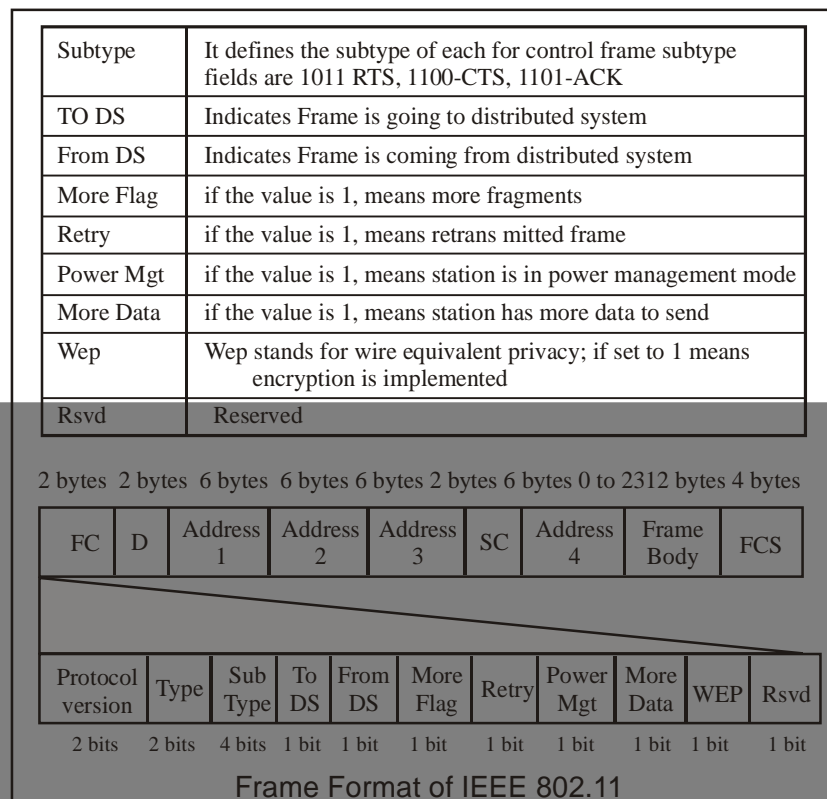
The MAC layer frame consists of nine fields.

1. Frame Control (FC)

This is 2 byte field and defines the type of frame and some control information. This field contains several different subfields.

These are listed in the table below:

Field	Explanation
Version	The Current Version is 0.
Type	Specifies the type of information in the frame body 00. Management, 01-control, and 10-data



2. **D** : It stands for duration and is of 2 bytes. This field defines the duration for which the frame and its acknowledgement will occupy the channel. It is also used to set the value of NAV for other stations.
3. **Addresses**
There are 4 address fields of 6 bytes length. These four addresses represent source, destination, source base station and destination base station.
4. **Sequence Control (SC)**
This 2 byte field defines the sequence number of frame to be used in flow control.
5. **Frame Body**
This field can be between 0 and 2312 bytes. It contains the information.
6. **FCS**
This field is 4 bytes long and contains 'CRC-32 error detection sequence.

IEEE 802.11 Frame Types

There are three different types of frames:

1. Management frame
2. Control frame
3. Data frame

1. **Management Frame** : These are used for initial communication between stations and access points.
2. **Control Frame**: These are used for accessing the channel and acknowledging frames. The control frames are RTS and CTS.
3. **Data Frame** : These are used for carrying data and control information.

802.11 Addressing

There are four different addressing cases depending upon the value of To DS And from DS subfields of FC field.

Each flag can be 0 or 1, resulting in 4 different situations.

1. If To DS = 0 and From DS = 0, it indicates that frame is not going to distribution system and is not coming from a distribution system. The frame is going from one station in a BSS to another.
2. If To DS = 0 and From DS = 1, it indicates that the frame is coming from a distribution system. The frame is coming from an AP and is going to a station. The address 3 contains original sender of the frame (in another BSS).
3. If To DS = 1 and From DS = 0, it indicates that the frame is going to a distribution system. The frame is going from a station to an AP. The address 3 field contains the final destination of the frame.
4. If To DS = 1 and From DS = 1, it indicates that frame is going from one AP to another AP in a wireless distributed system.

The table below specifies the addresses of all four cases.

TO DS	From DS	Address 1	Address 2	Address3	Address 4
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

2.3.5 Hiperlan

Q16. Write a short note about HIPER LAN.

Ans :

HIPERLAN stands for **high performance local area network**. It is a wireless standard derived from traditional LAN environments and can support multimedia and asynchronous data effectively at high data rates of 23.5 Mbps.

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 maximum data rate for the user depends on the distance of the communicating stations. With short distance(< 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 uses cellular-based data networks to connect to an ATM backbone. The main idea behind HIPERLAN is to provide an infrastructure or ad-hoc wireless with low mobility and a small radius. HIPERLAN supports isochronous traffic with low latency. The HiperLAN standard family has four different versions.

The key feature of all four networks is their integration of time-sensitive data transfer services. Over time, names have changed and the former HIPERLANs 2,3, 1nd 4 are now called HiperLAN2, HIPERACCESS, and HIPERLINK.

Table : HIPERLAN Protocol Family

	HIPERLAN 1	HIPERLAN 2	HIPERLAN 3	HIPERLAN 4
Application	wireless LAN	access to ATM fixed networks	wireless local loop	point-to-point wireless ATM connections
Frequency	5.1-5.3GHz			17.2-17.3GHz
Topology	decentralized ad-hoc/infrastructure	cellular, centralized	point-to-multipoint	point-to-point
Antenna	omni-directional		directional	
Range	50 m	50-100 m	5000 m	150 m
QoS	statistical	ATM traffic classes (VBR, CBR, ABR, UBR)		
Mobility	<10m/s		stationary	
Interface	conventional LAN	ATM networks		
Data rate	23.5 Mbit/s	>20 Mbit/s		155 Mbit/s
Power conservation	yes		not necessary	

Q17. Explain HIPERLAN1.

Ans :

HIPERLAN 1

The standard covers the Physical layer and the Media Access Control part of the Data link layer like 802.11. There is a new sub layer called Channel Access and Control sub layer (CAC). This sub layer deals with the access requests to the channels. The accomplishing of the request is dependent on the usage of the channel and the priority of the request.

CAC layer provides hierarchical independence with Elimination-Yield Non-Preemptive Multiple Access mechanism (EY-NPMA). MAC layer defines protocols for routing, security and power saving and provides naturally data transfer to the upper layers.

On the physical layer FSK and GMSK modulations are used in HiperLAN/1.

HiperLAN does not conflict with microwave and other kitchen appliances, which are on 2.4 GHz.

Elimination-yield non-preemptive priority multiple access (EY-NPMA)

EY-NPMA is a contention based protocol., EY-NPMA provides excellent support for different classes of traffic regarding quality of service and demonstrates very low collision rates. EY-NPMA is the medium access mechanism used by HIPERLAN Type 1. It uses active signalling.

Active signalling takes advantage of the fact that the current wireless technology enables us to have a slot time very much smaller than the average packet size. Each node that wants to access the medium transmits a non-data preamble pattern consisting of slots. This pattern is made up of alternating idle and busy

periods of different lengths (measured in slots). Conflict resolution and collision detection is done during this preamble. The main rule is that if a node detects a signal during one of its listening periods in its pattern, it aborts and defers until the next cycle. Otherwise, the node transmits its packet at the end of the pattern transmission.

With EYNPMA, each station may attempt to access the channel when a condition out of a group of three is met. The three conditions are:

- Channel free condition
- Synchronized channel condition
- Hidden elimination condition

The channel free condition occurs when the channel remains idle for at least a predefined time interval. A station willing to transmit senses the channel for this time interval, the station extends its period of sensing by a random number of slots (backoff).

The synchronized channel condition occurs when the channel is idle in the channel synchronization interval, which starts immediately after the end of the previous channel access cycle. The synchronized channel access cycle consists of three distinct phases:

- Prioritization
- Contention (Elimination and Yield) Transmission

Important features of the EY-NPMA

- No preemption by frames with higher priority after the priority resolution possible.
- Hierarchical independence of performance.
- Fair contention resolution of frames with the same priority.

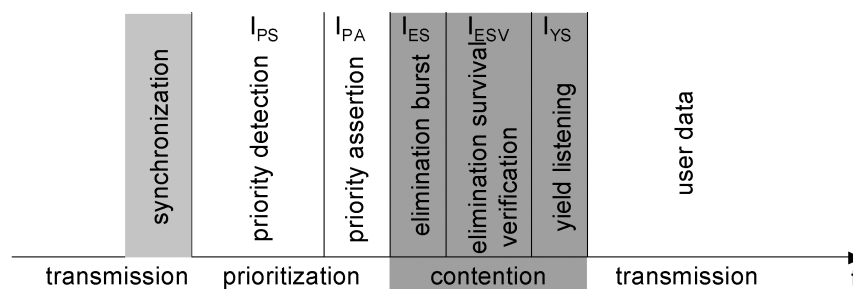


Fig.: Phase of the HIPERLAN 1 EY-NPMA access scheme

a) Prioritization Phase

Prioritization Phase is the first attempt at reducing the number of contenders for the channel. Every contender calculates the number of idle slots according to the priority of its data, and senses the channel during those slots. Contenders with highest priority data will have no idle slots, while those with lowest priority data will have all idle slots.

b) Elimination /Contention Phase

Elimination Phase is the second attempt at reducing the contenders. This phase consists of extending the priority pulse with a randomly calculated number of busy slots. The number of slots is independently calculated for each node. The immediately after this pulse, the node senses the channel. If the channel is busy, it defers transmission until the next cycle. If the channel is idle, it enters the yield phase.

The nodes that survive the Prioritization Phase keep on trying to gain access to the channel. During the Elimination Phase, a great percentage of the contending nodes is eliminated, but at least one of them survives. Every node that has not been defeated during the Prioritization Phase transmits an elimination pulse which is actually the lengthening of the priority pulse. Right after the end of this pulse, the nodes allow an idle slot, which is called survival verification slot, during which they sense the channel.

Yield Phase

Yield Phase is the last phase of EY-NPMA, and is the last try to reduce collisions. Only the nodes that have survived elimination phase start the yield phase. The node selects a random number of idle slots uniformly distributed between 0 and 9. At the end of the yield phase, the node again senses the channel. If the channel is idle, it starts its transmission.

Yield Phase is the last phase before the transmission of a data packet and it is the last effort to reduce the number of the contending nodes. The nodes that have survived the Elimination Phase enter the Yield Phase allowing a number of idle slots. Every node that detects transmission during these slots quits the current effort to gain access to the channel and waits till the next channel access cycle. If a node detects no transmission, it eventually transmits its data packet. Thus, a node lose in Yield Phase, when it listens some other node transmitting a data packet.

The number of the idle slots is random and uniformly distributed between 0 and 9.

Q18. Write about WATM.

Ans :

WATM

The concept of WATM considered as a potential framework for next-generation wireless communication networks capable of supporting integrated, quality-of-service (QoS) based multimedia services..

Need for WATM

The area of wireless transmission systems has been increasing rapidly. Mobility raises a new set of

questions, techniques, and solutions. This growth will occur in an environment characterized by rapid development of end-user applications and services towards the Internet and broadband multimedia delivery over the evolving fixed-wired infrastructure.

As ATM networks scale well from local area networks (LANs) to wide area networks (WANs), and there is a need for mobility in local and wide area applications, a mobile extension of ATM is required in order to have wireless access in local and wide environments. Many other wireless technologies, such as IEEE 802.11, typically only offer best-effort services or to some extent time-bounded services. However, these services do not provide as many QoS parameters as ATM networks do. WATM could offer QoS for adequate support of multimedia data streams.

Reference Model

The WATM system reference model, proposed by ATM Forum Wireless ATM (WATM) group, specifies the signalling interfaces among the mobile terminal, wireless terminal adapter, wireless radio port, mobile ATM switch and non-mobile ATM switch. It also specifies the user and control planes protocol layering architecture.

This model is commonly advocated by many communication companies, such as NEC, Motorola, NTT, Nokia, Symbionics, and ORL.

The major components of a Wireless ATM system are:

- a) WATM terminal
- b) WATM terminal adapter
- c) WATM radio port
- d) Mobile ATM switch
- e) Standard ATM network and
- f) ATM host.

The system reference model consists of a radio access segment and a fixed network segment. The fixed network is defined by "M (mobile ATM)" UNI and NNI interfaces while the wireless segment is defined by "R (Radio)" radio access layer (RAL) interface.

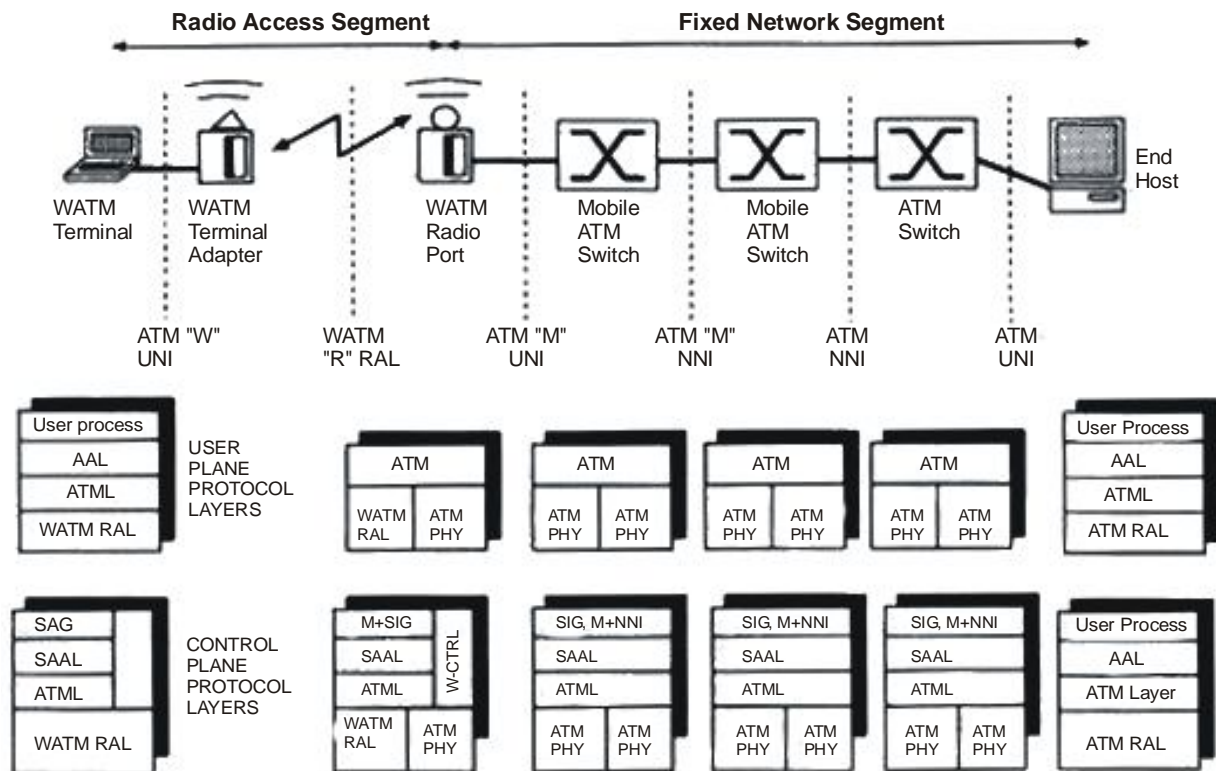


Fig.: WATM Reference Model

The "W" UNI is concerned with handover signaling, location management, wireless link and QoS control. The "R" RAL governs the signaling exchange between the WATM terminal adapter and the mobile base station. Hence, it concerns channel access, datalink control, meta-signaling, etc. The "M" NNI governs the signaling exchange between the WATM base station and a mobile capable ATM switch. It is also concerned with mobility-related signaling between the mobile capable ATM switches

Q19. What is BRAN? Explain about it.

Ans :

BRAN

The broadband radio access networks (BRAN), which have been standardized by the European Telecommunications Standards Institute (ETSI) could have been an RAL for WATM. The BRAN standard and IEEE 802.16 (Broadband wireless access, IEEE, 2002b) have similar goals.

BRAN standardization has a rather large scope including indoor and campus mobility, transfer rates of 25–155 Mbit/s, and a transmission range of 50 m–5 km. Standardization efforts are coordinated with the ATM Forum, the IETF, other groups from ETSI, the IEEE etc. BRAN has specified four different network types (ETSI, 1998a):

1. **HIPERLAN 1 :** This high-speed WLAN supports mobility at data rates above 20 Mbit/s. Range is 50 m, connections are multi-point-to-multi-point using ad-hoc or infrastructure networks ?
2. **HIPERLAN/2 :** This technology can be used for wireless access to ATM or IP networks and supports up to 25 Mbit/s user data rate in a point-to-multi-point configuration.

3. **HIPERACCESS:** This technology could be used to cover the 'last mile' to a customer via a fixed radio link, so could be an alternative to cable modems or xDSL technologies (ETSI, 1998c).
4. **HIPERLINK:** To connect different HIPERLAN access points or HIPERACCESS nodes with a high-speed link, HIPERLINK technology can be chosen.

As an access network, BRAN technology is independent from the protocols of the fixed network. BRAN can be used for ATM and TCP/IP networks as illustrated in Figure. Based on possibly different physical layers, the DLC layer of BRAN offers a common interface to higher layers. To cover special characteristics of wireless links and to adapt directly to different higher layer network technologies, BRAN provides a network convergence sub layer. This is the layer which can be used by a wireless ATM network, Ethernet, Fire wire, or an IP network. In the case of BRAN as the RAL for WATM, the core ATM network would use services of the BRAN network convergence sub layer.

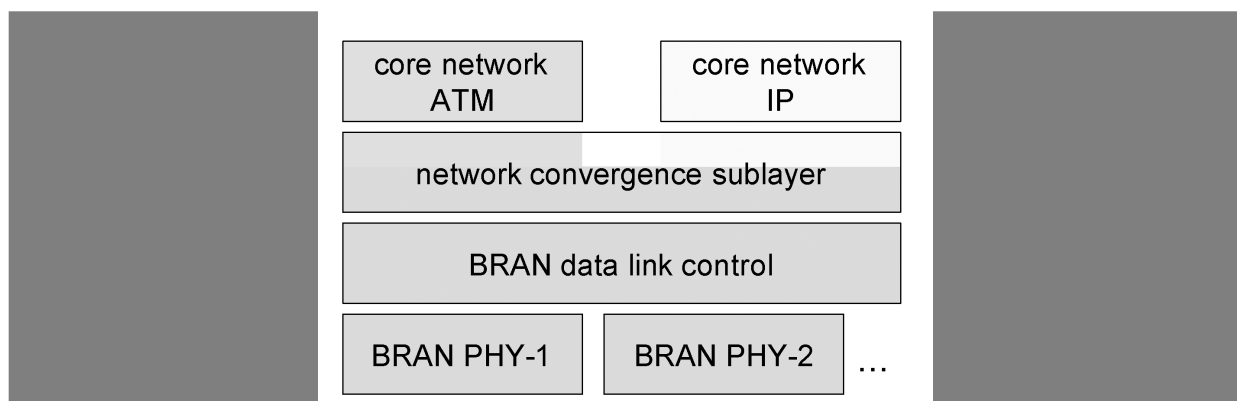


Fig. : Layered Model of BRAN Wireless Access Network

Features of HiperLAN2

High-throughput Transmission

Using OFDM in the physical layer and a dynamic TDMA/TDD-based MAC protocol, HiperLAN2 not only offers up to 54 Mbit/s at the physical layer but also about 35 Mbit/s at the network layer.

Connection-oriented

Prior to data transmission Hiper LAN2 networks establish logical connections between a sender and a receiver

Quality of Service Support

Support of QoS is much simpler. Each connection has its own set of QoS parameters (bandwidth, delay, jitter, bit error rate etc.).

Q20. Explain HiperLan 2

Ans :

Dynamic Frequency Selection

HiperLAN2 does not require frequency

Security support

Authentication as well as encryption are supported by HiperLAN2.

Mobility support

Mobile terminals can move around while transmission always takes place between the terminal and the access point with the best radio signal.

Application and network independence: HiperLAN2 was not designed with a certain group of applications or networks in mind. Access points can connect to LANs running ethernet as well as IEEE 1394 (Firewire) systems used to connect home audio/video devices.

Power saves: Mobile terminals can negotiate certain wake-up patterns to save power.

Reference Model And Configurations

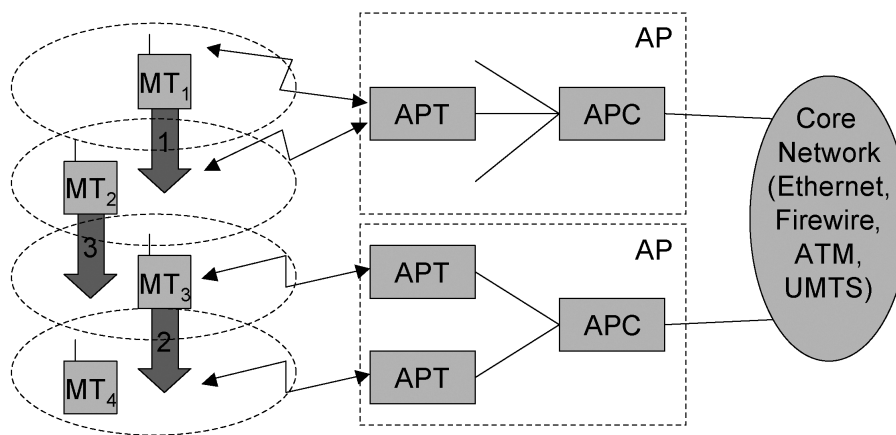


Fig.: HiperLAN2 Basic Structure and Handover Scenarios

The above Figure shows the standard architecture of an infrastructure-based HiperLAN2 network. Here, two **access points** (AP) are attached to a core network. Core networks might be Ethernet LANs, Firewire (IEEE 1394) connections between audio and video equipment, ATM networks, UMTS 3G cellular phone networks etc. Each AP consists of an **access point controller** (APC) and one or more **access point transceivers** (APT).

An APT can comprise one or more sectors (shown as cell here). Finally, four **mobile terminals**(MT) are also shown. MTs can move around in the cell area as shown. No frequency planning is necessary as the APs automatically select the appropriate frequency via **dynamic frequency selection**.

Three handover situations may occur:

- **Sector handover** (Inter sector): If sector antennas are used for an AP, which is optional in the standard, the AP shall support sector handover. This type of handover is handled inside the DLC layer
- **Radio handover** (Inter-APT/Intra-AP): As this handover type, too, is handled within the AP, no external interaction is needed.
- **Network handover** (Inter-AP/Intra-network): This is the most complex situation: MT₂ moves from one AP to another.

HiperLAN2 networks can operate in two different modes (which may be used simultaneously in the same network).

- **Centralized mode (CM):** In infrastructure-based mode all APs are connected to a core network and MTs are associated with APs.
- **Direct mode (DM):** The optional ad-hoc mode of HiperLAN2 directly exchanged between MTs if they can receive each other, but the network still controlled.

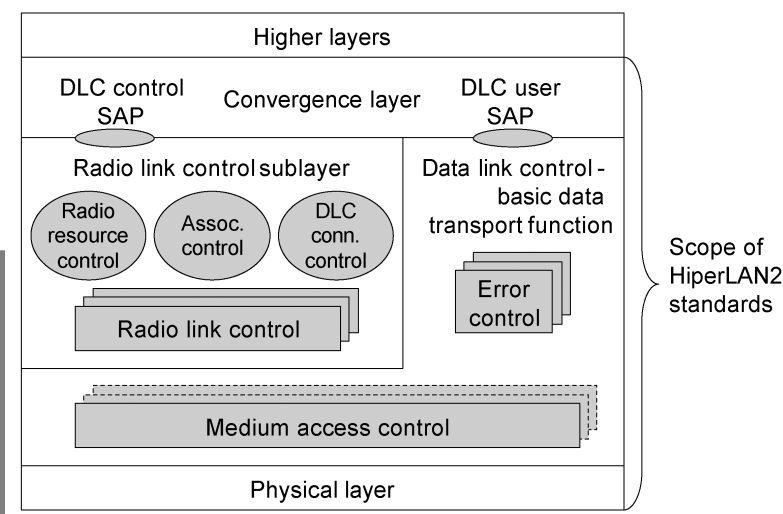


Fig.: HiperLAN2 Protocol Stack

The above figure shows the HiperLAN2 protocol stack as used in access points. Protocol stacks in mobile terminals differ with respect to the number of MAC and RLC instances (only one of each). The lowest layer, the **physical layer**, handles as usual all functions related to modulation, forward error correction, signal detection, synchronization etc. The **data link control (DLC)** layer contains the MAC functions, the RLC sub layer and error control functions. The **MAC** of an AP assigns each MT a certain capacity to guarantee connection quality depending on available resources.

Above the MAC DLC is divided into a control and a user part. The user part contains **error control** mechanisms. HiperLAN2 offers reliable data transmission using acknowledgements and retransmissions. The **radio link control (RLC)** sub layer comprises most control functions in the DLC layer (the CC part of an AP). The **association control function (ACF)** controls association and authentication of new MTs as well as synchronization of the radio cell via beacons.

The **DLC user connection control (DCC or DUCC)** service controls connection setup, modification, and release. Finally, the **radio resource control (RRC)** handles handover between APs and within an AP. On top of the DLC layer there is the **convergence layer**. This highest layer of HiperLAN2 standardization may comprise segmentation and reassembly functions and adaptations to fixed LANs, 3G networks etc.

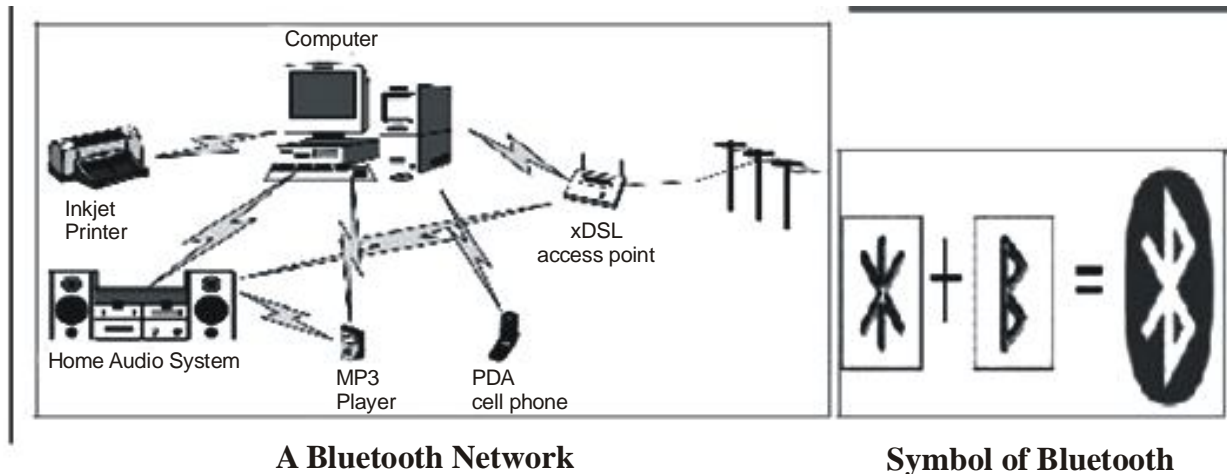
2.3.6 Bluetooth

Q21. Write a note on Bluetooth?

Ans :

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength radio transmissions in the ISM band from 2400–2480 MHz) from fixed and mobile devices, creating personal area networks (PANs) with high levels of security. Different type of network is needed to

connect different small devices in close proximity (about 10 m) without expensive wiring or the need for a wireless infrastructure. Bluetooth is a new standard suggested by a group of electronics manufacturers that will allow any sort of electronic tools from computers and cell phones to keyboards and headphones to make its own connections, without wires, cables or any direct action from a user.



The main strength of bluetooth is its ability to simultaneously handle both data and voice transmissions. It is capable of supporting one asynchronous data channel and up to three synchronous voice channels, or one channel sup-orting both voice and data. This ability combined with ad hoc device connection and automatic service discovery make it a superior solution for mobile devices and Internet applications. This grouping allows such novel solutions as a mobile hands-free headset for voice calls, print to fax capability, and automatically synchronizing PDA, laptop, and cell phone address book applications.

Bluetooth Features

- It is Wireless and automatic.
- Bluetooth is inexpensive (<\$5 per unit) It handles both data and voice
- Signals are omni-directional and can pass through walls and briefcases Bluetooth uses frequency hopping at rate of 1600 Lops/sec
- It operates on 79 channels in 2.4GHZ band with 1MHZ carrier spacing Pi-conet is the important terminology.

Q22. Explain the network topology of blue tooth.

Ans :

Network Topology

Piconet

A set of bluetooth devices sharing a common channel is called piconet. A piconet is a collection of devices connected via Bluetooth technology in an ad hoc fashion. A piconet starts with two connected devices, and may grow to eight connected devices. All Bluetooth devices are peer units and have identical implementations. However, when establishing a piconet, one unit will act as a **Master** and the other(s) as **slave(s)** for the duration of the piconet connection. Master is a Bluetooth device that sets the frequency hopping sequence. The Slave synchronizes to the Masters in time and frequency by following the Master's frequency hopping sequence. Every Bluetooth device has a unique.

Bluetooth device address and a 28-bit Bluetooth clock. The baseband part of the Bluetooth System uses a special algorithm, which calculates the frequency hop sequence from the master's clock and device address. In addition to controlling the frequency hop sequence, the Master controls when Slaves are to transmit using Time Division Multiplexing (TDM).

When there is just one Master and one Slave the system is called a **Point to Point** connection. When many Slaves are connected to one Master, the system is called a **Point to Multipoint**. Both these types are referred to as a **Piconet** and all follow the frequency hopping sequence of the Master. The Slaves in the Piconet only have links to the Master and no direct links between Slaves.

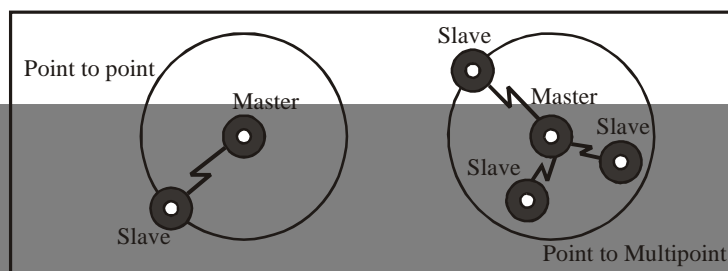


Fig. : Piconet

Formation of piconet

Two parameters are needed for the formation of piconet

- Hopping pattern of the radio it wishes to connect.
- Phase within the pattern i.e. the clock offset of the hops.

The global ID defines the hopping pattern. The master shares its global ID and its clock offset with the other radios which become slaves. The global ID and the clock parameters are exchanged using a FHS (Frequency Hopping Synchronization) packet.

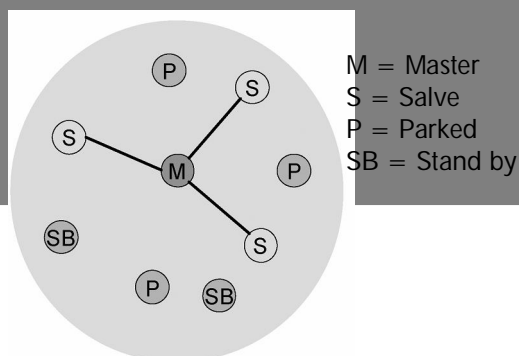


Fig. : Simple Bluetooth Piconet

There is no difference between terminals and base stations, two or more devices can form a piconet. The unit establishing the piconet repeatedly becomes the master, all other devices will be slaves. The hopping pattern is determined by the device ID, a 48-bit worldwide unique identifier. The phase in the hopping pattern is determined by the master's clock. After altering the interior clock according to the master a device may take part in the piconet. All active devices are assigned a 3-bit **active member**

address(AMA). All parked devices use an 8-bit **parked member address (PMA)**. Devices in stand-by do not need any address. All users within one piconet have the same hopping sequence and share the same 1 MHz channel. As more users join the piconet, the throughput per user drops quickly.

Scatternet

Bluetooth defines a structure called scatternet to facilitate inter piconet communication. A scatternet is formed by interconnecting multiple piconet. A group of piconet is called **scatternet**.

If a device wants to take part in more than one piconet, it has to coordinate to the hopping sequence of the piconet it wants to take part in. If a device acts as slave in one piconet, it just starts to synchronize with the hopping sequence of the piconet it wants to join. After synchronization, it acts as a slave in this piconet and no longer participates in its former piconet. To permit synchronization, a slave has to know the uniqueness of the master that determines the hopping sequence of a piconet. Before leaving one piconet, a slave informs the current master that it will be unavailable for a certain amount of time.

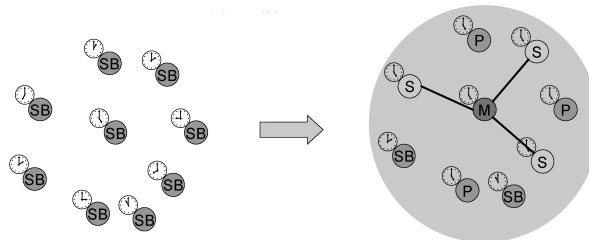


Fig. : Formation of piconet

The left over devices in the piconet continue to communicate normal.

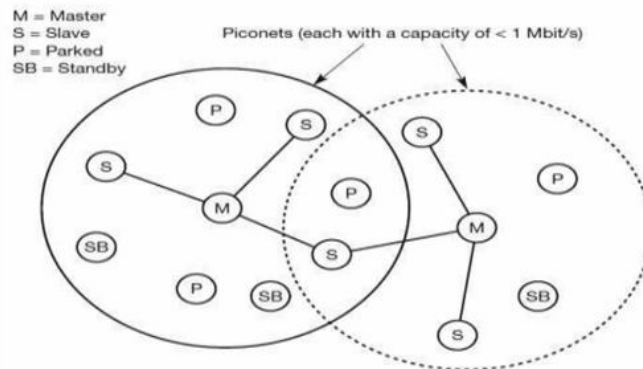
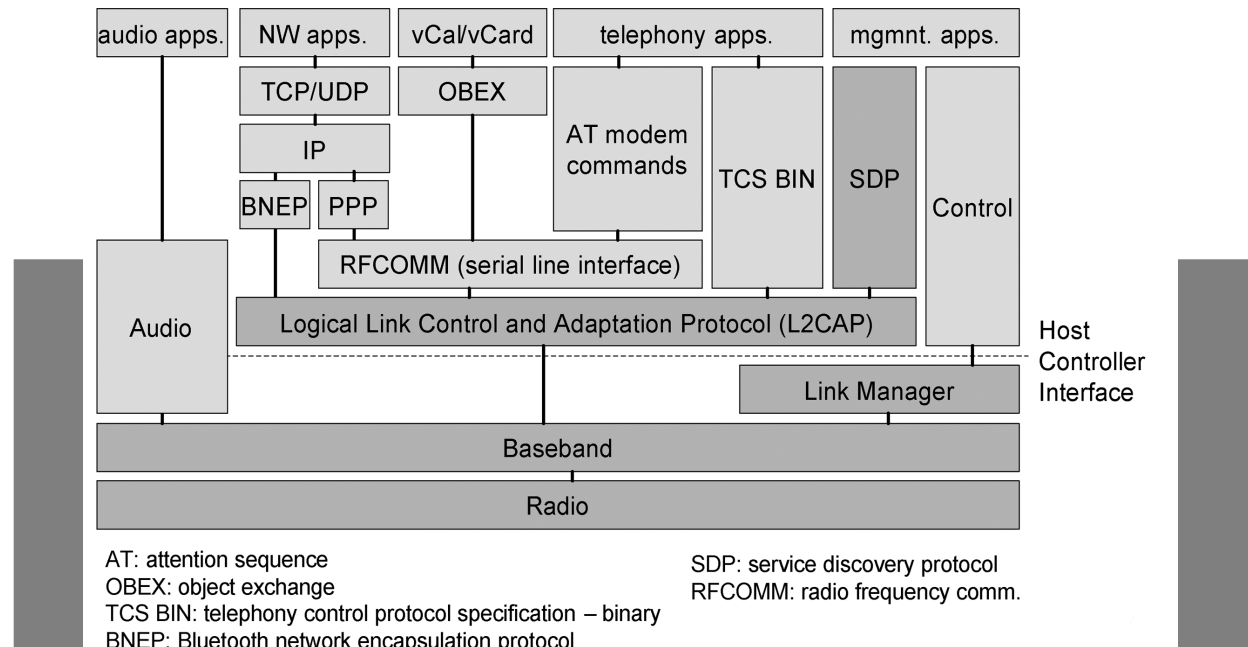


Fig. : Bluetooth Scatternet

A master can also go away from its piconet and act as a slave in another piconet. It is obviously not possible for a master of one piconet to act as the master of another piconet as this would direct to identical behavior. As soon as a master leaves a piconet, all traffic within this piconet is balanced until the master returns. Communication between different piconets takes place by devices jumping back and forth between these nets. If this is done occasionally, for instance, isochronous data streams can be forwarded from one piconet to another. On the other hand, scatternets are not yet supported by all piconet.

Q23. Explain Bluetooth protocol stack.*Ans. :***Bluetooth Protocol Stack****Fig.: Bluetooth Protocol Stack**

The Bluetooth protocol stack can be divided into:

Core Specification

Deals with the lower layers of the architecture and describes how the technology works. It describes the protocol from physical to data link layer along with management functions.

Profile Specification

Focuses on how to build interoperating devices using the core technology.

Bluetooth Radio

Specifies details of the air interface, including frequency, frequency hopping, modulation scheme, and transmission power.

Baseband

Concerned with connection establishment within a piconet, addressing, packet format, timing and power control.

Link Manager Protocol (LMP)

Establishes the link setup between Bluetooth devices and manages ongoing links, including security aspects (e.g. authentication and encryption), and control and negotiation of baseband packet size.

Logical Link Control and Adaptation Protocol (L2CAP)

Adapts upper layer protocols to the baseband layer. Provides both connectionless and connection-oriented services.

Service Discovery Protocol (SDP)

Handles device information, services, and queries for service characteristics between two or more Bluetooth devices.

Host Controller Interface (HCI)

Provides an interface method for accessing the Bluetooth hardware capabilities. It contains a command interface, which acts between the Baseband controller and link manager

TCS BIN (Telephony Control Service)

Bit-oriented protocol that defines the call control signaling for the establishment of voice and data calls between Bluetooth devices.

OBEX(OBJectEXchange)

Session-layer protocol for the exchange of objects, providing a model for object and operation representation

RFCOMM

A reliable transport protocol, which provides emulation of RS232 serial ports over the L2CAP protocol

WAE/WAP

Bluetooth incorporates the wireless application environment and the wireless application protocol into its architecture.

Physical Links

Different types of links can be established between master and slave. Two link types have been defined they are:

1. Synchronous Connection Oriented (SCO)

It Support symmetrical, circuit-switched, point-to-point connections . It is typically used for voice traffic. The Data rate is 64 kbit/s.

2. Asynchronous Connection-Less (ACL)

It Support symmetrical and asymmetrical, packet-switched, point-to-multipoint connections. It is typically used for data

transmission .Up to 433.9 kbit/s are used in symmetric or 723.2/57.6 kbit/s are used in asymmetric. The master uses polling. A slave may answer if it has used the preceeding slot.

Connection Establishment States**1. Standby**

The State in which Bluetooth device is inactive, radio not switched on, enable low power operation.

2. Page

The Master enters page state and starts transmitting paging messages to Slave using earlier gained access code and timing information.

3. Page Scan

The Device periodically enters page state to allow paging devices to establish connections.

4. Inquiry

The State in which device tries to discover all Bluetooth enabled devices in the close vicinity.

5. Inquiry Scan

Most devices periodically enter the inquiry scan state to make themselves available to inquiring devices.

Slave Connection State Modes**1. Active**

It participates in piconet It Listens, transmits and receives frames.

2. Sniff

It only listens on specified slots.

3. Hold

It does not support ACL frames. It has reduced power status. It May still participate in SCO exchanges.

4. Park

It does not participate on piconet and it Still retained as part of piconet.

Q24. What are the security services in blue tooth?

Ans :

Bluetooth Security

There are three modes of security for Bluetooth access between two devices.

- Non-secure
- Service level enforced security
- Link level enforced security

The following are the three basic security services specified in the Bluetooth standard:

Authentication

It verify the identity of communicating devices. User authentication is not provided natively by Bluetooth.

Confidentiality

It prevent information compromise caused by eavesdropping by ensuring that only authorized devices can access and view data.

Authorization

It allow the control of resources by ensuring that a device is authorized to use a service before permitting it to do so.

UNIT III

Mobile Network Layer: mobile IP, dynamic host configuration protocol, ad-hoc networks. Mobile Transport

Layer: Traditional TCP, classical TCP improvements, TCP over 2.5/3G wireless networks.

3.1 MOBILE NETWORK LAYER

3.1.1 Mobile IP

Need for Mobile IP

Q1. Explain the need for mobile IP.

Ans :

The IP addresses are designed to work with stationary hosts because part of the address defines the network to which the host is attached. A host cannot change its IP address without terminating on-going sessions and restarting them after it acquires a new address. Other link layer mobility solutions exist but are not sufficient enough for the global Internet.

Mobility is the ability of a node to change its point-of-attachment while maintaining all existing communications and using the same IP address.

Nomadcity allows a node to move but it must terminate all existing communications and then can initiate new connections with a new address.

Mobile IP is a network layer solution for homogenous and heterogeneous mobility on the global Internet which is scalable, robust, secure and which allows nodes to maintain all on going communications while moving.

Design Goals

Mobile IP was developed as a means for transparently dealing with problems of mobile users. Mobile IP was designed to make the size and the frequency of required routing updates as small as possible. It was designed to make it simple to implement mobile node software. It was designed to avoid solutions that require mobile nodes to use multiple addresses.

Requirements

There are several requirements for Mobile IP to make it as a standard. Some of them are :

1. Compatibility

The whole architecture of internet is very huge and a new standard cannot introduce changes to the applications or network protocols already in use.

Mobile IP is to be integrated into the existing operating systems. Also, for routers also it may be possible to enhance its capabilities to support mobility instead of changing the routers which is highly impossible. Mobile IP must not require special media or

MAC/LLC protocols, so it must use the same interfaces and mechanisms to access the lower layers as IP does. Finally, end-systems enhanced with a mobile IP implementation should still be able to communicate with fixed systems without mobile IP.

2. Transparency

Mobility remains invisible for many higher layer protocols and applications. Higher layers continue to work even if the mobile computer has changed its point of attachment to the network and even notice a lower bandwidth and some interruption in the service. As many of today's applications have not been designed to use in mobile environments, the effects of mobility will be higher delay and lower bandwidth.

3. Scalability and efficiency

The efficiency of the network should not be affected even if a new mechanism is introduced into the internet. Enhancing IP for mobility must not generate many new messages flooding the whole

network. Special care is necessary to be taken considering the lower bandwidth of wireless links. Many mobile systems have a wireless link to an attachment point. Therefore, only some additional packets must be necessary between a mobile system and a node in the network. It is indispensable for a mobile IP to be scalable over a large number of participants in the whole internet, throughout the world.

4. Security

Mobility possesses many security problems. A minimum requirement is the authentication of all messages related to the management of mobile IP. It must be sure for the IP layer if it forwards a packet to a mobile host that this host really is the receiver of the packet. The IP layer can only guarantee that the IP address of the receiver is correct. There is no way to prevent faked IP addresses and other attacks.

The goal of a mobile IP can be summarized as: 'supporting end-system mobility while maintaining scalability, efficiency, and compatibility in all respects with existing applications and Internet protocols'.

Q2. Define the terms used in mobile IP.

Ans :

Entities and Terminology

The following defines several entities and terms needed to understand mobile IP as defined in RFC 3344.

Mobile Node (MN) : 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 communicate with any other system in the internet as long as link-layer connectivity is given. Examples are laptop, mobile phone, router on an aircraft etc.

Correspondent node (CN): At least one partner is needed for communication. In the following the CN represents this partner for the MN. The CN can be a fixed or mobile node.

Home network: The home network is the subnet the MN belongs to with respect to its IP address. No mobile IP support is needed within the home network.

Foreign network: The foreign network is the current subnet the MN visits and which is not the home network.

Foreign agent (FA): The FA can provide several services to the MN during its visit to the foreign network. The FA can have the COA, acting as tunnel endpoint and forwarding packets to the MN. The FA can be the default router for the MN. FAs can also provide security services because they belong to the foreign network as opposed to the MN which is only visiting. FA is implemented on a router for the subnet the MN attaches to.

Care-of address (COA): The COA 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. Packet delivery toward the MN is done using a tunnel, i.e., the COA marks the tunnel endpoint, i.e., the address where packets exit the tunnel. There are two different possibilities for the location of the COA:

Foreign agent COA: The COA could be located at the FA, i.e., the COA is an IP address of the FA. The FA is the tunnel end-point and forwards packets to the MN. Many MN using the FA can share this COA as common COA.

Co-located COA: The COA is co-located if the MN temporarily acquired an additional IP address which acts as COA. This address is now topologically correct, and the tunnel endpoint is at the MN. Co-located addresses can be acquired using services such as DHCP.

Q3. What is Mobile IP network ? Explain the packet delivery process and working of mobile IP.

Or

Explain briefly about Mobile IP.

Ans :

Home agent (HA)

The HA provides several services for the MN and is located in the home network. The tunnel for packets toward the MN starts at the HA. The HA can be implemented on a router that is responsible

for the home network. This is obviously the best position, because without optimizations to mobile IP, all packets for the MN have to go through the router anyway.

2. One 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 MN comes in via the router; the HA sends it through the tunnel which again crosses the router.
3. Finally, a home network is not necessary at all. The HA could be again on the ZCouteC [but this time only acting as a manager for MNs belonging to a virtual home network.

All MNs are always in a foreign network with this solution.

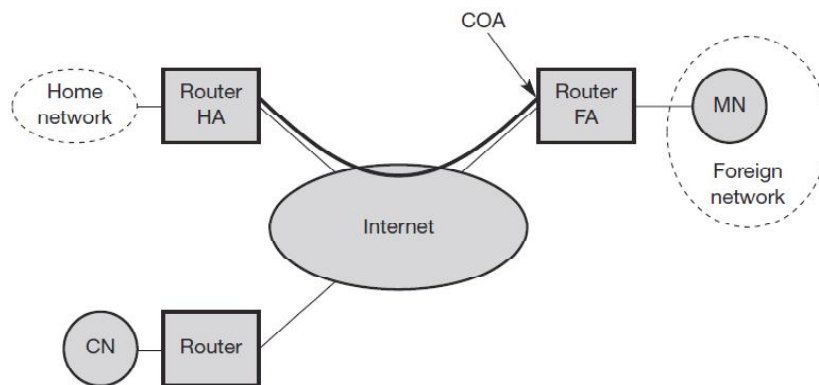


Fig. : Mobile IP example network

A CN is connected via a router to the internet, as are the home network and the foreign network. The HA is implemented on the router connecting the home network with the internet, an FA is implemented on the router to the foreign network. The MN is currently in the foreign network. The tunnel for packets toward the MN starts at the HA and ends at the FA, for the FA has the COA in the above example.

IP Packet Delivery

Consider the above example in which a correspondent node (CN) wants to send an IP packet to the MN. One of the requirements of mobile IP was to support hiding the mobility of the MN. CN does not need to know anything about the MN's current location and sends the packet as usual to the IP address of MN as shown below.

CN sends an IP packet with MN as a destination address and CN as a source address.

The internet, not having information on the current location of MN, routes the packet to the router responsible for the home network of MN. This is done using the standard routing mechanisms of the internet. The HA now intercepts the packet, knowing that MN is currently not in its home network. The packet is not forwarded into the subnet as usual, but encapsulated and tunnelled to the COA.

A new header is put in front of the old IP header showing the COA as new destination and HA as source of the encapsulated packet (step 2). The foreign agent now decapsulates the packet, i.e., removes the additional header, and forwards the original packet with CN as source and MN as destination to the MN (step 3). Again, for the MN mobility is not visible. It receives the packet with the same sender and receiver address as it would have done in the home network.

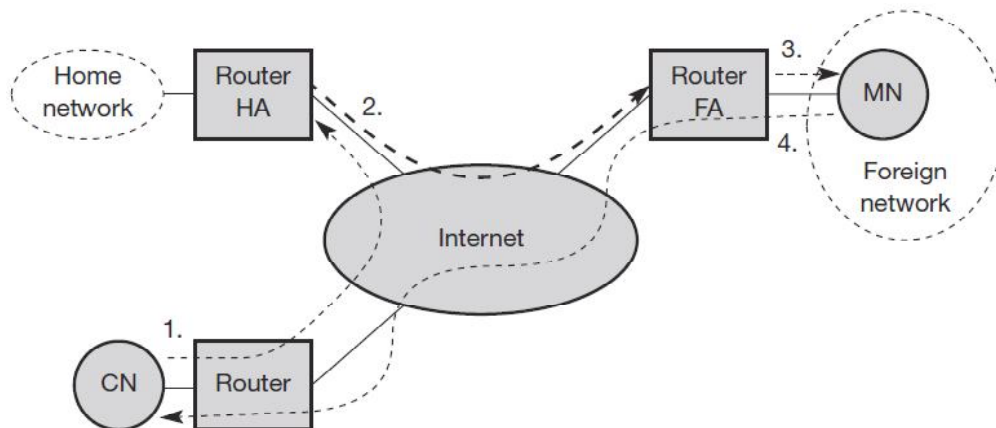


Fig. : Packet delivery to and from the mobile node

Sending packets from the mobile node (MN) to the CN is comparatively simple. The MN sends the packet as usual with its own fixed IP address as source and CN's address as destination (step 4). The router with the FA acts as default router and forwards the packet in the same way as it would do for any other node in the foreign network. As long as CN is a fixed node, the remainder is in the fixed Internet as usual. If CN were also a mobile node residing in a foreign network, the same mechanisms as described in steps 1 through 3 would apply now in the other direction.

Working of Mobile IP

Mobile IP has two addresses for a mobile host: one home address and one care-of address. The home address is permanent; the care-of address changes as the mobile host moves from one network to another. To make the change of address transparent to the rest of the Internet requires a home agent and a foreign agent. The specific function of an agent is performed in the application layer. When the mobile host and the foreign agent are the same, the care-of address is called a co-located care-of address.

Q4. What are the phases of mobile IP communication ?

Or

Explain agent discovery and agent registration.

Ans :

To communicate with a remote host, a mobile host goes through the following phases:

- ▶ agent discovery
- ▶ Agent Registration

1. Agent Discovery

A mobile node has to find a foreign agent when it moves away from its home network. To solve this problem, mobile IP describes two methods: agent advertisement and agent solicitation.

➤ Agent advertisement

For this method, foreign agents and home agents advertise their presence periodically using special **agent advertisement** messages, which are broadcast into the subnet. Mobile IP does not use a new packet type for agent advertisement; it uses the router advertisement packet of ICMP, and appends an agent advertisement message. The agent advertisement packet according to RFC 1256 with the extension for mobility is shown below :

0	7	8	15	16	23	24	31					
type		code		checksum								
#addresses		addr. size		lifetime								
router address 1												
preference level 1												
router address 2												
preference level 2												
...												
type = 16		length		sequence number								
registration lifetime				R	B	H	F	M	G	r	T	reserved
COA 1												
COA 2												
...												

The TTL field of the IP packet is set to 1 for all advertisements to avoid forwarding them. The **type** is set to 9, the **code** can be 0, if the agent also routes traffic from non mobile nodes, or 16, if it does not route anything other than mobile traffic. The number of addresses advertised with this packet is in **#addresses** while the **addresses** themselves follow as shown. **Lifetime** denotes the length of time this advertisement is valid.

Preference levels for each address help a node to choose the router that is the most eager one to get a new node.

The extension for mobility has the following fields defined: **type** is set to 16, **length** depends on the number of COAs provided with the message. The **sequence number** shows the total number of advertisements sent since initialization by the agent. By the **registration lifetime** the agent can specify the maximum lifetime in seconds a node can request during registration.

The following bits specify the characteristics of an agent in detail. The **R** bit (registration) shows, if a registration with this agent is required even when using a colocated COA at the MN. If the agent is currently too busy to accept new registrations it can set the **B**

bit. The following two bits denote if the agent offers services as a home agent (**H**) or foreign agent (**F**) on the link where the advertisement has been sent. Bits **M** and **G** specify the method of encapsulation used for the tunnel. While IP-in-IP encapsulation is the mandatory standard, **M** can specify minimal encapsulation and **G** generic routing encapsulation. the **V** bit specifies the use of header compression according to RFC 1144.

Now the field **r** at the same bit position is set to zero and must be ignored. The new field **T** indicates that reverse tunnelling is supported by the FA. The following fields contain the **COAs** advertised. A foreign agent setting the **F** bit must advertise at least one COA. A mobile node in a subnet can now receive agent advertisements from either its home agent or a foreign agent. This is one way for the MN to discover its location.

➤ Agent Solicitation

If no agent advertisements are present or the inter-arrival time is too high, and an MN has not received a COA by other means, the mobile node must send **agent solicitations**. Care must be taken to ensure that these solicitation messages do not flood the network, but basically an MN can search for an FA endlessly sending out solicitation messages. If a node does not receive an answer to its solicitations it must decrease the rate of solicitation exponentially to avoid flooding the network until it reaches a maximum interval between solicitations (typically one minute). Discovering a new agent can be done anytime, not just if the MN is not connected to one.

After these steps of advertisements or solicitations the MN can now receive a COA, either one for an FA or a co-located COA.

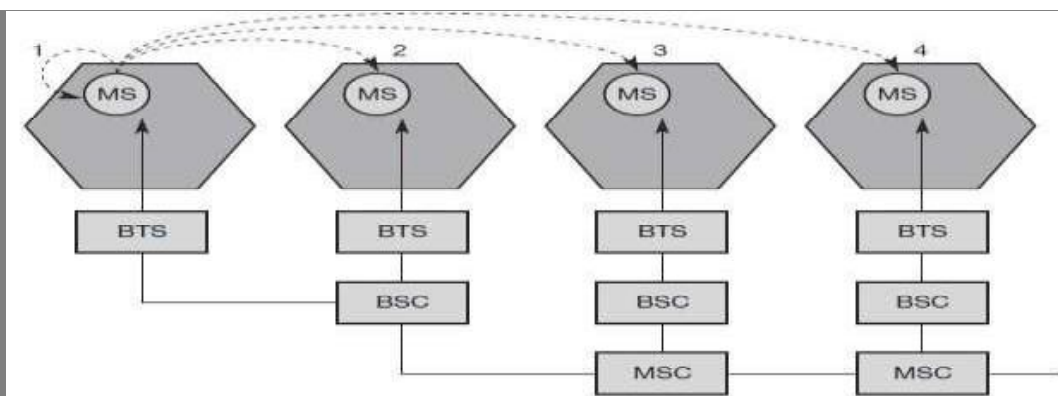
2. Agent Registration

Having received a COA, the MN has to register with the HA. The main purpose of the registration is to inform the HA of the current location for correct forwarding of packets.

Registration can be done in two different 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 forwards the request to the HA. The HA now sets up a **mobility binding**. Registration expires automatically after the lifetime and is deleted; so, an MN should reregister before expiration. This mechanism is necessary to avoid mobility bindings which are no longer used. After setting up the mobility binding, the HA sends a reply message back to the FA which forwards it to the MN.

If the COA is co-located, registration can be simpler, the MN sends the request directly to the HA and vice versa. This is also the registration procedure for MNs returning to their home network to register directly with the HA. UDP packets are used for the registration requests using the port no 434. The IP source address of the packet is set to the interface address of the MN, the IP destination address is that of the FA or HA.



➤ Registration Request

The first field **type** is set to 1 for a registration request. With the **S** bit an MN can specify if it wants the HA to retain prior mobility bindings. This allows for simultaneous bindings. Setting the **B** bit generally indicates that an MN also wants to receive the broadcast packets which have been received by the HA in the home network. If an MN uses a co-located COA, it also takes care of the decapsulation at the tunnel endpoint.

The **D** bit indicates this behavior. As already defined for agent advertisements, the bits **M** and **G** denote the use of minimal encapsulation or generic routing encapsulation, respectively. **T** indicates reverse tunneling, **r** and **x** are set to zero. **Lifetime** denotes the validity of the registration in seconds. A value of zero indicates deregistration; all bits set indicates infinity. The **home address** is the fixed IP address of the MN, **home agent** is the IP address of the HA, and **COA** represents the tunnel endpoint. The 64 bit **identification** is generated by the MN to identify a request and match it with registration replies. This field is used for protection against replay attacks of registrations. The **extensions** must at least contain parameters for authentication.

A **registration reply**, which is conveyed in a UDP packet, contains a **type** field set to 3 and a **code** indicating the result of the registration request.

➤ Registration Reply

The **lifetime** field indicates how many seconds the registration is valid if it was successful. **Home address** and **home agent** are the addresses of the MN and the HA, respectively. The 64-bit **identification** is used to match registration requests with replies. The value is based on the identification field from the registration and the authentication method. Again, the **extensions** must at least contain parameters for authentication.

Tunnelling and Encapsulation

Q5. Define tunnelling.

Ans :

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. Tunneling, i.e., sending a packet through a tunnel is achieved by using encapsulation.

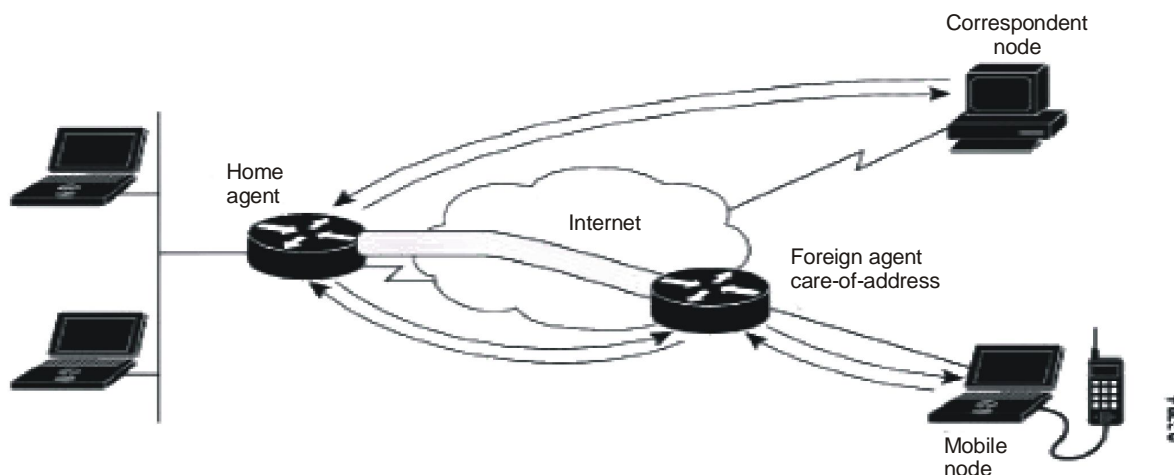
Q6. Why is mobile IP packet required to be forwarded through a tunnel.

Ans :

The Mobile Node is a device such as a cell phone, personal digital assistant, or laptop whose software enables network roaming capabilities.

The Home Agent is a router on the home network serving as the anchor point for communication with the Mobile Node.

The Foreign Agent is a router that may function as the point of attachment for the Mobile Node when it roams to a foreign network, delivering packets from the Home Agent to the Mobile Node.



Why Tunnelling ?

- ▶ Consider a situation when a Correspondent Node (CN) wants to send an IP packet to a Mobile Node (MN). All the CN knows about this MN is its IP address.
- ▶ The CN is totally unaware of the MN's location. (Which in fact is a major requirement of Mobile IP) and so sends it as usual to MN's IP address.
- ▶ The internet routes this packet to the Home router of the MN also called as Home Agent (HA).
- ▶ The HA now knowing that the MN is not in its home network send encapsulates and tunnels it to the COA.
- ▶ The Care-of-address (COA) defines the current location of the MN from an IP point of view (e.g. when a person Mr. XYZ stays as a guest in someone else's home , the letters he receive will be marked as Mr. XYZ ,C/O i.e. care-of Mr. ABC)
- ▶ Since internet routes are created based on the header contents of an IP packet, to route it from HA to COA, we need a new to create header for the packet to be transmitted.

- ▶ The new header on top of the original header is made (refer diagram-2). Now this will enable us to set a new direct route (a tunnel) to the MN from the HA as it is roaming.
- ▶ **Tunnelling**: It is the process of creating a tunnel by the HA to the COA to route packets to the Mobile Node as it roams.
- ▶ It establishes a pipe (a data stream between two connected ends) wherein the data is inserted and moves in FIFO order.

Q7. What is Encapsulation ? Explain about various encapsulation techniques.

Ans :

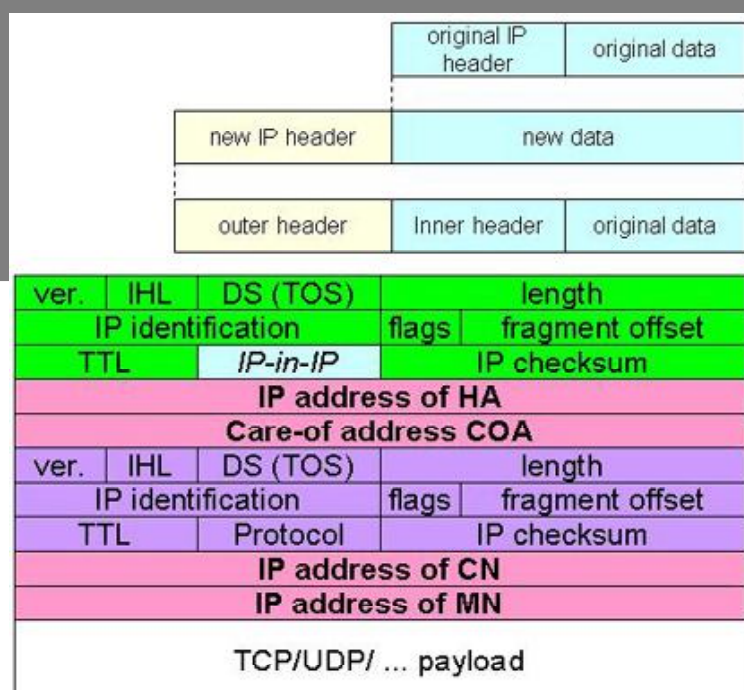
Encapsulation is the mechanism of taking a packet consisting of packet header and data and putting it into the data part of a new packet. The reverse operation, taking a packet out of the data part of another packet, is called **decapsulation**.

Three types of encapsulation protocols are specified for Mobile IP :

1. **IP-in-IP encapsulation**: required to be supported. Full IP header added to the original IP packet. The new header contains HA address as source and Care of Address as destination.
2. **Minimal encapsulation**: optional. Requires less overhead but requires changes to the original header. Destination address is changed to Care of Address and Source IP address is maintained as is.
3. **Generic Routing Encapsulation (GRE)**: optional. Allows packets of a different protocol suite to be encapsulated by another protocol suite.

1. IP-in-IP encapsulation

There are different ways of performing the encapsulation needed for the tunnel between HA and COA. Mandatory for mobile IP is **IP-in-IP encapsulation** as specified in RFC 2003. The following figure shows a packet inside the tunnel.



Ver: version field is 4 for IP version 4

Internet header length (IHL): denotes the length of the outer header in 32 bit words. **DS(TOS):** is just copied from the inner header,

Length : the **length** field covers the complete encapsulated packet.

The fields up to TTL have no special meaning for mobile IP and are set according to RFC 791. **TTL** must be high enough so the packet can reach the tunnel endpoint. The next field, here denoted with **IP in-IP**, is the type of the protocol used in the IP payload. This field is set to 4, the protocol type for IPv4 because again an IPv4 packet follows after this outer header. **IP checksum** is calculated as usual. The next fields are the tunnel entry as source address (the **IP address of the HA**) and the tunnel exit point as destination address (the **COA**).

If no options follow the outer header, the inner header starts with the same fields as above. This header remains almost unchanged during encapsulation, thus showing the original sender CN and the receiver MN of the packet. The only change is TTL which is decremented by 1. This means that the whole tunnel is considered a single hop from the original packet point of view. This is a very important feature of tunneling as it allows the MN to behave as if it were attached to the home network. No matter how many real hops the packet has to take in the tunnel, it is just one (logical) hop away for the MN. Finally, the payload follows the two headers.

Minimal encapsulation

- ▶ Minimal encapsulation is an optional encapsulation method for mobile IP.
- ▶ In methods like IP-in-IP encapsulation fields are redundant. So, here the number of fields is reduced without affecting the transmission.
- ▶ No field for fragmentation offset is present in inner header
- ▶ Minimal encapsulation does not work with already fragmented packets.

ver.	IHL	DS (TOS)	length	
IP identification			flags	fragment offset
TTL	min. encap.		IP checksum	
IP address of HA				
care-of address COA				
Protocol	S	reserved	IP checksum	
IP address of MN				
original sender IP address (if S=1)				
TCP/UDP/ ... payload				

Ver :	IP version (4 a IPV4).
DS (TOS):	copied from the inner header.
IHL:	Internet header length (a 32 bit word).
Length	length of complete encapsulated packet.
TTL	(Time To Live) must be high enough so that packet reaches the tunnel endpoint.
Protocol	55 '! Minimal encapsulation. meant for value of protocol
S	If s=1; the original sender address is included in packet.

Generic Routing Encapsulation

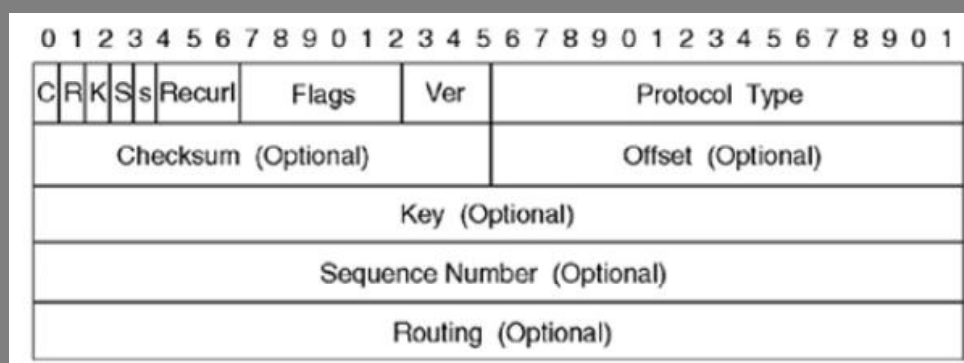
Generic routing encapsulation (GRE) is an IP encapsulation protocol which is used to transport IP packets over a network. Generic routing encapsulation (GRE) was initially developed by Cisco, but later become industry standard (RFC 1701, RFC 2784, RFC 2890).

Generic Routing Encapsulation (GRE) can tunnel any Layer 3 protocol including IP. In GRE (Generic Routing Encapsulation) an IP datagram is tunnelled (encapsulated) within another IP datagram.

One great advantage of GRE (Generic Routing Encapsulation) is that it allows routing of IP packets between private IPv4 networks which are separated over public IPv4 internet. GRE (Generic Routing Encapsulation) also supports encapsulating IPv4 broadcast and multicast traffic.

Generic routing encapsulation (GRE) tunnels are not secure because Generic routing encapsulation (GRE) does not encrypt its Data payload. In real-time, Generic routing encapsulation (GRE) used together with other secure tunnelling protocols like IPSec to provide network security.

Generic Routing Encapsulation (GRE) Header



Following are the fields of Generic Routing Encapsulation (GRE) Header.

Flag C (Checksum Present) : Used to indicate that the Checksum field is present and contains valid information, when set to 1.

Flag R (Routing Present) : Used to indicate that the Routing fields are present and contain valid information, when set to 1.

Flag K (Key Present) : Used to indicate that the Key field is present in the GRE header, when set to 1.

Flag S (Sequence Number Present) : Used to indicate that the Sequence Number field is present, when set to 1.

Flag s (Strict Source Route) : Set to 1 the routing information consists of Strict Source Routes

Recursion Control and Version Number are normally set to 0

Protocol Type : Protocol Type field is used to mention the protocol payload of the GRE packet. For IP, this field is set to 0x800

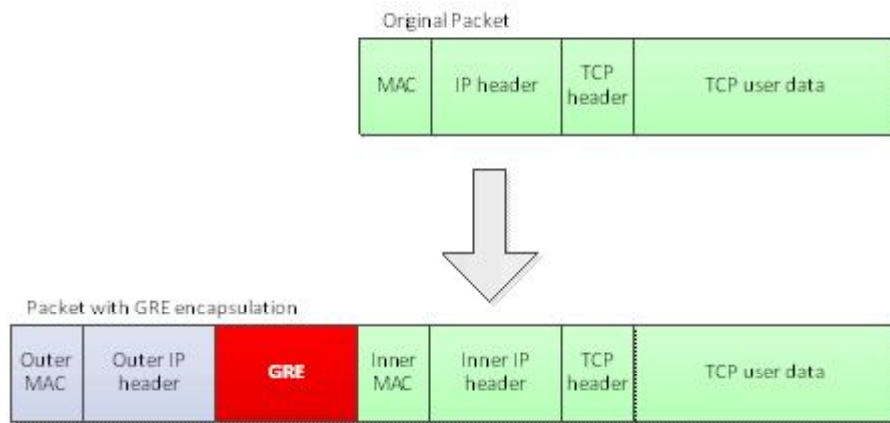
Checksum : Checksum field value is used to check the integrity of the GRE header and the payload.

Key : Key field value is used to authenticate the GRE packet's encapsulator.

Sequence Number : Sequence Number field value is used to track the sequence of GRE packets.

Generic Routing Encapsulation (GRE) Encapsulation

Following image shows the difference between original IP Datagram and Generic Routing Encapsulation (GRE) encapsulated IP Datagram.



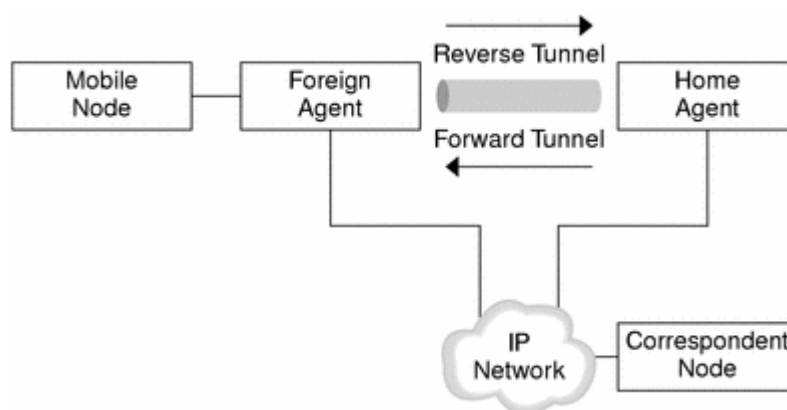
Reverse Tunnelling

Q8. What is reverse tunnelling ? Explain.

Ans :

The reverse path from MS to the CN looks quite simple as the MN can directly send its packets to the CN as in any other standard IP situation. The destination address in the packets is that of CN. But it has some problems explained below :

Quite often firewalls are designed to only allow packets with topologically correct addresses to pass to provide simple protection against misconfigured systems of unknown addresses. However, MN still sends packets with its fixed IP address as source which is not topologically correct in a foreign network. Firewalls often filter packets coming from outside containing a source address from computers of the internal network. This also implies that an MN cannot send a packet to a computer residing in its home network.



While the nodes in the home network might participate in a multi-cast group, an MN in a foreign network cannot transmit multi-cast packets in a way that they emanate from its home network without a reverse tunnel. The foreign network might not even provide the technical infrastructure for multi-cast communication (multi-cast backbone, Mbone).

If the MN moves to a new foreign network, the older TTL might be too low for the packets to reach the same destination nodes as before. Mobile IP is no longer transparent if a user has to adjust the TTL while moving. A reverse tunnel is needed that represents only one hop, no matter how many hops are really needed from the foreign to the home network.

Based on the above considerations, reverse tunnelling is defined as an extension to mobileIP (per RFC 2344). It was designed backward compatible to mobile IP and defines topologically correct reverse tunnelling to handle the above stated problems.

Q9. Write short note on IPv6.

Ans :

1. IPv6 is the next generation Internet Protocol designed as a successor to the IP version 4.
2. IPv6 was designed to enable high performance, scalable internet.
3. This was achieved by overcoming many of the weaknesses of IPv4 protocol and by adding several new features.
4. In IPv6, there are 2^{128} possible ways (about 3.4×10^{38} addresses).
5. IPv6 is written in hexadecimal and consists of 8 groups, containing 4 hexadecimal digits or 8 groups of 16 bits each.
6. The IPv6 header is a static header of 40 bytes in length and has only 8 fields. Option information is carried by the extension header which is placed after the IPv6 header.
7. IPv6 has no header checksum because checksums are for example above the TCP/IP protocol suite and above the Token Ring, Ethernet etc.
8. The IPv6 header contains an 8 bit field called the Traffic Class Field. This field allows the traffic source to identify the desired delivery priority of its packets.
9. The IPv6 has both a stateful and stateless address auto-configuration mechanism.
10. IPv6 has been designed to satisfy the growing and expanded need for network security.
11. Source and destination addresses are 128 bits (16 bytes) in length.
12. Packet flow identification for QoS handling by routers is included in the IPv6 header using the Flow Label Field.
13. ARP request frames are replaced with multicast neighbour solicitation messages.
14. ICMP router discovery is replaced with ICMPv6 router solicitation and router advertisement messages are required.
15. IPv6 has three different types of addresses.

Unicast: A unicast address defines a single computer. A packet sent to a unicast address is delivered to that specific computer.

Anycast: This is a type of address that defines a group of computers with addresses which have the same prefix. A packet sent to an anycast address must be delivered to exactly one of the members of the group which is closest or the most easily accessible.

Multicast: A multicast address defines a group of computers which may or may not share the same prefix and may or may not be connected to the same physical network. A packet sent to a multicast address must be delivered to each member of the set.

3.1.2 Dynamic Host Configuration Protocol

Q10. Explain briefly DHCP.

Ans :

The Dynamic Host Configuration Protocol (DHCP) is a client/server protocol designed to provide the four pieces of information for a diskless computer or a computer that is booted for the first time.

Dynamic Host Configuration Protocol is useful because it can make it easy to add new machines to the local network.

DHCP Operation

The DHCP client and server can either be on the same network or on different networks.

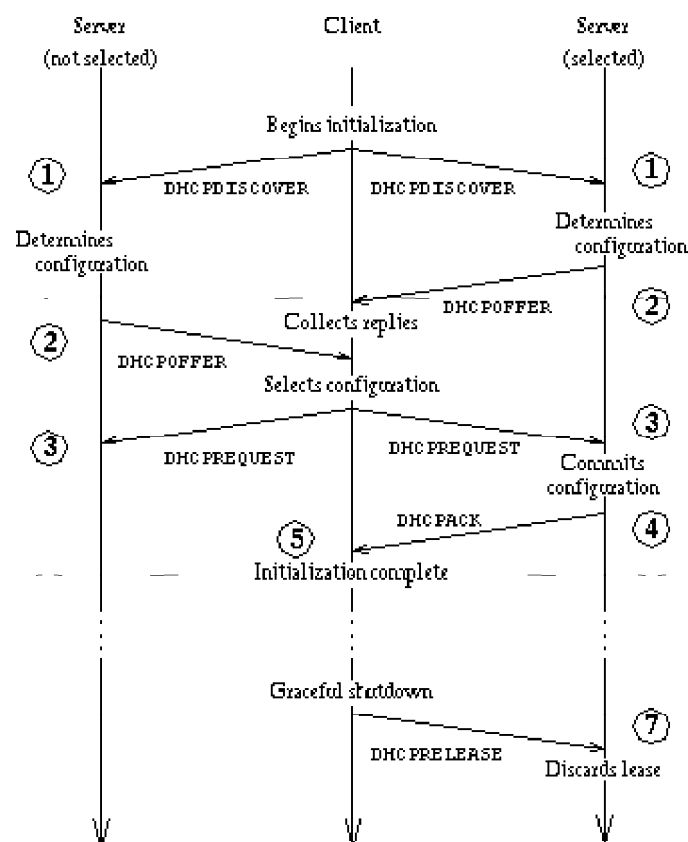
- **Same Network :** Although the practice is not very common, the administrator may put the client and the server on the same network as shown in Figure1.

How DHCP Works

The client and the server negotiate in a series of messages in order for the client to get the parameters it needs.

The following diagram shows the messages exchanged between the DHCP client and servers when allocating a new network address. Next is a detailed explanation of all the various messages and a description of the communication steps.

This process can involve more than one server but only one server is selected by the client. In the figure, the selected server is marked 'selected' and the other, 'not selected' server stands for all the possible not selected servers.



Description of the Communication Steps

1. The client broadcasts a DHCPDISCOVER.
2. Each server may respond with a DHCPOFFER message.
3. The client receives one or more DHCPOFFER messages from one or more servers and chooses one server from which to request configuration parameters.

The client broadcasts a DHCPREQUEST message.

4. Those servers not selected by the DHCPREQUEST message use the message as notification that the client has declined that server's offer.

The server selected in the DHCPREQUEST message commits the responds with a DHCPACK message containing the configuration parameters for the requesting client.

5. The client receives the DHCPACK message with configuration parameters. At this point, the client is configured.

If the client receives a DHCPNAK message, the client restarts the configuration process.

6. The client may choose to relinquish its lease on a network address by sending a DHCPRELEASE message to the server (e.g. on shutdown).

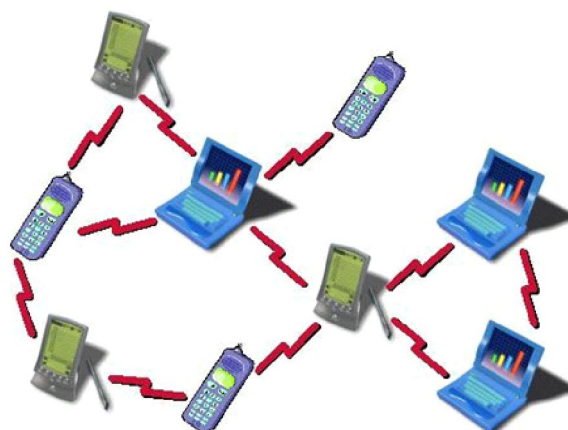
7. The server receives the DHCPRELEASE message and marks the lease as free.

3.1.3 AD-HOC Networks

Q11. What is a MANET ? Write the characteristics.

Ans :

It is an infrastructureless IP based network of mobile and wireless machine nodes connected with radio. In operation, the nodes of a MANET do not have a centralized administration mechanism. It is known for its routeable network properties where each node act as a "router" to forward the traffic to other specified node in the network.



Types of MANET

There are different types of MANETs including:

- ▶ **InVANETs** – Intelligent vehicular ad hoc networks make use of artificial intelligence to tackle unexpected situations like vehicle collision and accidents.
- ▶ **Vehicular ad hoc networks (VANETs)** – Enables effective communication with another vehicle or helps to communicate with roadside equipments.
- ▶ **Internet Based Mobile Ad hoc Networks (iMANET)** – helps to link fixed as well as mobile nodes.

Characteristics of MANET

- ▶ **In MANET**, each node act as both host and router. That is it is autonomous in behavior.
- ▶ **Multi-hop radio relaying**- When a source node and destination node for a message is out of the radio range, the MANETs are capable of multi-hop routing.
- ▶ Distributed nature of operation for security, routing and host configuration. A centralized firewall is absent here.
- ▶ The nodes can join or leave the network anytime, making the network topology dynamic in nature.
- ▶ Mobile nodes are characterized with less memory, power and light weight features.
- ▶ The reliability, efficiency, stability and capacity of wireless links are often inferior when

compared with wired links. This shows the fluctuating link bandwidth of wireless links.

- ▶ Mobile and spontaneous behavior which demands minimum human intervention to configure the network.
- ▶ All nodes have identical features with similar responsibilities and capabilities and hence it forms a completely symmetric environment.
- ▶ High user density and large level of user mobility.
- ▶ Nodal connectivity is intermittent.

Q12. Explain various routing protocols used in MANET.

Ans :

Generally routing protocols in MANETs are either based on the link-state (LS) routing algorithm or on the distance-vector (DV) routing-algorithm. Common for both of these algorithms is that they try to find the shortest path from the source node to the destination node. The main difference is that in LS based routing a global network topology is maintained in every node of the network.

In DV based routing the nodes only maintain information of and exchange information with their adjacency nodes. Keeping track of many other nodes in a MANET may produce overhead, especially when the network is large. Therefore one of the most important issues in MANET design is to come up with schemes that will contribute to reduce routing overheads.

Mobile Ad Hoc Network routing protocols fall into two general categories :

1. Proactive routing protocols
2. Reactive routing protocols

Different Routing Protocols

1. Flat Routing Protocols

Pro-Active/Table Driven routing Protocols

Reactive/On Demand Routing Protocols

2. Hybrid Routing Protocols
3. Hierarchical Routing Protocols
4. Geographical Routing Protocols

Flat routing protocols are divided into two classes;

proactive routing (table driven) protocols and **reactive** (on-demand) routing protocols.

Common for both protocol classes is that all nodes participating in routing play an equal role. They have further been classified after their design principles; proactive routing is mostly based on LS (link-state) while on-demand routing is based on DV (distance- vector).

Pro-Active/Table Driven routing Protocols

Proactive MANET protocols are table-driven and will actively determine the layout of the network. Through a regular exchange of network topology packets between the nodes of the network, a complete picture of the network is maintained at every single node.

There is hence minimal delay in determining the route to be taken. This is especially important for time-critical traffic (Scientific Research Corporation, 2004). However, a drawback to a proactive MANET of protocol is that the life span of a link is significantly short. This phenomenon is brought about by the increased mobility of the nodes, which will render the routing information in the table invalid quickly.

When the routing information becomes invalid quickly, there are many short-lived routes that are being determined and not used before they turn void. Hence, another drawback resulting from the increased mobility is the amount of traffic overhead generated when evaluating these unnecessary routes. This is especially aggravated when the network size increases. The fraction of the total control traffic that consists of actual practical data is further decreased.

Examples of Proactive MANET Protocols include:

1. Optimized Link State Routing, or OLSR
2. Topology Broadcast based on Reverse Path Forwarding, or TBRPF
3. Fish-eye State Routing, or FSR
4. Destination-Sequenced Distance Vector, or DSDV
5. Landmark Routing Protocol, or LANMAR

6. Clusterhead Gateway Switch Routing Protocol, or CGSR

Reactive/On Demand Routing Protocols

On-demand routing is a popular routing category for wireless ad hoc routing. It is a relatively new routing philosophy that provides a scalable solution to relatively large network topologies. The design follows the idea that each node tries to reduce routing overhead by only sending routing packets when communication is requested. Common for most on-demand routing protocols are the route discovery phase where packets are flooded into the network in search of an optimal path to the destination node in the network.

There are numerous on-demand routing protocols, but only two of them are more significant. These are Ad Hoc On-Demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR). These two have been chosen because both have been extensively evaluated in the MANET literature and are being considered by the Internet Engineering Task Force (IETF) MANET Working Group as the leading candidates for standardization. Thus, reactive MANET protocols are most suited for networks with high node mobility or where the node transmits data infrequently.

Examples of Reactive MANET Protocols include:

1. Ad Hoc On-Demand Distance Vector, or AODV
2. Dynamic Source Routing, or DSR.
3. Temporally Ordered Routing Algorithm, or TORA

Hybrid Routing Protocols

Since proactive and reactive routing protocols each work best in oppositely different scenarios, there is good reason to develop hybrid routing protocols, which use a mix of both proactive and reactive routing protocols. These hybrid protocols can be used to find a balance between the proactive and reactive protocols.

The basic idea behind hybrid routing protocols is to use proactive routing mechanisms in some areas of the network at certain times and reactive routing for the rest of the network. The proactive operations are restricted to a small domain in order to reduce

the control overheads and delays. The reactive routing protocols are used for locating nodes outside this domain, as this is more bandwidth-efficient in a constantly changing network.

Examples of Hybrid Routing Protocols include:

1. Cornell's Zone Routing Protocol (ZRP)
2. Scientific Research Corporation's Wireless Ad hoc Routing Protocol (WARP) – based on ZRP with additional enhancements for Quality of Service, or QoS support (Mobile Route TM)

Hierarchical Routing Protocols

As the size of the wireless network increases, the flat routing protocols may produce too much overhead for the MANET. In this case a hierarchical solution may be preferable. CGSR, HSR, ZRP and LANMAR are four hierarchical routing protocols that have different solutions to the organization of the routing of nodes in a MANET.

Examples of Hierarchical Routing Protocols include:

1. CGSR (Cluster head-Gateway Switch Routing)
2. HSR (Hierarchical State Routing)
3. ZRP (Zone Routing Protocol)
4. LANMAR (Landmark Ad Hoc Routing Protocol)

Geographical Routing Protocols

There are two approaches to geographic mobile adhoc networks :

1. Actual geographic coordinates (as obtained through GPS – the Global Positioning System)
2. Reference points in some fixed coordinate system

An **advantage** of geographic routing protocols is that they prevent network-wide searches for destinations. Control and data packets can be sent in the general direction of the destination if the recent geographical coordinates are known. This reduces control overhead in the network. The routing update must be done faster than the network mobility rate to make the location-based routing effective. This is because the nodes locations may change quickly in a MANET.

Examples of Geographical Routing Protocols include :

1. GeoCast (Geographic Addressing and Routing)
2. DREAM (Distance Routing Effect Algorithm for Mobility)
3. GPSR (Greedy Perimeter Stateless Routing).

3.2 MOBILE TRANSPORT LAYER

3.2.1 Traditional TCP

Q13. Write a short note on TCP.

Ans :

The **Transmission Control Protocol (TCP)** is one of the core protocols of the Internet protocol suite, often simply referred to as TCP/IP. TCP is reliable, guarantees in-order delivery of data and incorporates congestion control and flow control mechanisms. TCP supports many of the Internet's most popular application protocols and resulting applications, including the World Wide Web, e-mail, File Transfer Protocol and Secure Shell. In the Internet protocol suite, TCP is the intermediate layer between the Internet layer and application layer.

The major responsibilities of TCP in an active session are to :

- **Provide reliable in-order transport of data :** to not allow losses of data.
- **Control congestions in the networks:** to not allow degradation of the network performance,
- **Control a packet flow between the transmitter and the receiver:** to not exceed the receiver's capacity.

TCP uses a number of mechanisms to achieve high performance and avoid 'congestion collapse', where network performance can fall by several orders of magnitude. These mechanisms control the rate of data entering the network, keeping the data flow below a rate that would trigger collapse.

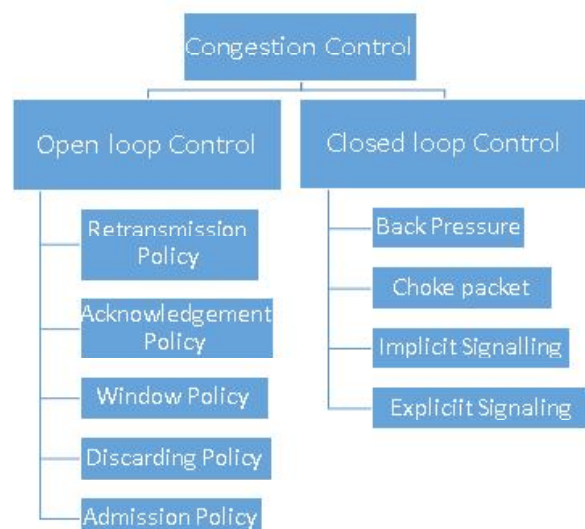
There are several mechanisms of TCP that influence the efficiency of TCP in a mobile environment. Acknowledgments for data sent, or lack of acknowledgments, are used by senders to implicitly interpret network conditions between the TCP sender and receiver.

Q14. How congestion is controlled in TCP ?

Ans :

Congestion Control

Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. In general, we can divide congestion control mechanisms into two broad categories: open-loop congestion control (prevention) and closed-loop congestion control (removal) as shown in Fig. below :



Open-Loop Congestion Control

In open-loop congestion control, policies are applied to prevent congestion before it happens. In these mechanisms, congestion control is handled by either the source or the destination.

Closed-Loop Congestion Control

Closed-loop congestion control mechanisms try to alleviate congestion after it happens.

Normally the sender window size is determined by the available buffer space in the receiver window (rwnd). In other words, we assumed that it is only the receiver that can dictate to the sender the size of the sender's window. We totally ignored another entity here-the network. If the network cannot deliver the data as fast as they are created by the sender, it must tell the sender to slow down. In other words, in addition to the receiver, the network is a second entity that determines the size of the sender's window.

Today, the sender's window size is determined not only by the receiver but also by congestion in the network.

The sender has two pieces of information: the receiver-advertised window size and the congestion window size. The actual size of the window is the minimum of these two.

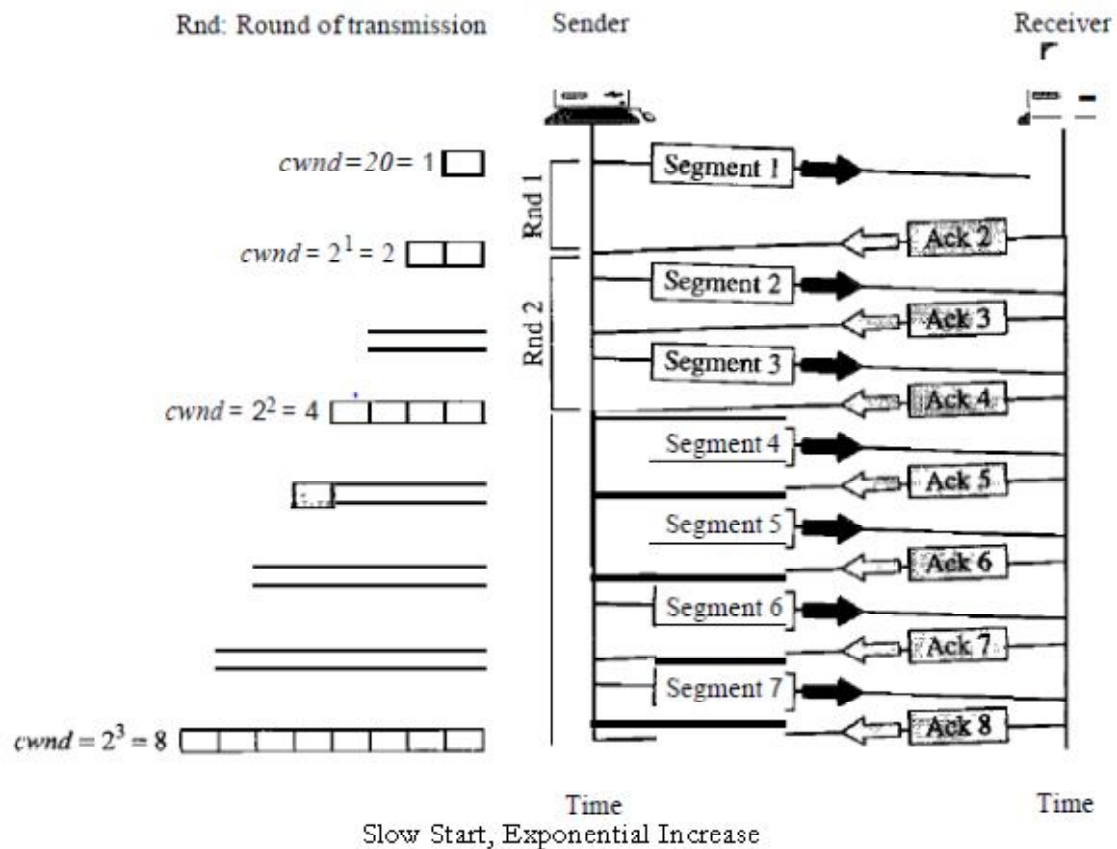
Actual window size = minimum (rwnd, cwnd)

Congestion Policy

- ▶ TCP's general policy for handling congestion is based on three phases: slow start, congestion avoidance, and congestion detection. In the slow-start phase, the sender starts with a very slow rate of transmission, but increases the rate rapidly to reach a threshold.
- ▶ When the threshold is reached, the data rate is reduced to avoid congestion. Finally if congestion is detected, the sender goes back to the slow-start or congestion avoidance phase based on how the congestion is detected.

Slow Start, Exponential Increase: One of the algorithms used in TCP congestion control is called slow start. This algorithm is based on the idea that the size of the congestion window (cwnd) starts with one maximum segment size (MSS). The MSS is determined during connection establishment by using an option of the same name. The size of the window increases one MSS each time an acknowledgment is received. As the name implies, the window starts slowly, but grows exponentially.

- ▶ As shown in the Figure below. Note that we have used three simplifications to make the discussion more understandable. We have used segment numbers instead of byte numbers (as though each segment contains only 1 byte). We have assumed that rwnd is much higher than cwnd, so that the sender window size always equals cwnd. We have assumed that each segment is acknowledged individually.
- ▶ The sender starts with cwnd = 1 MSS. This means that the sender can send only one segment. After receipt of the acknowledgment for segment 1, the size of the congestion window is increased by 1, which means that cwnd is now 2. Now two more segments can be sent. When each acknowledgment is received, the size of the window is increased by 1 MSS. When all seven segments are acknowledged, cwnd = 8.

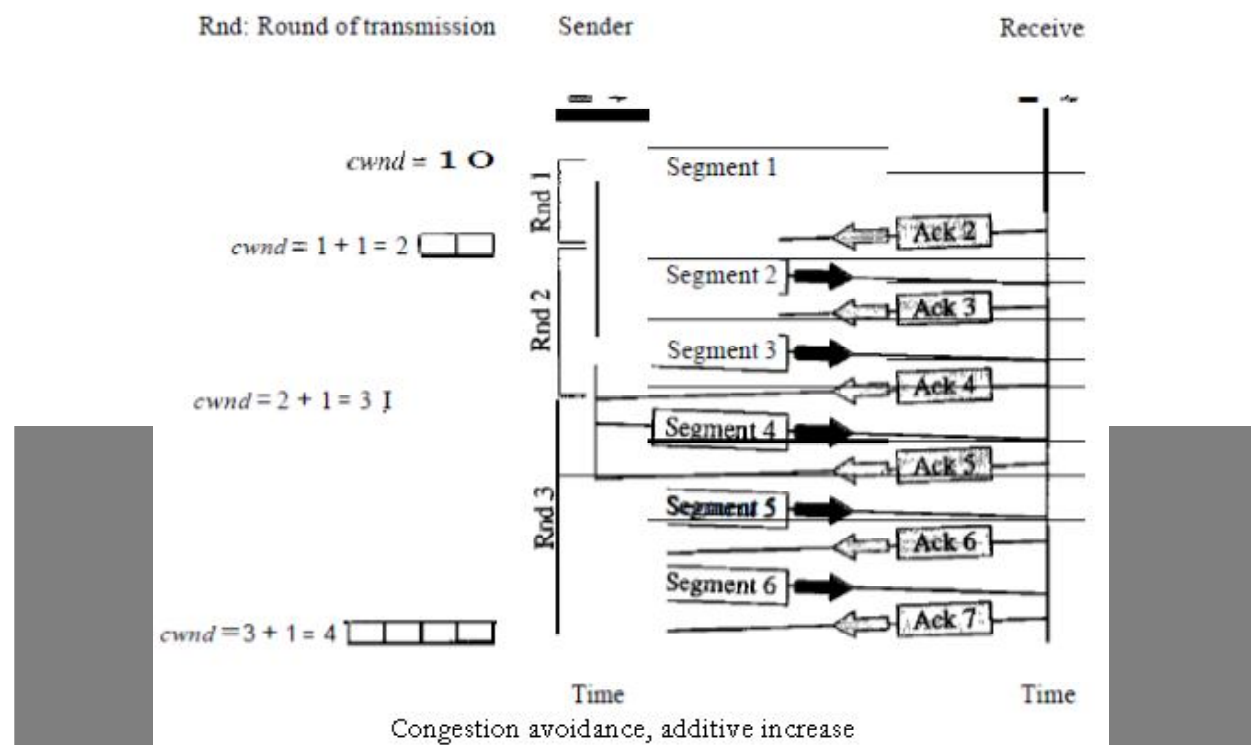


Slow start cannot continue indefinitely. There must be a threshold to stop this phase. The sender keeps track of a variable named *ssthresh* (slow-start threshold). When the size of window in bytes reaches this threshold, slow start stops and the next phase starts. In most implementations the value of *ssthresh* is 65,535 bytes.

Congestion Avoidance, Additive Increase: If we start with the slow-start algorithm, the size of the congestion window increases exponentially. To avoid congestion before it happens, one must slow down this exponential growth. TCP defines another algorithm called congestion avoidance, which undergoes an additive increase instead of an exponential one.

When the size of the congestion window reaches the slow-start threshold, the slow-start phase stops and the additive phase begins. In this algorithm, each time the whole window of segments is acknowledged (one round), the size of the congestion window is increased by 1.

To show the idea, we apply this algorithm to the same scenario as slow start, although we will see that the congestion avoidance algorithm usually starts when the size of the window is much greater than 1. Figure below shows the idea.



Congestion Detection : Multiplicative Decrease If congestion occurs, the congestion window size must be decreased. The only way the sender can guess that congestion has occurred is by the need to retransmit a segment. However, retransmission can occur in one of two cases: when a timer times out or when three ACKs are received. In both cases, the size of the threshold is dropped to one-half, a multiplicative decrease. Most TCP implementations have two reactions :

1. If a time-out occurs, there is a stronger possibility of congestion; a segment has probably been dropped in the network, and there is no news about the sent segments.

In this case TCP reacts strongly :

- a. It sets the value of the threshold to one-half of the current window size.
- b. It sets cwnd to the size of one segment.
- c. It starts the slow-start phase again.

2. If three ACKs are received, there is a weaker possibility of congestion; a segment may have been dropped, but some segments after that may have arrived safely since three ACKs are received. This is called fast transmission and fast recovery. In this case, TCP has a weaker reaction:

- a. It sets the value of the threshold to one-half of the current window size.
- b. It sets cwnd to the value of the threshold (some implementations add three segment sizes to the threshold).
- c. It starts the congestion avoidance phase.

An implementations reacts to congestion detection in one of the following ways:

- If detection is by time-out, a new slow-start phase starts.
- If detection is by three ACKs, a new congestion avoidance phase starts.

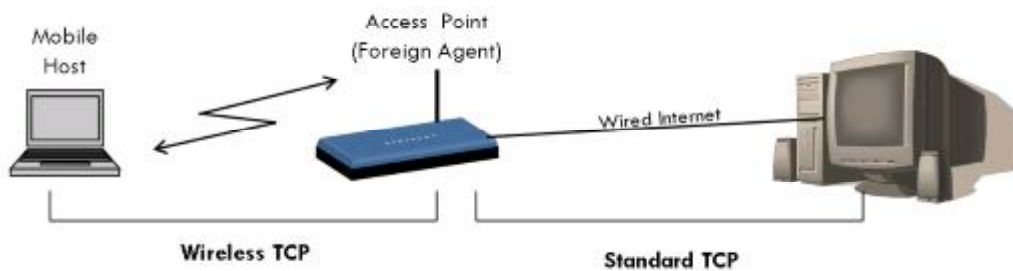
3.2.2 Classical TCP Improvements

Q15. Explain I- TCP.

Ans :

Indirect TCP (I-TCP)

- ▶ I-TCP segments a TCP onto fixed part and wireless part.



- ▶ The example shows a mobile host connected via a wireless link to an access point (AP). Also access node is connected to the internet via the wired Internet.
- ▶ Standard TCP is used to connect to the AP from fixed computer. No computer over the internet recognises any change to the TCP.
- ▶ The Access point acts as a proxy of mobile host and terminates the TCP connection.
- ▶ Therefore, the fixed computer now sees the AP as mobile host; on other hand the mobile host sees AP as the fixed computer.
- ▶ In between the AP and the mobile host a special TCP adapted to wireless links is used.
- ▶ A change is TCP is not needed as even as unchanged TCP produces the same round trip time.
- ▶ Such segmentation methods can be used is connection between mobile node and correspondent host when host is at the FA. So during handover, control transfers from one FA to another FA in the nearby cell.

Acknowledgements :

- ▶ Here the correspondent node (i.e. Sender) does not notice the wireless link or segmentation of the connection.
- ▶ The foreign Agent (FA) becomes or acts as a proxy and relays data in both directions.
- ▶ When the CN sends data, FA sends back a acknowledgement to it.
- ▶ When the mobile host receives a packet from FA, the mobile host also sends back an acknowledgement
- ▶ This acknowledgement is a local acknowledgement. It will not be forwarded to the CN.
- ▶ If a packet is lost in wireless transmission (i.e. no acknowledgement received) then FA will try re-transmitting it again.

Advantages of I-TCP:

1. I-TCP does not require any changes in TCP protocol as used by the different hosts in network.
2. Because of a strict partition between the two connections, transmission error on the wireless link will not propagate to the wired link. Therefore, flow will always be in a sequence.

3. The delay between the FA and Mobile host is small and if optimized properly, precise time-outs can be used to carry out retransmission of lost packets.
4. Different solutions can be implemented and tested between the FA and mobile host without jeopardizing the stability of the internet.
5. With two partitions, we can use a different transport layer protocol in the second half with the FA acting as a translator.

Dis-advantages of I-TCP:

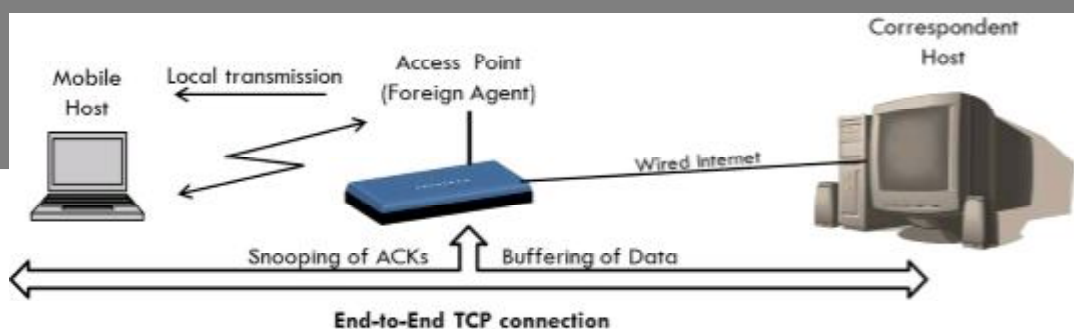
1. The end-to-end connection for which TCP has been designed will fail if the Foreign Agent (FA) crashes.
2. The foreign agent (FA) must be a trusted entity as the TCP connections end at this point.
3. In practical terms increased handover may latency may be much more problematic. (During handover from old FA to new FA, some delay will occur. During this period, some extra data will come at old FA. This data also needs to be send!!)

Q16. Explain Snooping TCP.

Ans :

Snooping TCP

- ▶ One of the main feature of I-TCP also goes on to become its major disadvantage i.e. segmentation of TCP.
- ▶ To overcome it but also to provide enhanced feature a new TCP was designed which worked completely transparent and also left the TCP end-to-end connection intact.
- ▶ The new idea for making an enhancement is to buffer the data close to the mobile host to perform fast local retransmission in case of packet loss. A good place to carry out this enhancement is at the foreign agent (FA).



Method :

- ▶ Here, the foreign agent instead of terminating all packet with destination mobile host, it buffers (i.e. temporarily stores all these packets). In addition to this, it also 'snoops' each packet flowing in both the directions for reading acknowledgements.
- ▶ Buffering towards the mobile host is carried out so that a retransmission can be done in case of missing acknowledgements.

- ▶ The FA buffers every packet until an acknowledgement is received from the mobile host.
- ▶ If the foreign agent does not receive an acknowledgement within the stipulated time, the packet or the acknowledgement has been lost.
- ▶ In such a situation, the FA can directly retransmit the packet without waiting for the correspondent host.

Transparency :

- ▶ To maintain transparency i.e. the communication happens only between the correspondent node (CN) and the mobile host, the FA doesn't send acknowledgement to the correspondent host as in I-TCP.
- ▶ The acknowledgement is sent by the Mobile host itself. The FA keeps on monitoring it.
- ▶ When the data flows for mobile host to CN, the FA snoops and checks the sequence of acknowledgement number. If a gap is found, FA sends signal to re-transmit.

Advantages of Snoop-TCP:

- ▶ The original TCP semantic i.e. end-to-end connection is preserved.
- ▶ The correspondent node need not be changed as all the new enhancements are made in the FA.
- ▶ During handover from one cell to another, there is no need to transfer the previous incoming data (as in I-TCP).
- ▶ In handover, the next foreign Agent (FA) need not use the same enhancements used here i.e. follow Snoop-TCP method.

Dis-Advantages of Snoop-TCP:

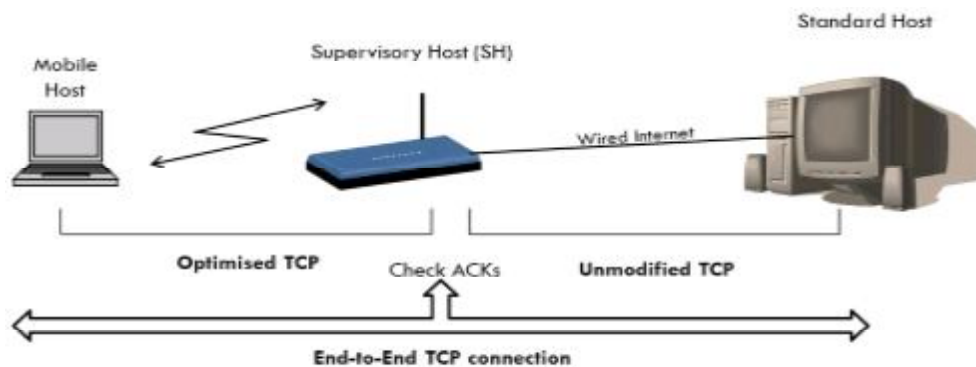
- ▶ If any encryption is applied at both ends, the snooping and buffering process would be a waste of time as no data can be read by FA.
- ▶ Does not fully isolate wireless link error from the fixed network (e.g. problems like congestion and interference may cause a delay in retransmission).
- ▶ The Mobile host needs to be modified to handle the NACK signals (No Acknowledgement) for reverse traffic (i.e. from MH to Sender)

Q17. Explain Mobile TCP.

Ans :

Mobile TCP

- ▶ The M-TCP splits up the connection into two parts :
 - An unmodified TCP is used on the Standard host-Supervisory Host section
 - An optimised TCP is used on the Supervisory Host- Mobile Host section.
- ▶ The **Supervisory Host (SH)** adorns the same role as the proxy (Foreign Agent) in I-TCP.
- ▶ The SH is responsible for exchanging data to both the Standard host and the Mobile host.
- ▶ Here in this approach, we **assume** that the error bit rate is less as compared to other wireless links.
- ▶ So if any packet is lost, the retransmission has to occur from the original sender and not by the SH. (This also maintains the end-to-end TCP semantic)
- ▶ The SH monitors the ACKs (ACK means acknowledgement) being sent by the MH. If for a long period ACKs have not been received, then the SH assumes that the MH has been disconnected (maybe due to failure or moved out of range, etc...).
- ▶ If so the SH **chokes** the sender by setting its window size to 0.
- ▶ Because of this the sender goes into persistent mode i.e. the sender's state will not change no matter how long the receiver is disconnected.
- ▶ This means that the sender will not try to retransmit the data.
- ▶ Now when the SH detects a connectivity established again with the MH (the old SH or new SH if handover), the window of the sender is restored to original value.

**Advantages :**

- ▶ Maintains the TCP end-to-end semantics. (No failed packet retransmission is done by the SH .All job handled by original sender)
- ▶ Does not require the change in the sender's TCP.
- ▶ If MH disconnected, it doesn't waste time in useless transmissions and shrinks the window size to 0.
- ▶ No need to send old buffer data to new SH in case of handover (as in I-TCP).

Disadvantages :

- ▶ M-TCP assumes low bit error which is not always true. So, any packet loss due to bit-errors occurring, then its propagated to the sender.
- ▶ Modifications are required for the MH protocol software.

3.2.3 TCP Over 2.5/3G Wireless Networks

Q18. Write the characteristics of TCP while deploying over 2.5/ 3.5 wireless links.

Ans :

The following characteristics have to be considered when deploying applications over 2.5G/3G wireless links :

- ▶ **Data rates:** While typical data rates of today's 2.5G systems are 10–20 kbit/s uplink and 20–50 kbit/s downlink, 3G and future 2.5G systems will initially offer data rates around 64 kbit/s uplink and 115–384 kbit/s downlink. Typically, data rates are asymmetric as it is expected that users will download more data compared to uploading.
- ▶ **Latency:** All wireless systems comprise elaborated algorithms for error correction and protection, such as forward error correction (FEC), check summing, and interleaving. FEC and interleaving let the round trip time (RTT) grow to several hundred milliseconds up to some seconds. The current GPRS standard specifies an average delay of less than two seconds for the transport class with the highest quality .
- ▶ **Jitter:** Wireless systems suffer from large delay variations or 'delay spikes'. Reasons for sudden increase in the latency are: link outages due to temporal loss of radio coverage, blocking due to high-priority traffic, or handovers. Handovers are quite often only virtually seamless with outages reaching from some 10 ms to several seconds .
- ▶ **Packet loss:** Packets might be lost during handovers or due to corruption. Thanks to link-level retransmissions the loss rates of 2.5G/3G systems due to corruption are relatively low.

UNIT IV

File Systems, World Wide Web, Wireless Application Protocol (WAP) and WAP 2.0.

4.1 FILE SYSTEMS

Q1. What is file system? What are the goals of file systems.

Ans :

file system is a method of organizing and retrieving files from a storage medium, such as a hard drive. File systems usually consist of files separated into groups called directories. Directories can contain files or additional directories. Today, the most commonly used file system with Windows is NTFS.

Without a file management, all files would have no organization and it would be impossible for a file with the same name to exist. Typically, files are managed in a hierarchy, which allows you to view files in the current directory and then navigate into any subdirectories.

Examples of file systems

- ▶ FAT (e.g., FAT16 and FAT32)
- ▶ GFS
- ▶ HFS
- ▶ NTFS

The general goal of a file system is to support efficient, transparent, and consistent access to files.

Efficiency is of special importance for wireless systems as the bandwidth is low so the protocol overhead and updating operations etc. should be kept at a minimum.

Transparency addresses the problems of location-dependent views on a file system. To support

mobility, the file systems should provide identical views on directories, file names, access rights etc., independent of the current location.

Standard file systems like the network file system (NFS) are very inefficient and almost unusable in a mobile and wireless environment.

Consistency Problem

The basic problem for distributed file systems that allow replication of data for performance reasons is the consistency of replicated objects.

To avoid inconsistencies many traditional systems apply mechanisms to maintain a permanent consistent view for all users of a file system.

This **strong consistency** is achieved by atomic updates similar to database systems.

Weak consistency implies certain periods of inconsistency that have to be tolerated for performance reasons.

However, the overall file system should remain consistent so conflict resolution strategies are needed for reintegration. **Reintegration** is the process of merging objects from different users resulting in one consistent file system.

Q2. Describe about Coda File system.

Ans :

Coda

The predecessor of many distributed file systems that can be used for mobile operation is the Andrew file system (AFS). Coda is the successor of AFS and offers two different types of replication: server replication and caching on clients.

Features

Coda has many features that are desirable for network file systems, and several features not found elsewhere.

1. Disconnected operation for mobile computing.
2. Is freely available under the GPL
3. High performance through client side persistent caching
4. Server replication
5. Security model for authentication, encryption and access control
6. Continued operation during partial network failures in server network
7. Network bandwidth adaptation
8. Good scalability
9. Well defined semantics of sharing, even in the presence of network failure

How Coda works

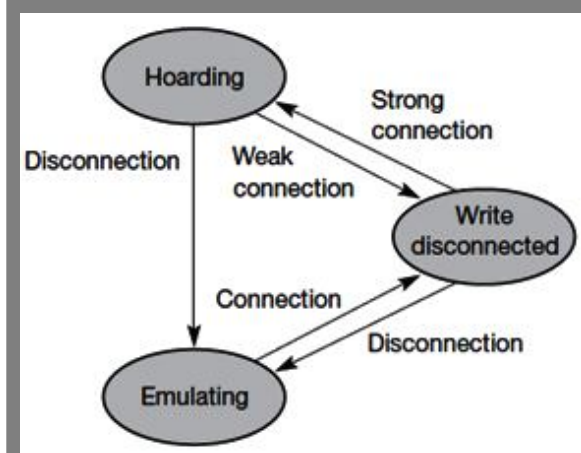


Fig. : States of a client in Coda

To provide all the necessary files for disconnected work, Coda offers extensive mechanisms for pre-fetching of files while still connected, called **hoarding**. If the client is connected to the server with a strong connection hoarding transparently pre-fetches files currently used. This automatic data collection is necessary for it is impossible for a standard user to know all the files currently used.

A user can pre-determine a list of files, which Coda should explicitly pre-fetch. Additionally, a user can assign priorities to certain programs. Coda now decides on the current cache content using the list and a least-recently-used (LRU) strategy.

Coda follows an optimistic approach and allows read and write access to all files. The system keeps a record of changed files, but does not maintain a history of changes for each file. The cache always has only one replicate.

The tool application specific resolver (ASR) was developed to automate conflict resolution. This means that the tools have to reconstruct a history of changes based on the replicate because Coda does not record every single change.

Another problem of Coda is the definition of a conflict. Coda detects only write conflicts.

Q3. What is little work file system ? write a note on it.

Ans :

Little Work

The distributed file system Little Work is, like Coda, an extension of AFS. Little Work only requires changes to the cache manager of the client and detects write conflicts during reintegration. Little Work has no specific tools for reintegration and offers no transaction service.

However, Little Work uses more client states to maintain consistency.

- ▶ **Connected:** The operation of the client is normal, i.e., no special mechanisms from Little Work are required. This mode needs a continuous high bandwidth as available in typical office environments using, e.g., a WLAN.
- ▶ **Partially connected:** If a client has only a lower bandwidth connection, but still has the possibility to communicate continuously, it is referred to as partially connected.
- ▶ **Fetch only:** If the only network available offers connections on demand, the client goes into the fetch only state. Networks of this type are cellular networks such as GSM with costs per

call. The client uses the replicates in the cache in an optimistic way, but fetches files via the communication link if they are not available in the cache. This enables a user to access all files of the server, but this also tries to minimize communication by working on replicates and reintegrate after reconnection using a continuously high bandwidth link.

- **Disconnected:** Without any network, the client is disconnected. Little Work now aborts if a cache mis-occurs, otherwise replicates are used.

Q4. Write a not on Ficus File system.

Ans :

Ficus

Ficus is a distributed file system, which is not based on a client/server approach. Ficus allows the optimistic use of replicates, detects write conflicts, and solves conflicts on directories. Ficus uses so-called **gossip protocols**. A mobile computer does not necessarily need to have a direct connection to a server. With the help of other mobile computers, it can propagate updates through the network until it reaches a fixed network and the server. Thus, changes on files propagate through the network step-by-step. Ficus tries to minimize the exchange of files that are valid only for a short time, e.g. temporary files.

Q5. Write about Mio-NFS file system.

Ans :

Mio-NFS

The system mobile integration of NFS (Mio-NFS) is an extension of the Network File System (NFS, (Guedes, 1995)). In contrast to many other systems, Mio-NFS uses a pessimistic approach with tokens controlling access to files. Only the token-holder for a specific file may change this file, so Mio-NFS avoids write conflicts.

Mio-NFS supports three different modes :

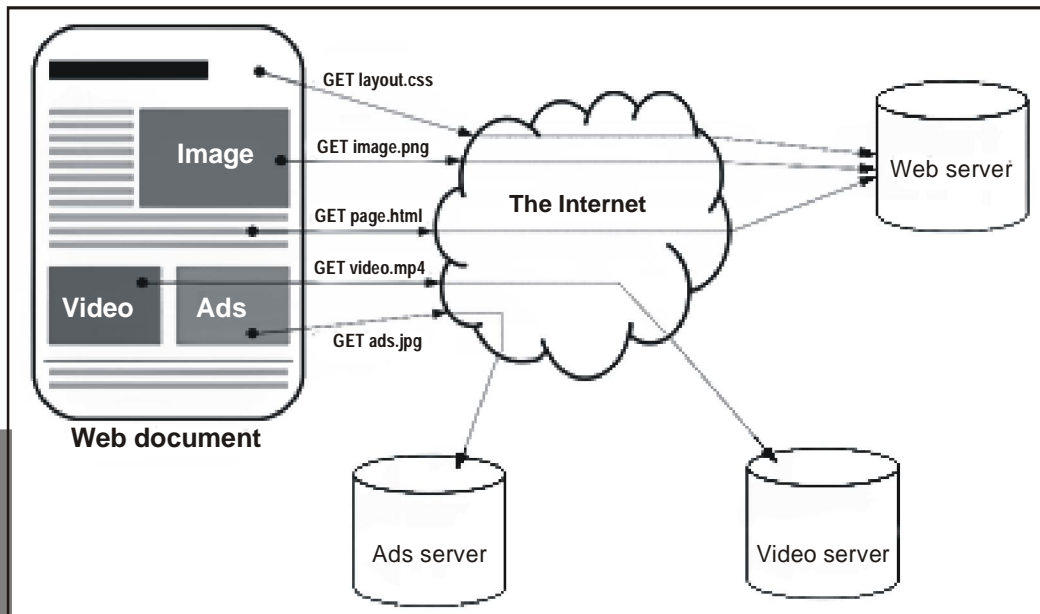
- **Connected:** The server handles all access to files as usual.
- **Loosely connected:** Clients use local replicates, exchange tokens over the network, and update files via the network.
- **Disconnected:** The client uses only local replicates. Writing is only allowed if the client is token-holder.

4.2 WORLD WIDE WEB

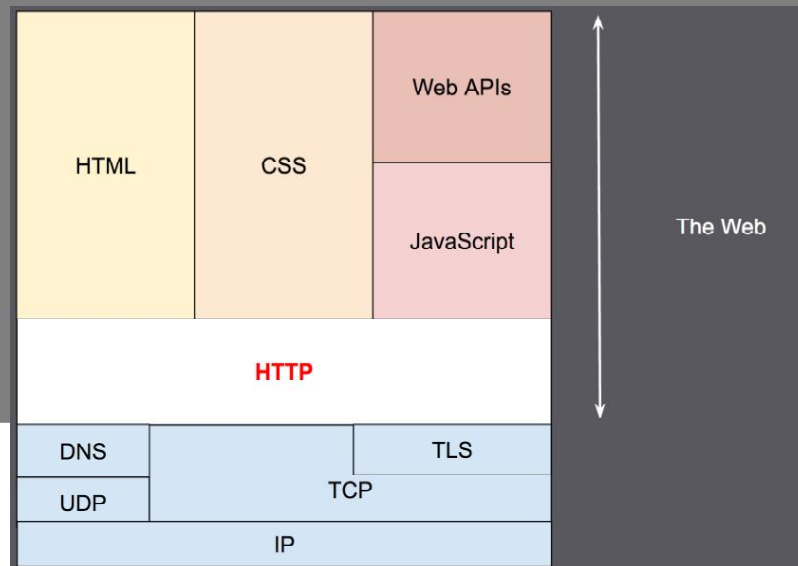
Q6. What is HTTP protocol? Explain its working.

Ans :

HTTP is a protocol which allows the fetching of resources, such as HTML documents. It is the foundation of any data exchange on the Web and a client-server protocol, which means requests are initiated by the recipient, usually the Web browser. A complete document is reconstructed from the different sub-documents fetched, for instance text, layout description, images, videos, scripts, and more.



Clients and servers communicate by exchanging individual messages (as opposed to a stream of data). The messages sent by the client, usually a Web browser, are called **requests** and the messages sent by the server as an answer are called **responses**.



HTTP is an extensible protocol which has evolved over time. It is an application layer protocol that is sent over TCP, or over a TLS-encrypted TCP connection, though any reliable transport protocol could theoretically be used. Due to its extensibility, it is used to not only fetch hypertext documents, but also images and videos or to post content to servers, like with HTML form results. HTTP can also be used to fetch parts of documents to update Web pages on demand.

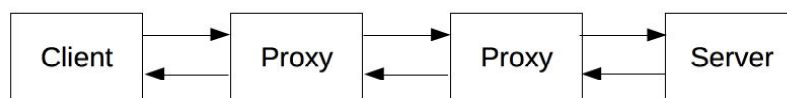
Q7. What are the components of HTTP protocol ?

Ans :

Components of HTTP-based Systems

HTTP is a client-server protocol: requests are sent by one entity, the user-agent (or a proxy on behalf of it). Most of the time the user-agent is a Web browser, but it can be anything, for example a robot that crawls the Web to populate and maintain a search engine index.

Each individual request is sent to a server, which will handle it and provide an answer, called the response. Between this request and response there are numerous entities, collectively designated as proxies, which perform different operations and act as gateways or caches, for example.

**Client : the user-agent**

The user-agent is any tool that acts on the behalf of the user. This role is primarily performed by the Web browser; a few exceptions being programs used by engineers, and Web developers to debug their applications.

The browser is **always** the entity initiating the request. It is never the server .

To present a Web page, the browser sends an original request to fetch the HTML document from the page. It then parses this file, fetching additional requests corresponding to execution scripts, layout information (CSS) to display, and sub-resources contained within the page (usually images and videos).

The Web browser then mixes these resources to present to the user a complete document, the Web page. Scripts executed by the browser can fetch more resources in later phases and the browser updates the Web page accordingly.

A Web page is a hypertext document. This means some parts of displayed text are links which can be activated (usually by a click of the mouse) to fetch a new Web page, allowing the user to direct their user-agent and navigate through the Web. The browser translates these directions in HTTP requests, and further interprets the HTTP responses to present the user with a clear response.

The Web server

On the opposite side of the communication channel, is the server which serves the document as requested by the client. A server presents only as a single machine virtually: this is because it may actually be a collection of servers, sharing the load (load balancing) or a complex piece of software interrogating other computers (like cache, a DB server, e-commerce servers, ...), totally or partially generating the document on demand.

A server is not necessarily a single machine, but several servers can be hosted on the same machine. With HTTP/1.1 and the Host header, they may even share the same IP address.

Proxies

Between the Web browser and the server, numerous computers and machines relay the HTTP messages. Due to the layered structure of the Web stack, most of these operate at either the transport, network or physical levels, becoming transparent at the HTTP layer and potentially making a significant

impact on performance. Those operating at the application layers are generally called **proxies**. These can be transparent, or not (changing requests not going through them), and may perform numerous functions :

- ▶ caching (the cache can be public or private, like the browser cache)
- ▶ filtering (like an antivirus scan, parental controls, ...)
- ▶ load balancing (to allow multiple servers to serve the different requests)
- ▶ authentication (to control access to different resources)
- ▶ logging (allowing the storage of historical information)

Q8. Write the features of HTTP.

Ans :

HTTP is Simple

Even with more complexity, introduced in HTTP/2 by encapsulating HTTP messages into frames, HTTP is generally designed to be simple and human readable. HTTP messages can be read and understood by humans, providing easier developer testing, and reduced complexity for newcomers.

HTTP is Extensible

Introduced in HTTP/1.0, HTTP headers made this protocol easy to extend and experiment with. New functionality can even be introduced by a simple agreement between a client and a server about a new header's semantics.

HTTP is stateless, but not sessionless

HTTP is stateless : there is no link between two requests being successively carried out on the same connection. This immediately has the prospect of being problematic for users attempting to interact with certain pages coherently, for example, using e-commerce shopping baskets. But while the core of HTTP itself is stateless, HTTP cookies allow the use of stateful sessions. Using header extensibility, HTTP Cookies are added to the workflow, allowing

session creation on each HTTP request to share the same context, or the same state.

HTTP and connections

A connection is controlled at the transport layer, and therefore fundamentally out of scope for HTTP. Though HTTP doesn't require the underlying transport protocol to be connection-based; only requiring it to be reliable, or not lose messages (so at minimum presenting an error). Among the two most common transport protocols on the Internet, TCP is reliable and UDP isn't. HTTP subsequently relies on the TCP standard, which is connection-based, even though a connection is not always required.

HTTP/1.0 opened a TCP connection for each request/response exchange, introducing two major flaws: opening a connection needs several round-trips of messages and therefore slow, but becomes more efficient when several messages are sent, and regularly sent: warm connections are more efficient than cold ones.

In order to mitigate these flaws, HTTP/1.1 introduced pipelining (which proved difficult to implement) and persistent connections: the underlying TCP connection can be partially controlled using the Connection header. HTTP/2 went a step further by multiplexing messages over a single connection, helping keep the connection warm, and more efficient.

Q9. Explain about HTTP Flow.

Ans :

HTTP Flow

When the client wants to communicate with a server, either being the final server or an intermediate proxy, it performs the following steps:

1. **Open a TCP connection:** The TCP connection will be used to send a request, or several, and receive an answer. The client may open a new connection, reuse an existing connection, or open several TCP connections to the servers.
2. **Send an HTTP message:** HTTP messages (before HTTP/2) are human-readable. With

HTTP/2, these simple messages are encapsulated in frames, making them impossible to read directly, but the principle remains the same.

GET / HTTP/1.1

Host: developer.mozilla.org

Accept-Language: fr

3. Read the response sent by the server:

HTTP/1.1 200 OK

Date: Sat, 09 Oct 2010 14:28:02 GMT

Server: Apache

Last-Modified: Tue, 01 Dec 2009 20:18:22 GMT

ETag: "51142bc1-7449-479b075b2891b"

Accept-Ranges: bytes

Content-Length: 29769

Content-Type: text/html

<!DOCTYPE html... (here comes the 29769 bytes of the requested web page)

4. Close or reuse the connection for further requests.

If HTTP pipelining is activated, several requests can be sent without waiting for the first response to be fully received. HTTP pipelining has proven difficult to implement in existing networks, where old pieces of software coexist with modern versions. HTTP pipelining has been superseded in HTTP/2 with more robust multiplexing requests within a frame.

HTTP Messages

HTTP/1.1 and earlier HTTP messages are human-readable. In HTTP/2, these messages are embedded into a new binary structure, a frame, allowing optimizations like compression of headers and multiplexing. Even if only part of the original HTTP message is sent in this version of HTTP, the semantics of each message is unchanged and the client reconstitutes (virtually) the original HTTP/1.1 request. It is therefore useful to comprehend HTTP/2 messages in the HTTP/1.1 format.

There are two types of HTTP messages, requests and responses, each with its own format.

Requests

An example HTTP request:

Requests consists of the following elements :

- ▶ An HTTP method, usually a verb like GET, POST or a noun like OPTIONS or HEAD that defines the operation the client wants to perform. Typically, a client wants to fetch a resource (using GET) or post the value of an HTML form (using POST), though more operations may be needed in other cases.
- ▶ The path of the resource to fetch; the URL of the resource stripped from elements that are obvious from the context, for example without the protocol (http://), the domain (here developer.mozilla.org), or the TCP port (here 80).
- ▶ The version of the HTTP protocol.
- ▶ Optional headers that convey additional information for the servers.
- ▶ Or a body, for some methods like POST, similar to those in responses, which contain the resource sent.

Responses

An example responses :

Responses consist of the following elements :

- ▶ The version of the HTTP protocol they follow.
- ▶ A status code, indicating if the request has been successful, or not, and why.
- ▶ A status message, a non-authoritative short description of the status code.
- ▶ HTTP headers, like those for requests.
- ▶ Optionally, a body containing the fetched resource.

Q10. What is HTML ?*Ans :*

First developed by Tim Berners-Lee in 1990, **HTML** is short for **Hyper Text Markup Language**. HTML is used to create electronic documents (called pages) that are displayed on the World Wide Web. Each page contains a series of connections to other pages called hyperlinks. Every web page you see on the Internet is written using one version of HTML code or another.

HTML code ensures the proper formatting of text and images so that your Internet browser may display them as they are intended to look. Without HTML, a browser would not know how to display text as elements or load images or other elements. HTML also provides a basic structure of the page, upon which Cascading Style Sheets are overlaid to change its appearance. One could think of HTML as the bones (structure) of a web page, and CSS as its skin (appearance).

Q11. Write about the mobility in HTTP*Ans :***HTTP 1.0 and mobility I**► **Characteristics**

- stateless, client/server, request/response
- needs a connection oriented protocol (TCP), one connection per request (some enhancements in HTTP 1.1)
- primitive caching and security

► **Problems**

- designed for large bandwidth (compared to wireless access) and low delay
- large and redundant protocol headers (readable for humans, stateless, therefore large headers in ASCII)
- uncompressed content transfer
- using TCP
 - huge overhead per request (3-way-handshake) compared with the content, e.g., of a GET request.

- slow-start problematic as is without having to deal with the wireless problem
- DNS lookup by client causes additional traffic and delays

► **Caching**

- quite often disabled by information providers to be able to create user profiles, usage statistics etc.
- dynamic objects cannot be cached
 - numerous counters, time, date, personalization, ...
- mobility quite often inhibits caches
- security problems
 - caches cannot work with authentication mechanisms that are contracts between client and server and not the cache
- today: many user customized pages, dynamically generated on request via CGI, ASP, ...

► **POSTing (i.e., sending to a server)**

- can typically not be buffered, very problematic if currently disconnected.

Q12. What are the approaches of www for a mobile devices ?*Ans :***Approaches toward a WWW for mobile devices**

- **Image scaling:** If a page contains a true color, high-resolution picture, this picture can be scaled down to fewer colors, lower resolution, or to just the title of the picture. The user can then decide to download the picture separately. Clipping, zooming, or detail studies can be offered to users if they are interested in a part of the picture.
- **Content transformation:** Many documents are only available in certain formats, e.g. (PDF).

Before transmitting such documents to a client without the appropriate reader, a special converter could translate this document into plain text.

- ▶ **Content extraction/semantic compression** : Besides transforming the content, could be extracted from a document and presented to a user. The user could then decide to download more information relating to a certain headline or keyword. An abstract from some given text could be automatically generated.
- ▶ **Special languages and protocols**: Other approaches try to replace HTML and HTTP with other languages and protocols better adapted to a wireless environment.
- ▶ **Push technologies**: Instead of pulling content from a server, the server could also push content to a client. This avoids the overhead of setting up connections for each item, but is only useful for some content, e.g. news, weather information, road conditions, where users do not have to interact much.

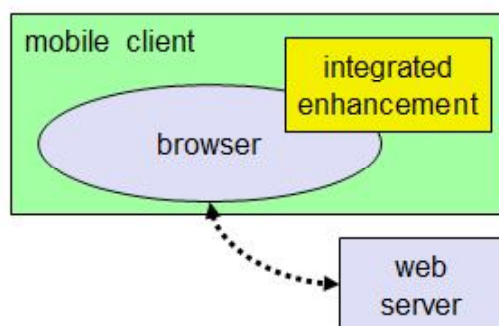
Q13. Describe WWW system architecture.

Ans :

System architecture

The classic underlying system architecture of the www is a client/server system.

The client, a web browser running as an application on a computer, requests content from a server, the web server running on another computer.

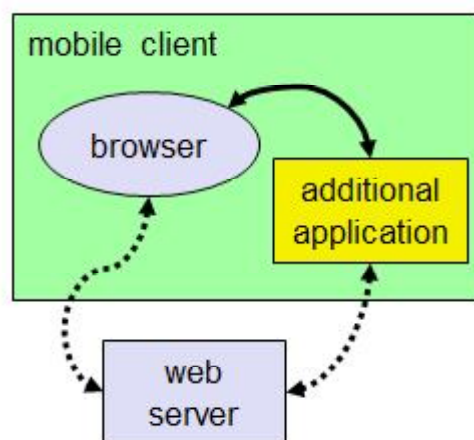


The browser uses the HTTP protocol for content transfer (see section 10.2.1).

Web pages are described using HTML (see section 10.2.2) and many more (proprietary) formats.

Caching is a major topic in the web client/server scenario. While caching is also useful for wired computers because it reduces the delay of displaying previously accessed pages, it is the only way of supporting (partially) disconnected web browsers.

Figure shows an architecture for an early approach to enhance webaccess for mobile clients.. However, this approach is not transparent for a browser as there are now two different ways of accessing content.



The typical enhancements for web browsing act as a transparent proxy as shown in Figure.

Client Proxy

The browser accesses the web server through the client proxy, i.e., the proxy acts as server for the browser and as client for the webserver. The proxy can now pre-fetch and cache content according to many strategies.

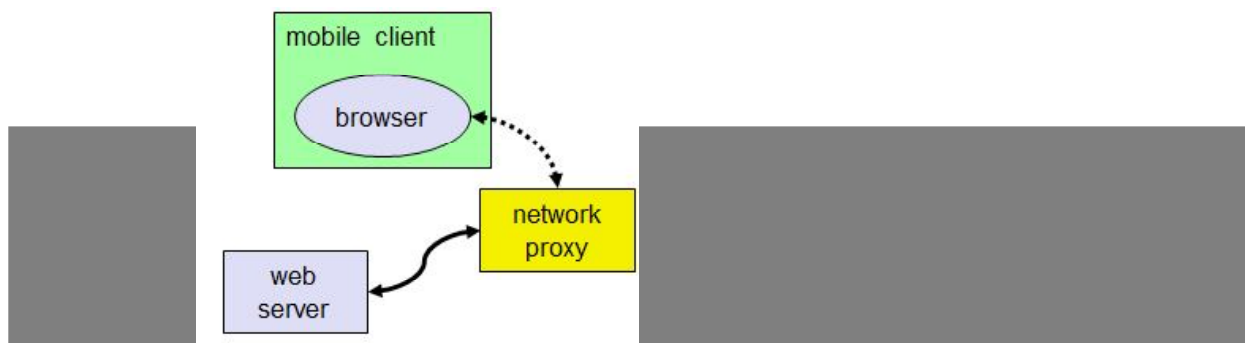
e.g., Caubweb, TeleWeb, Weblicator, WebWhacker, WebEx, WebMirror,...

Network Proxy

This network proxy can perform adaptive content transformation or pre-fetch and cache content. Pre-fetching and caching is useful in a wireless environment with higher error probability.

Adaptive content transformation for bad connections, pre-fetching, caching

e.g., TranSend, Digestor.



Client and Network Proxy

The benefits of client and network proxies can be combined, which results in a system architecture as shown in Figure.

Proxy can now interact better in pre-fetching and caching of data. The client proxy could inform, for example, the network proxy about user behavior, the network proxy can then pre-fetch pages according to this information. The whole approach is still transparent to the web server and the client browser.

4.3 WIRELESS APPLICATION PROTOCOL (WAP) AND WAP 2.0

Q14. Explain about WAP architecture.

Ans :

Wireless application protocol (WAP) is a communications protocol that is used for wireless data access through most mobile wireless networks. WAP enhances wireless specification interoperability and facilitates instant connectivity between interactive wireless devices (such as mobile phones) and the Internet.

WAP functions in an open application environment and may be created on any type of OS. Mobile users prefer WAP because of its ability to efficiently deliver electronic information.

1. WAP Architecture

- i. It provides a scalable and extensible environment for application development of mobile
- ii. This is achieved using layered design of protocol stack. The layers resemble the layers of OSI model.
- iii. Each layer is accessible by layers above as well as by other services and applications through a set of well defined interface.
- iv. External applications may access session, transaction, security and transport layers directly.

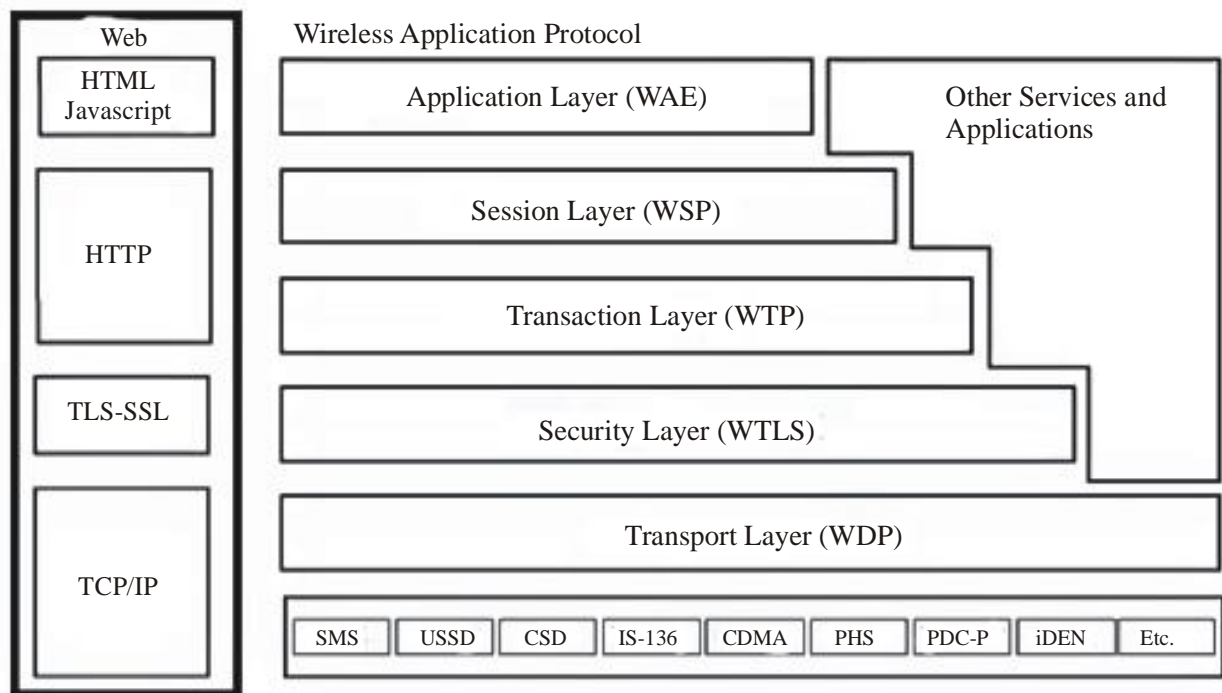


Fig. : WAP Architecture

2. Wireless Application Environment

- WAE is the uppermost layer in the WAP stack. It is general purpose environment based on combination of WWW and mobile telephony technologies.
- Its primary objective is to achieve interoperable environment that allows operators and service providers to build applications that can reach wide variety of wireless platforms.
- It uses URL and URI for addressing. Language used is WML and WML script. WML script can be used for validation of user input.

3. Wireless Telephony Application

- WTA provides a means to create telephony services using WAP. It uses WTA Interface (WTAI) which can be evoked from WML and for WML script.
- The Repository makes it possible to store WTA services in device which can be accessed without accessing the network. The access can be based on any event like call disconnect, call answer etc.
- Sometimes, there can be notification to user based on which WTA services are accessed by users. The notification is called WTA service indication.

4. Wireless Session Protocol

- WSP provides reliable, organized exchange of content between client and server.
- The core of WSP design is binary form of HTTP. All methods defined by HTTP 1.1 are supported.
- Capability negotiation is used to agree on common level of protocol functionality as well as to agree on a set of extended request methods so that full compatibility to HTTP applications can be retained.
- An idle session can be suspended to free network resources and can be resumed without overload of full-blown session establishment.
- WSP also supports asynchronous requests. Hence, multiple requests will improve utilization of air time.

5. Wireless Transaction Protocol

- i. WTP is defined as light-weight transaction-oriented protocol suitable for implementation in thin clients.
- ii. Each transaction has unique identifiers, acknowledgements, duplicates removal and retransmission.
- iii. Class 1 and Class 2 enable user to confirm every received message, however, in class 0, there is no acknowledgement.

- iv. WTP has no security mechanisms and no explicit connection set-up or tear-down phases.

6. Wireless Transport Layer Security

- i. WTLS is security protocol based on industry standard transport layer security (TLS). It provides transport layer security between a WAP client and the WAP Gateway/ Proxy.
- ii. The goals of WTLS are data integrity, privacy, authentication, Denial-of-service protection.
- iii. It has features like datagram support, optimized handshake and dynamic key refreshing.

7. Wireless Datagram Protocol

- i. WDP provides application addressing by port numbers, optional segmentation and reassembly, optional error detection.
- ii. It supports simultaneous communication instances from higher layer over a single underlying WDP bearer service. The port number identifies higher level entity above WDP.
- iii. The adaptation layer of WDP maps WDP functions directly on to a bearer based on its specific characteristics.

- iv. On the GSM SMS, datagram functionality is provided by WDP.

8. Optimal WAP Bearers

- i. The WAP is designed to operate over a variety of different service like SMS, 'Circuit Switched Data (CSD)', GPRS, 'Unstructured Supplementary Services Data(USSD)'.

Q15. Explain Wireless Datagram Protocol.*Ans :***Wireless Datagram Protocol (WDP)**

The **Wireless Datagram Protocol (WDP)** operates on top of many different bearer services capable of carrying data. At the T-SAP WDP offers a consistent datagram transport service independent of the underlying bearer. To offer this consistent service, the adaptation needed in the transport layer can differ depending on the services of the bearer.

The closer the bearer service is to IP, the smaller the adaptation can be. If the bearer already offers IP services, UDP is used as WDP. WDP offers more or less the same services as UDP. WDP offers **source** and **destination port numbers** used for multiplexing and demultiplexing of data respectively. The service primitive to send a datagram is **TD Unitdata.req** with the **destination address (DA)**, **destination port (DP)**, **Source address (SA)**, **source port (SP)**, and **user data (UD)** as mandatory parameters.

Destination and source address are unique addresses for the receiver and sender of the user data. These could be MSISDNs (i.e., a telephone number), IP addresses, or any other unique identifiers. The **T-DUnitdata.ind** service primitive indicates the reception of data. Here destination address and port are only optional parameters.

An **error code (EC)** is returned indicating the reason for the error to the higher layer. WDP is not allowed to use this primitive to indicate problems with the bearer service. It is only allowed to use the primitive to indicate local problems, such as a user data size that is too large.

If any errors happen when WDP datagram's are sent from one WDP entity to another (e.g. the destination is unreachable, no application is listening to the specified destination port etc.), the **wireless control message protocol (WCMP)** provides error handling mechanisms for WDP and should therefore be implemented. WCMP contains control messages that resemble the internet control message protocol messages and can also be used for diagnostic and informational purposes.

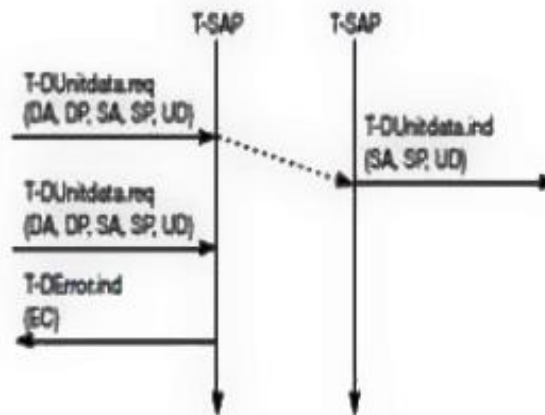


Fig. : WAP Service Primitives

WCMP can be used by WDP nodes and gateways to report errors. However, WCMP error messages must not be sent as response to other WCMP error messages. In IP-based networks, ICMP will be used as WCMP (e.g., CDPD, GPRS). Typical WCMP messages are **destination unreachable** (route, port, address unreachable), **parameter problem** (errors in the packet header), **message too big**, **reassembly failure**, **echo request/reply**.

An additional **WDP management entity** supports WDP and provides information about changes in the environment, which may influence the correct operation of WDP. Important information is the current configuration of the device, currently available bearer services, processing and memory resources etc. Design and implementation of this management component is considered vendor-specific and is outside the scope of WAP.

Q16. Write about Wireless Transport Layer Security

Ans :

Wireless Transport Layer Security (WTLS)

If requested by an application, a security service, the **wireless transport layer security (WTLS)**, can be integrated into the WAP architecture on top of WDP. WTLS can provide different levels of security (for privacy, data integrity, and authentication) and has been optimized for low bandwidth, high-delay bearer networks.

WTLS takes into account the low processing power and very limited memory capacity of the mobile devices for cryptographic algorithms. WTLS supports datagram and connection-oriented transport layer protocols. New compared to, e.g. GSM, is the security relation between two peers and not only between the mobile device and the base station. WTLS took over many features and mechanisms from TLS (formerly SSL, secure sockets layer, but it has an optimized handshaking between the peers.

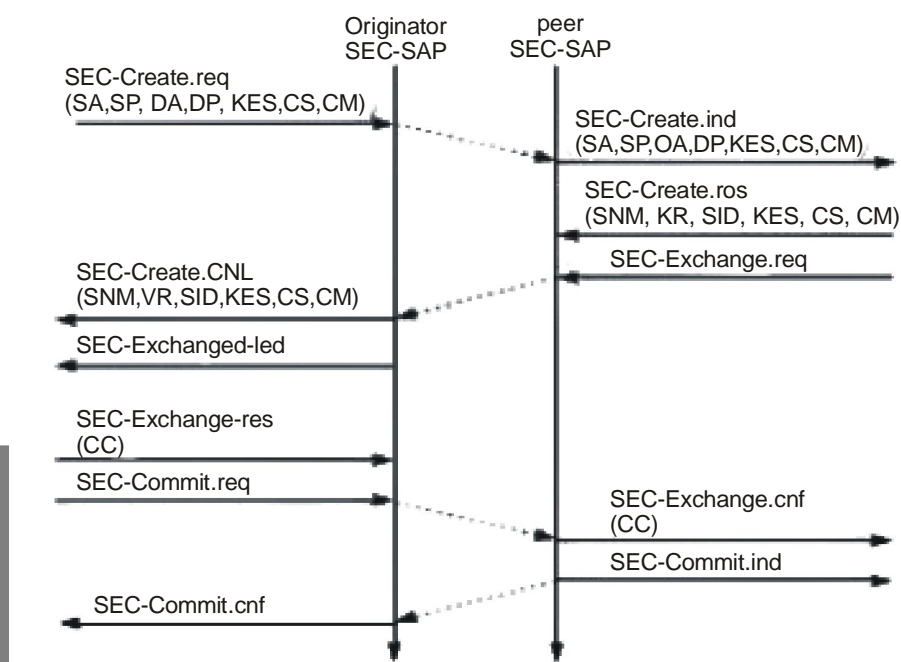


Fig. : WTLS Establishing a Secure Session

Before data can be exchanged via WTLS, a secure session has to be established. This session establishment consists of several steps: Figure illustrates the sequence of service primitives needed for a so-called 'full handshake'.

The originator and the peer of the secure session can both interrupt session establishment any time, e.g., if the parameters proposed are not acceptable.

The first step is to initiate the session with the SEC-Create primitive. Parameters are source address (SA), source port (SP) of the originator, destination address (DA), destination port (DP) of the peer. The originator proposes a key exchange suite (KES) (e.g., RSA, DH, ECC, a cipher suite (CS) (e.g., DES, IDEA, and a compression method (CM) (currently not further specified).

The peer answers with parameters for the sequence number mode (SNM), the key refresh cycle (KR) (i.e., how often keys are refreshed within this secure session), the session identifier (SID) (which is unique with each peer), and the selected key exchange suite (KES'), cipher suite (CS'), compression method (CM'). The peer also issues a SEC-Exchange primitive. This indicates that the peer wishes to perform public-key authentication with the client, i.e., the peer requests a client certificate (CC) from the originator.

The first step of the secure session creation, the negotiation of the security parameters and suites, is indicated on the originator's side, followed by the request for a certificate. The originator answers with its certificate and issues a SEC-Commit.req primitive. This primitive indicates that the handshake is completed for the originator's side and that the originator now wants to switch into the newly negotiated connection state. The certificate is delivered to the peer side and the SEC-Commit is indicated. The WTLS layer of the peer sends back a confirmation to the originator. This concludes the full handshake for secure session setup.

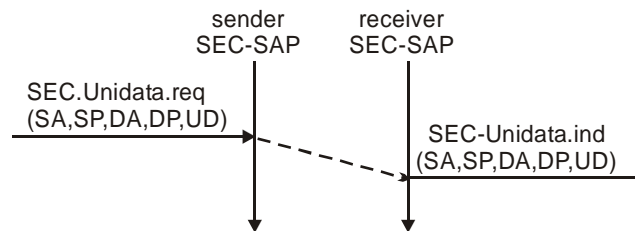


Fig. : WTLS Datagram Transfer

After setting up a secure connection between two peers, user data can be exchanged. This is done using the simple SEC-Unit. SEC-Unit data has exactly the same function as T-D Unit data on the WDP layer, namely it transfers a datagram between a sender and a receiver. This data transfer is still unreliable, but is now secure. This shows that WTLS can be easily plugged into the protocol stack on top of WDP. The higher layers simply use SEC-Unit data instead of T-D Unit data. The parameters are the same here: source address (SA), source port (SP), destination address (DA), destination port (DP), and user data (UD).

WTLS allows for different encryption mechanisms with different key lengths, it is quite clear that due to computing power on the handheld devices the encryption provided cannot be very strong. If applications require stronger security, it is up to an application or a user to apply stronger encryption on top of the whole protocol stack and use WTLS as a basic security level only. Many programs are available for this purpose. It is important to note that the security association in WTLS exists between the mobile WAP-enabled devices and a WAP server or WAP gateway only. If an application accesses another server via the gateway, additional mechanisms are needed for end-to-end security. If for example a user accesses his or her bank account using WAP, the WTLS security association typically ends at the

Q17. Explain about wireless transaction protocol.

Ans :

Wireless transaction protocol (WTP)

WTP has been designed to run on very thin clients, such as mobile phones. 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. In this context, a transaction is defined as a request with its response, e.g. for a web page. WTP offers many features to the higher layers. The basis is formed from three classes of transaction service as explained in the following paragraphs. Class 0 provides unreliable message transfer without any result message. Classes 1 and 2 provide reliable message transfer, class 1 without, class 2 with, exactly one reliable result message.

WTP achieves reliability using duplicate removal, retransmission, acknowledgements and unique transaction identifiers. No WTP-class requires any connection set-up or tear-down phase. This avoids unnecessary overhead on the communication link. WTP allows for asynchronous transactions, abort of transactions, concatenation of messages, and can report success or failure of reliable messages.

A special feature of WTP is its ability to provide a user acknowledgement or, alternatively, an automatic acknowledgement by the WTP entity. If user acknowledgement is required, a WTP user has to confirm every message received by a WTP entity. A user acknowledgement provides a stronger version of a confirmed service because it guarantees that the response comes from the user of the WTP and not the WTP entity itself. WTP class 0 Class 0 offers an unreliable transaction service without a result message.

The transaction is stateless and cannot be aborted. The service is requested with the TR-Invoke.req primitive as shown in Figure 10.14. Parameters are the source address (SA), source port (SP), destination

address (DA), destination port (DP) as already explained in section 10.3.2. Additionally, with the A flag the user of this service can determine, if the responder WTP entity should generate an acknowledgement or if a user acknowledgement should be used. The WTP layer will transmit the user data (UD) transparently to its destination. The class type C indicates here class 0. Finally, the transaction handle H provides a simple index to uniquely identify the transaction and is an alias for the tuple (SA, SP, DA, DP), i.e., a socket pair, with only local significance.

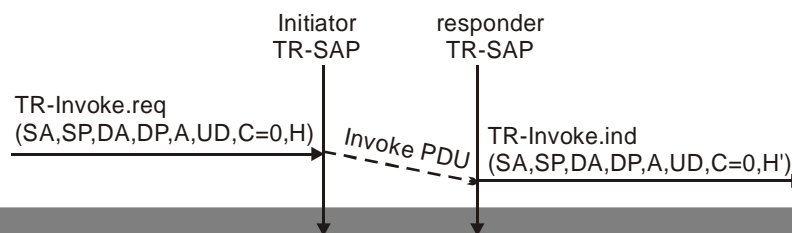


Fig. : Basic Transaction, WTP Class 0

The WTP entity at the initiator sends an invoke PDU which the responder receives. The WTP entity at the responder then generates a TR-Invoke.ind primitive with the same parameters as on the initiators side, except for which is now the local handle for the transaction on the responders side.

In this class, the responder does not acknowledge the message and the initiator does not perform any retransmission. Although this resembles a simple datagram service, it is recommended to use WDP if only a datagram service is required. WTP class 0 augments the transaction service with a simple datagram like service for occasional use by higher layers.

WTP class 1. Class 1 offers a reliable transaction service but without a result message. Again, the initiator sends an invoke PDU after a TR-Invoke.req from a higher layer.

This time, class equals „1, and no user acknowledgement has been selected as shown in Figure 10.15. The responder signals the incoming invoke PDU via the TR-Invoke.ind primitive to the higher layer and acknowledges automatically without user intervention.

The specification also allows the user on the responders side to acknowledge, but this acknowledgement is not required. For the initiator the transaction ends with the reception of the acknowledgement. The responder keeps the transaction state for some time to be able to retransmit the acknowledgement if it receives the same invoke PDU again indicating a loss of the acknowledgement.

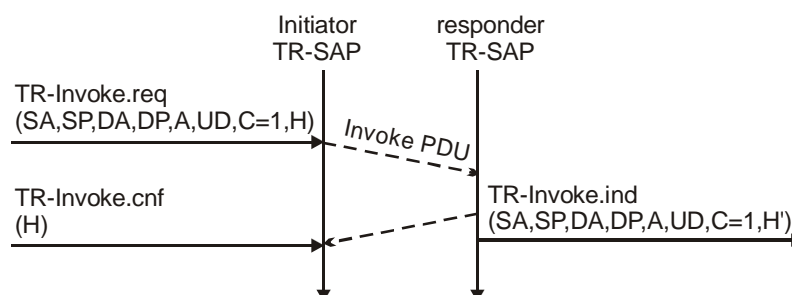


Fig. : Basic Transaction, WTP Class 1, no user Acknowledgement

If a user of the WTP class 1 service on the initiators side requests a user acknowledgement on the responders side, the sequence diagram looks like Figure. Now the WTP entity on the responders side does not send an acknowledgement automatically, but waits for the TR-Invoke.res service primitive from the user. This service primitive must have the appropriate local handle H for identification of the right transaction. The WTP entity can now send the ack PDU. Typical uses for this transaction class are reliable push services.

WTP class. 2 Finally, class 2 transaction service provides the classic reliable request/response transaction known from many client/server scenarios. Depending on user requirements, many different scenarios are possible for initiator/responder interaction.

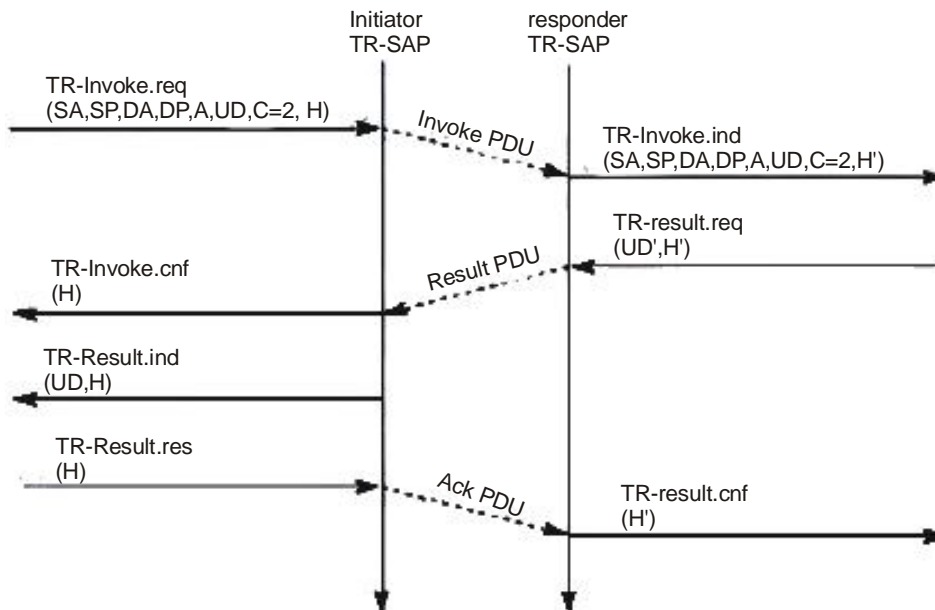


Fig. : Basic Transaction, WTP Class 2, no user Acknowledgement

An even more reliable service can be provided by user acknowledgement as explained above. The user on the responder's side now explicitly responds to the Invoke PDU using the TR-Invoke.res primitive, which triggers the TR-Invoke.cnf on the initiator's side via an ack PDU. The transmission of the result is also a confirmed service, as indicated by the next four service primitives. This service will likely be the most common in standard request/response scenarios as, e.g., distributed computing.

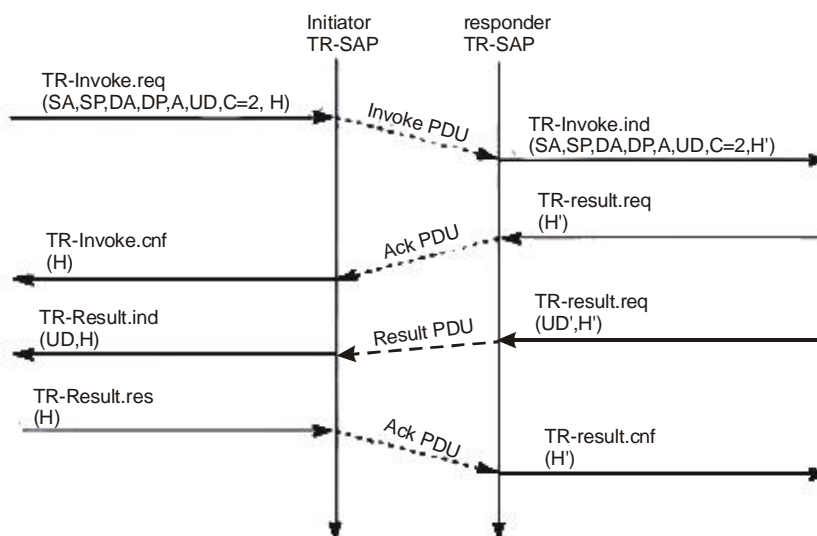


Fig. : Basic Transaction, WTP Class 2, with user Acknowledgement

After a time-out, the responder auto-matically generates an acknowledgement for the Invoke PDU. This shows the initiator that the responder is still alive and currently busy processing the request. WTP provides many more features not explained here, such as concatenation and separation of messages, asynchronous transactions with up to 215 transactions outstanding, i.e., requested but without result up to now, and segmentation/ reassembly of messages.

Q18. Explain Wireless Session Protocol.

Ans :

Wireless session protocol (WSP)

The **wireless session protocol (WSP)** has been designed to operate on top of the datagram service WDP or the transaction service WTP (WAP Forum, 2000e). For both types, security can be inserted using the WTLS security layer if required..WSP provides a shared state between a client and a server to optimize content transfer. HTTP, a protocol WSP tries to replace within the wireless domain, is stateless, which already causes many problems in fixed networks.

Many web content providers therefore use cookies to store some state on a client machine, which is not an elegant solution. State is needed in web browsing, for example, to resume browsing in exactly the same context in which browsing has been suspended. This is an important feature for clients and servers.

Client users can continue to work where they left the browser or when the network was interrupted, or users can get their customized environment every time they start the browser. Content providers can customize their pages to clients' needs and do not have to retransmit the same pages over and over again. WSP offers the following general features needed for content exchange between cooperating clients and servers:

- a) **Session management** : WSP introduces sessions that can be **established** from a client to a server and may be long lived. Sessions can also be **released** in an orderly manner. The capabilities of **suspending** and **resuming** a session are important to mobile applications. Assume a mobile device is being switched off – it would be useful for a user to be able to continue operation at exactly the point where the device was switched off. Session lifetime is independent of transport connection lifetime or continuous operation of a bearer network.
- b) **Capability negotiation**: Clients and servers can agree upon a common level of protocol functionality during session establishment. Example parameters to negotiate are maximum client SDU size, maximum outstanding requests, protocol options, and server SDU size.
- c) **Content encoding**: WSP also defines the efficient binary encoding for the content it transfers. WSP offers content typing and composite objects, as explained for web browsing. While WSP is a general-purpose session protocol, WAP has specified the **wireless session protocol/browsing (WSP/B)** which comprises protocols and services most suited for browsing-type applications. In addition to the general features of WSP, WSP/B offers the following features adapted to web browsing.

- d) **HTTP/1.1 functionality:** WSP/B supports the functions HTTP/1.1 offers, such as extensible request/reply methods, composite objects, and content type negotiation. WSP/B is a binary form of HTTP/1.1. HTTP/1.1 content headers are used to define content type, character set encoding, languages etc., but binary encodings are defined for well-known headers to reduce protocol overheads.
- e) **Exchange of session headers:** Client and server can exchange request/reply headers that remain constant over the lifetime of the session. These headers may include content types, character sets, languages, device capabilities, and other static parameters. WSP/B will not interpret header information but passes all headers directly to service users.
- f) **Push and pull data transfer:** Pulling data from a server is the traditional mechanism of the web. This is also supported by WSP/B using the request/response mechanism from HTTP/1.1. Additionally, WSP/B supports three push mechanisms for data transfer: a confirmed data push within an existing session context, a non-confirmed data push within an existing session context, and a non-confirmed data push without an existing session context.
- g) **Asynchronous requests :** Optionally, WSP/B supports a client that can send multiple requests to a server simultaneously. This improves efficiency for the requests and replies can now be coalesced into fewer messages. Latency is also improved, as each result can be sent to the client as soon as it is available.