INF-4086

GAUHATI UNIVERSITY
Centre for Distance and Online Education

Fourth Semester
(Under CBCS)

M.Sc.- IT

Paper: INF 4086

WIRELESS COMMUNICATION AND NETWORKS

CONTENTS:

SLM Development Team:

HoD, Department of Computer Science, Gauhati University
Programme Coordinator, M.Sc.-IT, GUCDOE
Prof. Shikhar Kr. Sarma, Department of IT, Gauhati University
Dr. Khurshid Alam Borbora, Assistant Professor, GUCDOE
Dr. Swapnanil Gogoi, Assistant Professor, GUCDOE
Mrs. Pallavi Saikia, Assistant Professor, GUCDOE
Dr. Rita Chakraborty, Assistant Professor, GUCDOE
Mr. Hemanta Kalita, Assistant Professor, GUCDOE

Course Coordination:

Dr. Debahari Talukdar	Director, GUCDOE
Prof. Anjana Kakoti Mahanta	Programme Coordinator, GUCDOE Dept. of Computer Science, G.U.
Dr. Khurshid Alam Borbora	Assistant Professor, GUCDOE
Dr. Swapnanil Giogoi	Assistant Professor, GUCDOE
Mrs. Pallavi Saikia	Assistant Professor, GUCDOE
Dr. Rita Chakraborty	Assistant Professor, GUCDOE
Mr. Hemanta Kalita	Assistant Professor, GUCDOE
Mr. Dipankar Saikia	Editor SLM, GUCDOE

Contributors:

Mr. Hemanta Kalita Assistant Professor, GUCDOE	(Block I : Units- 1, 2 & 3) (Block II : Unit- 1)
Ms. Neeharika Sonowal Teaching Associate Dept. of Computer Science, G.U.	(Block II : Units- 2, 3 & 4)
Dr. Dwipen Laskar Assistant Professor Dept. of Computer Science, G.U.	(Block II : Units- 5 & 6) (Block III : Unit- 1)
Mr. Deepjyoti Chetia Teaching Associate Dept. of Computer Science, G.U.	(Block II : Unit- 7) (Block III : Unit- 2)

Content Editor:

Dr. Dipen Nath	Assistant Professor Dept. of Computer Science Kokrajhar Govt. College

Cover Page Designing:

Bhaskar Jyoti Goswami	GUCDOE
Nishanta Das	GUCDOE

ISBN: 978-81-986642-4-2
June, 2025

© Copyright by GUCDOE. All rights reserved. No part of this work may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, or otherwise.

Published on behalf of Gauhati University Centre for Distance and Online Education by the Director, and printed at Gauhati University Press, Guwahati-781014.

CONTENTS:

BLOCK- I : WIRELL COMMUNICATIONS AND SYSTEM FUNDAMENTALS

BLOCK- II : WIRELESS NETWORKING

BLOCK- III : MOBILE IP AND WIRELESS APPLICATION PROTOCOL

BLOCK- I

WIRELL COMMUNICATIONS AND SYSTEM FUNDAMENTALS

Unit 1: Wireless Communication

Unit 2: Modulation Techniques

Unit 3: Radio Spectrum and Cellular System

UNIT-1

WIRELESS COMMUNICATION

Unit Structure:

1.1 INTRODUCTION

Wireless communication is a modern internet connectivity which enables users to transmit their data in the web. In this unit we will discuss about the concept of wireless communication with relevant examples. The cellular concepts along with the frequency reuse concepts are also discussed in this unit. We will also discuss about the cell splitting and cell sectoring concepts with the introduction to micro cells and the uses of repeaters. The different strategies, interference and system capacity are also discussed in this unit.

1.2 OBJECTIVES

After going through this unit learner will able to

- *understand* the concept of wireless communication systems;
- *learn* the different wireless techniques;
- *understand* the cellular concepts and frequency reuse;
- *understand* the concept of cell splitting and sectoring;
- *learn* about the uses of repeaters and microcell;
- *understand* strategies, interference and system capacity of wireless network.

1.3 WIRELESS COMMUNICATION

The concept of connecting a person at any time and at any place has become possible for the invention of wireless technology or communication. In wireless technology, focus is given on more personalized services and transaction supports which is reducing the surfing time. The mobile or cell phones which have the ability to browse the internet receive and send emails in a quick succession of time from any location in the world. Wireless communication involves some additional technologies and principles which are not associated with the wired communication. These technologies and principles are as follows

- **Antennas:** Wireless antenna is an instrument that helps transmitting and receiving electromagnetic signals. Using the transponder these antenna can share the information in a vast geographical area. The efficiency of an antenna as a radiator and as a receiver of RF (Radio Frequency) energy from space. It is related to the physical size of the antenna relative to the operating frequency. In two way communication, the same antenna often used for both the transmission and reception. An antenna will radiate power in all directions but it does not perform well in all the directions. The simplest pattern of an antenna is known as the isotropic antenna. Isotropic antenna radiates the power in all the directions equally. The radiation pattern of an isotropic antenna is actually a sphere with the antenna at the centre. The pattern of isotropic antenna is shown in the Figure 1.1. In the directional antenna the preferred direction of radiation is along in one axis.

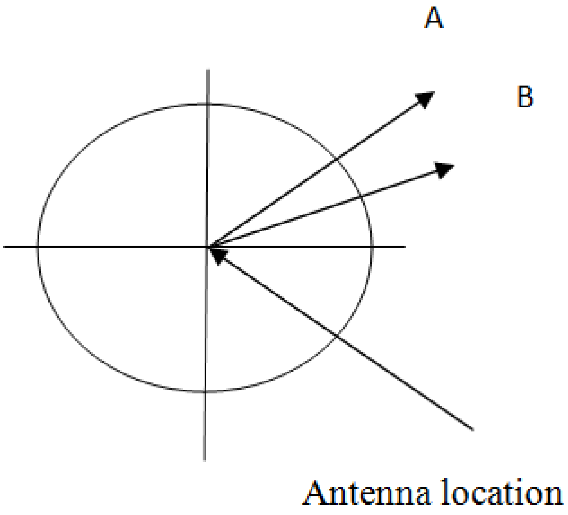


Figure 1.1: Omnidirectional Antenna

The radiation pattern determines the beam width of an antenna which is the common measurement of the directivity of an antenna. Amongst different types of available antennas, two basic antennas are half-wave dipole and quarter-wave vertical antenna. Half-wave dipole antenna consists of two horizontal collinear conductors of equal length. There is a small gap between these two conductors. A quarter-wave vertical antenna is commonly used in automobile radio and portable radios. Another important type of antenna is the parabolic reflective antenna. This type of antenna is used basically in terrestrial microwave and the satellite communications.

- **Receiver Sensitivity and Selectivity**: Receiver sensitivity indicates its ability to pick up a weak signal. For a receiver both the sensitivity and the selectivity are equally important. Selectivity is the ability of a receiver to differentiate desired signals from adjacent signals. Sensitivity also distinguishes the noise and other interferences in signals. More sensitive receiver means, the receiver is larger and heavier and require more power and as a result it is more expensive to build and design.

- **Signal absorption**: The UHF (Ultra High Frequency) radio waves for cellular communication are subject to absorption by different objects and structures between the cell and the handheld device. The radio waves absorb by different objects in different degrees. The cell phone used an open field and has a greater range and therefore it does not require as many closely cells which means a fixed transmitters and receivers.

- **Signal Propagation**: The radio waves propagate in the space in a predictable way. At the UHF frequencies allocated to the wireless web, radio wave behaves less predictability in comparison to the others. When a signal reaches in the receiver end without any reflections, diffractions and scattering, is known as the propagation in the line-of-sight directions. In ground wave propagation, the waves propagate on the surface of the earth. This effect is found in frequencies up to 2 MHz. The best known example of ground wave communication is AM radio. Sky wave propagation is used in amateur radio and some international broadcasts such as BBC and Voice of America. The sky wave propagation signals are reflected from the ionized layer of the upper atmosphere that is ionosphere and back down to the earth. In sky wave propagation mode signals can be picked up thousands of kilometers from the transmitter. The ground wave and the sky wave propagation are unable to operate when the frequency is above 30 MHz. In this situation the communication must be in line-of-sight. For a satellite communication, signal is not reflected by ionosphere and for this reason a signal is transmitted between an earth station and a satellite overhead.

1.4 PRINCIPLES OF CELLULAR NETWORKS

The main aim of cellular networks is to increase the capacity available for mobile radio telephone service. Before the cellular radio the mobile radio telephone service was provided by a high end transmitter and receiver. The main technique of cellular network is the use of several multiple low-power transmitters. Because the range of these transmitters is very small, an area can be divided into cells, and each cell is served by its own antennas. Each cell is served by base station, consisting of transmitters, receiver and control unit. Adjacent cells are assigned different frequency to avoid the interference or crosstalk. The matrix of square cells is the simplest layout of cellular network which is shown in the Figure 1.2. This layout is not ideal. A mobile user within a cell moves towards the cell boundaries. It is more suitable if all of the adjacent antennas are equidistant. A hexagonal pattern provides for equidistant antenna but practically this pattern is not used.

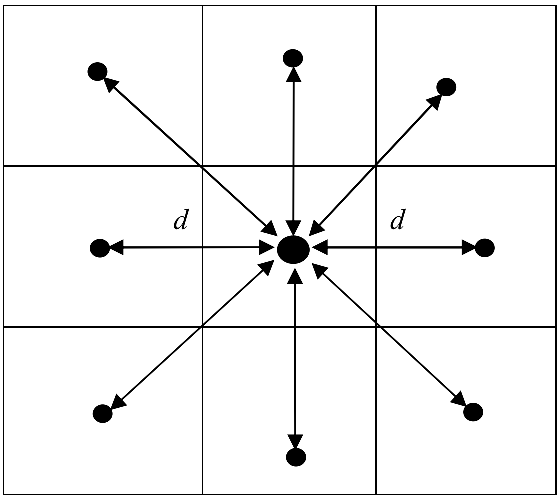


Figure 1.2: Square Pattern of Cellular Geometry

1.4.1 Concept of Frequency Reuse

In a cellular system each cell has a base transceiver. The transmission power of each cell is controlled to allow communication within the cell using the given frequency band. The objective of frequency reuse is to use the same frequency band in multiple cells at some distance from one another. The design issue of frequency reuse is to determine the minimum separation between two cells that uses the same frequency band to avoid the interference. In frequency reuse, various patterns of frequency reuse are possible. If a pattern consists of N cells and each cell is assigned the same number of frequencies than each cell can have K/N frequencies, where K is the total number of frequencies allotted to the system. For AMPS (Advanced Mobile Phone System), K = 395, N=7 which is the smallest pattern that can provide sufficient isolation between two cell which uses the same frequency. This means that on average, there can be at most 57 frequencies per cell.

1.4.2 Increasing the Capacity of the System

In a cellular system, the traffic is likely to increase with the rise in the number of customers. As a result there remains insufficient frequency bands assigned to cells to handle its calls. The following are the approaches that have been used to handle this situation.

Adding new channels: When a system is setup, initially not all the channels are used. As the system is expanded, the unused channels are added in a sequence order.

Frequency borrowing: Frequency borrowing means, frequencies are taken from adjacent cells by congested cells. Dynamic allocation of frequencies to the cell can also be possible in some situations.

Cell splitting: Cells in high usage area can be split into smaller cells. In general the cells are about 6.5 to 13 kilometers in size. The smaller cells are split themselves but in practical 1.5 km cells are close to the minimum size of general solution. The power level used must be reduced to keep the signal within the cell. The signals pass from cell to cell as the mobile unit moves from one place to other, which requires transferring the call from one base transceiver to another. This process is known as handoff. Handoff is much more frequent for the smaller cells. The division cells for providing more capacity is shown in the Figure 1.3.

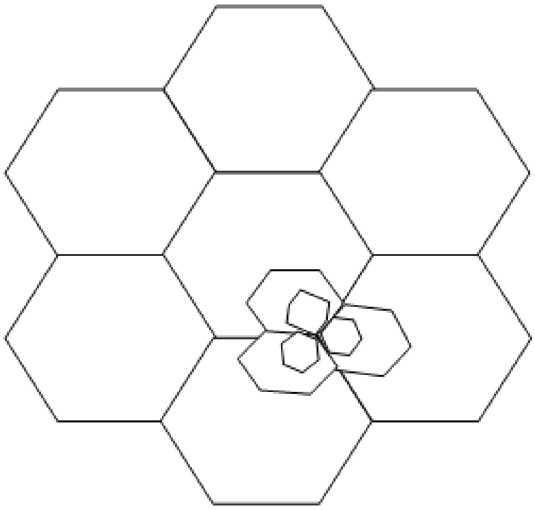


Figure 1.3: Cell Splitting

Cell sectoring: In cell sectoring, cells are divided into number of sectors and each cell with its own set of channels. Typically a cell contains 3 or 6 sectors and each sector is assigned a separate subset of the cell's channel and directional antennas at the base station.

Microcells: As the cells become smaller, antenna moves from the top of small building and the side of large building and to the lamp posts, where it form a microcells. Microcells are useful in city streets in congested areas, along highways, and in the public buildings.

1.4.3 Operation of Cellular Systems

In a cellular system the main component of a cell is the Base Station (BS). The base station includes an antenna, a controller, and number of transceivers, for communicating on the channels assigned to that cell. In a base station, the controller is used to handle the call process between the mobile units and the network. In this system, at any time, different number of mobile units may be active and moving about within the cell, communicating with the base stations. Each base station is connected to a Mobile Telecommunications Switching Office (MTSO) by a wireless link. The overview of cellular System is shown the Figure 1.4.

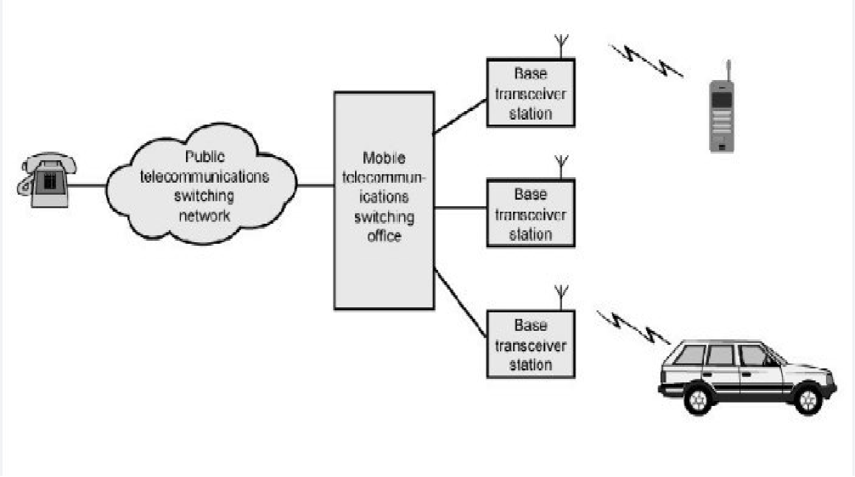

Public telecommunications switching network
Mobile telecommunications switching office
Base transceiver station
Base transceiver station
Base transceiver station

Figure 1.4: Overview of Cellular System

Image Source: https://images.app.goo.gl/ee1VvgooG356J5wr7

The MTSO connects calls between mobile units to mobile units. It is also connected to the public telephone or telecommunications network. MTSO can make a connection between a fixed subscriber to the public network and mobile subscriber to the cellular network. It also assigns a voice channel to each call and monitors the calls for billing purpose. The cellular system is fully automated. In this system, two types of channels are available between the mobile units and base stations. They are as follows-

- **Control Channels:** It is used to exchange information which involves setting up and maintaining calls and establishing relationship between a mobile unit and its nearest base stations.
- **Traffic Channels**: It carries a voice or data connection between the available users.

- **Mobile Unit Initialization**

When the mobile unit is turned on, it scans and selects the strongest set-up control channel used for the system. Different frequency band cells repetitively broadcast on different set-up channels. The receivers also select the strongest set-up channel and monitor it. As a result the mobile unit automatically selects the base antenna of the operated cell. Then a communication is established between the mobile unit and the MTSO controlling cell, through the base station. This communication is used to identify the user and register its location. The scanning process is repeated periodically to account for the motion as long as the mobile unit is on. Now if the mobile unit enters a new cell, then a new base station is selected.

- **Mobile Originated Calls**

The mobile unit originates a call by sending or forwarding the called unit on the previously selected set-up channel. The receiver at the mobile unit firstly examine whether the set-up channel is idle or not. When an idle channel is detected, the mobile unit may transmit on the corresponding reverse channel. Then the MTSO tries to complete the connection with the called unit. For this purpose, MTSO sends a paging message to the specific base stations depending on the called mobile unit number. Each base station transmits the paging message or signals on its own assigned setup channel. The called mobile unit recognizes its number on the set-up channel, which sends the response to the MTSO. Now the MTSO setup a path or circuit between the called and calling base stations. At the same time, the MTSO selects an available traffic channel in the cell within each base station. The two mobile units then tune their respective assigned channels. While the connection is maintained, the two mobile units exchange their information through their respective base stations and the MTSO is termed as ongoing call.

1.4.4 Mobile Radio Propagation Effects

There exist different types of complexities in radio communication which are not found in wired communications. The general areas of signal strength and signal propagation are as follows-

- Signal strength: The strength of the signal between the base station and the mobile unit must be strong enough to maintain the signal quality at the receiver end. But as the signal strength is not too much strong, so it will create an interference with the channels using the same frequency band. There are several complicating factors which will reduce the signal strength and the affect is varying in different place and situations. For example the noise created by automobile is much more in urban areas in comparison to the rural area. Also the signal strength varies dynamically as the mobile unit moves from one place to the other.

Stop to Consider

Even if signal strength is within an effective range, signal propagation effects may cause errors in the signals.

1.4.5 Handoff

The term handoff is used in U.S. cellular standard documents. The handoff and handover are appearing in technical literature but the meaning is the same. It is referred to as the process of transferring ongoing call or the data connectivity from one base station to another base station as the mobile unit moves from one cell to another. There are different ways of handling the handoff in different system. To make a handoff decision, different performance metrics may be used, which are as follows-

Cell blocking probability: New call may be blocked due to the load which is excess of base station traffic capacity. In this situation mobile unit is handed off to the adjacent cell on the basis of traffic capacity.

Call dropping probability: A call may be terminated due to the call dropping probability which is caused by the handoff.

Probability of unsuccessful handoff: Unsuccessful handoff occurs due to the poor reception condition.

Handoff blocking probability: The probability that a handoff cannot be terminated successfully.

Interruption duration: Interruption duration means the time during a handoff, a mobile unit is not connected to either base station.

1.5 REPEATERS USED IN CELLULAR NETWORKS

Repeater is an electronic device used to increase the signal strength of a cellular network. Repeater receives a signal from a base station, amplify it and then transmits it to the low strength area. Using of repeaters help to reduce the signal degradation problem, which are caused by tall buildings, hills and long distances. The main goal of repeater is to amplify weak signals. If the signals from mobile device are too weak, repeater plays a vital role in enhancing the signal strength. Generally repeaters help to reach the signals to the area where signals from base station cannot reach, such as some rural areas, underground locations, tunnels etc. In some situations, repeaters are also used to reduce the interference between the signals and improve the signal-to-noise ratio (SNR). The working of a repeater in a cellular network is depicted in Figure 1.5.

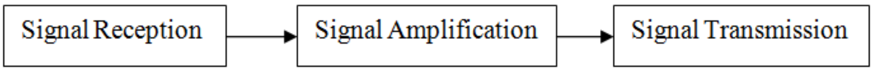


Figure 1.5: Working of a Repeater

In the signal reception part, repeater will first receive the weak signals transmitted from the base station or the mobile device. This is done basically with the help of the antenna. In the second part, after receiving the weak signals repeater will amplify the signal with the help of its amplifier. Finally after amplification, the repeater will transmit the strong signals to the corresponding locations or direction. There are different types of repeaters used in cellular network. The analog repeaters are used only to amplify the signals. These repeaters are simple but can reduce the noise along with the signals. Before retransmitting the signals, digital repeaters process the signal first. In the processing, signals are filtered and errors are corrected ensuring that only perfect or cleanest signals are sent to the desired locations. In comparison to the analog and digital repeaters one advanced repeater is used in cellular network which is known as Base Transceiver Station (BTS) repeater. It is basically part of the base station infrastructure and can handle both uplink and download transmissions.

Check Your Progress-I

1. Multiple Choice Questions

(i) The best known example of ground wave communication is

(a) AM radio
(b) Amateur radio
(c) Satellite communication
(d) Line-of-sight

(ii) The objective of frequency reuse is to use

(a)Different frequency band in multiple cells
(b) Same frequency band in multiple cells
(c) Fixed frequency band
(d) Dynamic frequency band

(iii) In a cellular system the main component of a cell is

(a) Cellscripting
(b) Cellblocking
(c) Base stations
(d) Microcell

(iv) Traffic channel carries

(a) Frequency reuse
(b) Only the frequencies
(c) Macrocells
(d) Voice and data connection between users.

(v) The process of transferring ongoing call from one base station to another base station is known as

(a) Handoff
(b) Call transferring
(c) Call switching
(d) Channel transferring

2. State WhetherTrue or False

(i) A quarter-wave vertical antenna is commonly used in automobile radio.

(ii) The design issue of frequency reuse is to avoid the interference.

(iii) There is no requirement of antenna at the base station.

(iv) In frequency reuse, only one pattern of frequency reuse is possible.

(v) The main goal of repeater is to amplify weak signals.

1.6 INTERFERENCE IN CELLULAR NETWORKS

Interference refers to any unwanted signal or noise that prevents the normal communication between a mobile device and the network. There are different strategies and techniques in cellular network to handle or reduce interference.

1.6.1 Types of Interference

There are different types of interferences in cellular networks, these are as follows-

- **Co-Channel Interference**: The channels which are using same frequency band in a cellular network is known as the co-channel and the interference from these channel is called the co-channel interference. An example of co-channel interference is when a transmitter of radio is operating on the same frequency. For reducing the co-channel interference the cells are clustered as close as possible. The main reasons of co-channel interference are bad weather condition and the poor frequency planning.
- **Adjacent Channel Interference**: The adjacent channel interference occurs when signal from two communication channels, which are located next to each other, interfere to

each other. There are different reasons of adjacent cannel interference these are as follows-

-Inadequate frequency separation: the signals from adjacent channel can overlap into one another, if the frequency spacing between the channels is too narrow.

-Lack of perfect filtering: If the filtering techniques are not perfectly maintained in the base station and the mobile devices, the adjacent channel interference is occurs.

1.6.2 Interference Management

Interference can be managed by the following ways

- **Proper Cell planning:** The area where users are more concentrated, the base station can use the smaller cells to reduce the interference.
- **Frequency Reuse:** By designing the system by proper frequency reuse techniques, the interference can be reduced.
- **Power Control:** Adjusting the power control scheme for the mobile devices and the base stations the interference of the system can be reduced. The different design issues make it desirable to include a dynamic power control capability in a cellular system. Cellular system uses two kinds of power control – one is open-loop power control and the other one is the closed-loop power control. The open-loop power control depends solely on the mobile unit, where there is no feedback from the base station and used in some spread spectrum system. In closed-loop power control system, it adjusts the signal strength in the reverse channel that means the way from mobile to the base station. The base station makes the power adjustment command to the mobile unit on the control channel.

1.7 SYSTEM CAPACITY OF CELLULAR NETWORK

In cellular network, the system capacity refers to the maximum number of users and total number of data traffic that can be supported in a given area. The system capacity is influenced by the several factors which are as follows-

Frequency spectrum: The system capacity is always dependent on the frequency spectrum. More spectrums mean more bandwidth resulting in allowing more users. Spectrum efficiency plays a vital role in terms of capacity of the system.

Architecture of the cellular network: System capacity also depends upon the architecture of the network. The division of cells into macro and micro cells increases the system capacity of the cellular networks.

Interference management: It is the crucial factor for maintaining the capacity of the network. Proper interference management may increase the capacity of the system.

Load balancing: The proper load balancing across the cells can enhance the capacity of the system.

Check Your Progress-II

3. State Whether True or False

(i) Interference refers to noise that prevents the normal mobile communication.

(ii) Co-Channel Interference cannot be reduced.

(iii) The open-loop power control depends solely on the mobile unit.

(iv) In closed-loop power control, signal strength cannot be adjusted.

(v) The system capacity depends upon the frequency spectrum

1.8 SUMMING UP:

- In wireless communication, it is possible to connect a person at any time and at any place.
- Wireless antenna is an instrument that helps transmitting and receiving electromagnetic signals.

- The simplest pattern of an antenna is known as the isotropic antenna and it radiates the power in all the directions equally.
- When a signal reaches in the receiver end without any reflections, diffractions and scattering, it is known as the propagation in the line-of-sight directions.

- There are different types of antennas for signal transmission purposes. Amongst all these, two basic antennas are half-wave dipole and quarter-wave vertical antenna.

- The main technique of cellular network is the use of several multiple low-power transmitters.

- The objective of frequency reuse is to use the same frequency band in multiple cells at some distance from one another.

- Frequency borrowing means, frequencies are taken from adjacent cells by congested cells.

- Handoff refers to the process of transferring ongoing call or the data connectivity from one base station to another base station as the mobile units move from one cell to another.

- Repeater is an electronic device used to increase the signal strength of a cellular network. It receives a signal from a base station, amplify it and then transmits the same to the low strength area.

- Interference refers to any unwanted signal or noise that prevents the normal communication between a mobile device and the network.

- Interference can be managed by using different techniques like frequency reuse, power control etc.

- System capacity in cellular network refers to the maximum number of users and total number of data traffic that can be supported in a given area.

1.9 ANSWER TO CHECK YOUR PROGRESS

1. (i) (a) (ii) (b) (iii) (c) (iv) (d) (v) (a)

2. (i) T (ii) T (iii) F (iv) F (v) T

3. (i) T (ii) F (iii) T (iv) F (v) T

1.10 POSSIBLE QUESTIONS

(1) Explain the concept of wireless communication.

(2) Explain how antenna helps in transmitting and receiving signals in wireless communication.

(3) What are the different types of antennas used in wireless communication?

(4) What is cellular network?

(5) Explain the operation of the cellular system.

(6) What is signal absorption?

(7) What is signal propagation? Explain different types of signal propagation techniques.

(8) Explain the concept of frequency reuse.

(9) What is frequency borrowing?

(10) What is cell splitting? Explain how it helps increasing the capacity of the system.

(11) What is cell sectoring?

(12) Explain the effects of mobile radio propagation.

(13) What is handoff? Explain the different performance metrics is used to make a handoff decision.

(14) Explain the uses of repeaters in cellular networks.

(15) Explain the different types of interference in cellular network.

(16) How can you measure the system capacity in cellular network?

(17) Explain the different approaches used for increasing the capacity of the system.

1.11 REFERENCES AND SUGGESTED READINGS

- Stallings W.; *Wireless Communication and Networking*
- Theodore, Rappaport S.; *Wireless Communications, Principles*, *Practice*;
- Matthew S Gast; *802.11 Wireless Networks*;
- Feher K. ; Wireless Digital Communications;
- Tse D. & Vishwanath P.; *Fundamentals of Wireless Communication*; Cambridge University Press

***

UNIT- 2
MODULATION TECHNIQUES

Unit Structure:

2.1 INTRODUCTION

The process where a low frequency signal is super imposed on a high frequency carrier wave is known as modulation. Here in this unit we will discuss different modulation techniques and know how the carrier wave varies according to their modulation techniques. In this unit we will also discuss the transmission of digital data to analog data and the three basic modulation techniques amplitude-shift keying (ASK), frequency-shift keying (FSK) and phase-shift keying (PSK).The transmission of Frequency Hopping Spread

Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) will also be discussed in this unit.

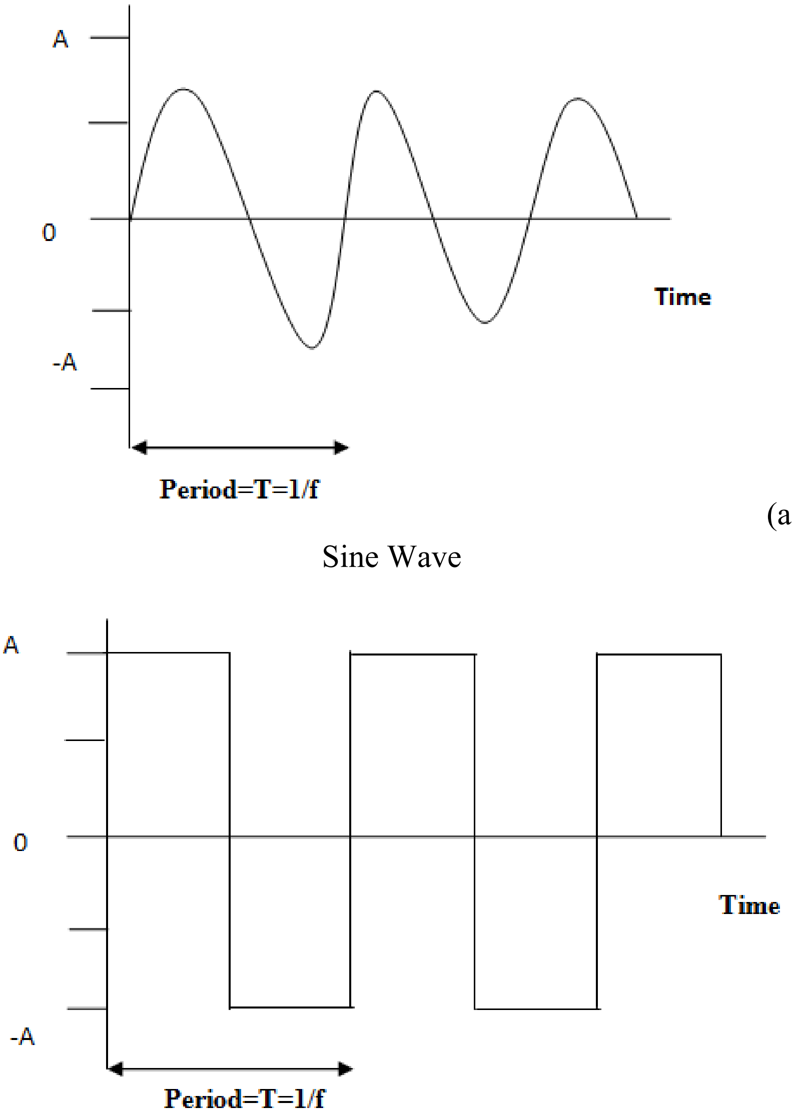
2.2 OBJECTIVES

After going through this unit learners will be able to

- *understand* the concept of modulation and its different techniques;
- *understand* the concept of Amplitude Modulation (AM), Frequency Modulation (FM) and Phase Modulation (PM);
- *learn* how digital data can be transmitted to analog signals;
- *understand* the concept of Amplitude Shift Keying(ASK), Frequency Shift Keying(FSK) and Phase Shift Keying(PSK);
- *learn* how Quadrature Amplitude Modulation(QAM) technique can be used in wireless communication;
- *understand* the concept of Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS).

2.3 SIGNALS FOR CONVEYING INFORMATION

The process of encoding source data into a carrier signal with the frequencies is known as the modulation. In all the modulation techniques, involves three fundamental frequency domain parameters which are amplitude, frequency and phase. An electromagnetic signal can be either analog or digital. An analog signal is one in which the signal intensity varies in a sequential manner over time. So we can say that there is no any break in the signal. On the other hand, a digital signal is one in which the signal intensity maintains a constant level for a period of time and then it changes to another constant level. The analog signal might represent speech, and the digital signal represents binary 1s and 0s. The simplest sort of signal is a periodic signal. In periodic signal the same signal pattern repeats over time. The periodic analog signal which is in sine wave and the digital signal which is in square wave are shown in the Figure 2.1.



(a)

Sine Wave

(b) Square wave

Figure 2.1 Examples of Periodic Signals

A signal s(t) is defined to be periodic if and only if

$$s(t + T) = s(t), \text{ where } -\infty < t < +\infty$$

and T is the period of the signal. Otherwise, the signal is a periodic. The general sine wave can be represented by three parameters: peak amplitude (A), frequency (f) and phase (ϕ). The peak amplitude is the maximum value over a period of time. This peak amplitude is measured in volts. The frequency is the rate at which the signal repeats. T is the amount of time taken for one complete repetition. Therefore, T = 1/f. Phase is the relative position in time within a single period of a signal. The general sine wave can be written as follows-

$s(t) = A \sin(2\pi ft+\phi)$………………………… (2.1)

The function with the equation (2.1) is known as a sinusoid.

2.3.1 Amplitude Modulation

In amplitude modulation, the amplitude of a carrier wave varies in accordance with the modulated signals. Amplitude modulation can be depicted by the Figure 2.2.

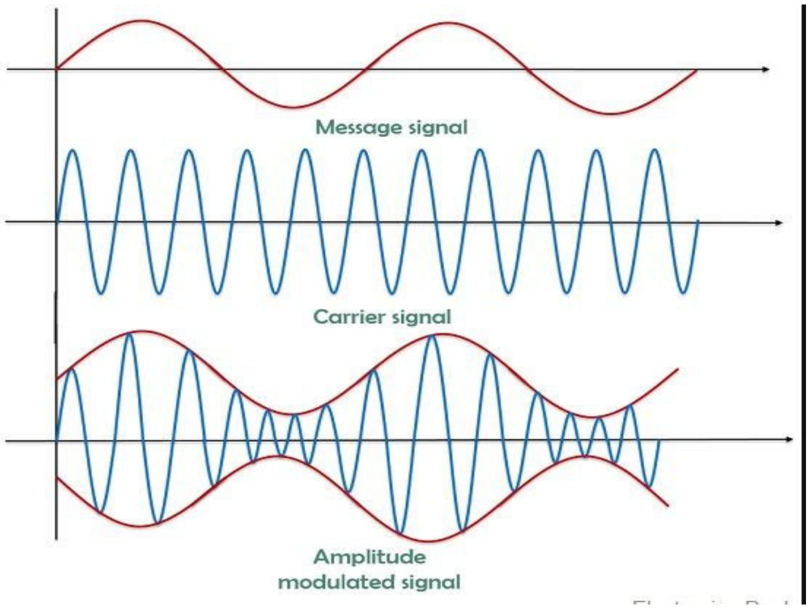


Figure 2.2 Amplitude Modulation

Image source: https://electronicsdesk.com/wp-content/uploads/2019/01/Amplitude-modulated-waveform.jpg

Mathematically the process can be expressed as

$s(t) = [1 + n_a x(t)] \cos 2\pi f_c t$ ………………….(2.2)

Here,

$2\,\pi f_c t$→ is the carrier wave

x(t) → is the input signal which is used for carrying data.

n_a→ Modulation index. It is the ratio of the amplitude of the input signal to the carrier wave.

The resultant AM signal consisting of the carrier wave with lower and upper side bands is known as the Double Sideband Transmitted Carrier (DSBTC). It is observed that the amplitude modulation involves the multiplication of the input signal by the carrier. The envelope of the resulting signal is $[1 + n_a x(t)]$ and envelope is an exact modification of the original signal as long as $n_a < 1$. When $n_a >$ 1, the envelope will cross the time axis and the information is lost. A popular variant of amplitude modulation is known as single sideband (SSB). In SSB only one sideband is considered by eliminating the other sideband. The main advantage of SSB approach is that only half of the bandwidth is required necessitating less power. Another type of amplitude modulation is Vestigial Side Band modulation. This is almost like Single Side band, except that the carrier frequency is preserved and one of the side bands is eliminating through filtering. Vestigial side band modulation is usually found in television broadcasting.

Application of Amplitude Modulation:

1. Radio broadcasting: Amplitude modulation is used in radio broadcasting for long distances mainly medium-wave and long-wave band.
2. Air-traffic control: Amplitude modulation is used in air-craft communication.
3. Television: Amplitude modulation is also used in black-and-white television for the audio portion.

2.3.2 Frequency Modulation

Frequency modulation is used to encode information in the carrier wave by changing its frequency. Here the amplitude of the carrier wave is unchanged. It can be said that the frequency modulation is occurred when the frequency of a carrier wave is changed based upon the amplitude of the input signal. Frequency modulation is depicted in Figure 2.3.

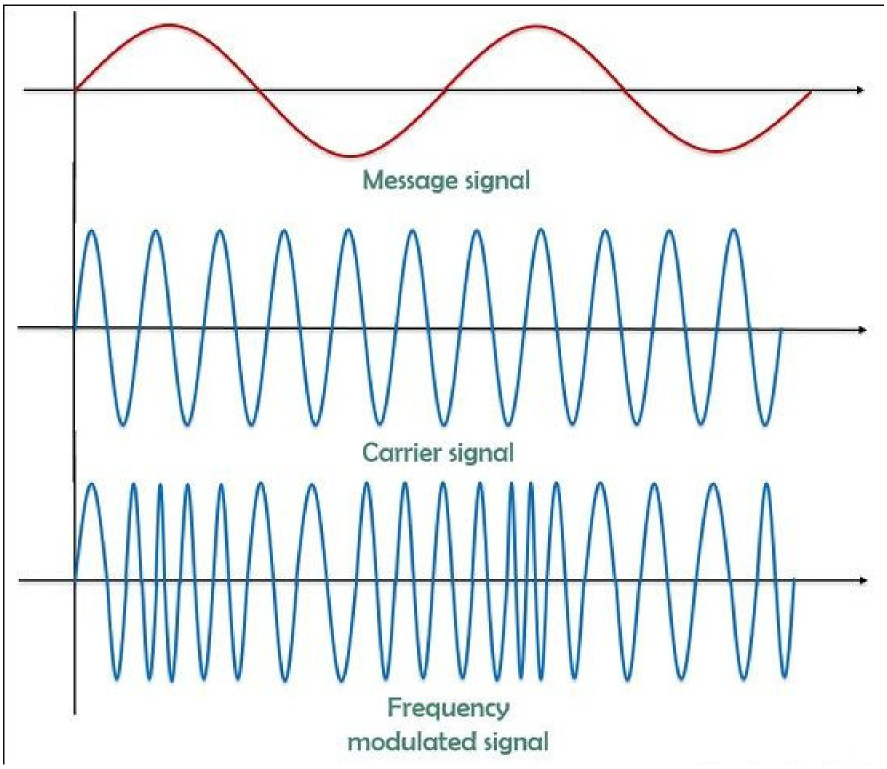


Figure 2.3 Frequency Modulation

Image source: https://electronicsdesk.com/wp-content/uploads/2019/01/Frequency-modulated-waveform.jpg

Frequency modulation is special case of angle modulation. The angle modulation is expressed as follows

$s(t) = A_c \cos [2\pi f_c t + \phi(t)]$…………………………..(2.3)

For frequency modulation, the derivative of the phase is proportional to the modulating signal that means

$\phi'(t) = n_f m(t)$……………………………….(2.4)

$n_f \rightarrow$ is the frequency modulation index

In frequency modulation, modulation effects in frequency but not in amplitude, which makes frequency modulation is more robust against different type of noises and interferences. Frequency modulation is widely used in radio for broadcasting music, speech and other form of audios, because it has the better sound quality and more resistance to interferences in comparison to amplitude modulation.

Application of Frequency Modulation:

1. **Frequency Modulation Radio broadcasting:** The most common use of frequency modulation is FM radio broadcasting. It provides better sound quality and less noisy signals in comparison to the amplitude modulation.
2. **TV and two ways Radio broadcasting:** In FM television, the audio signal is often transmitted using FM. As a result it provides high quality and clear sound along with the video signals.
3. **Satellite communication:** Frequency modulation is also used in satellite communication because it is suited for transmission of signals over long distances with less noise.
4. **Sound synthesizer and music productions:** Frequency modulation is used in sound synthesizing and transmission of music over long distances in different networks.
5. **Radar system and Instrumentation:** Frequency modulation is used in the radar system which includes frequency-modulated continuous wave (FMCW) radar. Frequency modulation can be used in some specific instrumental system such as sensor system which uses the frequency modulation to encode information about some physical quantities.

2.3.3 Phase Modulation

Phase modulation is similar to frequency modulation. The shapes of the frequency modulation and the phase modulation are very similar. Actually it is impossible to tell apart without knowledge of modulation function. In phase modulation, instead of changing in the frequency of the carrier wave, the phase of the carrier wave changes. In phase modulation, the phase is proportional to the modulating signals, which can be expressed as follows

$\phi(t) = n_p m(t)$……………………………….(2.5)

Where n_p is the phase modulation index.

In frequency modulation, the frequency of the carrier is directly changed according to the modulating signal. But in phase modulation, the phase of the carrier wave is directly changed according to the modulating signal, and this leads to a change in frequency.

Application of Phase Modulation:

1. Communication System: Phase modulation is often used in the digital communication systems, where information is encoded in different phase shifts of the carrier.
2. FM Radio and TV: Although the frequency modulation is common in radio and TV broadcasting, the phase modulation is also used for the same purpose.
3. Radar System and Signal Processing: Phase modulation is used in some radar systems and certain types of signal processing modules where phase modulation techniques are employed for better resistance to interference.
4. Sound Synthesis: Phase modulation is used in sound synthesizers that generate complex tones and textures by modulating the phase of the carrier wave.

2.4 TRANSMITTING DIGITAL DATA TO ANALOG SIGNALS

The common example of transmitting digital data using the analog signal is transmitting digital data through the public telephone network. At the initial state there were no use of digital devices in the telephone network. But at present the digital devices are attached to the network via modems (modulator-demodulator), which is used to convert digital data into analog signals and analog data into digital signals. We have already mentioned that modulation involves three basic characteristics-amplitude, frequency and phase. There are also three basic modulation techniques for transforming digital data to analog signals: amplitude-shift keying (ASK), frequency-shift keying(FSK) and phase-shift keying(PSK). In all of the techniques the resulting signals inhabit a bandwidth which is centered on the carrier frequency.

2.4.1 Amplitude Shift Keying (ASK)

In ASK the binary values 1 and 0s are represented by the two different amplitudes of the carrier frequency. Commonly one of the amplitude is zero, which means that one binary digit is represented by the presence at constant amplitude of the carrier wave and other by the absence of the carrier wave. The resulting transmitted signal for one bit time is-

$$s(t) = \begin{cases} A\cos(2\pi f_c\, t) & binary\ 1 \\ 0 & binary\ 0 \end{cases} \ldots\ldots\ldots\ldots\ldots(2.6)$$

Here the carrier signal is $A\cos(2\pi f_c\, t)$.
ASK is prone to sudden gain changes and as a result it is not an efficient technique. ASK is used on voice grade line but it is typically used only up to 1200 bps. In optical fiber, the ASK technique is used for transmitting digital data. For LED (Light-emitting diode) transmitters the equation 2.6 is valid. In LED one signal element is represented by light pulse, while the other is represented by the absence of light pulses.

2.4.2 Binary Frequency-Shift Keying (BFSK)

The most common frequency-shift keying is the binary frequency shift keying. In BFSK, two different frequencies are represented by two binary values near the carrier frequency. The transmitted signals for one bit of time can be represented by the following equation

$$s(t) = \begin{cases} A\cos(2\pi f_1 t) & binary\ 1 \\ A\cos(2\pi f_2\, t) & binary\ 0 \end{cases} \ldots\ldots\ldots\ldots\ldots..(2.7)$$

f_1 and f_2 are two offset from the carrier frequency f_c which are equal but opposite amount. BFSK is less susceptible to error in comparison to ASK. It is typically used on voice grade line up to 1200 bps. BFSK is also used for high-frequency radio transmission. Multiple FSK (MFSK) is stronger than BFSK, where more than two frequencies are used.

2.4.3Binary Phase-Shift Keying(BPSK): This is the simplest scheme using two phases to represent the two binary digits. The resulting transmitted signals for one bit time is expressed as follows-

$$s(t)=\begin{cases} A\cos(2\pi f_c t) \\ A\cos(2\pi f_c t + \pi) \end{cases}$$

$$= \begin{cases} A\cos(2\pi f_c t) & binary\ 1 \\ -A\cos(2\pi f_c t) & binary\ 0 \end{cases} \quad \ldots\ldots\ldots\ldots\ldots (2.8)$$

The phase shift of 180^0 is equivalent to flipping the sine wave or multiplying it by -1. Figure 2.4 shows the ASK, BFSK and BPSK modulation techniques used for modulation of analog signals for digital data.

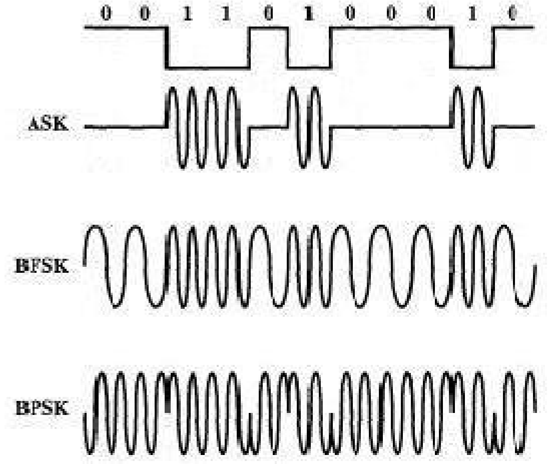


Figure 2.4Modulations of Analog Signals for Digital Data

Image Source: https://www.researchgate.net/profile/Samet-Tilkioglu/publication/323258413/figure/fig8/AS:672844497301505@1537430037813/ASK-BFSK-and-BPSK-Modulation-Types34.jpg

2.4.4Quadrature Phase-Shift Keying(QPSK)

QPSK is a phase modulation method using four phases. It can be expressed by the equation 2.9 as follows

$$s(t) = \begin{cases} Acos(2\pi f_c t\ + \frac{\pi}{4}) \\ A\cos\ (2\pi f_c t\ + \frac{3\pi}{4}) \\ A\cos\ (2\pi f_c t\ - \frac{3\pi}{4}) \\ A\cos\ (2\pi f_c t\ - \frac{\pi}{4}) \end{cases} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots..(2.9)$$

The phase will be changed according to the following conditions

- When 11, the angle is $\frac{\pi}{4}$

- When 01, the angle is $\frac{3\pi}{4}$
- When 00, the angle is $-\frac{3\pi}{4}$
- When 10, the angle is $-\frac{\pi}{4}$

For the convenience of modulator structure we map 1 to $\sqrt{1/2}$ and binary 0 to -$\sqrt{1/2}$.Thus a binary 1 is represented by a scaled version of the carrier wave and a binary 0 is represented by scaled version of the negative of the carrier wave at a constant amplitude. Then the two modulated signals are added together. The transmitted signal can be expressed through equation 2.10 as follows-

$$s(t) = \frac{1}{\sqrt{2}} I(t) \cos 2\pi f_c t - \frac{1}{\sqrt{2}} Q(t) \sin 2\pi f_c t \ldots\ldots\ldots\ldots.(2.10)$$

Stop to Consider

Four-Level PSK is more efficient use of bandwidth, and it can be achieved if each signaling element represents more than one bit.

2.4.5 Quadrature Amplitude Modulation (QAM)

In some wireless standards, QAM signaling technique is used. QAM is the combination of ASK and PSK. It can be considered as the logical extension of the QPSK. In QAM, it is possible to send two different signals simultaneously on the same carrier frequency. Each carrier in QAM is ASK modulated. At the receiver end two signals are demodulated and the results are combined to producing the binary input.

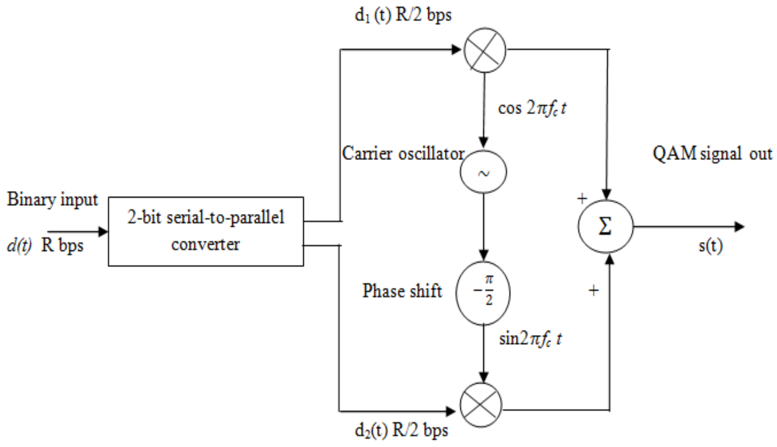


Figure 2.5 QAM Modulator

The QAM modulator is shown in the Figure 2.5. In the modulator the input is a stream of binary bits arriving at a rate of R bps. This stream then converted to two separate bit streams of R/2. The binary 0 is represented by the absence of the carrier wave. But the binary 1 is represented by the presence of the carrier wave at constant amplitude. The two modulated signals are added together and then transmitted. It can be expressed through equation 2.11 as shown below-

$$s(t) = d_1(t) \cos 2\cos 2\pi f_c t + d_2(t) \sin 2\pi f_c t \ldots\ldots(2.11)$$

2.5 FREQUENCY HOPPING SPREAD SPECTRUM (FHSS)

In FHSS, radio signals are transmitted by rapidly changing the carrier frequency among the many frequencies occupying a large spectral band. Here hopping occurs from frequency to frequency at fixed interval of times. The variation of changes is controlled by a code which is known to transmitter and the receiver. FHSS is used to avoid interference and to prevent eavesdropping. It also enables code-division multiple access (CDMA) communication. A typical block diagram of FHSS transmitter and receiver are shown in the Figures 2.6 and 2.7 respectively.

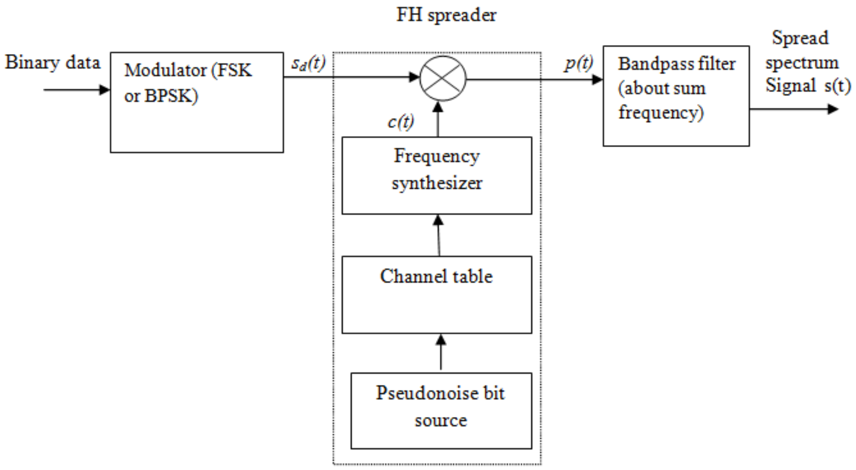


Figure 2.6: Transmitter of FHSS

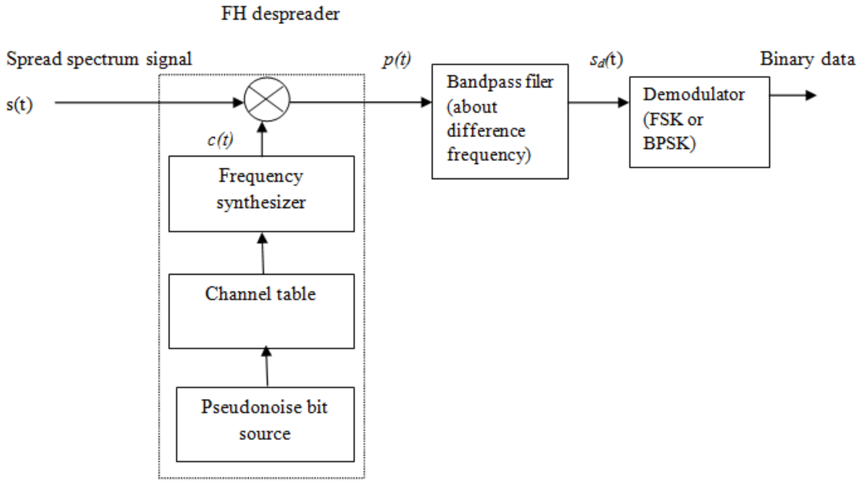


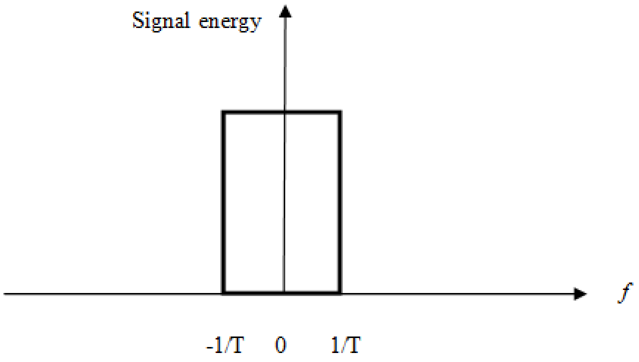
Figure 2.7: Receiver of FHSS.

For transmission purpose, binary data are fed into a modulation using frequency-shift keying (FSK) or binary phase-shift keying (BPSK). A pseudonoise serves as an index into a table of frequencies. At each successive interval, a new carrier frequency *c(t)* is selected. Then this frequency is modulated by the signal produced from the initial modulator to produce a new signal *s(t)* with the same shape. On the receiving end, the spread spectrum is demodulated using the same sequence of pseudonoise-derived frequencies and produces the output.

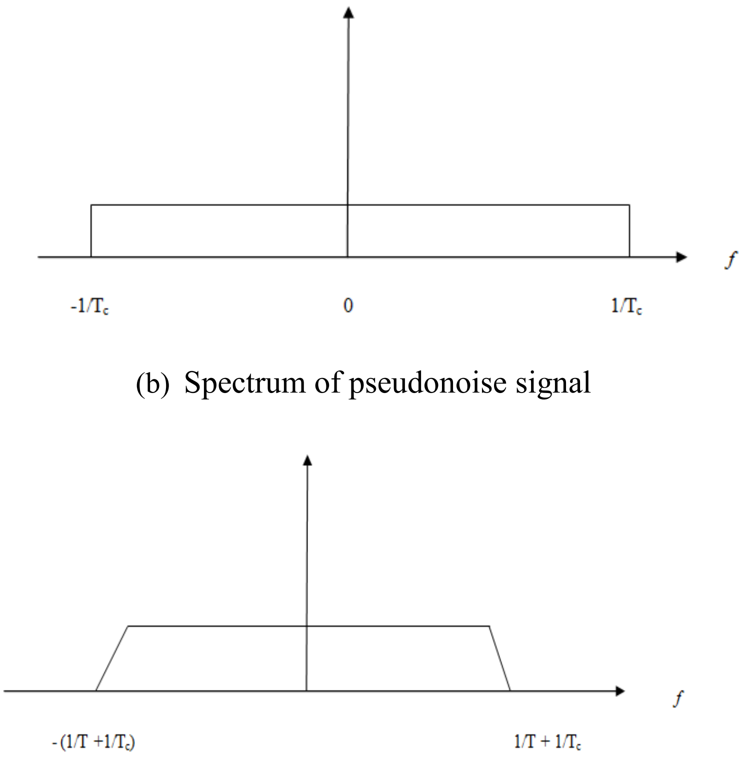
2.6 DIRECT SEQUENCE SPREAD SPECTRUM (DSSS)

In DSSS, each bit in the original signal is represented by the multiple bits. There is one technique for DSSS, which combines the stream of digital information with the spreading code bit stream using an exclusive-OR (XOR). In DSSS, information of one bit inverts the spreading code bits, while the information of zero bits is transmitted without inversion. The spectrum spreading achieved by the DSSS can be determined by the Figure 2.8.

Suppose in an example, the signal has a bit width of T and this is equivalent to the data rate of 1/T. In this situation the spectrum of the signal depends upon the encoding technique. This encoding technique is approximately 2/T. The spectrum of the Pseudo noise signal is 2/T$_c$. Figure 2.8 (c) shows the resulting spectrum spreading. The amount of spreading that is achieved is a direct result and that direct result is of the data rate of the Pseudonoise stream.



(a) Spectrum of data signal



(b) Spectrum of pseudonoise signal

(c) Spectrum of combined signal

Figure 2.8 Approximate Spectrum of Direct Sequence Spread Spectrum Signal

Check Your Progress:

1. Multiple Choice Questions

(i) An electromagnetic signal can be

(a) Either analog or digital

(b) Only analog

(c) Only digital

(d) Neither analog nor digital

(ii) Digital signal represents by

(a) Any number

(b) Octal number

(c) Hexadecimal number

(d) Binary number

(iii) A popular variant of amplitude modulation is known as
(a) Single sideband (SSB)
(b) Double sideband
(c) Triple sideband
(d) No sideband

(iv) Frequency modulation is used to encode information in the carrier wave by changing its (a) Amplitude
(b) Frequency
(c) Phase
(d) None of the above

(v) Modem is used for
(a) Converting only digital data
(b) Converting only analog signals
(c) Converting anlog-to-digital and digital-to-analog
(d) None of the above

2. State Whether True or False

(i) In phase modulation, the phase of the carrier wave is directly changed according to the modulating signal.

(ii) Frequency modulation cannot be used in Radio broadcasting.

(iii) In ASK, the binary values are represented by the two different amplitudes of the carrier frequency.

(iv) QPSK is an example of amplitude modulation.

(v) QAM is the combination of ASK and PSK.

(vi) FHSS is used to prevent eavesdropping.

(vii) Vestigial Side Band modulation is a type of phase modulation.
(viii) Frequency modulation cannot be used in sound synthesizing.
(ix)ASK is more efficient than PSK.

(x) FHSS enables the Code Division Multiple Access (CDMA) communication.

2.7 SUMMING UP:

- The process of encoding source data into a carrier signal with the frequencies is known as the modulation.
- Three fundamental frequency domain parameters are amplitude, frequency and phase, and they are found in all analog modulation techniques.
- The analog signal might represent speech, and the digital signal represents binary 1 and 0s.
- In amplitude modulation, the amplitude of a carrier wave varies in accordance with the modulated signals.
- The resultant AM signal consists of the carrier wave with lower and upper side bands and this is known as the Double Sideband Transmitted Carrier (DSBTC).
- In phase modulation, the phase of the carrier wave changes instead of the frequency of the carrier wave.
- The three basic modulation techniques for transforming digital data to analog signals are: amplitude-shift keying (ASK), frequency-shift keying (FSK) and phase-shift keying (PSK).
- In BFSK, two different frequencies are represented by two binary values near the carrier frequency.
- In QAM, it is possible to send two different signals simultaneously on the same carrier frequency.
- In DSSS, each bit in the original signal is represented by the multiple bits.
- There is one technique for DSSS that combines the stream of digital information with the spreading code bit stream using an exclusive-OR (XOR).

2.8 ANSWER TO CHECK YOUR PROGRESS

1. (i)(a)(ii) (d) (iii) (a) (iv) (b) (v) (c)

2. (i) True (ii) False

(iii) True (iv) False

(v) True (vi) True

(vii)False (viii) False

(ix) False (x) True

2.9 POSSIBLE QUESTIONS

1. What are the fundamental frequency domain parameters?
2. What is a periodic signal?
3. What is Amplitude Modulation (AM)? How can you express AM mathematically?
4. What is Frequency modulation? Explain its applications.
5. Differentiate between frequency modulation and phase modulation
6. What is ASK? Explain its modulation techniques.
7. Explain the BFSK modulation technique.
8. Differentiate between BPSK and QPSK.
9. What is QAM? Explain the QAM modulator.
10. What is Frequency Hopping Spread Spectrum (FHSS)?
11. Explain the working of transmitter and receiver of FHSS.
12. What is Direct Sequence Spread Spectrum (DSSS)?

2.10 REFERENCES AND SUGGESTED READINGS

- Stallings W.; *Wireless Communication and Networking*
- Theodore, Rappaport S.; *Wireless Communications, Principles*, *Practice*;
- Matthew S Gast; *802.11 Wireless Networks*;
- Feher K. ; Wireless Digital Communications;
- Tse D. & Vishwanath P.; *Fundamentals of Wireless Communication*; Cambridge University Press

***

UNIT- 3

RADIO SPECTRUM AND CELLULAR SYSTEM

Unit Structure:

3.1 INTRODUCTION

In this unit we will discuss about the spectrum allocation policy and its associated factors. The frequency bands are generally categorized in different ranges and higher frequency band is particularly used for the mobile communication system. Here we also discuss the scarcity of radio spectrum, capacity of the cellular system and mobility management. Finally in this unit we will discuss about the software defined radio and the working of cognitive radios.

3.2 OBJECTIVES

After going through this unit learners will able to-

- *learn* about spectrum allocation policy and its important factors;
- *understand* the concept of scarcity of radio spectrum;
- *understand* the concept of capacity of the cellular system;
- *learn* about the channel assignment problems with an insight to the possible solutions;
- *understand* the concept of handoff and location management;
- *understand* the concept of software defined radio and cognitive radio.

3.3 SPECTRUM ALLOCATION POLICY

Spectrum allocation refers to the regulation and distributions of electromagnetic spectrum by the regulatory bodies to ensure efficient use of radio spectrums within the range of electromagnetic frequencies of a telecommunication system. This telecommunication system includes television broadcasting, satellite communications, and Wi-Fi networks. There is a policy of the regulatory bodies which includes how spectrum is assigned to various services and the interferences can be prevented among the users. There are some important factors of the spectrum allocation which are as follows-

(i) **Frequency Band:** Different frequency bands are allocated to different services. For example Amplitude Modulation radio assigns lower frequency in comparison to the other radio frequencies. It is recommended that higher frequencies must be assigned for mobile communications and satellite services. The frequency band are typically categorized as follows

- Extreme Low Frequency (ELF): less than (<) 3kHz
- Very Low Frequency (VLF): 3 kHz to 30 kHz
- Low Frequency (LF): 30 kHz to 300 kHz
- Medium Frequency (MF): 300 kHz to 3 MHz

- High Frequency (HF): 3 MHz to 30 MHz
- Very High Frequency (VHF): 30 MHz to 300 MHz
- Ultra-High Frequency (UHF): 300 MHz to 3 GHz
- Super High Frequency (SHF): 3 GHz to 30 GHz
- Extremely High Frequency (EHF): 30 GHz to 300 GHz.

(ii) Licensing: Governments typically issue the licenses to use the spectrum for specific period of time under certain conditions.

(iii) Spectrum Sharing: In some special cases multiple users may share the same spectrum.

(iv) International Coordination: As the electromagnetic spectrum is a global resource, so there is a high necessity to have international agreements as well as coordination. The International Telecommunication Union (ITU) plays a vital role in coordination of spectrum allocation on a global scale to avoid the interference across the borders.

3.4 SCARCITY OF RADIO SPECTRUM

Scarcity of radio spectrum refers to the limited availability of the usable spectrum relative to the huge demand of wireless communication services. The demand of the spectrum increases as the uses of mobile phones, IoT devices, satellite services, Wi-Fi networks and other wireless technologies increases, while the physical electromagnetic spectrum is finite. The following are some factors for the scarcity of the radio spectrum-

(i) Growing demand of the wireless services: The expanded data usage, the uses of mobile devices are gradually increasing with rise in technology from 4G to 5G and in the future 6G. As a result, the demands are increasing in the wireless services for more bandwidth.

(ii) Limited frequency band: The frequencies which are suitable for the mobile communication and high-performance technologies are limited. The lower and the mid-range frequencies are more important for wide coverage.

(iii) Signal attenuation: Although the high frequency bands are used for the advanced technologies, these frequencies offer lower coverage and are affected with signal attenuation. For reducing the signal attenuation, the infrastructures need upgradation.

(iv) Proper coordination: It must be ensured that there exists no interference during the allocation of the spectrum. Radio station, TV broadcasters, mobile network and the wi-fi services need to be proper coordinated to confirm that these technologies are not overlapping to each other and is not causing unwanted noise.

Several strategies have been proposed to address spectrum scarcity. Some of the strategies are as follows-

- **Spectrum Sharing:**
  One of the best solutions of the scarcity of spectrum is to share the spectrum between multiple users or multiple services. The spectrum can be shared dynamically as it can be adjusted according to demand and availability.

- **Efficient Spectrum Management:**
  For efficient management of the spectrum, old technologies can be reformed for a better utilization and optimization in the spectrum usage. Moreover, some efficient modulation techniques can help to manage within the same spectrum.

- **Use of Higher Frequencies:**
  Expanding the lower frequency band into higher frequency band could provide more spectrums for wireless services. However, it is not an easy task to overcome the technical challenges related to the range and the interference.

- **International Coordination:**
  The ITU and other global bodies play a significant role in coordinating spectrum worldwide. For preventing the cross-border interference, global agreement on the allocation of spectrum is essential. This agreement also ensures that the services like satellite communication and mobile communication can operate globally without disruption.

3.5 CAPACITY OF THE CELLULAR SYSTEM

The capacity of the cellular system refers to the maximum number of users or devices supported within a specified range. For a noiseless channel Nyquist states that if the rate of signal transmission is $2B$, then a signal with frequencies no greater than B is sufficient to carry the signal rate. Now we consider the relationship among data rate, noise and error rate. The parameter involved in this situation is the signal-to-noise ratio (SNR). SNR is the ratio of the power in a signal to the power contained in the noise that is present at a particular point of the transmission. Typically, SNR is measured at the receiver end. At the receiver point an attempt is made to process the signal and delete the unwanted noise. The SNR ratio is reported in decibels and can be expressed in the following equation (3.1)

$$\mathrm{SNR} = 10 \log_{10} \frac{signalpower}{noisepower} \ldots\ldots\ldots\ldots\ldots\ldots (3.1)$$

From the above equation we can conclude that a high SNR will mean a high-quality signal. The SNR is important in the transmission of the digital data. According to the Shannon's result, the maximum channel capacity can be expressed in bits per second as indicated in the equation (3.2).

$$\mathrm{C} = \mathrm{B} \log_2(1 + SNR) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.. (3.2)$$

where, C is the capacity of the channel in bits per second and B is the bandwidth of the channel in Hertz. The capacity of the cellular system depends on the following factors-

(i) **Bandwidth**: Bandwidth of the cellular system determines how much data can be transmitted per unit of time. So, the capacity of the system is high if the bandwidth is high. The absolute bandwidth of a signal is the width of the spectrum. Many signals have an infinite bandwidth but energy contained in a relative narrow band frequency. Actually, this band is called effective bandwidth or simply bandwidth.

(ii) **Frequency Reuse:** The objective of frequency reuse is to use the same frequency band in multiple cells at some distance from one another. The design issue of frequency reuse is to determine the minimum separation between two cells that uses the same frequency band to avoid the interference. In frequency reuse, various patterns of frequency reuse are possible. The frequency reuse utilizes several co-channel cells separated by a distance. It may cause co-channel interference if the distance is not sufficiently large. Let the cellular system have P number of co-channel interfering cells. Then the signal-to-interference ratio (S/I) for a mobile receiver in the active cell is shown in the equation (3.2)

$$\frac{S}{I} = \frac{S}{\sum_{i=1}^{p} I_p} \text{..............} (3.2)$$

Here S→ desired signal power from serving base station and
I_p→ is the interference power from p_{th} interfering co-channel cell base station.

(iii) **Number of Channels**: Whenever a cellular system is setup, not all the channels are used. As the system is expanded, it can be managed by adding new channels in orderly fashion.

(iv) **Frequency Borrowing and Cell Splitting:** Generally, frequencies are taken from the adjacent cells by congested cells. In some special cases, frequency can also be assigned dynamically. Cell splitting technique also increases the capacity of the cellular system. Cells in areas of high usage can be split into some smaller cells. In general, cells are about 6.5 to 13 km in size. The smaller cells can themselves be split, however, the 1.5km cells are close to minimum practical size. Using the smaller cells the power level must be reduced to keep the signal within the cell.

(v) **Transmission Power and Network Planning:** The amount of power used by the mobile devices and the base station indicate how far the signal can be travelled and how many users can be involved without any interference. Powerful or efficient network design and optimization technique can play an important role in increasing the capacity of the system.

3.6 CHANNEL ASSIGNMENT PROBLEM

Channel assignment problem is related to the allocation of limited frequencies to the base station. When frequency is assigned to the channels, it will lead some constraints such as interference and maintaining the quality of service due to the various factors. The channel assignment problem can be solved by following factors-

- **Frequency Reuse:** Cellular network uses the frequency reuse for the efficient utilization of the available spectrum. The same frequency can be reused in different cells.
- **Interference Management**: The main challenge in channel assignment problem is to maintain the interference between cells. The adjacent cells must use the different channels to avoid co-channel interference.
- **Fixed and Dynamic Channel Assignment:** In fixed channel assignment, each cell is assigned pre-allocated fixed channels. This approach is easy to implement but it will lead to inefficient channel usage if the network and the traffic control are not properly balanced. In dynamic channel assignment, channels are allotted dynamically to the cells on priority basis.

- **Graph Coloring**: In graph coloring, cells are represented as nodes in a graph and the edges are represented by interfaces. The main objective of the graph coloring is to color the graph with the minimum number of colors or channels, such that two adjacent cells do not share the same color or channel.

Stop to Consider

In dynamic channel assignment, channels are assigned dynamically according to the request of the base station. So, it is easy to adapt to any changes in the system.

Check Your Progress –I

1. **Multiple Choice Questions**

(i) The limited availability of the usable spectrum relative to the huge demand of wireless communication services is referred to

(a) Mobility management

(b) Spectrum management

(c) Demand spectrum

(d) Scarcity of spectrum

(ii) The maximum number of users or devices that supported within a specified range in a cellular network is known as

(a) Capacity of the system

(b) Mobility management

(c) Maximum spectrum

(d) Channel assignment

(iii) The absolute bandwidth of a signal is the

(a) Capacity of the system

(b) width of the spectrum

(c) Total bandwidth

(d) Signal strength

(iv) In graph coloring, cells are represented as

(a) as different colors

(b) signal

(c) frequency

(d) as nodes of graph

2. **State Whether True or False**

(i) Amplitude modulation radio assigns lower frequency in comparison to the frequency modulation radio.

(ii) The spectrum cannot share dynamically.

(iii) For preventing the cross-border interference, global agreement on the allocation of spectrum is essential.

(iv) The capacity of the system is high if the bandwidth is low.

(v) Channel assignment problem is related to the allocation of limited frequencies to the base station.

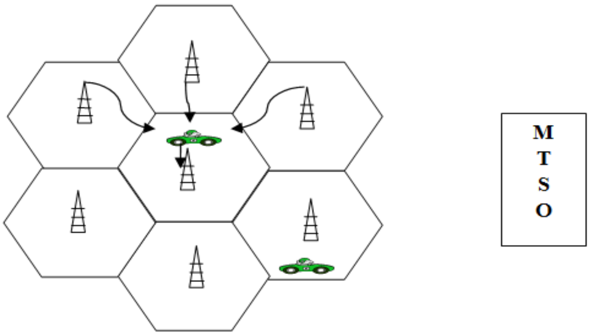
3.7 MOBILITY MANAGEMENT

The use of cellular system is fully automated. There is no any action requirement from the user for initiating the calls. From user's side it is only requirement of placing or answering a call. There are two types of channels available between the mobile unit and the base station. These two channels are-

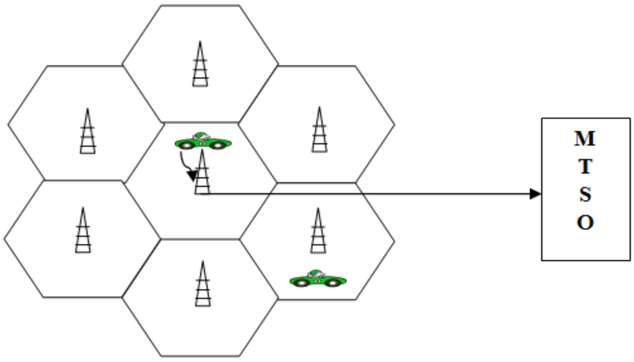
- **Control Channel:** Control channels are used to exchange information for establishing a relationship between a mobile unit and the nearest base station.
- **Traffic Channel:** Traffic channels carry a voice or data connection between users.

Figure 3.1 describes the steps required for a call between two mobile users within an area which is controlled by a single mobile telecommunications switching office (MTSO). When the mobile unit is turned on, it will scan and select the strongest setup control used for the system which is shown in the Figure 3.1(a). Cells continuously broadcast different frequency bands on different setup channel. The receiver will select best setup channel and monitors it and as a result the mobile unit automatically selects the base station's antenna. Then a communication is setup between mobile unit and MTSO. This communication is setup for identifying the user and registers its location. As the unit moves, the scanning process is repeated periodically until the mobile unit is on. A new base station is selected if the unit enters a new cell. The receiver of the mobile unit first examines whether the setup channel is idle by checking information in the forward channel which is from the base station. When channel is found idle, the mobile unit may transmit on the corresponding reverse channel that means to the base station. Then the base station sends the request to the MTSO. The MTSO tries to complete the connection to the called unit. A paging message is sent to the base stations depending on the called mobile unit number which is shown in the Figure 3.1(c). The base channels transmit the paging message on its own setup channel. The call can be accepted by the called mobile unit by recognizing its number on the setup channel which responds to that base station. The MTSO set up a circuit between the calling and called base stations. Ongoing call is possible while the connection is maintained by the two mobile units for exchanging their information going through their respective base stations and the MTSO which is shown in the

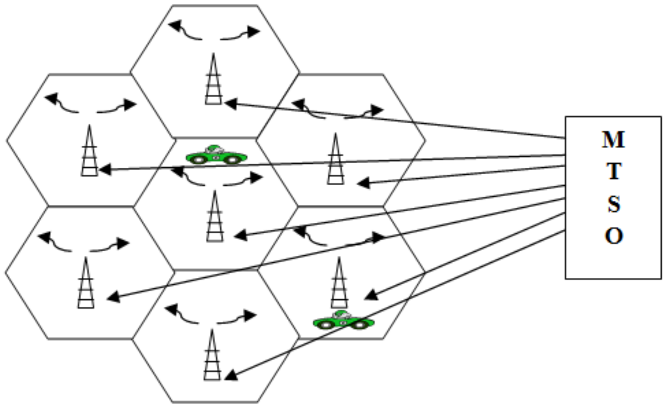
Figure 3.1(e). When the mobile unit moves out from the range of one cell to another, the traffic channel has to change to one assigned to the base station in the new cell which is shown in the Figure 3.1(f).



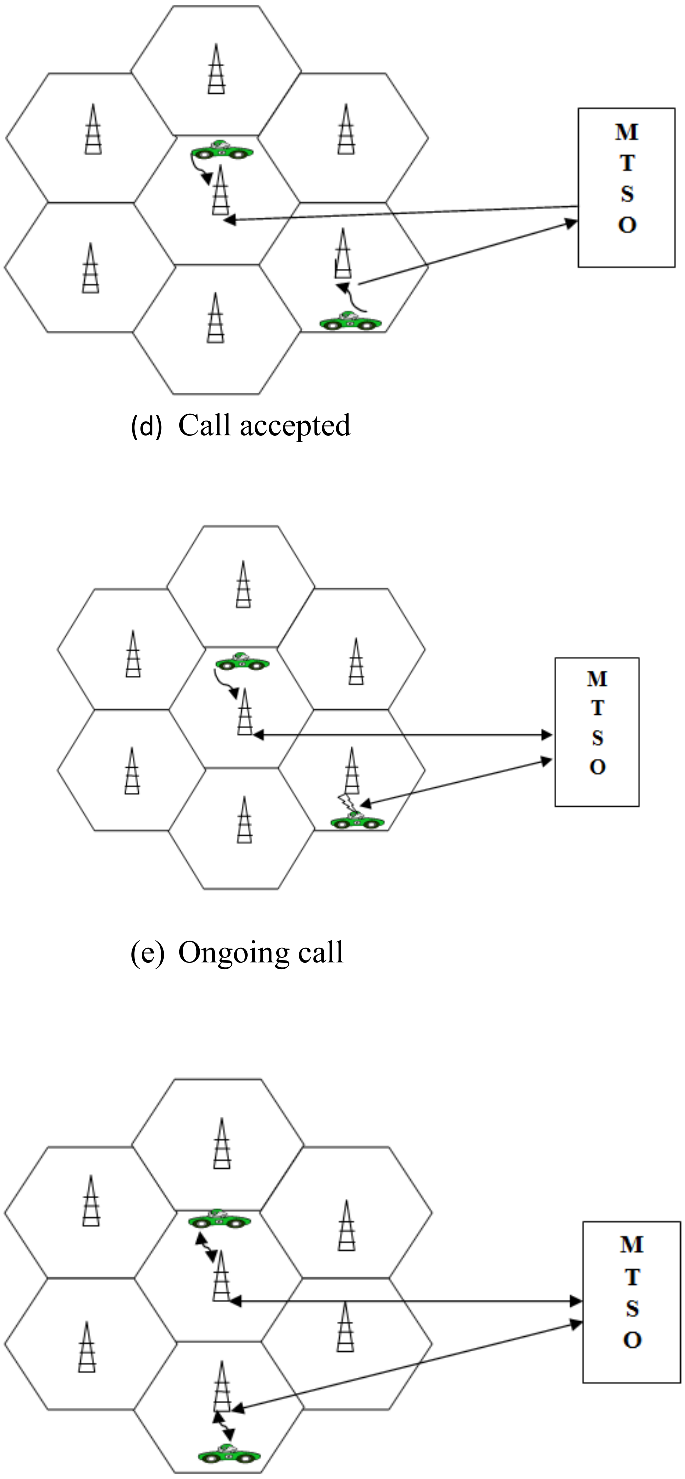
(a) Monitoring for strongest signal



(b) Request for Connection



(c)Paging message



(d) Call accepted

(e) Ongoing call

(f) Handoff

Figure 3.1 Steps of Mobile Cellular Call

3.8 HANDOFF AND LOCATION MANAGEMENT

Handoff and location management are the two crucial concepts in mobile communication. Handoff is the procedure for changing the assignment of a mobile unit from one base station to another as the mobile moves from one cell to another. Handoff ensures that the user's mobile device maintains a continuous connection as it moves through different coverage areas. Handoff may be network initiated where the decision is made on the basis of network measurement of the received signals from the mobile unit. The following are some performance matrices to make this type of decisions.

(i) Call blocking probability: Due to the heavy load on the base station, the new call may be blocked. In this situation mobile unit handed off to a neighboring cell based on the traffic capacity.

(ii) Call dropping and completion probability: The probability of that a call may be terminated due to the handoff. Again, the probability that an ongoing call is not terminated before its completion time.

(iii) Handoff blocking probability: This probability indicates that a handoff cannot be completed successfully.

(iv) Handoff probability: The probability that a handoff may be occurs before the completing the calls.

(v) Interrupt duration and handoff delay: Interrupt duration is the length of time during a handoff in which a mobile unit is not connected to the base station. Handoff delay occurs when no base station is available for accepting the transfer. Generally, the handoff delay occurs when the user is out of network coverage.

The main parameter used to make handoff decision is the measurement of the signal strength from the mobile unit at the base station. The Figure 3.2 shows the handoff between two Cells. Here shows the average received power level at two adjacent base stations as the mobile unit moves from the base station A at L_A to the base station B at L_B.

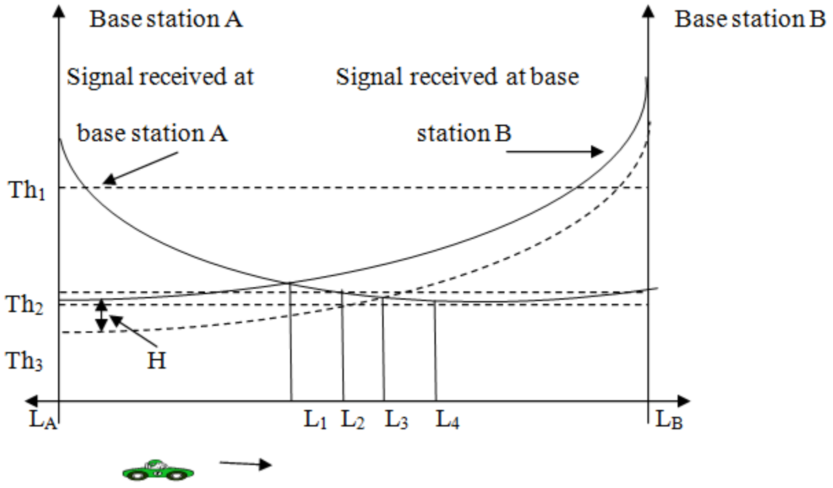


Figure 3.2 Handoff between two Cells

When the mobile unit moves from base station A to B, the handoff occur when the signal strength at B first exceeds that at A. In the Figure 3.2 the handoff occurs at the point L_1. At this point the signal strength still adequate but is declining. Handoff only occurs for the two reasons-

(i) The signal at the current base station is sufficiently weak

(ii) The other signal is stronger of the two.

If the threshold is quite low compared to the crossover signal strength, the mobile unit may move far away from the new cell. This will reduce the communication link and as a result the call may be dropped.

3.9 SOFTWARE DEFINED RADIO (SDR)

SDR is a special type of communication system where the hardware components are replaced by running software on a general purpose of computers. Generally, the replaced hardware components are mixers, amplifiers and the filters. In SDR most of the signal processing tasks like modulation, demodulation, encoding, decoding etc. are performed software instead of fixed hardware circuits. The physical part of radio that handles signal reception is known as RF Front End. This includes antennas and other hardware components like amplifiers or mixers. In SDR some software algorithms are used for modulation and demodulation, filtering, error correction. In SDR

Control interface allows for adjusting parameters such as frequency or power through user interfaces or other software.

Some of the basic advantages of SDR are as follows-

- **(i) Easy implementation:** SDR allows easy updates or changes to the system by modifying the software. It provides the facility to use same hardware to support multiple communication protocol simply by changing or installing the required software.
- **(ii) Cost:** SDR uses software to handle the signal processing, so that the system has lower hardware cost. Components like antenna, amplifiers are same across different applications which will reduce the need of special components.
- **(iii) Multiband support:** SDR can support multiple frequency bands which is especially beneficial for the emergency radio services.
- **(iv) Remote Operability:** SDR can be configured to carry out a range of activities which includes system monitoring, streamlining operations and around the clock-monitoring of predefined operations. Moreover, the SDR system can also be installed as standalone system.

SDR can be used as an amateur radio to explore different bands and communication methods. SDR is used in modern cell networks, Wi-Fi systems. SDR can also be used for military and emergency services.

3.10 COGNITIVE RADIO (CR)

Cognitive radio is an advanced form of SDR. CR uses Artificial Intelligence (AI) and Machine Learning (ML) techniques to automatically adapt to the radio environment. The main purpose of cognitive radio is to enhance the spectrum efficiency for detecting the available channels and adjusting its transmission parameters without causing interference to licensed users.

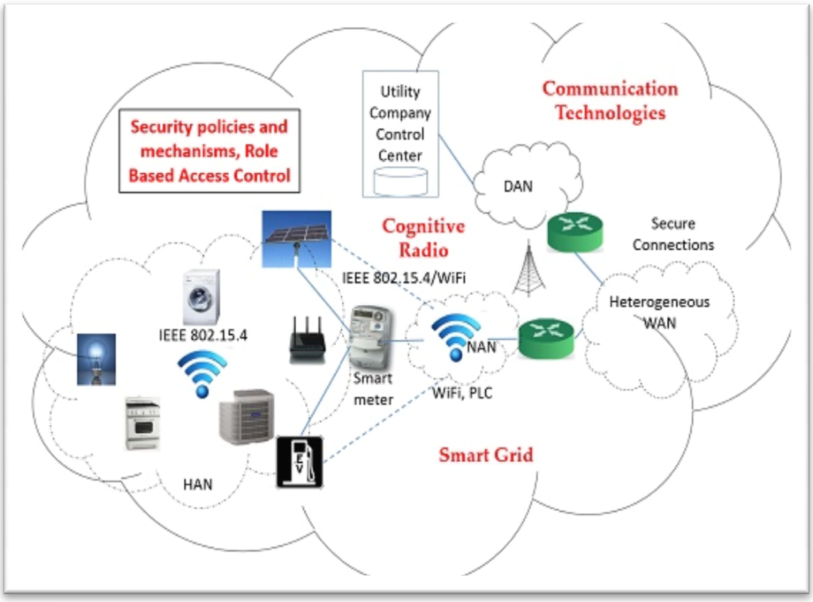


Figure 3.3 Architecture of Cognitive Radio

Image Source:https://pub.mdpi-res.com/computers/computers-05-00007/article_deploy/html/images/computers-05-00007-ag.png?1581058562

The architecture of cognitive radio is shown in the Figure 3.3. Cognitive radio continuously monitors the spectrum to identify the spectrum holes also called unused frequency bands. These spectrum holes can be used by secondary users without creating any problem to the licensed users. Once the spectrum holes are identified it can be dynamically accessing the spectrum. Dynamic spectrum access allows the secondary user to utilize spectrum temporarily which improves the spectrum utilization. Cognitive radios learn the environment using AI or some machine learning algorithms which will analyze the spectrum transmission parameters and predict future spectrum availability. The working principle of cognitive radio is shown in the Figure 3.3.

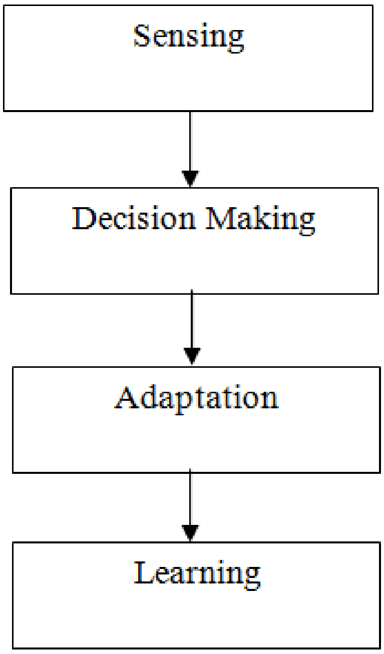


Figure 3.3 Working of Cognitive radio

In the sensing steps the cognitive radio gathers the information about which frequency band is currently used and which one is left idle.

In the decision-making step, based on the sensed information, cognitive radio will determine which available frequencies can be used without interfering the licensed user. In the adaption steps, it will change some parameter like power level, modulation and the frequency scheme to enhance the performance without any interference. Finally in the learning steps, cognitive radio can learn from past spectrum use and update their decision-making process for future communication.

3.10.1 Application of Cognitive Radio

- **Emergency service:** In times of emergency, cognitive radio help by providing reliable communication.
- **Wireless Networks:** It can be used for improving the Wi-Fi performance, cellular networks and other communication system.

- **TV White Space:** Unused portion of the TV spectrum can be accessed by cognitive radios. It is also used for providing internet services in rural areas.
- **Military Services:** Cognitive radios can also be used in the military services for secure communication where radio activities are essential.
- **Internet of Things (IoT):** Cognitive radio can upgrade the IoT network ensuring consistent performance for the IoT devices.

Check Your Progress –II

3. Multiple Choice Questions

(i) The use of cellular system is

(a) Fully automated
(b) Regulated
(c) Co-related
(d) User initiated

(ii) The channel carries a voice or data connection between users is known as

(a) Control channel
(b) Bus channel
(c) Traffic channel
(d) Frequency channel

(iii) The procedure for changing the assignment of a mobile unit from one base station to another as the mobile moves from one cell to another is known as

(a) Change allocation
(b) Cell assignment
(c) Handoff
(d) Call mobility

(iv) The advanced form of software defined radio is

(a) FM radio
(b) AM radio
(c) TDM radio
(d) Cognitive radio

4. State Whether True or False

(i) Control channels are used to exchange information for establishing a relationship between a mobile unit and the nearest base station.

(ii) Cells continuously broadcast same frequency bands.

(iii)SDR cannot be used for military and emergency services.

(iv)Cognitive radio uses AI and machine learning techniques.

(v) SDR can support multiple frequency bands.

3.11 SUMMING UP

- Spectrum allocation refers to the regulation and distributions of electromagnetic spectrum by the regulatory bodies to confirm the efficient use of Radio spectrum within the range of electromagnetic frequencies for any telecommunication system.
- It is recommended that higher frequencies must be assigned for mobile communications and satellite services.
- Electromagnetic spectrum being a global resource, international agreements as well as coordination is essential.
- Scarcity of radio spectrum refers to the limited availability of the usable spectrum relative to the huge demand of wireless communication services.
- The capacity of the cellular system refers to the maximum number of users or devices that are supported within a specified range.
- The objective of frequency reuse is to use the same frequency band in multiple cells at some distance from one another.

- The channel assignment problem can be solved by some factors like frequency reuse, interference management, fixed and dynamic channel assignment, graph coloring etc.
- The use of cellular system is fully automated. So, there is no any action requirement from the user for initiating the calls.
- There are two types of channels available between the mobile unit and the base station: control channel and traffic channel.
- Control channels are used to exchange information for establishing a relationship between a mobile unit and the nearest base station and traffic channels carry a voice or data connection between users.
- Call between two mobile users within an area is controlled by a single mobile telecommunications switching office (MTSO).
- Handoff ensures that the user's mobile device maintains a continuous connection during its movement through different coverage areas.
- The main parameter used to make handoff decision is the measurement of the signal strength from the mobile unit at the base station.
- Software Defined Radio (SDR) is a special type of communication system where the hardware components are replaced by running software on general purpose computers.
- The main purpose of cognitive radio is to enhance the spectrum efficiency for detecting the available channels and adjusting its transmission parameters without causing interference to licensed users.

3.12 ANSWER TO CHECK YOUR PROGRESS

1. (i) (d) (ii) (a) (iii) (b) (iv) (d)

2. (i) True (ii) False (iii) True (iv) False
   (v) True

3. (i) (a) (ii) (c) (iii) (c) (iv) (d)

4. (i) True (ii) False (iii) False (iv) True
(v) True

3.13 POSSIBLE QUESTIONS

1. What is spectrum allocation policy? How is it implemented?
2. What is scarcity of radio spectrum?
3. Explain the different factors of scarcity of radio spectrum.
4. How can you express the capacity of the cellular system?
5. What is bandwidth of a channel?
6. What is frequency reuse?
7. Explain the frequency borrowing and cell splitting techniques.
8. How is the channel assignment problem related to the frequency band?
9. What are the different types of channels available between the mobile unit and the base station?
10. Explain the steps of a mobile cellular call.
11. Explain handoff and location management in mobile communication.
12. What are the reasons for occurring handoff?
13. What is Software Defined Radio (SDR)?
14. What are the advantages of SDR?
15. What is Cognitive radio? Explain its architecture.
16. Explain the working principle of cognitive radio.

3.14 REFERENCES AND SUGGESTED READINGS

- Stallings W.; *Wireless Communication and Networking*;
- Theodore, Rappaport S.; *Wireless Communications, Principles, Practice*;
- Matthew S Gast; *802.11 Wireless Networks*;

- Feher K.; Wireless Digital Communications;
- Tse D. & Vishwanath P.; *Fundamentals of Wireless Communication*; Cambridge University Press

***

BLOCK- II

WIRELESS NETWORKING

Unit 1: Multiple Access Techniques for Wireless Communication

Unit 2: Telephone Networks

Unit 3: Wireless Data Services-I

Unit 4: Wireless Data Services-II

Unit 5: Wireless LAN Technologies

Unit 6: Advanced Wireless Technologies

Unit 7: 802.11

UNIT- 1

MULTIPLE ACCESS TECHNIQUES FOR WIRELESS COMMUNICATION

Unit Structure:

1.1 INTRODUCTION

All multiple access techniques have been developed keeping in the mind the divergent advantages offered through digital technology. In this unit, we will discuss about various multiple access schemes from different aspects. Here we will discuss the Frequency Division Multiple Access (FDMA), Time Division Multiple Access(TDMA), Code Division Multiple Access(CDMA) and Space Division Multiple Access (SDMA) schemes. We will also discuss about Spread Spectrum Multiple Access (SSMA), Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS). The packet radio access scheme and the working of some packet access radio-protocols will also discuss in this unit

1.2 OBJECTIVES

After going through this unit learners will be able to

- *understand* the concept of different multiple access schemes;
- *learn* about the advantages and disadvantages of FDMA,TDMA, CDMA and SDMA;
- *understand* the concept of SSMA, DSSS and FHSS;
- *understand* the concept of packet radio access;
- *learn* about the different characteristics of packet-radio-access protocols.

1.3 MULTIPLE ACCESS SCHEME

Multiple access schemes allow mobile users for sharing the radio resources to gain high quality performance. The mechanism of medium access control can regulate user's access to the medium using frequency division multiplexing (FDM), time division multiplexing (TDM), code division multiplexing (CDM) and packet radio access scheme. In wireless mobile system, the radio spectrum is divided into a large number of narrowband channels for use in frequency division duplex (FDD) to provide frequency division multiple accesses (FDMA). But in the time division multiple access, user can share same radio channel in a fixed time slot. In case of wideband transmission large numbers of transmitters are allowed to transmit using the time division multiple access (TDMA) or code division multiple access (CDMA). Some basic concepts of multiple access schemes are briefly described below.

1.3.1 Frequency Division Multiple Access (FDMA)

In FDMA, the allocation of frequencies to the transmission channel is done according to the FDM scheme. This FDM scheme is either in a fixed or dynamic pattern. In the frequency division duplex (FDD) system the users are assigned a pair of suitable voice channel for forwarding and reverse transmission simultaneously. In FDMA, each transceiver simultaneously transmits and receives radio signals with a proper separation between the signals for avoiding any interference. FDMA is usually implemented in the narrow band system. FDMA uses continuous transmission and requires less overhead for link improvement. To prevent interference between adjacent frequencies, a small frequency gap termed as “guard bands” is introduced in FDMA.

Advantages of FDMA:

- **Simplicity**: FDMA is relatively simple to implement and it does not require any complexity for sending and receiving signals.
- **Minimum Interference:** Since each user is allocated distinct frequency, so the chance of occurrence of interference is very low.
- **Continuous Transmission:** FDMA supports continuous transmission without any need for time-based allocation.

Disadvantages of FDMA:

- **Inefficient bandwidth utilization:** Since the user is allocated a fixed bandwidth, so bandwidth is waste if user is not continuously transmitting data.
- **Limited scalability:** FDMA supports limited number users due to the finite spectrum and frequency channels.
- **Guard band required:** Requirement of guard band reduces the overall spectrum efficiency. Guard band is waste due to this gap.

1.3.2 Time Division Multiple Access (TDMA)

TDMA offers a scheme by allocating certain time slots for communication through the time division multiplexing. This scheme provides users a fixed time slot in cyclic manner. Each frame contains N number of time slot to accommodate N number of users. 8-slot TDMA scheme is used in a GSM system which will increase the number of available channels by eight times. Figure 1.1 shows a FDMA/TDMA/FDD scheme used in GSM system.

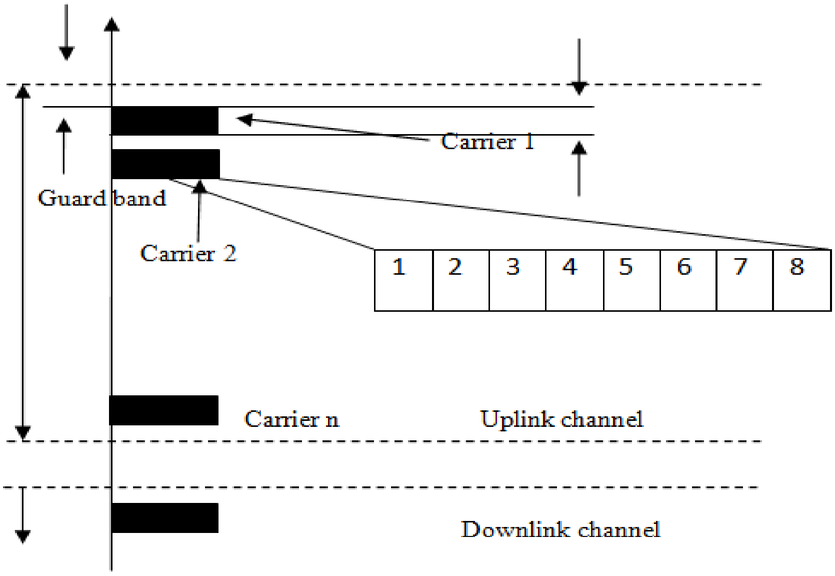


Figure 1.1 FDMA/TDMA/FDD in GSM

In FDMA, users are assigned distinct frequencies, but in TDMA users can share same frequency in different time slots. This will prevent overlapping and interferences among the users. Since the system assigns a precise timing, TDMA must ensure synchronization between the base station and all the devices. TDMA is efficient in terms of bandwidth utilization because multiple users can share same frequency without any noise or interferences

Advantages of TDMA:

- **Efficient use of frequency spectrum:** TDMA allows multiple users with same frequency band in different time slots.
- **Error control:** As time is managed in fixed slots, so error is less in TDMA.
- **Compatibility:** TDMA can be combined with other access methods.

Disadvantages of TDMA:

- **Synchronization required:** In TDMA synchronization is required for the channels.
- **Waiting time:** Waiting time may introduce some delay, especially in systems with large number of users.

1.3.3 Code Division Multiple Access (CDMA)

TDMA system use a large number of frequency band for the fixed time allocation. But, in CDMA system multiple users share the same frequency band at the same time. Users are separated by a corresponding unique pseudorandom orthogonal code sequence (PN code). Here, all users use the same frequency band with different PN codes. At the receiving end, the required channel is decoded with the same PN code. In CDMA, the receiver signal from closer mobile increases the noise for a weak signal coming from relatively distant mobiles and this will reduce the receiving probability. This causes near-far problem and can be solved by the power control technique. Since CDMA uses same frequency band to its neighboring cells, it can use microscopic spatial diversity to provide handoff with the help of mobile switching centre. This will reduce the multi path fading as the signal is spread over a large spectrum. Reducing the interferences will increase the capacity of the CDMA system. For this reason, CDMA can be implemented with a given time slot through time division multiplexing in a cell.

Advantages of CDMA:

- **Efficient use of spectrum:** CDMA allows multiple users to share same frequency band without any interference.
- **Error control:** CDMA is more resistant in controlling the interference and multipath fading.
- **Security:** CDMA is more secure in comparison to the multiple access techniques
- **Reduce call drop rates:** CDMA allows smooth transition between the base stations.
- **Clear voice quality:** In CDMA system voice quality is clearer and more distinct.

Disadvantages of CDMA:

- **Complexity:** CDMA system is complex in terms of infrastructure and processing.
- **Power control:** Each connecting device in CDMA requires adjusting the transmission power in real time to avoid the interference or noises.

1.3.4 Space Division Multiple Access (SDMA)

SDMA controls the radio signal for each user in the space. For this purpose, SDMA uses a spot beam antenna. In this scheme, different antenna beam is generated for the coverage of different areas of the cells. In some of the cases, the sectorized antennas can also be used in SDMA. The spot beam may also be changing through the programmable beam steering antennas. This beam steering antenna will steer energy in the direction of the user and reduce the interference from the other user. A well-focused beam at the base station can spatially filter each desired user properly to improve reverse link. It will provide a benefit to the subscribers to work with less battery power. Figure 1.2 shows that n users are accommodated on the same frequency in omnidirectional antenna system. Again, in the Figure 1.3, the same number of users can be placed in a smaller space which will be covered by the sectored antennas. Thus, it will increase the overall capacity by three times in comparison to omnidirectional antenna.

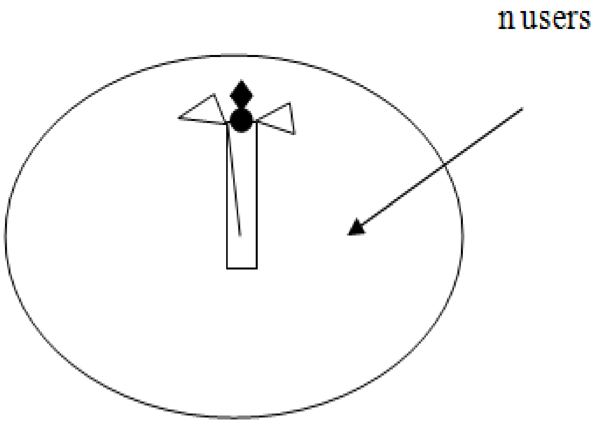


Figure 1.2 SDMA using omnidirectional antenna

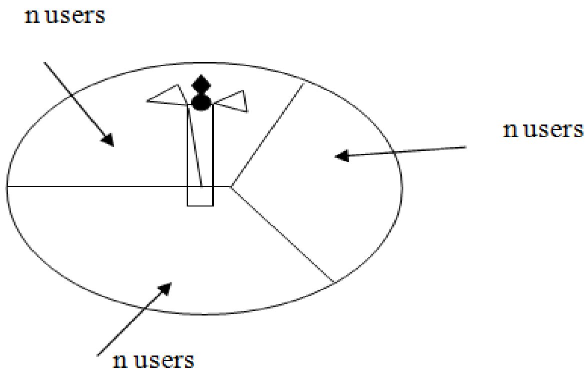


Figure 1.3 SDMA using sectored antenna.

Check Your Progress-I

1. **Multiple Choice Questions**

(i) In FDMA, the allocation of frequencies to the transmission channel is according to the

(a) TDM scheme
(b) FDM scheme
(c) CDM scheme
(d) None of the above

(ii) A frequency gap between two adjacent frequencies is known as

(a) Frequency gap
(b) Channel gap
(c) Guard band
(d) Time gap

(iii) A fixed time slot is given in

(a) FDMA
(b) CDMA
(c) SDMA
(d) TDMA

(iv) In CDMA, users are separated with

(a) PN code
(b) SN code
(c) Frequency code
(d) Channel code

(v) Multipath fading is reduced on

(a) CDMA
(b) TDMA
(c) FDMA
(d) None of the above

2. State Whether True or False

(i) FDMA is usually implemented in the narrow band system.

(ii) To prevent the interference TDMA scheme uses guard band.

(iii) In TDMA scheme, a user is given a fixed time slot in a cyclic fashion.

(iv) Antennas cannot be used in SDMA scheme.

(v) In CDMA, all users use the same frequency band with the same PN code.

1.3.5 Spread Spectrum Multiple Access (SSMA)

SSMA allows multiple users to share same frequency spectrum simultaneously using spread spectrum technology. SSMA is used in a system like cellular network, GPS and Wi-Fi network. In SSMA, the signal is spread across a wider frequency band for which it makes it more resistant to narrowband interfaces. This is the reason why SSMA allows multiple users to share the same communication channel. This can be achieved by code division and time or frequency division.

Code division: Users are assigned unique codes which are often called spreading codes and assigned signals are separated based on these codes. This is similar to CDMA technique.

Time or frequency division: SSMA can also be achieved by splitting the bandwidth into small parts in terms of time and frequency.

Two common techniques for SSMA are as follows:

Direct Sequence Spread Spectrum (DSSS):

In DSSS each bit in the original signal is represented by multiple bits in the transmitted signal, using a spreading code. One technique for DSSS is to combine the binary information with the spreading code bit stream using an XOR. Two general categories of spreading sequences have been used one is PN sequences and the other is orthogonal codes. In DSSS CDMA systems, both the PN and orthogonal codes have been used.

Frequency Hopping Spread Spectrum (FHSS):

In FHSS, signal is broadcast over a random series of radio frequencies hopping from frequency to frequency at a fixed interval of time. This method involves rapidly changing the carrier frequency according to the predefined pattern. This will help avoiding the interference and improve the security.

1.4 PACKET RADIO ACCESS

Medium accesses use fixed assignment methods and are efficient for a steady flow of data traffic. But due to the bursty traffic these dedicated channels are the waste of resources during the absence of data and thus mobile calls are more costly if bill is charged on the basis of call duration. The packet radio is preferable for solving the problem of bursty traffic. Packet radio access to the medium either randomly or in some coordinated fashion. The random-access scheme does not require any call set up procedure. In this access scheme the subscriber uses a contention technique to transmit the data packet to a common channel and senses the acknowledgement for a successful transmission. In case of any collision detected the sender resends the data after a random interval of time but that is greater than the round-trip delay time of the network. In this way, a large number of users can access the medium with the least overhead or control mechanisms. This access method is known as pure ALOHA which is shown in the Figure 1.4. The pure ALOHA can be evaluated on the basis of average delay (*D*) and the throughput (T). In random access if a data packet is of duration τ is sent at time t_1, and then the data packet from the other user must be after $t_1 + \tau$ to avoid any collision between the packets.

The traffic occupancy for the packet radio can be expressed as shown in the equation (1.1)

$$R = \lambda\tau \text{ ……………………….(1.1)}$$

R → shows the channel utilization and lies between 0 and 1.

The normalized throughput (T) can be given as offered load (R) times the probability of successful transmission (P_r). The probability of n packets is generated by the subscriber for a Poisson distribution can be shown as the equation (1.2)

$$P_r(n)=R^n e^{-R/n!} \text{.......................................}(1.2)$$

From the above equation, the radio access protocol can be found as random access, scheduled access or hybrid access according to the access scheme used. In the random-access, users send data without any coordination between them. In the scheduled access, the users transmit messages within some allocated time slots and the combination of these two schemes is known as the hybrid radio access.

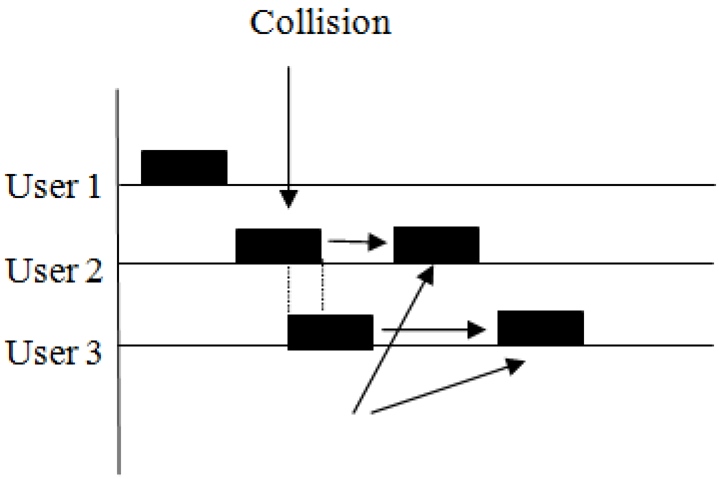


Figure 1.4 Pure ALOHA protocol

In case of pure ALOHA, the vulnerable time is 2τ. During this interval, probability of packet generation can be expressed as the equation (1.3).

$$P_r(n) = \frac{(2R)^n e^{-2R}}{n!} \text{...}(1.3)$$

Pure ALOHA was refined by introducing some time slots greater than the packet duration time. For these time slots users have the facility to synchronize and be allowed to transmit at the beginning of the time slot. This will prevent the partial collision and termed as the slotted ALOHA protocol which is shown in the Figure 1.5. The slotted ALOHA combined with TDMA is referred as the reservation ALOHA (R-ALOHA) protocol which is shown in the Figure 1.6. In R-ALOHA protocol, some packets slots are assigned with some priority and it is possible for users to reserve the slots for future transmission. Users can transmit these packets either permanently or on request. In the R-ALOHA scheme there exists reservation period followed by a transmission period. To reserve a transmission slot, a small duration data packet is sent. This will cause a larger delay but provide a better throughput. Sometimes the packet reservation multiple access is used in an implicit reservation scheme. The slots forming a frame are used to provide access to subscriber. Later the status of the occupied slots is broadcasted from the base station. All the accessing users compete for the empty slots and it will be allowed to access if there is no any collision. Finally, the status is updated for the next frame status broadcasting. If there is a collision then the present status is retransmitted for the competition for the next frame.

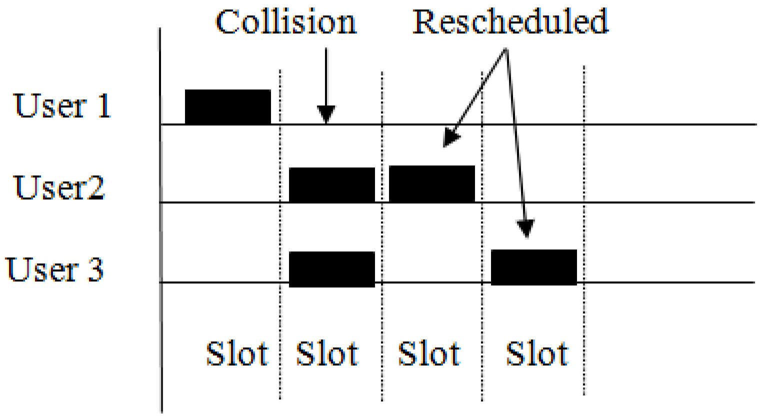


Figure 1.5 Slotted ALOHA protocol

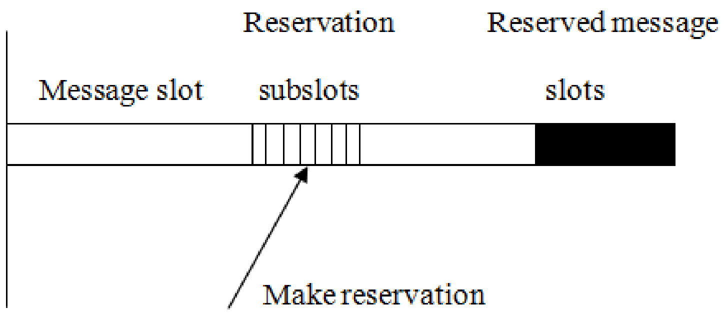


Figure 1.6 Reservation ALOHA

1.5 MULTIPLE ACCESS WITH COLLISION AVOIDANCE (MACA)

Multiple Access with collision avoidance (MACA) schemes solve the problem of hidden terminal of the wireless medium. Collision may be occurring if more than one terminal sends the RTS(request to send) in the same time. In the wireless communication, the channel or the carrier senses multiple access with collision avoidance (CSMA/CA) protocol. In this situation, clients wait for a random amount of time before trying to resend after the collision. CSMA/CA reduces the collision using fragmentation. In fragmentation CSMA/CA sends many smaller frames instead of one large frame. This will reduce the probability of collisions but adds some overheads. These RTS/CTS and fragmentation schemes are used in wireless standard 802.11b. Another popular channel access method is polling. In the polling method, each computer is polled in sequence if it wants to transmit its data. In case of answer is “yes” then that particular user is permitted and the other user is kept waiting. In this way, users can send their messages in a proper sequence order and as a result the collision is prevented.

Check Your Progress-II

3. (i) The packet radio is preferable for solving the problem of

(a) Coding error
(b) Packet error
(c) Both Coding and Packet errors
(d) Burst traffic in the signal

(ii) The combination of random access and the scheduled access known as

(a) Hybrid radio access
(b) End radio access
(c) Multiple radio access
(d) None of the above

(iii) The slotted ALOHA combined with TDMA is referred as

(a) R-ALOHA
(b) Term-ALOHA
(c) Pure-ALOHA
(d) All of the above

(iv) The problem of hidden terminal of the wireless medium is solved by

(a) Protocol
(b) Base station
(c) BACA
(d) MACA scheme

(v) Polling is a

(a) Selection method
(b) Channel access method
(c) Channel allocation method
(d) Channel split method

1.6 SUMMING UP

- Multiple access schemes allow many mobile users for sharing the radio resources to gain the high and good quality performance.
- The mechanism of medium access control can regulate user access to the medium using the frequency division multiplexing (FDM), time division multiplexing (TDM), code division multiplexing (CDM) and packet radio access scheme.

- In FDMA, the allocation of frequencies to the transmission channel is according to the FDM scheme and FDM scheme is either in a fixed or in dynamic pattern.
- FDMA is usually implemented in the narrow band system and it uses continuous transmission and requires less overhead for link improvement.
- TDMA offers a scheme by allocating certain time slots for communication through the time division multiplexing and this scheme is efficient in terms of bandwidth utilization because multiple users can share same frequency without any noise or interference.
- In CDMA system, multiple users share the same frequency band at the same time and users are separated by a corresponding unique pseudorandom orthogonal code sequence (PN code).
- Space Division Multiple Access (SDMA)controls the radio signal for each user in the space.
- In the SDMA scheme, different antenna beam is generated for the coverage of different areas of the cells.
- SSMA allows multiple users to share same frequency spectrum simultaneously using spread spectrum technology.
- The common techniques for SSMA are Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).
- The packet radio is preferable for solving the problem of bursty traffic it accesses to the medium either randomly or in some coordinated fashion.

- In the packet radio access scheme, the subscriber uses a contention technique to transmit the data packet to a common channel and senses the acknowledgement for a successful transmission.
- Multiple access with collision avoidance (MACA) schemes solves the problem of hidden terminal of the wireless medium.
- In the wireless communication, the channel or the carrier senses multiple access with collision avoidance (CSMA/CA) protocol.
- CSMA/CA protocol reduces the collision using fragmentation. In fragmentation, CSMA/CA sends many smaller frames instead of one large frame.

1.7 ANSWER TO CHECK YOUR PROGRESS

1. (i) (b) (ii) (c) (iii) (d) (iv) (a) (v) (a)
2. (i) True (ii) False (iii)True (iv) False (v) False
3. (i) (d) (ii) (a) (iii) (a) (iv) (d) (v) (b)
4. (i) False (ii) True (iii) False (iv) True (v) True

1.8 POSSIBLE QUESTIONS

1. What are the purposes of multiple access schemes?
2. What is FDMA? How is it implemented?
3. What are the advantages and disadvantages of FDMA?
4. What is TDMA? Explain the advantages and disadvantages of TDMA.
5. Explain the CDMA in comparison to the TDMA and FDMA.

6. Explain the advantages and disadvantages of CDMA scheme.
7. What is SDMA? What are different types antennas used in SDMA?
8. What are the two common techniques of SSMA?
9. What is packet radio access? How is it implemented?
10. Differentiate between pure ALOHA and slotted ALOHA.
11. Explain the working of Reservation ALOHA(R-ALOHA).
12. How is CSMA/CA protocol implemented in wireless communication?

1.9 REFERENCES AND SUGGESTED READINGS

- Stallings W.; *Wireless Communication and Networking*;
- Theodore, Rappaport S.; *Wireless Communications, Principles*, *Practice*;
- Matthew S Gast; *802.11 Wireless Networks*;
- Feher K. ; Wireless Digital Communications;
- Tse D. & Vishwanath P. ;*Fundamentals of Wireless Communication*; Cambridge University Press

***

UNIT- 2
TELEPHONE NETWORKS

Unit Structure:

2.1 INTRODUCTION

The field of telecommunications is advancing rapidly, leading to significant improvements in wireless communication technologies and services. Fixed telephone networks, or landline networks, have been the foundation of global voice communication. These networks use physical infrastructure like twisted pairs or fiber-optic cables to create dedicated user connections and use pulse and touch-tone to dual-tone frequencies for communication. These networks convert the analog signals in their transmission line into digital signals. They also need to be switched to different networks since it is a fixed setup, so there are multiple short distances and direct end-to-end connections. So, when connecting between different local setups, the signals must travel through multiple local networks before reaching the desired end. But even though fixed networks offer stable communication, they lack mobility and face challenges in meeting dynamic, large-scale connectivity needs.

To overcome these difficulties, wireless networks were introduced, revolutionizing modern communication by eliminating the necessity for physical connections. Instead of physical medium, they use radio waves, satellites, and cellular infrastructure to facilitate data transmission, resulting in greater mobility and scalability. This flexibility mainly arises due to the absence of multiple small local direct connections, and a single end user can connect directly to the central server, making long-distance communications more direct and faster. Further, these networks support various services, from mobile voice calls and text messages to high-speed internet access and real-time data applications. As wireless technology continues to evolve, it has become the predominant communication method, supporting applications in telecommunications, healthcare, transportation, and many more.

This unit will examine the differences between wireless and fixed telephone networks. We'll explore their unique architectures with an insight into the benefits as well as the limitations. We'll also break down the basic ideas of traffic routing in wireless networks, including circuit and packet switching, which play a crucial role in making data transmission run smoothly. Further, we'll dive into the X.25 protocol, one of the first standards for packet-switched networks, to see how it helps ensuring reliable data communication.

2.2 OBJECTIVES

After studying this chapter, you will be able to

- *differentiate* between wireless and fixed telephone networks, their architectures, advantages, and limitations.
- *explain* Traffic routing in wireless networking by analyzing the principles of circuit and packet switching.
- *understand* the X.25 protocol's structure, functionality, and role in packet-switched data communication.
- *examine* network efficiency and performance and how switching methods impact data transmission, reliability, and speed.
- *analyze* the evolution of wireless communication and how early technologies like X.25 impacted the development of modern network standards.

2.3 WIRELESS VS FIXED TELEPHONE NETWORKS

Progress in mobile communications has resulted in the growth of wireless and fixed telephone networks, each addressing unique needs and functions. Although these networks differ significantly in technology, characteristics and setup, their common goal is to facilitate communication. Let's explore the key differences between these two types of networks.

Stop to Consider

The first-ever mobile phone call was made in 1973 using a 2.5-pound device, while fixed telephone networks date back to the late 19th century.

2.3.1 Transfer of Information

Fixed telephone networks transmit data using specific physical infrastructure, incorporating a mix of landline connections which includes fiber optic cables, copper cables, microwave links and satellite links. These connections provide stable and reliable communication channels, making them ideal for uninterrupted conversations. On the other hand, wireless networks utilize radio frequency (RF) links for data transfer. Unlike fixed infrastructure, wireless networks adopt a dynamic, decentralized model, transmitting information through base stations and antennas. The absence of physical connections makes wireless networks more flexible and adaptable for mobile communication.

2.3.2 Adaptability and Flexibility

Fixed networks encounter challenges due to their dependence on physical infrastructure. Enhancing network capacity or connectivity often requires the installation of additional cables such as high-capacity fiber optic or coaxial cables that leads to significant costs and delays. This limitation renders fixed networks less suitable in environments that demand quick adjustments or mobility. In contrast, wireless networks offer considerable flexibility, rapidly adapting to user location and density shifts. They enable seamless communication as users move across different cells or regions, aided by advancements like dynamic frequency allocation and automatic base station reassignment. This adaptability is essential for facilitating mobile communication in urban and rural settings.

Stop to Consider

Fixed networks rely on physical infrastructure for stable communication, while wireless networks use RF links for flexibility and mobility. Wireless systems adapt quickly to user movement, making them ideal for dynamic communication needs.

2.3.3 Bandwidth Availability and Constraints

The bandwidth of a fixed connection depends on the cables, which generally have a higher bandwidth range. Advanced cables, such as fiber optic cables, can enhance this, enabling high-speed data transmission suitable for data-dependent applications like high-definition video calling or enterprise-level communication. However, wireless networks often encounter a significant bandwidth limit due to the restricted RF spectrum of cellular communication. Due to this limitation, the development has led to more efficient spectrum management methods. Although, the bandwidth has been improving due to incorporating newer technological advancements in wireless networks, the wired fixed networks still remain superior in terms of stability and bandwidth quality.

2.3.4 Roaming and Mobility

Mobility is one of the main reasons for developing wireless networks instead of relying on existing fixed telephone networks. In fixed networks, a subscriber’s endpoint cannot change unless they alter the connection, which limits the use of fixed networks in dynamic scenarios. Wireless networks address this issue with built-in support for roaming across different areas, ensuring uninterrupted service for users even as they move between various base stations.

Self-Asking Question

Fixed networks rely on cables and infrastructure, while wireless networks use RF signals. How does this affect their deployment in rural vs. urban areas?

Check Your Progress

1. What is a key difference between fixed and wireless networks in transferring information?
   A. Wireless networks use fiber-optic cables
   B. Fixed networks rely on electromagnetic waves
   C. Wireless networks transmit data through the air, while fixed networks use physical cables
   D. Fixed networks cannot provide internet access
2. Fixed networks generally offer higher bandwidth than wireless networks.**(True/False)**
3. How do wireless networks maintain continuous connectivity when users move between regions?
   A. By using fixed IP addresses
   B. Through base station handoffs and mobile IP
   C. By restricting user mobility
   D. Through satellite synchronization

Answers:

1. C 2. True 3.B

2.4 TRAFFIC ROUTING IN WIRELESS NETWORKS

The main issue in efficiently handling the traffic between connected devices is the unavailability of physical connections in a wide-area network. Thus, routing is needed to determine how the data will be transmitted efficiently from one device to another. Two primary routing techniques are circuit and packet switching. These two technologies provide different ways of connecting the source with the destination device using interlinked nodes.

Fig. 2.1 illustrates a simple network with traffic switching. Starting with a host device (A or B), we connect to a destination server (D),and it must pass through a series of interconnected nodes known as switch nodes. These nodes are responsible for creating the path that links the destination to the source node. For instance, for data to travel from A to D, it may route through 4, 5, and 3, or it may also take the route from 4 to 1 to 2 to 3. Therefore, the routing must be performed as efficiently as possible to ensure minimal time and resource usage.

The intermediate nodes are normally point-to-point links, often using either frequency division multiplexing (FDM) or time division multiplexing (TDM). The sole purpose of an intermediate node is to switch data so that it receives the correct location. Generally, a network might not be fully connected, so there is a high chance of a direct connection not existing between a pair of nodes. Still, there will most likely be more than one reliable path to connect the pair indirectly. This ensures the reliability of the network.

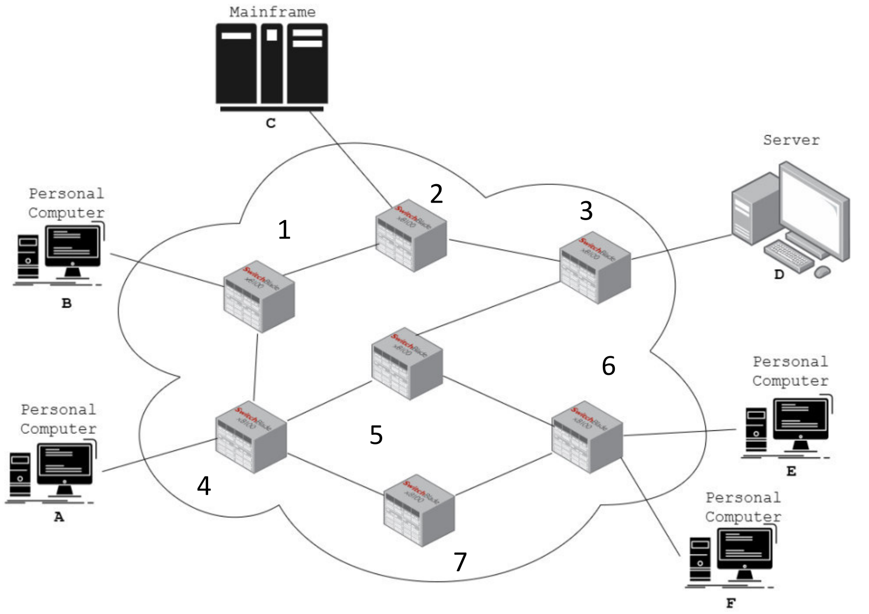


Fig. 2.1 Simple switching network

Stop to Consider

Routing Efficiency: If a network has multiple possible paths between a source and a destination, what factors determine the best path selection?

Check Your Progress

1. What is a major difference between circuit switching and packet switching?
   A. Packet switching requires a dedicated path
   B. Circuit switching divides data into packets
   C. Packet switching sends data in individual packets without a fixed path
   D. Circuit switching is only used in the internet
2. Intermediate nodes in wireless networks help ensure reliable communication by performing __________ and __________. (**Fill in the blanks**)
3. Why is packet switching preferred in modern wireless networks?
   A. It is more expensive
   B. It reduces efficiency
   C. It supports dynamic routing and efficient bandwidth use
   D. It uses outdated technology

Answers:
1. C 2. Error checking, routing 3.C

2.4.1 Circuit Switching

Circuit switching is a popular and effective technique that handles both data and voice communication. In this method of communication, a dedicated path or channel is established between the host and client node for the transmission. The path involves linking nodes to form a dedicated channel between sender and receiver. The most popular use of circuit switching is in telephone networks, where this circuit switching ensures a direct and non-stop connection between two devices until the session is terminated.

Stop to Consider

The first-ever circuit-switched telephone call was made by Alexander Graham Bell in 1876!

2.4.1.1 Communication via Circuit Switching

Circuit switching is done in three phases, regarding the above image:

1. **Circuit setup:** An end-to-end circuit path must be established before data transmission can occur. To establish a connection, the sender first looks for its directly connected node and sets it up as an interlinked node if it is not the one the sender is looking for. (Say the sender A needs to initiate a path to E, so it seems for its immediate dedicated connection, which turns out to be 4. Since the node is not E so,4 is set up as an interlinked node). Then, based on the routing data, availability, and cost, the interlinked nodes allocate a free channel towards the next interconnected node (primarily using FDM or TDM on 5) on the link. (By this, a dedicated path will be established from A to 5 through 4). This series will continue as the intermediate node establishes internal paths from multiple stations to multiple nodes. (Then, node 5 dedicates a channel to node six and internally ties that channel to the channel from node 4. Afterward, 6 completes the connection to E.) After a base path is set, a test is performed from the source node to the receiver node to check if it is available to accept the connection, and then the connection gets established.

2. **Data Transfer:** After the circuit is set up, data transfer can now occur between end nodes (say, A to D or E). Depending on the nature of the network, the transmission may be analog (voice) or binary. This data will flow directly and continuously between the sender and receiver, and the connection will remain active despite no data flow. This ensures consistent quality throughout the system. A sample path between A and E is: A-4 link, internal switching through 4, 4-5 channels, internal switching through 5, 5-6 channels, and internal switching through 6, 6-E links.

3. **Circuit disconnect:** After the transfer period, the connection is terminated by one of the two nodes. Then, the

communication path is released along with the dedicated resources (Signals will propagate to nodes 4, 5, and 6).
The best-known example of a circuit-switching network is the public telephone network.

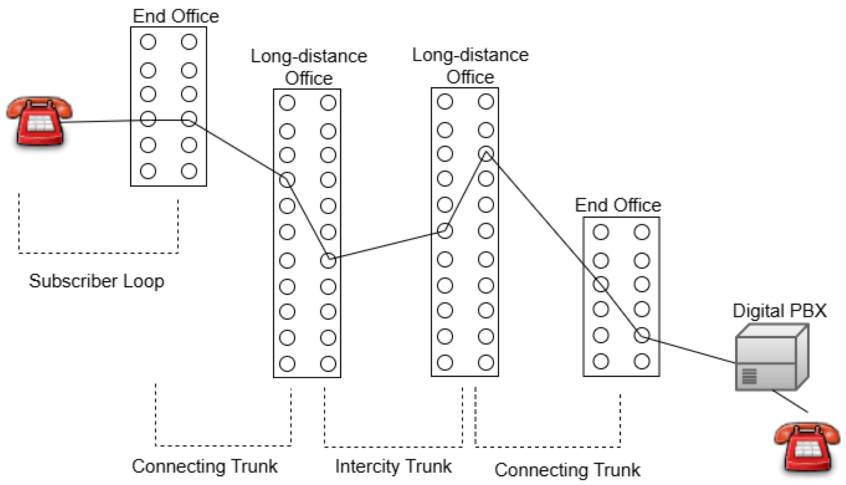


Fig. 2.2 Connection over a Public Circuit Switching Network

The above figure demonstrates a circuit-switching network on a public switched telephone network (PSTNs). Although designed and used to handle voice data only, this network evolved to work with a substantial amount of data traffic, which is converted to a digital network through a modem. Circuit switching is also extensively called private branch exchange and is used as an interconnected network of telephones in an office or resident building.

A public telecommunications network is described using four broad component categories:

1. **Subscribers**: These devices connect to the network, including telephones. Telephones represent the most advanced type of device connected to this network. However, the amount of data traffic increases due to the use of devices like modems, which handle digital bits instead of voice.

2. **Subscriber Line**: The link between the subscriber and the network (also known as a local loop). It typically uses twisted pairs and is 1 to 10 kilometers long. A subscriber line is also sometimes called a local or subscriber loop.

3. **Exchanges**: Exchanges are the switching centers responsible for managing switching protocols. An exchange that directly serves as a subscriber is an end office. Typically, an end office can connect to thousands of local subscribers. Consequently, having such a large number of subscribers leads the network to maintain over 10^8 direct links, making switching essential. Therefore, intermediate switching is employed to manage the vast number of subscribers within a local area.

4. **Trunks**: Trunks are the intermediate branches in between exchanges. They carry numerous voice-frequency circuits either through synchronous TDM or FDM and are sometimes termed carrier systems. Subscribers here connect directly to the end office, which switches the traffic across the subscriber and other exchanges. The different exchanges then manage the routing and switching across end offices.

Circuit switching has achieved universal acceptance due to its ability to match the usage of analog signal transmissions. However, in today's digital world, it has reached its capability and certain disadvantages have become more evident. Despite these inefficiencies, circuit switching remains one of the most dominant and attractive technologies in both wide-area and local-area networking.

Stop to Consider

1. Circuit switching ensures a dedicated path between sender and receiver, guaranteeing consistent quality. However, consider how this impacts network efficiency when there is no active data transmission.

2. The public switched telephone network (PSTN) is a classic example of circuit switching with modern advancements in digital communications.

Check Your Progress

1. Which of the following correctly lists the three phases of circuit switching?
   - A. Setup, Data Transfer, Disconnection
   - B. Routing, Transmission, Termination
   - C. Transmission, Reception, Disconnection
   - D. Initiation, Switching, Dropping

2. In circuit switching, the connection is released when no data is being transmitted. **(True/False)**

3. What roles do exchanges and trunks play in circuit-switched networks?
   - A. Exchanges provide user authentication, trunks carry audio files
   - B. Exchanges connect users locally, trunks carry calls between networks
   - C. Exchanges store data, trunks route SMS only
   - D. Both are used for packet-based routing

Answers:

1. A 2. False 3.B

2.4.2 Packet Switching

Extended area circuit switching was initially designed to be used in voice but has also been used in data communications. As the use of circuit switching became increasingly popular amongst data communications, some glaring problems became evident:

- Data connections don’t require fixed terminal-to-host connection switching in a circuit, as they occur in bits, which makes this very inefficient.
- Also, in a circuit-switching network, the devices require the same data rate, i.e., all the devices in the network should have the same data rate, which limits the interconnectivity of the devices and curbs the number of devices.

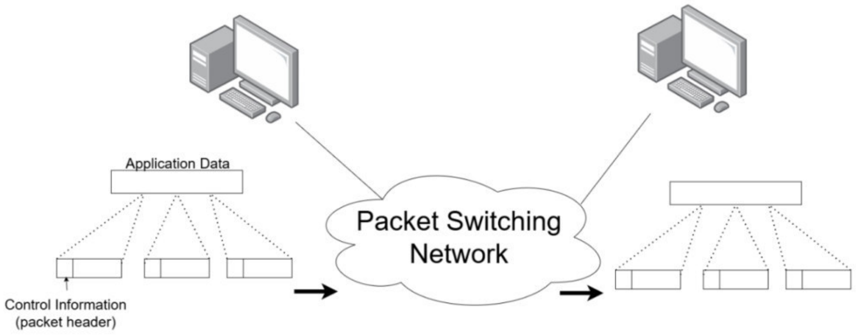
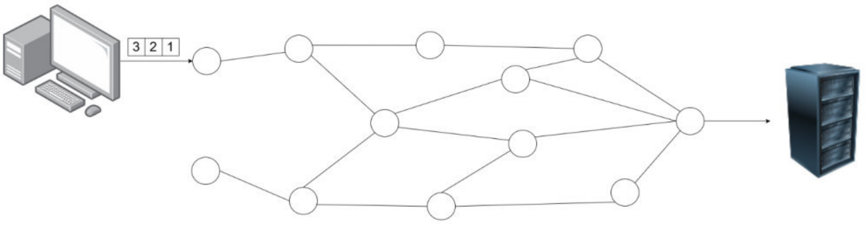


Fig. 2.3 Use of Packets

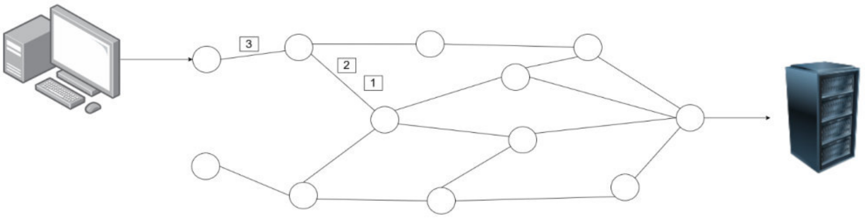
To mitigate these issues, packet switching was introduced, where a shared network is used among devices. In this system, the original data is divided into chunks known as packets. These data packets then travel independently over the packet-switching network using the most efficient available route and are reassembled at their destination. A typical upper size limit on a packet is 1000bytes. Each packet, along with a chunk of the data (or entire data for a short message), also has a header that contains essential control information, like the network details the packet needs to reach its destination. Each intermediate node holds the packet briefly to check its information header and pass it on further if it is not meant for that data.

Stop to Consider

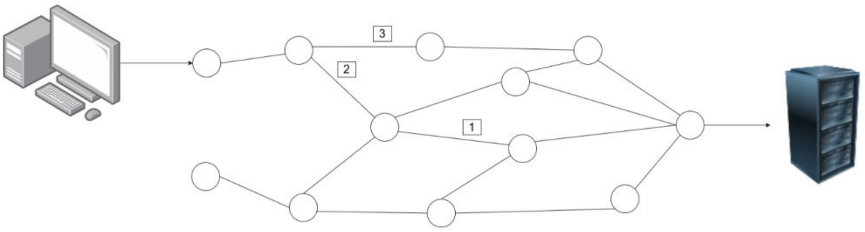
1. Packet switching was originally developed in the 1960s and became the foundation for the modern internet.
2. Unlike circuit switching, packet switching allows data to be divided into packets that take independent routes.



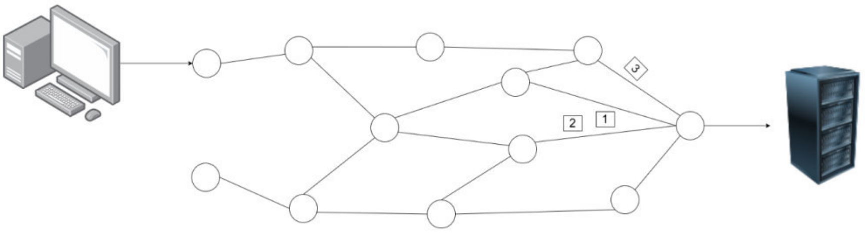
(a)



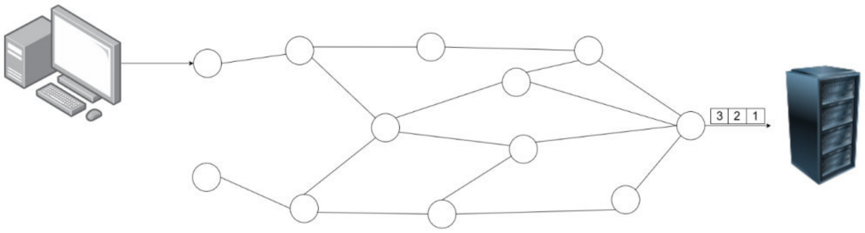
(b)



(c)



(d)



(e)

Fig. 2.4 Packet Switching Datagram approach

Figure 2.4 illustrates the essential operation of the packet-switching approach. Here, a transmitting host device sends a message as a sequence of packets (in Fig. 2.4a). Each packet contains control information that specifies the destination station. The packets are first sent to the next node, which the sending station attaches. Upon arrival at the node, each packet is briefly stored, the next leg of the route is determined, and then it is added to the link. Following this, the packets are transmitted to the next node (fig 2.4 b). Once the link becomes available, the packets move through the network to reach the intended destination. This process continues until the packet arrives at the final destination terminal (fig 2.4 e).

The primary characteristics of the packet-switching approach are:

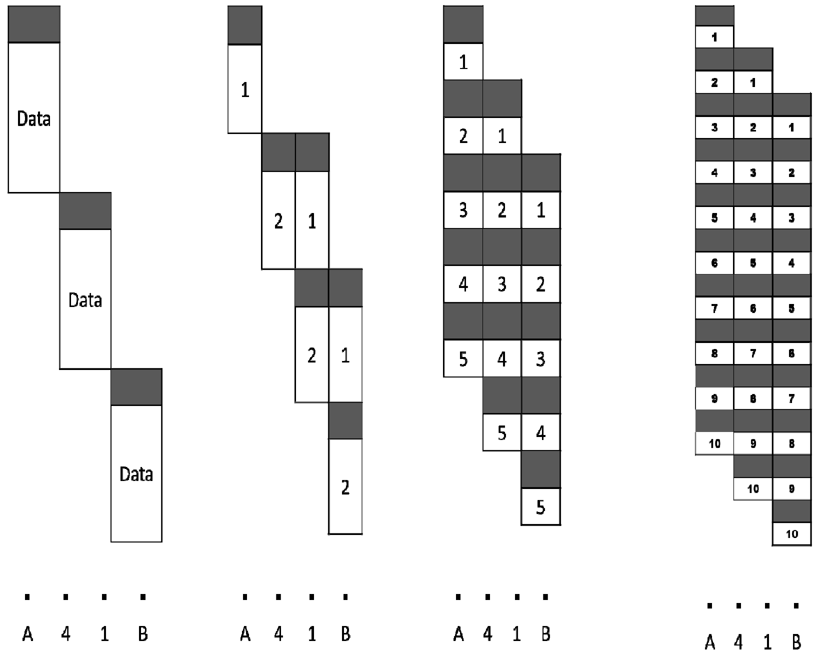
1. **Dynamic Routing**: The packets efficiently choose different routes based on availability, ensuring optimal use of resources. This also ensures that data will always reach its destination, even if a few intermediate nodes fail.
2. **Shared Network**: Several users can use the same network simultaneously, promoting optimal network utilization and reducing cost.
3. **Scalability**: Can adapt to high traffic utilization throughout the network architecture. Also, it is very easy to add/remove nodes from the topology.

Stop to Consider

1. The first large-scale implementation of packet switching was in ARPANET, which eventually led to the creation of the internet.
2. Given that each packet carries a header, which increases overhead, at what point do you think the benefits of packet switching outweigh the disadvantages?
3. If a network experiences high congestion, how do you think packet switching handles data transmission compared to circuit switching?

Packet Size:

The size of the packet can determine the transmission time. Let us understand it through an example as depicted in figure 2.5 below:



(b) 1-packet message

(a) 2-packet message

(c) 5-packet message

(d) 10-packet message

Fig. 2.5 Effect of Packet Size on Transmission Time

Consider a virtual circuit from A to B via nodes 4 and 1 (see Fig. 2.1). The message is 40 bytes long, with each packet including a 3-byte control header at the start. Consequently, sending the complete message as a single packet requires 43 bytes (3 for the header + 40 for the message), which is then transmitted from station A to node 4. Upon receiving the packet at destination host 4, it is retransmitted to node 1 and then sent to B. Ignoring switching time for simplicity, the total transmission time is 43 bytes × 3 (packet transmission instances) = 129 byte-times.

If we split the message into two packets of 20 bytes each with the 3-byte headers, node four will begin transmitting the first packet immediately after it receives it without waiting for the second part. This overlap results in a time savings of approximately 92-bytetimes. Dividing the message into five packets allows each node to start transmission even earlier, reducing the overall wait time by about 77 bytes. However, the transmission time may increase if the message is divided into too many packets. Although the packets become smaller, the fixed header size increases the number of headers, limiting the maximum number of packets into which a message can be effectively divided.

Self-Asking Questions

Consider a packet-switching network of *N* nodes, connected by the following topologies:

a) Star: One central node with no attached station; all other nodes attach to the central node.

b) Loop: Each node connects to two other nodes to form a closed loop.

c) Fully connected: Each node is directly connected to all other nodes.

For each case, give the average number of hops between stations.

2.4.3 Advantages and Disadvantages of Packet Switching over Circuit Switching

Line efficiency is noticeably improved in packet-switching environment, because multiple packets can dynamically share a single node-to-node link over time, optimizing available bandwidth. The packets are systematically queued and subsequently transmitted as quickly as possible over the link without significant delays. In contrast, in a circuit-switching environment, time on a node-to-node link is pre-allocated utilizing synchronous time division multiplexing. This reserved link may remain idle for significant periods because a portion of its time is earmarked for an unused connection, leading to potential resource wastage.

A packet-switching network is flexible, as it can adjust data rates to accommodate varying conditions. Two stations operating at differing data rates can efficiently exchange packets because each station connects to its node at the designated data rate appropriate for its needs.

When traffic escalates on a circuit-switching network, some calls may be blocked; this indicates that the network firmly refuses to accept additional connection requests until the load is manageable. In contrast, on a packet-switching network, although packets continue to be accepted, delivery delays may increase as the network handles the heavier load. Moreover, a system of priorities can be implemented in packet-switching networks. Therefore, if a node has multiple packets queued for transmission, it can judiciously send the higher-priority packets first. As a logical consequence, these packets will experience considerably less delay than those deemed lower-priority, thereby improving their chances for timely delivery.

Self-Asking Question

What is a key advantage of packet switching?

a) Requires a dedicated communication channel
b) More efficient use of bandwidth
c) Guaranteed transmission speed for all packets
d) Only supports voice communication

However, there are notable disadvantages associated with packet switching. Each time a packet passes through a packet-switching node, it incurs a delay not present in circuit switching. At a minimum, this delay includes a transmission delay equal to the packet's length in bits divided by the incoming channel rate, expressed in bits per second; this time, it represents the duration it takes to absorb the packet into an internal buffer. Additionally, there may be variable delays arising from the processing and queuing that occur within the node.

Due to the varying characteristics of the packets traveling between a given source and destination, such as differences in length and routes taken, the overall packet delay can vary substantially. This unpredictability, termed jitter, can be undesirable for specific applications, especially real-time applications like telephone voice communication and real-time video streaming, where consistent delivery is crucial. To efficiently route packets through the network, each packet must contain some overhead information, including the destination address and often sequencing information; this additional data reduces the communication capacity available for carrying user data, a concern that is typically non-existent in circuit switching once the circuit has been established and configured.

Furthermore, transferring information through packet switching involves more complex processing at each node compared to traditional circuit switching. In contrast, once a circuit is established in circuit switching, virtually no processing is needed at each switch, simplifying the overall transmission process.

Table 2.1 Difference between Packet Switching and Circuit Switching

Aspect	**Packet Switching**	**Circuit Switching**
Connection Type	Shared, dynamic connection	Dedicated connection
Resource Usage	Efficient, on-demand	Reserved, even when idle
Suitability	Burst-oriented data	Continuous data
Latency	Variable, may require reassembly	Minimal latency during session

Check Your Progress

1. What is typically included in a packet header?
   A. Usernames and passwords
   B. Destination address and sequence number
   C. Audio and video content
   D. Encryption algorithms only
2. Packet switching typically results in lower line efficiency than circuit switching.**(True/False)**
3. Packet switching enables dynamic routing, which is beneficial because it allows data to take the __________ path depending on network conditions.**(Fill in the blank)**
4. Why can jitter be a problem in real-time communications like VoIP?
   A. It makes calls more secure
   B. It causes delays and audio distortion
   C. It enhances voice clarity
   D. It increases bandwidth usage

Answers:

1. B 2. False 3. Optimal/Best 4.B

2.5 X.25 PROTOCOL

X.25, developed by (Telecommunication Standardization Sector) ITU-T, is a suite of protocols used in packet switching in computer networking. It operates on the OSI model's first three layers - the physical, data link, and network layer. This generally allows the same physical line to access numerous logical channels.

2.5.1 Key Features:

1. Packet Size: X.25 packets can carry up to 128 bytes of data.
2. Assembly and Disassembly: Data is assembled into packets at the source device (host) and disassembled at the destination device.
3. Error Handling: X.25 includes error checking and retransmission logic to ensure reliable data transfer.
4. Routing: The protocol handles network-level routing and switching of packets.

An X.25 network consists of interconnected nodes to which user equipment can connect. The user end of the network is known as Data Terminal Equipment (DTE), and the carrier’s equipment is Data Circuit-terminating Equipment (DCE). X.25 routes packets across the network from DTE to DTE. X.25 networks use the connection-mode network service.

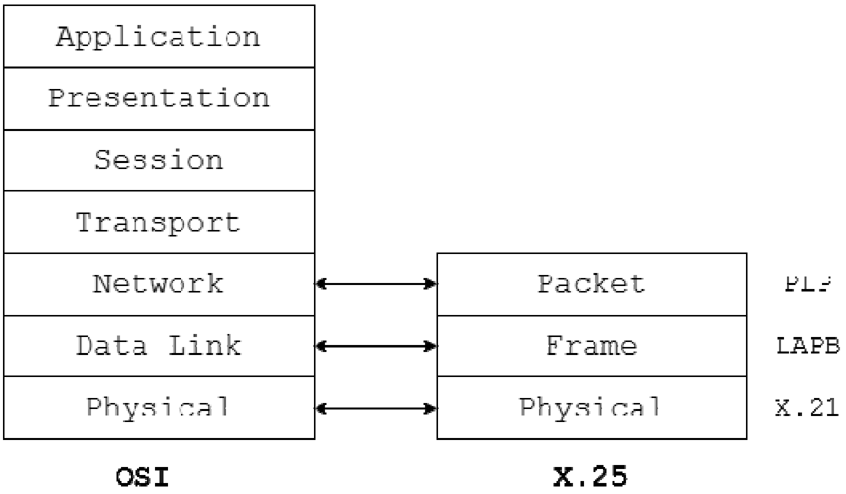


Fig. 2.6 Layer Mapping of X.25 with OSI Model

The protocol layers are briefly discussed below:

1. **Physical Layer:** This layer deals with the mechanical and electrical interfaces and the physical connections between devices. The physical layer interface of X.25 is also called X.21 bis, and this X.21 implementer is usually used for linking.

2. **Data Link Layer:** Also termed as the Frame layer, this layer ensures reliable data packet transfer. Also, it provides a communication link and error-free transmission between X.25 devices. This is done through a series of ISO High-Level-Data Link Layer (HDLC) standards called LAPB (Link Access Procedure Balanced) protocol. LAPB also uses DTE (Data Terminal Equipment) or DCTE (Data Circuit-Terminating Equipment) at the start or end of a data transmission session. This layer also checks errors at each hop, making it more error-free and bit-oriented. It also sequences the delivery of packets or data frames, making it one of the most essential parts of the X.25 protocol.

3. **Network Layer:** It is also called the packet layer in the X.25 protocol. This layer handles end-to-end communications and data delivery across DTE devices through logical addressing, packet switching, and routing. It also defines how to address and deliver the X.25 packets at end nodes on a network with the help of SVCs (Switched Virtual Circuits) or PVCs (Permanent Virtual Circuits). Packet Switching Exchange (PSE) is responsible for this layer's task of handling transmitting data packets or frames, flow control, and transfer over external virtual circuits. PSE transmits data from one

DTE device to another through the use of X.25 PSN and hence is considered the backbone of X.25 Network.

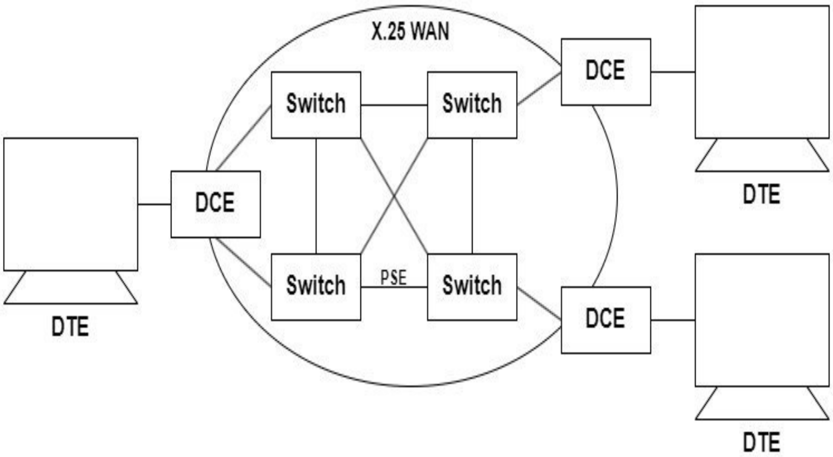


Fig. 2.7 X.25 Network Circuit

2.5.2 Uses of X.25

- X.25 transfers transparent data, particularly in asynchronous data streams generated by devices like credit card readers. These devices connect to a Packet Assembler/Disassembler (PAD) that organizes asynchronous data streams into X.25 packets for efficient transmission across the network.
- X.25 is essential to modern Point-of-Sale credit card and debit card authorization tasks.
- X.25 has been the base of developing other packet-switched protocols like TCP/IP and ATM.
- X.25 has been around since the mid-1970s, so it is well-debugged and stable, and there are no data errors on modern X.25 networks.

Check Your Progress

1. X.25 protocol uses the ______ layer for end-to-end transmission (packet). **(Fill in the blank)**
2. Which three layers of the OSI model does the X.25 protocol operate on?
   A. Physical, Data Link, Network
   B. Session, Presentation, Application
   C. Transport, Network, Data Link
   D. Data Link, Session, Application
3. What is the role of the Packet Switching Exchange in an X.25 network?
   A. It encrypts user data
   B. It manages routing, switching, and forwarding of packets
   C. It compresses all transmitted packets
   D. It only handles error detection at the physical layer
4. Error handling is essential in X.25 because it ensures reliable data transmission over potentially unreliable physical links.**(True/False)**

Answers:

1. Network 2.A 3. B 4. True

2.6 SUMMING UP

The progression of mobile communications has dramatically impacted the growth of fixed and wireless networks, each tailored to meet distinct demands. Fixed networks depend on physical infrastructure such as fiber optics and copper wires, providing dependable, high-bandwidth options for seamless communication. In contrast, wireless networks utilize radio frequencies and a decentralized model, prioritizing adaptability and flexibility for users on the move. These differences make fixed networks suitable for steady, high-speed connections, while wireless networks shine in situations that require mobility and rapid scalability.

Bandwidth and mobility are key factors that further set apart these two types of networks. Typically, fixed networks offer superior bandwidth, owing to advanced cabling like fiber optics, which supports high-speed data applications. Conversely, wireless networks face limitations from the finite radio frequency spectrum, relying on innovative spectrum management techniques to enhance bandwidth utilization. Furthermore, while fixed networks tend to limit user mobility because of their stationary endpoints, wireless networks enable unhindered roaming, allowing users to shift locations without severing communication.

Effective data routing is essential for wireless networks due to the lack of dedicated physical pathways. Concepts like circuit switching and packet switching help meet this requirement. Circuit switching, often seen in traditional telephone systems, establishes a dedicated connection between sender and receiver throughout the call. While this ensures reliable quality, it lacks efficiency in the context of contemporary digital communications. In contrast, packet switching breaks data into smaller segments that travel independently across the network, dynamically selecting the best route. This method improves resource utilization and adaptability, making it well-suited for burst-oriented data.

Yet, packet switching does come with challenges, such as varying delays and jitter, which can affect real-time applications like voice and video calls. Nonetheless, its features, including dynamic routing, shared network usage, and scalability, render packet switching more appropriate for modern networking requirements. In contrast, circuit switching still holds relevance for specific scenarios where uninterrupted and predictable communication is critical.

Lastly, protocols such as X.25 highlight early developments in packet switching, functioning across the OSI model's physical, data link, and network layers. This suite of protocols established the foundation for contemporary packet-switching methods, facilitating efficient and reliable data transmission over shared network resources. Overall, the advancement of both fixed and wireless networks and the evolution of routing methods underscores the intricate relationship between technology and communication needs.

2.7 POSSIBLE QUESTIONS

1. What is the principal application that has driven the design of circuit-switching networks?
2. Distinguish between static and alternate routing in a circuit-switching network.
3. Consider a simple telephone network consisting of two end offices and one intermediate switch with a 1-MHz full-duplex trunk between each end office and the intermediate switch. The average telephone is used to make four calls per 8-hour workday, with a mean call duration of six minutes. Ten percent of the calls are long-distance. What is the maximum number of telephones an end office can support?
4. What are some of the limitations of using a circuit-switching network for data transmission? If there is no malfunction in any of the stations or nodes of a network, is it possible for a packet to be delivered to the wrong destination? And why?
5. A circuit-switched network allocates 128 kbps bandwidth for a single connection. If 100 simultaneous connections are supported, calculate the total bandwidth required by the network.
6. In a circuit-switched network, a dedicated 64 kbps channel is allocated for a call that lasts for 2 minutes. However, during the call, the user only speaks 60% of the time. Calculate the channel utilization efficiency.
7. Explain the flaw in the following reasoning: Packet switching requires control and address bits to be added to each packet. This introduces considerable overhead in packet switching. In circuit switching, a transparent circuit is established. No extra bits are needed. Therefore, there is no overhead in circuit switching, and because there is no overhead in circuit switching, line utilization must be more efficient than in packet switching.
8. In a packet-switched network, 10 users share a 10 Mbps link. Each user transmits data at 1 Mbps for 20% of the time and is idle for the remaining 80%. Calculate the probability that more than five users are transmitting

simultaneously and determine whether the network can handle the load without congestion.

9. A 1 MB file is transmitted over a packet-switched network. Each packet has a 20-byte header. If the file is divided into packets of 1000 bytes each (including the header), calculate the total overhead incurred and the actual data transmitted.
10. What are the primary advantages of wireless networks over fixed networks?
11. Explain how bandwidth availability differs between fixed and wireless telephone networks.
12. Why do wireless networks require dynamic frequency allocation?
13. Compare and contrast fixed and wireless networks in terms of infrastructure, adaptability, and bandwidth availability.
14. How does roaming work in wireless networks, and why is it an essential feature?
15. Discuss the challenges of deploying fixed networks in developing countries and how wireless networks can bridge connectivity gaps.
16. A fiber optic connection provides a bandwidth of 1 Gbps, while a typical 4G LTE network offers a maximum bandwidth of 100 Mbps. Calculate the factor by which the fiber optic connection is superior in bandwidth capacity.
17. If a wireless network covers a 10 km radius with base stations placed every 2 km, how many base stations are needed to ensure complete coverage without signal drop-offs?
18. Compare and contrast circuit switching with packet switching regarding efficiency, reliability, and real-time communication suitability.
19. Explain the role of subscriber lines, exchanges, and trunks in circuit-switched networks.
20. Define packet switching and explain how it differs from circuit switching.
21. Discuss how packet-switching supports fault tolerance and network scalability. Provide examples of real-world applications.
22. Explain why circuit switching may lead to resource wastage compared to packet switching.

23. Describe how packet switching manages congestion compared to circuit switching.
24. Compare and contrast circuit switching and packet switching in terms of efficiency, delay, and flexibility.
25. Discuss the role of packet overhead in packet-switched networks and its impact on communication efficiency.
26. What is the difference between Switched Virtual Circuits (SVCs) and Permanent Virtual Circuits (PVCs) in X.25?
27. Why is X.25 still used in Point-of-Sale (POS) systems?
28. Discuss the advantages and disadvantages of X.25 in modern networking. How does it compare to more recent networking protocols like TCP/IP?
29. Explain the role of DTE, DCE, and PSE in X.25 communication with a suitable diagram.

2.8 REFERENCES AND SUGGESTED READINGS

1. Theodore S. Rappaport (2002), Wireless Communications -Principles Practice,2nd edition, Prentice Hall of India, New Delhi.
2. William Stallings (2009), Wireless Communications and Networks,2nd edition, Pearson Education, India.
3. Kaveh PahLaven, Prashanth Krishna Murthy (2007), Principles of Wireless Networks -A Unified Approach, Pearson Education, India.

***

UNIT- 3
WIRELESS DATA SERVICES – I

Unit Structure:

3.1 INTRODUCTION

Dedicated mobile data services were inefficient because the leading cellular systems that used circuit switching for data communications had started encountering significant difficulties in employing modem signals for advanced services. This situation created a demand for packet data services, which also facilitated wireless packet transfers. Wireless data services have revolutionized information transmission and access, allowing for uninterrupted communication over long distances without relying on physical cables. They enable real-time data exchange for various applications, including mobile internet browsing and essential enterprise communications. Early advancements in wireless data services included technologies such as Cellular Digital Packet Data (CDPD), ARDIS (Advanced Radio Data Information Service), and RAM Mobile Data, which established the groundwork for today's mobile communication networks. These systems offered packet-switched data services that ensured efficient and dependable data transmission across cellular and private radio networks. CDPD was specifically designed to work with existing cellular networks, allowing efficient packet-based communication over unused cellular channels. Meanwhile, ARDIS, developed for enterprise and governmental use, offered secure and robust wireless data transfer. RAM Mobile Data also played a pivotal role in facilitating wireless messaging and enterprise solutions.

3.2 OBJECTIVES

After studying this chapter, you will be able to

- *understand* the fundamentals of wireless data services, their significance and evolution.
- *analyse* the architecture and describe CDPD, ARDIS and RAM principles and applications.
- *explore* how enterprise, government and consumer applications utilize wireless data services, particularly CDPD, ARDIS and RAM.
- *assess* these early wireless data services' security, reliability and efficiency.

3.3 CELLULAR DIGITAL PACKET DATA (CDPD)

CDPD is a data service for first and second-generation U.S. cellular systems that utilizes an entire 30 kHz AMPS channel on a shared basis. It provides mobile packet data connectivity to existing data networks and other cellular systems without requiring additional bandwidth. CDPD takes advantage of the unused air time that occurs between successive radio channel assignments by the MSC. It is estimated that for 30% of the time, a particular cellular radio channel is unused, allowing packet data to be transmitted until the MSC selects that channel to provide a voice circuit.

CDPD directly overlays existing cellular infrastructure and utilizes existing base station equipment, making installing it straightforward and cost-effective. Furthermore, CDPD operates independently of the MSC, having its traffic routing capabilities. CDPD occupies voice channels solely on a secondary, non-interfering basis, and packet channels are dynamically assigned (hopped) to different cellular voice channels as they become free, causing the CDPD radio channel to vary over time.

Stop to Consider

1. Early ATMs and point-of-sale (POS) systems utilized CDPD for secure wireless transactions before mobile broadband became common.
2. Law enforcement extensively employed CDPD for real-time data access in patrol cars, serving as a precursor to today’s LTE-based public safety networks.

Similar to conventional first-generation AMPS, each CDPD channel is duplex. The forward channel acts as a beacon and transmits data from the PSTN side of the network, while the reverse channel connects all mobile users to the CDPD network and serves as the access channel for each subscriber. Collisions may occur when multiple mobile users attempt to access the network simultaneously. Each CDPD simplex link occupies a 30 kHz RF channel, with data transmitted at 19,200 bps. Since CDPD is packet-switched, many modems can access the same channel on an as-needed, packet-by-packet basis. CDPD supports broadcast, dispatch, electronic mail, and field monitoring applications. GMSK BT=0.5 modulation is implemented, allowing existing analog FM cellular receivers to detect the CDPD format without redesigning CDPD transmissions to easily use fixed-length blocks. User data is protected with a Reed-Solomon (63,47) block code utilizing 6-bit symbols. For each packet, 282 user bits are encoded into 378-bit blocks, allowing for the correction of up to eight symbols. Two lower-layer protocols are employed in CDPD. The mobile data link protocol (MDLP) conveys information between data link layer entities (layer two devices) across the CDPD air interface. The MDLP establishes logical data link connections on a radio channel using an address in each packet frame. It also provides sequence control to maintain the order of frames across a data link connection, along with error detection and flow control. The radio resource management protocol (RRMP) is a higher layer three protocol that manages the radio channel resources of the CDPD system and allows an M-ES to locate and utilize a duplex radio channel without interfering with standard voice services. The RRMP manages base station identification and configuration messages for all M-ES stations, supplying information that the M-ES can use to identify available CDPD channels without prior knowledge of the channel usage history. The RRMP oversees channel hopping commands, cell handoffs, and M-ES power change commands. CDPD version 1.0 employs the X.25 vast switched, many modems can access the same channel on an as-needed, packet-by-packet basis. CDPD supports broadcast, dispatch, electronic mail, and field monitoring applications. GMSK BT=0.5 modulation is implemented, allowing existing analog FM cellular receivers to detect the CDPD format without redesigning CDPD transmissions to easily use fixed-length blocks. User data is protected with a Reed-Solomon (63,47) block code utilizing 6-bit symbols. For each packet, 282 user bits are encoded into 378-bit blocks, allowing for the correction of up to eight symbols. Two lower-layer protocols are employed in CDPD. The mobile data link protocol (MDLP) conveys information between data link layer entities (layer two devices) across the CDPD air interface. The MDLP establishes logical data link connections on a radio channel using an address in each packet frame. It also provides sequence control to maintain the order of frames across a data link connection, along with error detection and flow control. The radio resource management protocol (RRMP) is a higher layer three protocol that manages the radio channel resources of the CDPD system and allows an M-ES to locate and utilize a duplex radio channel without interfering with standard voice services. The RRMP manages base station identification and configuration messages for all M-ES stations, supplying information that the M-ES can use to identify available CDPD channels without prior knowledge of the channel usage history. The RRMP oversees channel hopping commands, cell handoffs, and M-ES power change commands. CDPD version 1.0 employs the X.25 vast area network (WAN) sub-profile and frame relay capabilities for internal subnet works. Table 3.1, in the summary section, describes the link layer characteristics for CDPD.

Check Your Progress

1. CDPD transmits data at 19,200 bps over a 30 kHz channel. What is its spectral efficiency?
   A. 0.64 bps/Hz
   B. 1.6 bps/Hz
   C. 2.0 bps/Hz
   D. 3.0 bps/Hz

2. Which error correction technique was used in CDPD?
   A. Turbo Codes
   B. LDPC
   C. Hamming Codes
   D. Reed-Solomon Codes

Answers:

1. *Spectral efficiency = 19200/30000=0.64 bps/Hz*
2. *D*

3.3.1 Cellular Digital Packet Data (CDPD) Network Architecture

Figure 3.1 depicts a typical CDPD network architecture. It is important to note that subscribers (the mobile end system, or M-ES) connect through mobile database stations (MDBS) to access the internet via intermediate systems (MD-IS), which serve as both servers and routers for the subscribers. This allows mobile users to connect to the internet or the PSTN. CDPD can transport Internet Protocol (IP) or OSI Connectionless Protocol (CLNP) traffic through the I-interface.

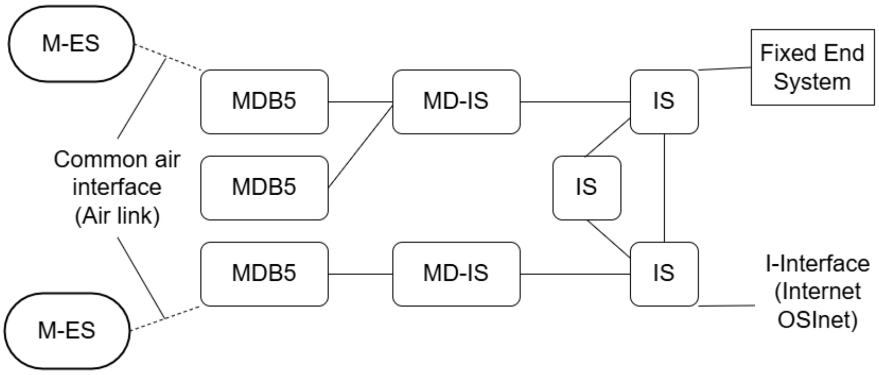

M-ES
Common air interface (Air link)
M-ES
MDB5
MDB5
MDB5
MD-IS
MD-IS
IS
IS
IS
Fixed End System
I-Interface (Internet OSInet)

Figure 3.1 The CPDP Network

The CDPD network comprises several interconnected elements that facilitate data transmission between mobile users and fixed-end systems (such as the internet or private networks). These components include:

Mobile End Station (M-ES):

1. The M-ES represents the mobile user's device, such as a laptop, handheld computer, or vehicle-mounted terminal equipped with a CDPD modem. It communicates with the network through the Common Air Interface (CAI), enabling wireless connectivity to the nearest Mobile Data Base Station (MDBS).
2. **Mobile Data Base Station (MDBS):**
   The MDBS is an access point for mobile users, a radio base station that manages the wireless link between the M-ES and the CDPD network. It dynamically utilizes unused cellular channels to transmit packet data, ensuring efficient bandwidth usage. Multiple MDBS units may be deployed across the network to provide coverage and support handoff mechanisms as users move between different areas.
3. **Intermediate Server for CDPD Traffic (MD-IS):**
   The MD-IS is a crucial intermediary in the CDPD network, handling packet switching and routing between the MDBS and the Internet Service (IS). It aggregates data from multiple MDBS units and applies compression, encryption and error correction techniques before forwarding packets to their destinations. Additionally, the MD-IS manages mobile users' authentication, billing and session maintenance.

4. **Internet Service (IS):**
   The IS (or Interconnecting Service) is a gateway between the CDPD network and external fixed-end systems, such as corporate networks, internet service providers, or other data networks. It enables seamless data exchange between mobile users and remote servers, ensuring end-to-end connectivity. Multiple IS nodes may exist in a CDPD network to provide redundancy and enhance performance.
5. **Fixed End System**:
   The Fixed End System represents external hosts or servers with which mobile users communicate through the CDPD network. These could include email servers, corporate databases, web applications, or other internet-connected services.
6. **I-Interface (Internet/OSInet)**:
   The I-Interface connects the CDPD network to the broader internet or private networks. It ensures that data packets can be transmitted beyond the CDPD infrastructure, allowing mobile users to access remote applications and services.

Stop to Consider

1. The MD-IS applies encryption and authentication before forwarding packets. How do modern mobile networks enhance security beyond these methods?
2. The CDPD architecture was one of the earliest implementations of mobile internet, allowing vehicles and field workers to access data wirelessly in the 1990s.
3. Due to its secure authentication and encryption features, CDPD was widely used by law enforcement and military units for real-time communication.

How the CDPD Network Operates

1. **Mobile Access via Common Air Interface (CAI):**
   The M-ES establishes a wireless connection with the nearest MDBS through the Common Air Interface (CAI), which

provides a standardized radio link for packet data transmission.

2. **Data Handling and Forwarding by MDBS:**
   The MDBS receives packets from the M-ES and forwards them to an appropriate MD-IS, which acts as an intelligent relay node for CDPD traffic.
3. **Packet Switching and Authentication by MD-IS:**
   The MD-IS processes the incoming data, ensuring proper routing, encryption and authentication before passing the packets to the appropriate IS.
4. **Interconnection with External Networks via IS and I-Interface:**
   The IS bridges the CDPD network and fixed-end systems, allowing mobile users to interact with Internet-based services or corporate networks via the I-Interface.
5. **Seamless Communication with Fixed-End Systems:**
   Finally, the data packets reach the fixed-end system, completing the communication process. Responses from fixed-end systems follow the same path back to the mobile user.

Check Your Progress

1. If a CDPD network has 5 MDBS units, each supporting 100 mobile users with an average data rate of 9,600 bps per user, the total data traffic handled by a single MD-IS is ______ bps.**(Fill in the blanks)**

2. Which is a key architectural difference between CDPD and modern LTE networks?
   A. LTE relies on MDBS and MD-IS
   B. CDPD supports higher data speeds
   C. LTE uses an all-IP core network, while CDPD uses circuit-switched routing
   D. CDPD has better handoff protocols

3. SIM-based authentication in LTE and 5G networks evolved from CDPD's basic authentication and encryption methods.**(True/False)**

Answers:

1. *5*100*9600=4800000 bps*
2. *C*
3. *True*

3.4 ADVANCED RADIO DATA INFORMATION SYSTEMS (ARDIS)

Advance Radio Data Information Systems (ARDIS) is a private network service provided by Motorola and IBM based on MDC 4800 and RD-LAP (Radio Data Link Access Procedure) protocols developed at Motorola. ARDIS provides 800 MHz two-way mobile data communications for short-length radio messages in urban and in-building environments and users travelling at low speeds. Short ARDIS messages have lower retry rates but high packet overhead, while long messages spread the overhead over the packet's length but have a higher retry rate. ARDIS has been deployed to provide excellent in-building penetration and large-scale spatial antenna diversity is used to receive messages from mobile users. When a mobile sends a packet, many base stations tuned to the transmission frequency attempt to detect and decode the transmission to provide diverse reception for the case when multiple mobiles contend for the reverse link. ARDIS base stations have very low functions and are responsible only for addition or removal of forward error correction code. All message transfers, even to a device on the same base station, must rise to a message switch centre. A simplified view of the ARDIS network hierarchy is shown in Figure 3.2.

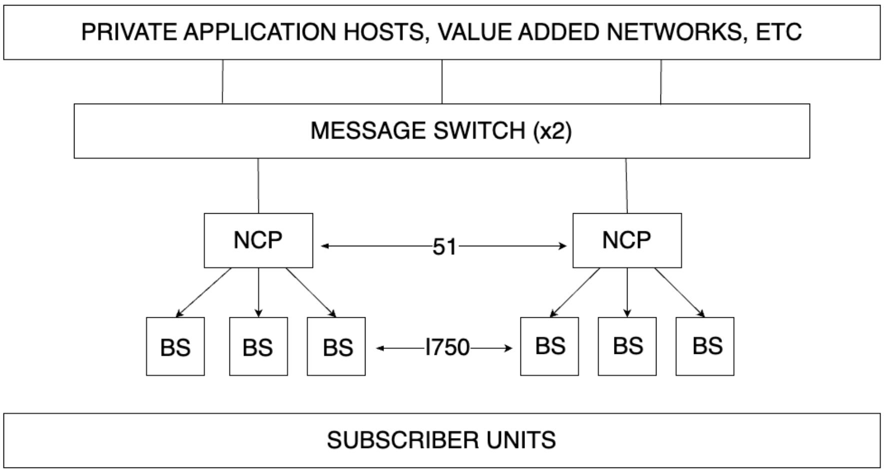


Figure 3.2TheARDIS Network Hierarchy

Subscriber units communicate with low-function base stations that act as relay points to the network communications processor (NCP). Here, all decisions are made regarding which transmitter to key (and when), whether to set busy or not, and so on. While NCPs are regionalized for control and backup, some service a single city. Until a few years ago, the subscriber unit working in Chicago was not expected to appear in New York City. ARDIS's "blue collar" subscriber base was not big roamers. Executive class users, particularly those using E-mail, forced useful changes. There is no concept of a control channel. All control rests in the NCP. The single allocated channel is used only for data transmission.

Stop to Consider

1. ARDIS has different trade-offs for short and long messages. How do modern mobile networks optimize for low latency while minimizing retries?
2. ARDIS base stations perform minimal processing, unlike modern cellular networks. How does this impact network efficiency and scalability?
3. Initially, ARDIS did not support roaming across cities. How do modern networks handle seamless roaming and what technological advancements have made it possible?

3.4.1 System Details

By ARDIS count, their 1750 ARDIS base stations cover 417 geographicareas5 (CSMA/MSAs). NCR, a nationwide user, sees it as 427 metropolitan areas, a reminder of the confusion that can creep in with these urban designations. Either way, ARDIS coverage is broader than BSWD 270 metropolitan areas.

Ignoring redundancy, 45 operational NCPs service these 1750 base stations. The wireline connection between the base station and NCP is a T1/T3 digital service arranged as shown in Figure 3.3.

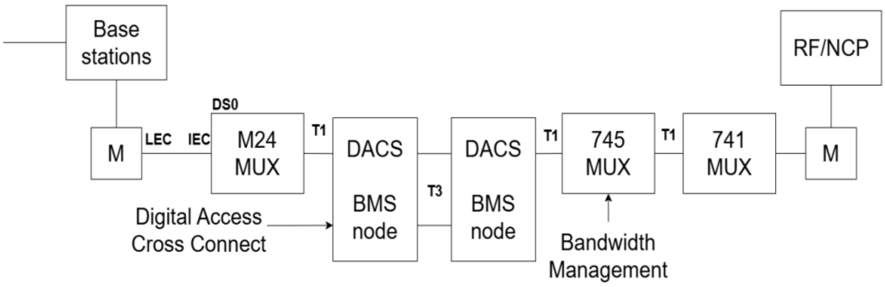


Figure: 3.3 ARDIS base station to RF/NCP wireline configuration

3.4.2 System Components and Flow

1. Base Station

- The base station serves as the initial transmission point for mobile data.
- It is connected to the system via Local Exchange Carrier (LEC) or Inter Exchange Carrier (IEC) networks.

2. Digital Access Cross-Connect

- This is a switching system that helps route digital signals efficiently.
- It allows for flexible management of the communication paths within the network.

3. M24 Multiplexer (M24 Mux)

- Converts 24 DS0 (Digital Signal 0) channels into a single T1 connection.
- This multiplexing process optimizes bandwidth by consolidating multiple data streams into one.

4. DACS (Digital Access Cross-Connect System)

- Provides switching and routing between different network nodes.
- Works with BMS (Base Management System) nodes to manage and regulate traffic.

5. BMS Node

- Acts as an intermediary for network management and traffic control.
- Ensures efficient data transfer through the system.

6. T3 Connection

- Higher-capacity transmission link (44.736 Mbps) used between BMS nodes.

- Supports large-scale data communication between different sections of the system.

7. Bandwidth Management (745 Mux & 741 Mux)

- 745 Mux: Manages bandwidth by optimizing how data flows through the network.
- 741 Mux: Further processes the data before sending it to the RF/NCP system.

8. RF/NCP (Radio Frequency/Network Control Processor)

- The final destination in this wireline configuration.
- Handled radio transmissions and network control tasks.
- Ensures proper communication between base stations and mobile users.

Thus, ARDIS base stations can ensure the detection of simultaneous transmissions, provided the users are sufficiently spaced apart. Table 3.1, in the summary section, presents some characteristics of ARDIS.

Check Your Progress

1. How does ARDIS manage load balancing and fault tolerance with 1750 base stations and 45 NCPs?
   A. Through centralized control
   B. By manually rerouting data
   C. By distributing load among NCPs and rerouting during faults
   D. It does not support fault tolerance
2. What is the difference between the M24 multiplexer and modern optical multiplexing techniques?
   A. M24 uses fiber optics
   B. Modern optical multiplexing supports far higher bandwidth with techniques like DWDM
   C. M24 uses DWDM
   D. Optical networks are less efficient than M24
3. Digital Access Cross-Connect Systems (DACS) are considered a precursor to software-defined networking (SDN).**(True/False)**

Solutions:

1. C 2. B 3. True

Self-Asking Questions

Explain how Digital Access Cross-Connect (DACS) improves network flexibility and compare it to modern packet-switching technologies.

....

....

....

3.5 RAM MOBILE DATA (RMD)

RAM Mobile Data (RMD) is a public two-way data service utilizing the Mobitex protocol developed by Ericsson. It offers street-level coverage for both short and long messages in urban environments. Ram Mobile Data was founded by Ram Broadcasting Corporation as American Mobile Data Communications, Inc. in 1988. The company's name was changed to Ram Mobile Data in 1989. RAM Mobile Data was the U.S. Operator of the Mobitex network.

Stop to Consider

RAM Mobile Data was one of the first public data services based on packet switching, a fundamental concept in modern internet and mobile networks.

While RAM supports voice and data transmission, it is primarily designed for data and facsimile use. Fax messages are sent as regular text to a gateway processor, which converts them into the appropriate format by combining them with a background page. Consequently, the packet-switched wireless transmission consists of a message of standard length rather than a larger fax image, allowing the end-user to receive what looks like a standard fax. Here are some key characteristics of the RAM mobile data service. Table 3.1, in the summary section, compares its primary characteristics with CPDP and ARDIS.

Stop to Consider

1. Given that RAM Mobile Data operated on the Mobitex protocol, how did this influence its efficiency in handling short and long messages?
2. Unlike traditional fax transmission, RAM Mobile Data converts text into a message format before transmission. How did this improve network efficiency?

Check Your Progress

1. What was the primary function of RAM Mobile Data?
   A. High-speed voice calls
   B. Analog TV streaming
   C. Packet-switched wireless data services
   D. Optical backbone for 4G

2. How did the Mobitex protocol in RAM Mobile Data achieve efficient data transmission?
   A. Through circuit switching
   B. Using Ethernet-like frame formats
   C. Through asynchronous packet switching with store-and-forward
   D. By limiting user bandwidth

Answers:
1. C 2.C

3.6 SUMMING UP

The chapter discusses three wireless data communication technologies: CDPD (Cellular Digital Packet Data), ARDIS (Advanced Radio Data Information Service) and RMD (RAM Mobile Data). These technologies have significantly facilitated mobile data transfer across various applications over time.

- CDPD leverages existing cellular networks for packet-based data transmission, providing high data rates and efficient spectrum utilization. It uses slotted CSMA/CD for channel access and integrates strong error correction techniques to improve reliability.
- ARDIS was primarily developed for enterprise and government applications. It offers a dependable yet lower-speed data service with substantial error handling through interleaving strategies.
- RMD operates at moderate data rates and utilizes slotted CSMA for channel access, ensuring efficient data transmission while maintaining error resilience through trellis-coded modulation and interleaving methods.

A summarized comparison between the technologies is given in Table 3.1

Table 3.1: A comparison between CPDP, ARDIS and RAM

Characteristics	**CPDP**	**ARDIS**		**RAM**
Protocols	MDLP, RRMP, X.25	MDC 4800	RDLAP	Mobitex
Channel Data Rate (bps)	19,200	4800	19,200	8000
Channel Bandwidth (kHz)	30	25	25	12.5
Spectrum Efficiency (b/Hz)	0.64	0.19	0.77	0.64
Random Error Strategy	Cover with burst protect	Convolutional ½, k=7	Trellis coded modulation, rate = 3/4	12, 8 Hamming code
Brust Error Strategy	RS 63,47 (6bits per symbol)	Interleave 16bits	Interleave 32 bits	Interleave 21 bits
Fading Performance	Withstands 2.2 ms fade	Withstands 3.3 ms fade	Withstand 1.7ms fade	Withstands 2.6ms fade
Channel Access	Slotted DSMA/CD	CSMA non-persistent	Slot CS<A	Slotted CSMA

3.7 POSSIBLE QUESTIONS

1. Explain how CDPD utilizes idle cellular channels and discuss its advantages over dedicated data channels.

2. Compare the circuit-switched nature of AMPS voice calls with the packet-switched approach of CDPD.

3. Describe the function of the Mobile Data Link Protocol (MDLP) and its role in maintaining data integrity in CDPD.

4. CDPD operates independently of the MSC. What are the benefits and challenges of this approach in mobile communication?

5. Explain the significance of channel hopping in CDPD and how it ensures non-interference with voice communications.

6. Explain the role of the Mobile End System (M-ES) in the CDPD network and how it establishes communication.

7. Describe the function of the Mobile Data Base Station (MDBS) in handling CDPD traffic. How does it dynamically manage idle cellular channels?

8. What is the significance of the Intermediate Server (MD-IS) in CDPD? Discuss its role in packet switching, encryption, and authentication.

9. Explain how the I-Interface connects the CDPD network to external networks like the Internet or private corporate systems.

10. Compare the packet-switching mechanism of CDPD with circuit-switched voice calls in traditional AMPS networks.

11. How does the CDPD network architecture ensure seamless communication between mobile users and fixed-end systems?

12. How does ARDIS handle simultaneous transmissions, and what are the spatial constraints involved?

13. Describe the historical development of RAM Mobile Data, including its founding and rebranding.

14. What were the key characteristics of RAM Mobile Data, and how did they benefit urban communication?

15. Explain the function of the Mobitex protocol in RAM Mobile Data and its advantages over circuit-switched networks.

16. Compare RAM Mobile Data’s data transmission approach with modern mobile broadband networks.

17. How did RAM Mobile Data optimize fax transmission, and what were its advantages over traditional faxing methods?

3.8 REFERENCES AND SUGGESTED READINGS

1. Theodore S. Rappaport (2002), Wireless Communications -Principles Practice, 2nd edition, Prentice Hall of India, New Delhi.
2. William Stallings (2009), Wireless Communications and Networks, 2nd edition, Pearson Education, India.

***

UNIT- 4

WIRELESS DATA SERVICES – II

Unit Structure:

4.1 INTRODUCTION

In today's interconnected world, wireless data services are critical in facilitating seamless communication, data transfer and internet access across various applications. These services have evolved dramatically from mobile phones to broadband networks, supporting faster and more effective communication technologies. This chapter examines key aspects of wireless data services, including Common Channel Signaling (CCS), Integrated Services Digital Network (ISDN), Broadband ISDN and Asynchronous Transfer Mode (ATM). It also explores Signaling System No. 7 (SS7), which is the backbone of modern telecommunications networks by ensuring reliable signaling and data transmission. Understanding these technologies is crucial for grasping how wireless communication networks operate, manage signaling and maintain data integrity, security and efficiency. By the end of this chapter, readers will gain insights into the architecture, protocols and performance metrics governing wireless data services, laying a foundation for more advanced studies in wireless networking.

4.2 OBJECTIVES

After studying this chapter, you will be able to:

- *understand* the Fundamentals of signaling and explain the importance of signaling in telecommunication networks.
- *analyze* Common Channel Signaling (CCS) and ISDN to explore CCS-based signaling systems, their architecture and the services of ISDN.
- *examine* the Role of ATM and SS7 in high-speed communication and the significance of SS7 in modern networks.
- *evaluate* Signaling Performance and Network Efficiency to discuss key performance metrics and challenges in signaling systems.
- *understand* the X.25 Protocol and its applications, their structure, functionality and role of X.25 in packet-switched networks.

4.3 COMMON CHANNEL SIGNALING (CCS)

Common channel signaling (CCS) is a digital communication technique that simultaneously transmits user data, signaling data, and other types of traffic across a network. This is accomplished using out-of-band signaling channels, which logically separate network data from user data (voice) on the same channel. In second-generation wireless systems, CCS transmits user data and control signals between the subscriber and the base station, from the base station to the MSC and between MSCs. Although the concept of CCS implies dedicated parallel channels, it is implemented in a TDM format for serial data transmission.

Before the introduction of CCS in the 1980s, signaling traffic between the MSC and a subscriber was transmitted on the same band as the end-user's audio. The network control data exchanged between MSCs in the PSTN was also sent in-band, requiring network information to be carried within the same channel as the subscriber's voice traffic throughout the PSTN. This approach, known as in-band signaling, limited the capacity of the PSTN because the rates of network signaling data were significantly restricted by the constraints of the voice channels in use. Consequently, the PSTN had to manage signaling and user data sequentially (rather than simultaneously) for each call.

Stop to Consider

1. Every time you make a phone call or send an SMS; CCS plays a role in routing the call or message efficiently.
2. Before CCS, telephone networks used in-band signaling, which meant that dial tones and call routing signals were transmitted within the same frequency range as voice calls.

CCS is an out-of-band signaling technique that enables much faster communication between two nodes within the PSTN. Instead of being limited to signaling data rates similar to audio frequencies, CCS supports data rates ranging from 56 kbps to several megabits per second. As a result, network signaling data is transmitted through a separate, out-of-band signaling channel, while user data travels through the PSTN. CCS dramatically increases the number of users served by trunked PSTN lines, but it requires dedicating a portion of trunk time to the signaling channel used for network traffic. The SS7 family of protocols, as defined by the Integrated Services Digital Network (ISDN), is used to provide CCS in first-generation cellular systems.

Since network signaling traffic is bursty and brief, the signaling channel can operate in connectionless manner, efficiently employing packet data transfer techniques. CCS typically utilizes variable-length packet sizes along with a layered protocol structure. The cost of maintaining a parallel signaling channel is minimal compared to the capacity improvements that CCS provides across the PSTN. The same physical network connection (e.g., a fiber optic cable) often carries user traffic and network signaling data.

Stop to Consider

- **Shift from In-Band to Out-of-Band Signaling:** How did the transition from in-band signaling to Common Channel Signaling (CCS) improve the efficiency of telecommunications network?
- **CCS and Modern Networks:** Given that CCS enables out-of-band signaling, how does this influence the reliability and scalability of modern digital networks?

Advantages of Common Channel Signaling over Conventional Signaling–

CCS has several advantages over conventional signaling, which are outlined below:

- ***Faster Call Setup*****:** In CCS, high-speed signaling networks are utilized to transfer call setup messages, resulting in shorter delay times than conventional multi-frequency signaling methods.
- ***Greater Trunking (or Queueing) Efficiency*****:** CCS features shorter call setup and teardown times, reducing call-holding time and less network traffic. This efficiency becomes particularly evident during heavy traffic conditions.
- ***Information Transfer*****:** CCS enables the transfer of additional information alongside the signaling traffic, providing features such as caller identification and voice or data recognition.

CASE STUDY: A distributed central switching office using CCS

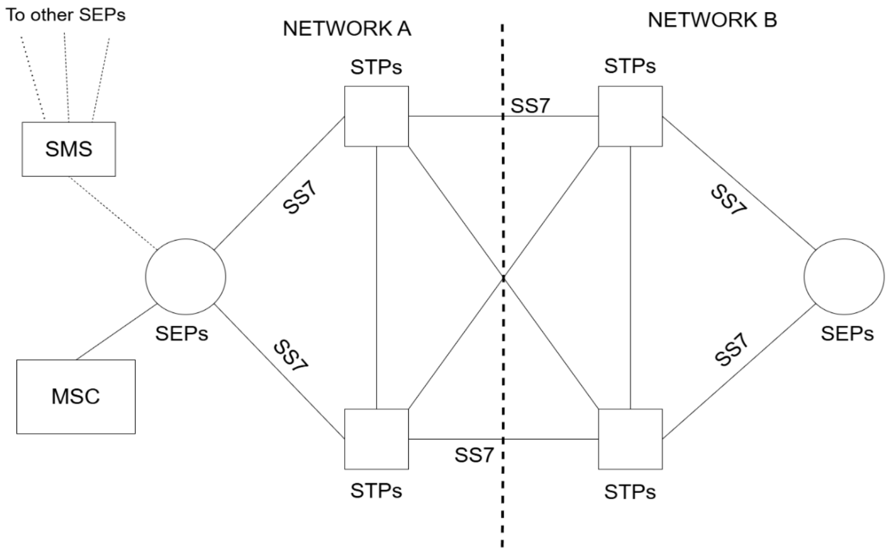
As wireless services attract more users, the backbone networks linking Mobile Switching Centers (MSCs) increasingly rely on network signaling to keep messages intact, guarantee seamless connectivity for every mobile user, and maintain a strong network that can bounce back from any setbacks. The Common Channel Signaling (CCS) framework is fundamental for controlling and managing second and third-generation network functions. With out-of-band signaling networks connecting MSCs worldwide, the entire wireless network can effortlessly update and track specific mobile users, no matter where they are.

Figure 4.1 illustrates that the CCS network architecture consists of central switching offices strategically located across different regions, each featuring embedded switching endpoints (SEPs), signaling transfer points (STPs), a service management system (SMS) and a database service management system.

The MSC provides subscribers access to the PSTN through the SEP, which implements a stored-program-control switching system known as the service control point (SCP). The SCP utilizes CCS to set up calls and access the network database, guiding the SEP in generating billing records based on the call information it collects.

The STP oversees the message switching between nodes in the CCS network. SEPs must connect to the SS7 network through at least two STPs to enhance transmission reliability or redundancy. This dual-STP configuration, known as a mated pair, ensures network connectivity even if one STP experiences a failure.

The SMS holds all subscriber records and manages subscribers' access to toll-free databases. Meanwhile, the DBAS is the administrative database that maintains service records and investigates fraud throughout the network. The SMS and DBAS work hand in hand to deliver a wide array of customer and network services, drawing loosely from SS7 principles.



SEPs: Switching end points
STPs: Signaling Transfer Points
SMS: Service Management System
SS7 : Signaling System No. 7

Fig- 4.1*TheArchitecture of a Common Channel Signaling (CCS) network, depicting STPs, SEPs and SMS embedded within a central switching office, based on SS7.*

Check Your Progress

1. How does CCS differ from traditional in-band signaling in terms of efficiency?
   A. CCS is slower but more secure
   B. CCS sends signaling data over the same channel as voice
   C. CCS uses a separate channel, making it more efficient and faster
   D. CCS only supports analog signals

2. If an in-band system transmits at 8 kbps and CCS transmits at 64 kbps, CCS is ______ times faster.**(Fill in the blank)**

Answers:

1. C   2. 8

4.3 ISDN

ISDN, which stands for Integrated Services Digital Network, represents an exciting international communications standard that allows us to send voice, video and data smoothly over digital and traditional phone wires. This innovative system will enable data to travel seamlessly globally via end-to-end digital connectivity.

In the past, the telephone network depended entirely on an analog system, connecting users through wires. This older system encountered several challenges—it was often inefficient, prone to breakdowns and struggled with noise, making long-distance calls tricky. However, beginning in the 1960s, the telephone system underwent a significant transformation, gradually transitioning its internal connections to a more sophisticated packet-based digital switching system. Despite this advancement, the final segment, from the local central office to customer equipment, relies mainly on the reliable analog Plain Old Telephone Service (POTS) line.

A pivotal movement began with the International Telephone and Telegraph Consultative Committee, now known as the International Telecommunications Union Telecom Sector (ITUT). This organization, part of the United Nations, is crucial in coordinating and standardizing telecommunications worldwide. The original recommendations for ISDN were introduced in CCITT Recommendation I.120 in 1984, which established initial guidelines for implementing ISDN, paving the way for today's telecommunications advancements.

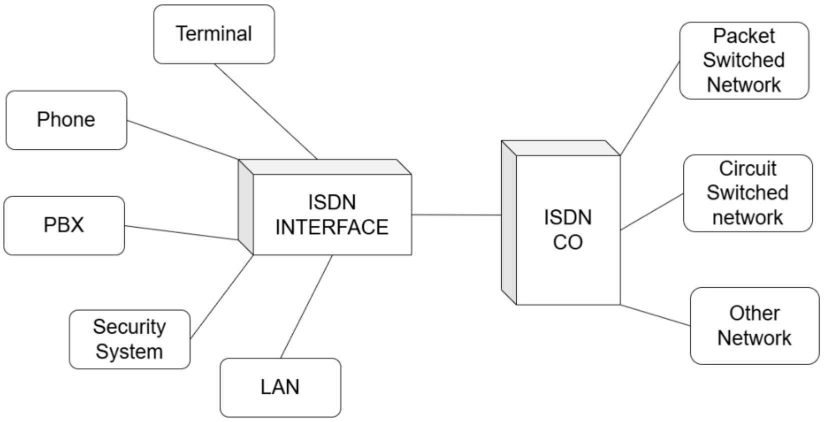


***Fig. 4.2** ISDN User Interface*

ISDN supports data transfer rates of 64 Kbps. Most ISDN lines offered by telephone companies give two lines simultaneously, called *Bearer channels* or *B-channels*. One can use one line for voice and the other for data or both lines to give data rates of 128 Kbps, three times the data rate provided by today's fastest modems. Some switches limit B channels to a capacity of 56 Kbps. Depending on the ISDN link location, a data channel (D channel) handles signaling low-speed packet mode data transfer at 16 Kbps or 64 Kbps.

Self-Asking Questions

What challenges did traditional analog phone systems face that ISDN aimed to overcome?

…………………………………………………………

…………………………………………………………

…………………………………………………………

ISDN end-users can choose between the basic rate interface (BRI) or the primary rate interface (PRI). The BRI is designed to serve low-capacity terminals, such as single-line telephones, while the PRI is meant for high-capacity terminals, like PBXs. Both the BRI and PRI support B channels at 64 Kbps data rates. The D channel provides 64 Kbps for the primary rate and 16 Kbps for the introductory rate. The BRI offers two 64 Kbps bearer channels and one 16 Kbps signaling channel (2B+D), whereas the PRI features twenty-three 64 Kbps bearer channels and one 64 Kbps signaling channel (23B+D) in North America and Japan. The primary rate interface in Europe offers thirty basic information channels and one 64 Kbps signaling channel (30B+D). The PRI service is designed to operate over DS-1 or CEPT level 1 links.

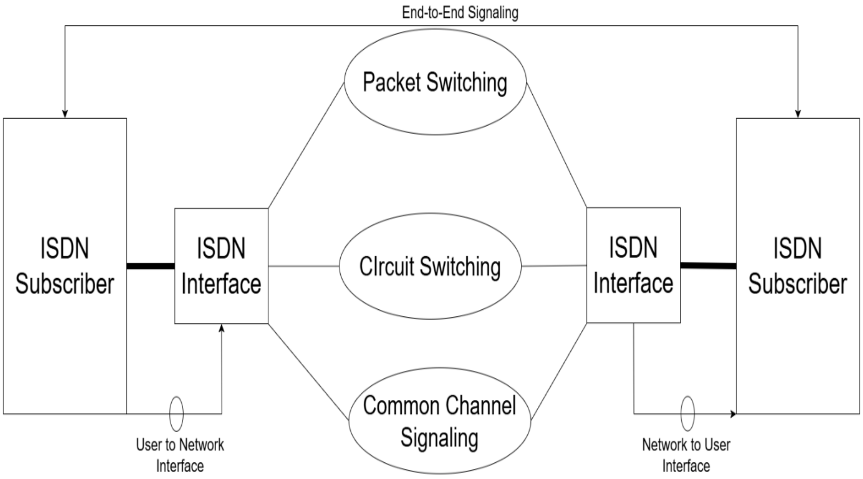


***Fig. 4.3** Block diagram of an Integrated service Digital Network. Even though the diagram illustrates parallel channels, the TDM-based serial data structure uses a signal twisted pair.*

Several ISDN circuits may be concatenated into high-speed information channels (H channels). H channels are used by the ISDN backbone to provide efficient data transport for many users on a single physical connection and may also be used by PRI end-users to allocate higher transmission rates on demand. ISDN defines HO channels (384 Kbps), H11 (1536 Kbps) and H12 channels (1920 Kbps)as shown in the Table 4.1 below.

Table 4.1: Types of Bearer Services in ISDN

Service Mode	**Service Type**	**Transmission Speed**	**Channel Type**
Circuit mode	Unrestricted	64kpbs, 384kpbs, 1.5Mpbs	B, H0, H11
Circuit mode	Speech	64kbps	B
Packet radio	Unrestricted	Depends on throughput	B, D (or C)

Stop to Consider

1. **A Step Towards Broadband:** ISDN was once considered a major breakthrough, offering faster speeds than traditional dial-up and enabling early video conferencing.

2. **Legacy Technology:** While ISDN is largely replaced by broadband solutions, some industries, like broadcasting and emergency services, still use it for reliability.

4.4.1 Some Features of ISDN are:

1. The main feature of ISDN is its ability to integrate voice and data on the same line, which was impossible with traditional telephone systems.
2. ISDN services can transmit maximum data, including voice, data, video and fax, over a single line while ensuring at least two simultaneous connections.
3. ISDN enables access to packet-switched networks since it functions as a circuit-switched telephone system. As a result, it provides superior voice quality compared to analog phones.

Check Your Progress

1. What is the main difference between ISDN BRI and PRI?
   A. BRI is only used in offices
   B. PRI offers more B-channels than BRI
   C. BRI has higher bandwidth than PRI
   D. PRI does not support voice
2. If a user is using both 64 kbps B-channels in ISDN BRI, the maximum achievable data rate is ______ kbps.**(Fill in the blank)**
3. ISDN integrates voice and data on the same lines, but modern broadband is significantly more efficient.**(True/False)**

Solutions:

1.B 2. 128 3.True

4.4.2 Broadband ISDN

When ISDN was first designed, data rates from 64 Kbps to 1.544 Mbps effectively met all existing transmission needs. However, as telecommunications network applications evolved, these rates felt somewhat limiting. ISDN was developed to enable high-speed communication to accommodate better the demands of next-generation technology, known as broadband. The initial version of ISDN utilizes baseband transmission to ensure a smooth start.

ISDN is an incredible standard that enables the concurrent delivery of voice, video and data via fiber optic telephone lines. Broadband ISDN provides remarkable data rates, surpassing several million bits per second (bps). However, the original ISDN format uses baseband transmission; a fantastic alternative known as B-ISDN facilitates broadband transmission and can reach rates of 1.5 Mbps or more.

There are two basic types of ISDN interfaces:

- Basic Rate Interface (BRI), and
- Primary Rate Interface (PRI).

BRI comprises two B channels at 64 Kbps each and one D channel at 16 Kbps, achieving a total bandwidth of 144 Kbps. This service is tailored to satisfy the demands of most individual users and is prevalent in both residential and commercial settings. Conversely, PRI is aimed at users who need greater capacity, like larger businesses or offices. Its channel framework typically contains 23 B channels and one D channel of 64 Kbps, culminating in 1536 Kbps.

4.4.3 Advantages of ISDN

There are many advantages of ISDN. In this section, we will look at them.

Speed: The modem signifies a remarkable breakthrough in computer communications. It allows computers to exchange information by converting digital data into analog signals, which travel through traditional phone networks. However, these analog lines have a maximum capacity of approximately 56 Kbps. Although many modems can reach this speed, the data transfer rate usually hovers around 45 Kbps, varying with connection quality. ISDN or Integrated Services Digital Network, presents itself as a contemporary alternative to the outdated telephone service, which was not equipped to accommodate our information-intensive society. ISDN enables the simultaneous operation of multiple digital channels over the same wiring as analog lines. The best part? The phone company's switches can manage these digital connections, allowing you to send digital signals using the same physical cables rather than analog ones. You can easily acquire ISDN service from your usual telephone provider, allowing connections for phones, computers and fax machines. The primary enhancement is the increased speed and reliability, allowing you to communicate via voice, data, fax, and even video—all through a single line. With BRI-ISDN, one can achieve an impressive uncompressed data transfer speed of 128 Kbps. Additionally, the latency on an ISDN line is generally about half that of an analog line, providing exceptional efficiency and connecting an ISDN.

Multiple Devices: Before ISDN, managing several devices simultaneously required a dedicated phone line for each device. One needs separate lines for the telephone, fax machine, computer, router and live video conferencing. If someone needs to send a file while talking on the phone or participating in a video call, one needs to undergo the daunting task of managing multiple expensive phone lines. However, ISDN enables us to streamline various digital data sources and effortlessly route information where needed. Because these lines are digital, they significantly reduce noise and interference, making it easier to combine all those signals. ISDN refers explicitly to a set of digital services provided through one standard interface; without it, you would have to deal with several different line interfaces.

Signaling: ISDN provides a dedicated signal channel shared across all B channels, known as standard channel signaling. Unlike the traditional method, where the phone company sends a ring voltage signal to your phone's bell (referred to as an "In-Band signal"), ISDN transmits a digital packet on a separate channel (called an "Out-of-Band signal"). This setup ensures established connections to remain undisturbed, allowing for lightning-fast call setups. For context, while a V.34 modem may take 30-60 seconds to connect, an ISDN call can link up in under 2 seconds. The signaling system also conveys who is calling, the type of call (data or voice)and the dialed number. With this information, ISDN-compatible phone equipment can efficiently route the call.

4.4.4 Applications of ISDN

ISDN, along with new and low-cost hardware, is changing rapidly. Some of the increasingly valuable applications include:

Internet Access: ISDN is among the most utilized applications for internet connectivity. Unlike even the quickest modem connections, ISDN delivers web graphics nearly instantly and can cut download times by more than 75%. It can also outperform shared, high-bandwidth office connections.

Video Conferencing: ISDN facilitates videoconferencing by using one channel for voice and another for moving video images. This allows remote professionals to communicate face-to-face. As a rapidly growing application, ISDN is currently the only feasible option for effective videoconferencing. Previously, high-quality video and voice transmission over distances required costly equipment and leased lines, justified only for the most essential needs of large corporations. Consequently, these video conferencing systems were limited to point-to-point connections; for example, linking a headquarters with satellite offices was manageable, but large-scale teleconferencing was unfeasible.

Education: *Distance Learning* can be seen as telecommuting for students. Just as ISDN has enabled telecommuting for many professionals, it is also making *distance learning* a reality for innovative public and private schools, high schools and colleges nationwide. Interactive voice, data, image and video facilitate the learning experience for students who cannot physically attend a classroom.

Large-Scale File Transfers: As computer applications have increasingly focused on graphics, PC communications now integrate images, sound and even full-motion video, enabling a more visual way to convey information.

Check Your Progress

1. Why was ISDN developed?
   A. To increase analog bandwidth
   B. To digitize and integrate voice and data services
   C. To eliminate need for internet
   D. To replace satellite phones
2. ISDN played a key role in early internet access and video conferencing.**(True/False)**
3. Which modern technology has largely replaced ISDN in homes and offices?
   A. PSTN
   B. Dial-up modems
   C. Broadband (DSL, fiber, cable)
   D. Walkie-talkies

Solutions:
1.B 2.True 3.C

4.5 ATM

Synchronous Transfer Mode (ATM), or cell relay, is similar to packet switching. In ATM, data transfer occurs in discrete chunks, allowing multiple logical connections to be multiplexed over a single physical connection.

However, ATMs organize the chunks into fixed-size cells. ATM is a general protocol known for its minimal errors and effective flow control capabilities. Flow control reduces the processing time of ATM cells, minimizes the overhead bits required in each cell, and enables ATM to achieve higher data rates. Additionally, because of the use of fixed-size cells, the processing needed at each node is simplified, facilitating the use of ATM at high data rates.

4.5.1 ATM Logical Connections

In ATM, the logical connections are called virtual channel connections (VCCs). They resemble the virtual circuits found in packet-switching networks and serve as the fundamental unit of the ATM network. A VCC is established between two end users across the network, enabling variable-rate, full-duplex transmission of fixed-size cells. Additionally, VCCs facilitate user-network exchanges (such as control signaling) and network-network exchanges (which involve management and routing).

In ATM, an additional sub layer of processing has been added to manage the virtual path concept (see Figure 4.4). A virtual path connection (VPC) consists of multiple virtual channel connections (VCCs) sharing the same endpoints. Consequently, all cells traversing the VCCs within a single VPC are switched simultaneously.

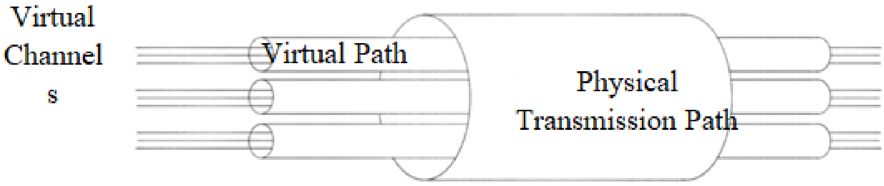


Fig. 4.4Relationships of ATM control

The virtual path concept emerged due to a trend in high-speed networking where control costs are rising as a more significant part of overall network expenses. This technique helps control costs by bundling connections that share common routes into a single unit. Consequently, network management efforts can be directed towards fewer groups of connections rather than numerous individual connections.

4.5.2 ATM Cells

The fixed-size cells in ATM include a 5-octet header and a 48-octet data field. This use of small fixed cells brought forward many advantages. Primarily, its use of small cells reduces the delay while queuing for a higher priority cell since a smaller size will lead to less wait time even if it arrives just behind a lower priority cell that just accessed the resource, e.g., transmitters. Also, these fixed-size cells are more efficient when switching, which proved advantageous for ATM's very high data rates. Switching hardware mechanisms also became more straightforward to implement.

HEADER Format

Figure 4.5 below illustrates a header from user and internal network perspectives. A generic flow control field in the user-network view enables end-to-end functions not present in the network view. However, the network-view header expands the virtual path identifier from 8 to 12 bits. This expansion increases the number of internal **Virtual Path Connections** (VPCs) available to subscribers and for network management.

Stop to Consider

ATM was widely used in backbone networks before the rise of IP-based networking. Although it is less common today, it's principles still influence modern networking, including MPLS (Multiprotocol Label Switching).

The Generic Flow Control (GFC) fields manage cell flow at the client user-network interface. This field helps customers control traffic flow based on various quality-of-service parameters. For instance, it can indicate multiple priority levels to regulate data flow in a service-dependent system. Additionally, the GFC mechanism is often used to alleviate short-term overload conditions in a network.

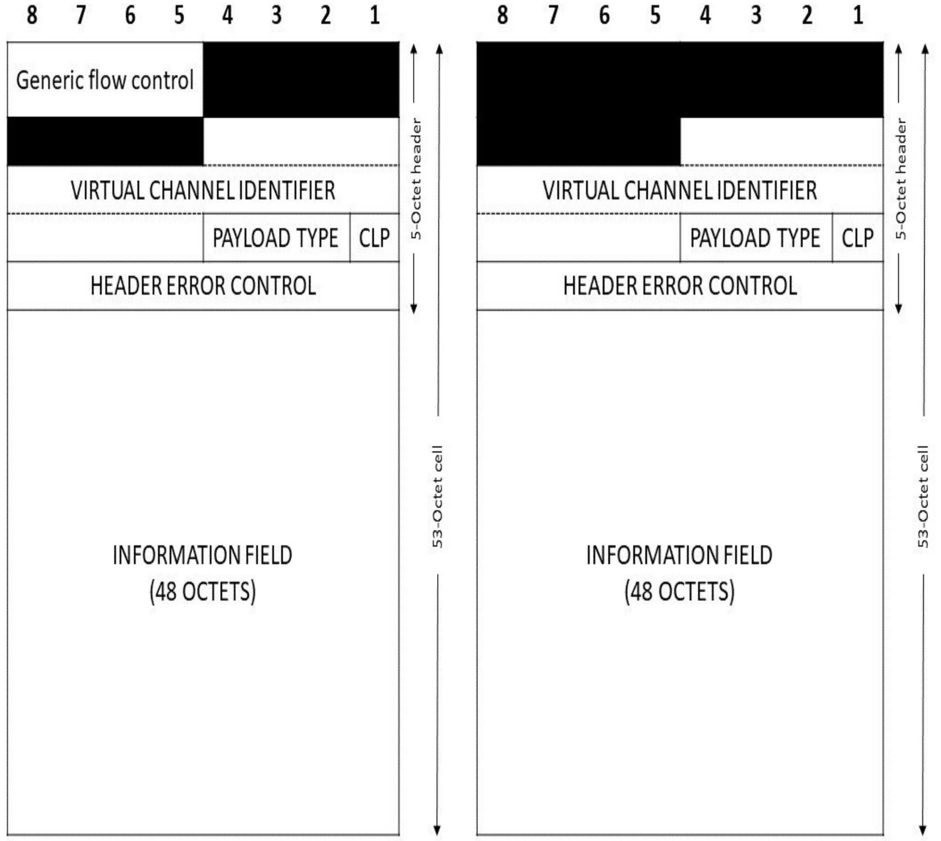


Fig. 4.5ATM Cell Format

The Payload Type (PT) field indicates the type of data contained in the data field. Table 4.2 presents the various categories of data transmitted along with their encoding. A zero value in the first bit signifies user information; the second bit indicates whether congestion has occurred; the third bit, known as the service data unit (SDU) type bit, differentiates between the two types of ATM SDUs associated with a connection. SDU refers to the 48-octet payload of a cell. If the first bit’s value is 1, it shows that the cell carries network maintenance or management data. This signal facilitates the addition of network management cells to a user VCC without affecting the data. Therefore, the PT field helps lay out the in-band control data.

The Virtual Path Identifier (VPI) serves as a routing field within the network. It consists of 8 bits at the user-network interface and 12 bits at the network-network interface, enabling support for more virtual paths. Similarly, the Virtual Channel Identifier (VCI) routes communications to and from the end user, effectively functioning as a service access point.

Table 4.2: Payload Type Categories

PT Coding	**Interpretation**		
0 0 0	User data cell	Congestion experience	SDU type = 0
0 0 1	User data cell	Congestion not experience	SDU type = 1
0 1 0	User data cell	Congestion experience	SDU type = 0
0 1 1	User data cell	Congestion experience	SDU type = 1
1 0 0	OAM segment associated cell		
1 0 1	OAM end-to-end associated cell		
1 1 0	Resource management cell		
1 1 1	Reserved (future use)		

*OAM = Operations, Admin and Maintenance

The Cell Loss Priority (CLP) field guides the network during congestion. A value of 0 signifies a higher-priority cell that should only be discarded as a last resort. Conversely, a value of 1 means the cell is eligible for discarding within the network. Users can utilize this field to insert additional information into the network, marked with a CLP of 1, which will be sent to the destination if there is no congestion. The network may assign a value of 1 to any data cell violating the agreed traffic parameters between the user and the network. In such cases, the switch responsible for this assignment recognizes that the cell exceeds the agreed parameters but is still manageable. If the network experiences congestion later, this cell will be prioritized for discard over those that comply with the approved traffic limits.

The Header Error Control (REC) field is an 8-bit error code that can correct single-bit errors in the header and detect double-bit errors. For most existing protocols, the data used for error code calculation is generally much longer than the resulting error code size, facilitating effective error detection. In the case of ATM, however, the input for the calculation is only 32 bits, compared to the 8 bits of the code. This relatively short input enables the code to detect errors and in some cases, perform actual error correction due to sufficient redundancy within the code, allowing recovery from specific error patterns.

The error protection function enables recovery from single-bit header errors and ensures a low probability of delivering cells with erroneous headers during burst error conditions. The error characteristics of fiber-based transmission systems appear to involve single-bit and relatively large burst errors. Some transmission systems may not fully utilize the more time-consuming error correction capability.

Check Your Progress

1. What is a major difference between packet switching and ATM?

   A. ATM is only analog

   B. Packet switching uses fixed-size packets

   C. ATM uses fixed-size cells for uniform transmission

   D. Packet switching cannot handle video

2. A Virtual Channel Connection (VCC) is part of a Virtual Path Connection (VPC), meaning VPCs group multiple ______. **(Fill in the blank)**

3. Why are ATM cells fixed at 53 bytes in size?

   A. To support analog transmission

   B. To simplify switching and reduce delay

   C. To save memory

   D. To allow flexible packet sizes

4. The Payload Type (PT) field in ATM cells indicates the type of content and control information. **(True/False)**

5. What is the purpose of the Generic Flow Control (GFC) field in an ATM header?

   A. Audio compression

   B. Cell synchronization

   C. Local flow control at the user-network interface

   D. Error correction

6. What does a Cell Loss Priority (CLP) value of 1 indicate? **(MCQ)**

   A. The cell has the highest priority

   B. The cell should be retransmitted

   C. The cell is encrypted

   D. The cell may be discarded during congestion

Answers:

1.C 2.VCCs 3.B 4.True 5.C
6.D

4.5.3 ATM Service Categories

An ATM network is designed to transfer various types of traffic simultaneously, including real-time flows such as voice, video, and bursty TCP flows. While each traffic flow is treated as a stream of 53-octet cells traveling through a virtual channel, the method by which each data flow is processed within the network depends on its characteristics and the application's quality of service requirements. For instance, real-time video traffic must be delivered with minimal delay variation.

Stop to Consider

ATM service categories were designed to accommodate both real-time and non-real-time applications, making ATM one of the first networking technologies to prioritize Quality of Service (QoS) for different types of traffic.

In this subsection, we summarize ATM service categories, which an end system uses to identify the required service types. The ATM Forum has defined the following service categories:

Real-time service: When discussing various applications, one key difference is how much delay and variability of delay—known as jitter—each application can handle. Real-time applications are designed to deliver information to users in a way that closely resembles the source. For instance, these applications are crucial in scenarios where timely delivery is essential, such as video conferencing or online gaming.
Some examples of real-time ATM Services include:

Constant bit rate (CBR): CBR service is likely the simplest to define. It is utilized by applications that need a fixed data rate continuously available throughout the connection's duration, along with a relatively tight upper limit on transfer delay. CBR is frequently used for uncompressed audio and video content. Examples of CBR applications include videoconferencing, interactive audio (e.g., telephony), audio/video distribution (e.g., television, distance learning, pay-per-view), and audio/video retrieval (e.g., video-on-demand, audio library).

Real-time variable bit rate (rt-VBR): The rt-VBR category is designed for time-sensitive applications, specifically those that require tightly constrained delays and variations in delay. The main distinction between applications suited for rt-VBR and those for CBR is that rt-VBR applications transmit at varying rates over time. In other words, an rt-VBR source can be described as somewhat bursty. For instance, the standard video compression method produces a sequence of image frames with varying sizes. The actual data rate fluctuates since real-time video necessitates a consistent frame transmission rate. The rt-VBR service offers the network more flexibility than CBR, enabling it to statistically multiplex multiple connections over the same dedicated capacity while delivering the required service to each connection.

Non-real-time service:

Non-real-time services support applications that exhibit bursty traffic patterns without strict delay and variation requirements. This gives the network greater flexibility in managing these traffic flows, enabling higher statistical multiplexing to enhance network efficiency.

There are several ways to utilize non-real-time service, including the following:

- Non-real-time variable bit rate (nrt-VBR)
- Available bit rate (ABR)
- Unspecified bit rate (UBR)
- Guaranteed frame rate (GFR)

For specific non-real-time applications, it is possible to characterize the expected traffic flow so that the network can deliver significantly improved quality of service (QoS) in terms of loss and delay. Such applications can utilize the non-real-time variable bit rate (nrt-VBR) service. With this service, the end system specifies a peak cell rate, a sustainable or average cell rate, and a measure of how bursty or cluster-like the cells may be. Using this information, the network can allocate resources to achieve low delay and minimal cell loss. The nrt-VBR service can be employed for data transfers with critical response-time requirements. Examples include airline reservations, banking transactions, and process monitoring.

An ATM network's capacity is partially used to support CBR along with two varieties of VBR traffic. There is additional capacity due to two factors: (1) not all resources are exclusively allocated to CBR and VBR, and (2) the bursty characteristic of VBR traffic often results in underutilization of the committed capacity. This surplus capacity can then be used for Unspecified Bit Rate (UBR) service, which is well-suited for applications tolerant of variable delays and occasional cell losses, typical of TCP-based traffic. UBR functions on a first-in-first-out (FIFO) principle, using the excess capacity not utilized by other services, which can result in delays and inconsistent losses. Unlike other services, UBR does not require an initial commitment from the source and lacks congestion feedback, positioning it as a best-effort service. Applications for UBR include text, data, and image transfers, messaging, distribution, retrieval, and tasks with remote terminals telecommuting). Bursty applications that depend on a reliable end-to-end protocol like TCP can detect network congestion through increased round-trip delays and packet loss. However, TCP does not provide a mechanism to ensure fair resource allocation among multiple TCP connections. Moreover, TCP is not as effective at alleviating congestion as it could be by incorporating explicit feedback from congested nodes within the network.

To enhance the service provided to bursty sources that would otherwise rely on UBR, the available bit rate (ABR) service has been established. An application utilizing ABR specifies a peak cell rate (PCR) that it will employ and a minimum cell rate (MCR) that it requires. The network allocates resources to ensure all ABR applications receive at least their MCR capacity. Any unused capacity is then fairly and systematically distributed among all ABR sources. The ABR mechanism employs explicit feedback to sources to guarantee that capacity is allocated equitably. Any capacity that remains unused by ABR sources stays available for UBR traffic.

An example of an application using ABR is LAN interconnection. In this scenario, routers are the end systems connected to the ATM network. The latest addition to the set of ATM service categories is Guaranteed Frame Rate (GFR), specifically designed to support IP backbone sub-networks. GFR offers improved service compared to UBR for frame-based traffic, including IP and Ethernet. A primary objective of GFR is to enhance the handling of frame-based traffic that travels from a LAN through a router onto an ATM backbone network. Such ATM networks are increasingly being utilized by large enterprises, carriers, and Internet service provider networks to consolidate and extend IP services across wide areas. While ABR is also an ATM service intended to provide a greater degree of guaranteed packet performance over ATM backbones, ABR is relatively challenging to implement between routers across an ATM network. With the growing emphasis on using ATM to support IP-based traffic, particularly traffic originating from Ethernet LANs, GFR may present the most appealing alternative for providing ATM service.

Check Your Progress

1. What are the two main categories of ATM services?
   A. Analog and digital
   B. Real-time and non-real-time
   C. Constant Bit Rate (CBR) and Variable Bit Rate (VBR)
   D. Secure and insecure
2. What is a major limitation of Unspecified Bit Rate (UBR)?
   A. It uses encryption
   B. It has no guaranteed bandwidth or delivery
   C. It is used only for video
   D. It prioritizes all data equally
3. How does Available Bit Rate (ABR) manage bandwidth?
   A. By dropping packets randomly
   B. By using fixed bandwidth per user
   C. By dynamically adjusting rates based on network load
   D. By using encryption to throttle bandwidth

Answers:

1.C *2. B* *3.C*

4.6 SIGNALING SYSTEM NO .7(SS7)

Signaling System No. 7 (SS-7) is a set of protocols widely used to perform telecommunication all over the globe. It was developed in 1975. This protocol is limited to telephonic calls and works in number translation, local number portability, prepaid billing, Short Message Service (SMS) etc. These are all possible only because of this protocol. The key factor in its wide use is enabling autonomous registration and automated roaming in first-generation cellular systems.

4.6.1 Protocols

SS7 is a worldwide suite of signaling protocols used in telecommunications to establish, route and manage calls. It creates a dependable framework for exchanging signaling messages among network components such as switches, databases and service control points. In contrast to conventional in-band signaling, SS7 operates as an out-of-band signaling system, utilizing a separate channel (the signaling link) to exchange control information independently apart from voice or data traffic.

SS7 employs a layered architecture similar to the OSI model, where various protocols manage separate functions like message transport, call control, database inquiries and intelligent network services. The Message Transfer Part (MTP) guarantees reliable message routing, while upper-layer protocols like the ISDN User Part (ISUP), Transaction Capabilities Application Part (TCAP) and Mobile Application Part (MAP) facilitate advanced telecommunication services. These protocols support vital network functions, including call setup, mobile roaming, SMS routing, and toll-free number translation. Figure 4.6 below is a detailed breakdown of the key protocols in the SS7 architecture.

4.6.2 Network Services Part (NSP)

The NSP offers ISDN nodes a dependable and effective way to exchange signaling traffic via connectionless services. Within SS7, the SCCP supports interconnections in packet data networks and facilitates connection-oriented networking with virtual circuit networks. This enables network nodes to communicate globally, regardless of the application or context of the signaling traffic.

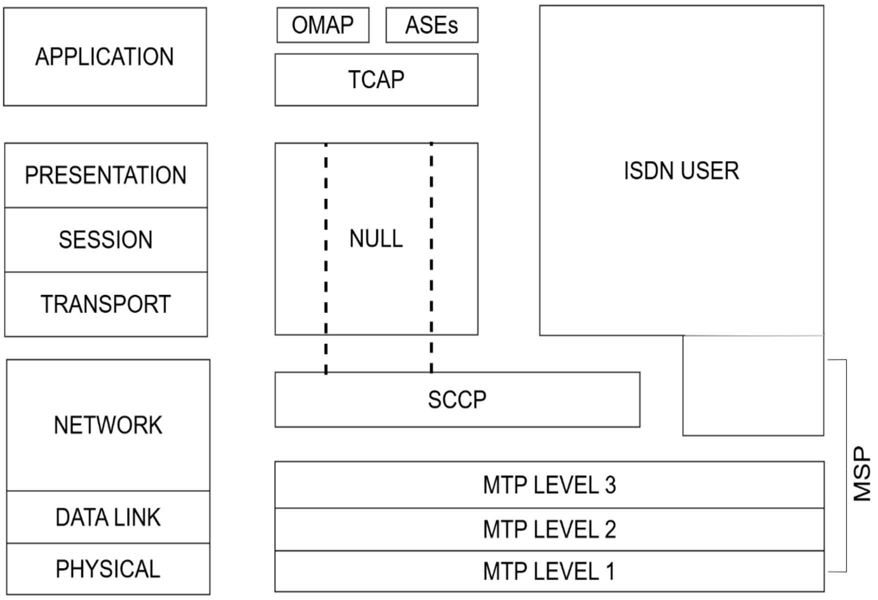


Fig. 4.6. SS7 protocol architecture

OMAP: Operations Maintenance and Administration Part
ASE: Application Service Element
TCAP: Transaction Capabilities Application Part
SCCP: Signaling Connection Control Part
MTP: Message Transfer Part
NSP: Network Service Part

4.6.2.1 Message Transfer Part (MTP)

The function of the MTP is to ensure that signaling traffic can be transferred and delivered reliably between the end-users and the network. MTP is provided at three levels. Figure 4.7 shows the functionality of various MTP levels that will be described.

Signaling data link functions (MTP Level 1) provide an interface to the actual physical channel over which communication occurs. Physical channels may include copper wire, twisted pair, fiber, mobile radio, or satellite links and are transparent to the higher layers. CCITT recommends that MTP Level 1 use 64 kbps transmissions, whereas ANSI recommends 56 kbps. The minimum data rate provided for telephony control operations is 4.8 Kbps.

Signaling link functions (MTP Level 2) correspond to the second layer in the OSI reference model and provide a reliable link for traffic transfer between two directly connected signaling points. Variable length packet messages, called message signal units (MSUs), are defined in MTP Level 2. A single MSU cannot have a packet length that exceeds 272 octets, and a standard 16-bit cyclic redundancy check (CRC) checksum is included in each MSU for error detection. A range of error detection and correction features are provided in MTP Level 2.

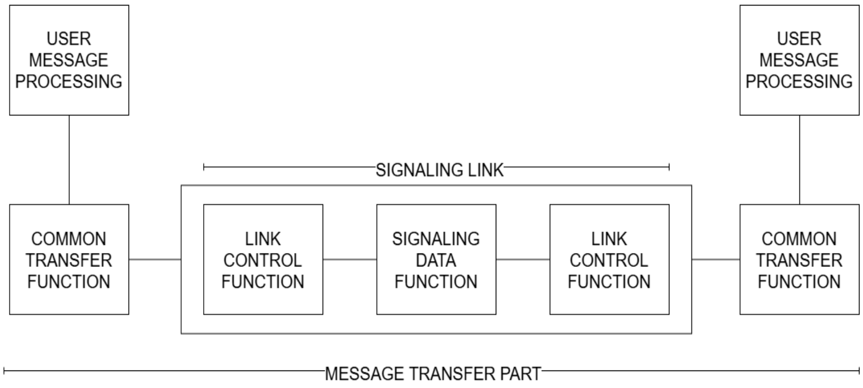


Fig. 4.7. Functional Diagram of *Message Transfer Part*

MTP Level 2 also provides flow control data between two signaling points to sense link failure. If the receiving device does not respond to data transmissions, MTP Level 2 uses a timer to detect link failure and notifies the higher levels of the SS7 protocol, which takes appropriate actions to reconnect the link.

Signaling network functions (MTP Level 3) provide procedures that transfer messages between signaling nodes. As in ISDN, there are two MTP Level 3 functions: signaling message handling and network management. Signaling message handling is used to provide routing, distribution, and traffic discrimination (discrimination is the process by which a signaling point determines whether or not a packet data message is intended for its use). Signaling network management allows the network to reconfigure in case of node failures. It has provisions to allocate alternate routing facilities in the case of congestion or blockage in parts of the network.

4.6.2.2 Signaling Connection Control Part (SCCP)

The signaling connection control part (SCCP) improves the addressing functions of the MTP. Although the MTP has limited addressing options, SCCP utilizes local addressing through subsystem numbers (SSNs) to identify users at a signaling node. Additionally, SCCP enables users to send global title messages, including 800 and non-billed numbers. As illustrated in Table 4.3, SCCP offers four service classes: two that are connectionless and two that are connection-oriented.

Table 4.3: SCCP Services

Class of Service	**Type of Service**
Class 0	Basic connection class
Class 1	Sequenced MTP connectionless class
Class 2	Basic connection-oriented class
Class 3	Flow control connection-oriented class

SCCP comprises four functional blocks. The SCCP connection-oriented control block facilitates data transfer on signaling connections. The SCCP management block provides functions to manage congestion and failure conditions that cannot be addressed at the MTP. The SCCP routing block forwards messages received from the MTP or other functional blocks.

Check Your Progress

1. What is the primary advantage of SS7 using out-of-band signaling?
   - A. It increases audio quality
   - B. It separates signaling from voice channels, allowing faster and secure control
   - C. It eliminates the need for switching
   - D. It increases the number of voice channels
2. Which of the following are SS7 network functions besides basic call routing?
   - A. Call hold and mute
   - B. Billing and text messaging
   - C. Mobile roaming and number translation
   - D. Firewall and antivirus
3. The SCCP in SS7 improves addressing capabilities by allowing ______ level routing of signaling messages.**(Fill in the blank)**

Answers:

1.B *2.C* *3.Global Title*

4.6.3 User part

As shown in Figure 4.6, the SS7 user part provides call control, management functions and call setup capabilities to the network. These represent the higher layers in the SS7 reference model and utilize the transport facilities offered by the MTP and SCCP. The SS7 user part comprises the *ISDN user part* (ISUP), the *transaction capabilities application part* (TCAP), and the *operations maintenance and administration part* (OMAP). The telephone user part (TUP) and the data user part (DUP) are included within the ISUP.

4.6.3.1 Integrated Services Digital Network User Part (ISUP)

The ISUP provides signaling functions for carriers and supplementary services for voice, data, and video within an ISDN environment. Previously, telephony requirements were included in the TUP; however, this is now considered a subset of ISUP. ISUP employs the MTP to transfer messages between various exchanges. An ISUP message includes a routing label that indicates the source and destination of the message, a circuit identification code (CIC), and a message code that defines the format and function of each message. These messages have variable lengths, with a maximum of 272 octets, including MTP level headers. In addition to the essential bearer services in an ISDN environment, user-to-user signaling, closed user groups, calling line identification, and call forwarding facilities are also provided.

4.6.3.2 Transaction Capabilities Application Part (TCAP)

The transaction capabilities application part in SS7 refers to the application layer that invokes the services of the SCCP and the MTP in a hierarchical format. One application at a node can thus execute an application at another node and utilize these results. Therefore, TCAP focuses on remote operations. IS-41 utilizes TCAP messages.

4.6.3.3 Operation Maintenance and Administration Part (OMAP)

The OMAP functions include monitoring, coordination, and control capabilities to ensure possible trouble-free communications. OMAP supports diagnostics recognized throughout the global network to determine loading and specific subnet work behaviors.

4.6.4 Signaling traffic

The main activities that contribute to the highest signaling traffic in a network, all handled through SS7, are call setups, inter-MSC handoffs, and location updates. To establish a call, information exchange is necessary about the location of the calling subscriber (including call origination and calling-party procedures) and the calling subscriber’s location. Both the calling and called subscribers may be mobile. When a mobile subscriber transitions between MSCs during a handoff, this results in a greater volume of information exchanged. Table 4.4 presents the signaling traffic produced for call setup in GSM (Mei93). The network refreshes the location update records whenever a subscriber moves to a new location. The signaling traffic created by the location update process, as a subscriber travels within and across VLR areas, is shown in Table 4.5.

Table 4.4: Signaling load for call setup and handoffs in GSM

Call originating from a Mobile	**Load**
Information on the originating MSC and the terminating switch	120bytes
Information on the originating MSC and the associated VSR	550 bytes
Call terminating at a Mobile	
Information on the switch and the terminating MSC	120bytes
Information on the terminating MSC and associated VLR	612 bytes
Information on the originating switch and the HLR	126 bytes
Inter MSC handoffs	
Information on the new MSC and associated VLR	148 bytes
Information on the new MSC and old MSC	383 bytes

Table 4.5: Signaling Load for Location Updating in GSM

Location Updating	**Load**
Information on the current MSC and associated VLR	406 bytes
Information on the current VLR and HLR	55 bytes
Information on the new VLR and old VLR	406 bytes
Information on the new	213 bytes
Information on the old VLR and HLR	95 bytes
Information on the new VLR and HLR	182 bytes

Check Your Progress

1. MTP Level 2 ensures reliable SS7 transmission through error detection, flow control, and retransmission.**(True/False)**

1. How does SS7 enable mobile roaming in early cellular networks?
   A. By switching towers based on IP
   B. Through base station polling
   C. By updating the HLR and VLR during registration
   D. By using packet switching

2. The SCCP in SS7 enhances message routing by enabling ______ level addressing, beyond point codes.**(Fill in the blank)**

Answers:
1.True 2.C 3.Global Title

4.6.5 Services of SS7

The SS7 network provides a robust framework for managing signaling and control in modern telecommunications. Its three primary service types are Touchstar, 800 services and alternative billing services. Details are provided below.

Touchstar– This type of service, also known as CLASS, consists of switch-controlled offerings that provide users with various call management capabilities. Services such as call return, call forwarding, repeat dialing, call blocking, call tracing, and caller ID are available. These features enable users to manage incoming and outgoing calls more effectively by enhancing call handling, security, and convenience. Some key features included under Touchstar services are:

- ***Call Return*:** Allows users to automatically redial the last incoming call, even if it was unanswered.

- ***Call Forwarding*****:** Enables users to redirect incoming calls to another number, ensuring they remain reachable even when away from their primary location.
- ***Repeat Dialing*****:** This service offers an automatic redial feature that continuously attempts to connect to a busy number until the call goes through.
- ***Call Blocking*****:** Permits users to block specific numbers from contacting them, boosting privacy and security.
- ***Call Tracing*****:** Aids law enforcement and service providers in tracking the source of a call. It is typically used in emergencies or for investigating harassing calls.
- ***Caller ID*****:** Displays the caller's number and, in some cases, their name, allowing recipients to identify incoming calls before answering.

Touchstar services significantly enhance users' control over call management, ensuring better accessibility, security and efficiency within the telecommunications network.

800 services– The Bell System introduced these services to provide toll-free access for callers to the services and databases offered by private parties. The service subscriber covers the costs associated with processing the calls. The service is provided under the 800-NXX plan and the 800 Database plan. In the 800-NXX plan, the first six digits of an 800 call are used to select the interexchange carrier (IXC). In the 800 Database plan, the call is referenced in a database to identify the appropriate carrier and routing information.

- ***800-NXX Plan*****:** Under this plan, the first six digits of an 800 number (prefix and exchange) determine the interexchange carrier (IXC) responsible for handling the call. This method allows for a straightforward routing mechanism based on number assignments, though it has limitations in flexibility and customization.

- ***800 Database Plan*****:** This approach involves querying a centralized database to establish the appropriate carrier and routing information for an 800-number call. Unlike the 800-NXX plan, this method offers greater flexibility in call routing, enabling dynamic allocation of services based on geographic location, time of day, or specific customer needs.

The introduction of 800 services revolutionized customer service and business communications, providing a seamless and cost-effective way for organizations to interact with clients while improving call routing efficiency through SS7-enabled databases.

Alternate Billing Service and Line Information Database—

Shortened to ADB/LIDB, these services utilize the CCS network to allow the calling party to bill a call to a personal number (which can be a third-party number, collect call, calling card, etc.) from any number. These services enable a caller to charge a call to an alternative number instead of the originating one, providing greater convenience and flexibility in payment methods.

The key functionalities include:

- ***Third-Party Billing*****:** Allows a call to be billed to a different telephone number, subject to authorization by the billed party.
- ***Collect Calls*****:** This permits the recipient of a call to accept the charges on behalf of the caller. It is often used for emergency or long-distance communication.
- ***Calling Card Calls*****:** Facilitates a mechanism for users to charge a call to a pre-registered calling card, which is authenticated through the LIDB.

The Line Information Database (LIDB) is a central repository for storing subscriber-related billing and validation information. When an alternate billing request is initiated, the SS7 network queries the LIDB to confirm authorization and identify the appropriate billing mechanism. This facilitates seamless processing and fraud prevention, making alternate billing services essential to modern telecommunications infrastructure.

Check Your Progress

1. Which of the following are features of Touchstar services?
    A. Call waiting and call forwarding
    B. Text messaging and call encryption
    C. 5G data offloading
    D. Call compression
2. How do the 800-NXX and 800 Database plans differ?
    A. NXX is dynamic, DB is static
    B. NXX uses fixed routing, DB allows intelligent routing
    C. Both use the same mechanism
    D. DB uses circuit switching, NXX does not
3. What is the primary role of the Line Information Database (LIDB)?
    A. Provide voicemail
    B. Store customer location
    C. Verify calling card and billing info
    D. Track call duration
4. Call tracing in SS7 helps identify the path and origin of a suspicious or malicious call.**(True/False)**
5. How does SS7 help process collect calls and third-party billing?
    A. By encrypting voice
    B. By authenticating callers via LIDB and routing calls through alternate billing systems
    C. By using cloud APIs
    D. By reducing call time

Answers:

1.A 2.B 3.C 4.True 5.B

4.6.6 Performance of SS7

The performance of the signaling network is assessed by connection setup time (response time) or the end-to-end signaling information transfer time. The specific hardware configuration and switching software implementation influence the delays in the signaling point (SP) and the STP. The maximum limits for these delay times have been specified in the CCITT recommendations Q.706, Q.716, and Q.766 [4].

Congestion Control in SS7 networks– As the number of subscribers grows, it is crucial to prevent congestion in the signaling network during heavy traffic. SS7 networking protocols offer various congestion control schemes that help traffic bypass failed links and nodes.

Check Your Progress

2. Which of the following are key parameters used to measure SS7 performance?
   A. Latency, CPU speed
   B. Call Setup Time, Message Delivery Delay, Throughput
   C. Signal strength, Bandwidth
   D. Temperature, Uptime
3. SS7 uses congestion control mechanisms like message queuing and rerouting to prevent overloads and maintain performance.**(True/False)**

Solutions:

1.B 2.True

4.7 SUMMING UP

This unit explored the wireless data services and how signaling and communication technology forms the backbone for the modern telecommunication services. Here, we explained Common Channel Signaling (CCS), Integrated Services Digital Network (ISDN), Broadband ISDN, Asynchronous Transfer Mode (ATM) and Signaling System No. 7 (SS7), their architectures and application and uses. The underlying method behind these technologies shows how wireless communications network operate, evolve and support connectivity all around the globe and how it layered the foundation for modern network systems.

Key takeaways from this chapter are:

- The role of signaling in telecommunication networks, emphasizing its importance in maintaining connectivity, security and data integrity.
- The architecture and functionality of CCS and ISDN, demonstrating how digital networks enable voice, video and data transfer over integrated services.
- The significance of ATM and SS7 in modern high-speed communication, highlighting their impact on network efficiency and signaling performance.
- The structure and applications of the X.25 protocol, illustrating its use in packet-switched data transmission.

4.8 POSSIBLE QUESTIONS

1. Explain the working principles of Common Channel Signaling (CCS).
2. Discuss the advantages of CCS over in-band signaling regarding capacity and speed.
3. What role does SS7 play in CCS, and how has it evolved in modern digital networks?
4. How does the layered protocol structure of CCS enhance its performance in telecommunication networks?
5. Explain the working principles of ISDN and its role in digital communication.
6. Discuss the advantages of ISDN over traditional analog telephone networks.
7. Compare the different types of ISDN services: BRI, PRI, and H channels.
8. How does ISDN provide both circuit-switched and packet-switched communication?
9. What were the main limitations of ISDN, and why has it been largely replaced by modern broadband technologies?
10. What is the key difference between BRI and PRI in ISDN?
11. Why was ISDN developed, and how did it improve traditional telephone services?
12. How does ISDN signaling differ from traditional analog phone signaling?

13. What are some real-world applications of ISDN? Can you think of a modern technology that has replaced it?
14. How did ISDN contribute to the development of internet access and video conferencing?
15. What is the purpose of ATM's Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI)?
16. How does an ATM achieve high-speed data transfer with minimal errors?
17. Why does ATM use fixed-size cells instead of variable-size packets?
18. Explain how ATM handles congestion control using the CLP field and traffic management techniques.
19. What is the primary difference between real-time and non-real-time ATM service categories?
20. Describe a scenario where real-time variable bit rate (rt-VBR) service would be more appropriate than CBR.
21. Why is the Unspecified Bit Rate (UBR) service considered to be a "best-effort" service?
22. How does ABR ensure fair bandwidth allocation among multiple connections?
23. What are the advantages of using GFR for IP traffic over an ATM backbone?
24. Compare and contrast Constant Bit Rate (CBR) and Variable Bit Rate (VBR) services in ATM networks. How do they handle different types of data?
25. Discuss the limitations of ATM's UBR service and how GFR was introduced to address some of these challenges.
26. Why does CCS offer greater trunking efficiency compared to conventional signaling?
27. What additional information can be transferred using CCS apart from call setup messages?
28. Explain the difference between CCS and conventional signaling.
29. What are the three primary services of SS7?
30. Define Touchstar services and mention any three features it includes.
31. How do 800 services work, and what are the two types of 800-number plans?
32. What is the Line Information Database (LIDB) function in SS7?

33. List the key functionalities of alternate billing services in SS7.
34. Define connection setup time and explain its significance in SS7 performance.
35. How does congestion control work in SS7 networks?
36. What are the advantages of CCS over conventional signaling?
37. Describe the architecture of the SS7 network with a diagram. Explain the roles of different components such as SSP, STP, and SCP.
38. Discuss the services of SS7 in detail, including Touchstar, 800 services, and alternate billing services.
39. How does SS7 improve network efficiency and security? Provide real-world applications.
40. Explain the process of congestion control in SS7. How does it ensure uninterrupted service during high-traffic loads?

4.9 REFERENCES AND SUGGESTED READINGS

1. Theodore S. Rappaport (2002), Wireless Communications-Principles Practice, 2nd edition, Prentice Hall of India, New Delhi.
2. William Stallings (2009), Wireless Communications and Networks, 2nd edition, Pearson Education, India.
3. Kaveh Pah Laven, Prashanth Krishna Murthy (2007), Principles of Wireless Networks -A Unified Approach, Pearson Education, India.
4. Freeman, Roger. (2005). CCITT Signaling System No. 7. 10.1002/0471728489.ch17.

***

UNIT- 5

WIRELESS LAN TECHNOLOGY

Unit Structure:

5.1 INTRODUCTION

Wireless LAN technology or WLAN is the extension of Wired Local Area Networks. Unlike wired local area networks, all the devices are liked without the use of wires. It is relatively new communication technology that wired LANs and uses Radio Frequency (RF) to transmit and receive data over the air. WLAN overcomes many demerits of wired LANs such as providing mobility of the users within a broad coverage area without losing the connection to the network. In the previous chapter, various wireless services were discussed. In this chapter, we will discuss about Wireless LAN technology, its classifications, system architecture and protocol formats of IEEE 802.11and IEEE 802.16 standards.

5.2 OBJECTIVES

After going through this unit, you will be able to:

- *understand* the fundamental concepts of Wireless LAN technologies, and wireless LAN requirements.
- *differentiate* between Infrared LANs, Spread Spectrum and Narrowband Microwave LANs.
- *describe* the system and protocol architecture of 802.11 standards.
- *illustrate* the various services provided by 802.11 standards.
- *explain* the concept of WiMAX technology.

5.3 WIRELESS LAN APPLICATIONS

Wireless LAN has many applications which can be broadly divided into four categories, viz., LAN extension, Cross building interconnect, Nomadic Access and Ad-hoc networking.

- **LAN Extension**: In the past, extension of LAN connection was time consuming and the connected devices were difficult to relocation. Situations where cabling of devices is impractical or where no predefined network infrastructure is not available, there we can easily extend the desired LAN network easily with the help of wireless LAN technology. Figure 5.1 shows a basic common wireless LAN setup common where a backbone wired LAN (e.g., Ethernet), connects the servers and workstations and uses bridges or routers for network links. A control module (CM) is used as an interface to connect the wireless LAN to the backbone. These types of WLANs are known as single cell LAN configurations. Multiple cell WLAN configures are also possible with more than one control modules.

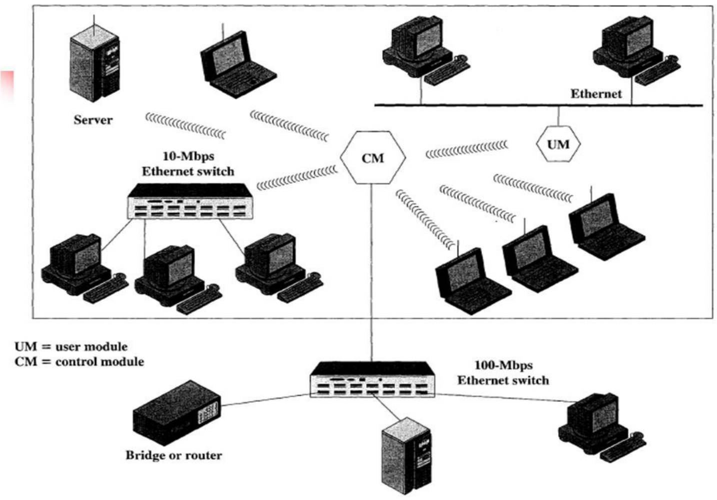


Figure 5.1 Single-Cell Wireless LAN Configuration [Stallings, 2004]

- **Cross Building Interconnect**: Wireless LAN can also be used to connect the LANs of nearby buildings through a point-to-point (P2P) communication to allow seamless data transfers. The P2P communication is served as a wireless communication between the LANs.

- **Nomadic Access**: Nomadic access allows to wireless connection between a LAN hub or server and a terminal device such as Laptop, mobile etc in which user can connect from different location.
- **Ad-hoc Networking**: a decentralized wireless network in which network devices (also called as **nodes**) communicates or connects to each other directly without relying on a fixed infrastructure such as access points and routers. Here, each device acts as a host and a router for forwarding data to other devices or nodes. There are various types of Ad-hoc networks, viz., Mobile Ad Hoc Networks (MANETs), Vehicular Ad Hoc Networks (VANETs), Wireless Sensor Networks (WSNs), and Internet-Based Mobile Ad Hoc Networks (iMANETs).

5.4 WIRELESS LAN REQUIREMENTS

Similar to any LAN, a wireless LAN should have requirements high capacity, ability to cover short distances, full connectivity among attached stations and broadcast capability. Some other additional requirements are as follows.

- **Throughput:** Throughput of a WLAN signifies the actual amount of data successfully travels over a communication channel within a specific time interval. To achieve the best throughput, a WLAN needs an efficient Medium Access Control (MAC) protocol to maximize its throughput. An efficient MAC protocol optimizes data transmission and reduces collisions in communication.
- **Scalability:** A wireless LAN should be scalable. It should support hundreds of nodes across multiple cells to achieve scalability.
- **Backbone LAN connection**: Usually, an infrastructure WLAN needs to connect to a wired backbone LAN with interconnection with stations. This can be easily accomplished through the use of control

modules that connect to both types of LANs. In addition to this, accommodations for ad hoc wireless networks and mobile users may also be required.

- **Transmission security and robustness:** Wireless local area networks (LANs) are vulnerable to interference and are easily intercepted if they are not built properly. A robust wireless LAN's architecture must ensure reliable data transmission even in noisy and congested environment and, should also provide some degree of protection against eavesdropping. Even in a noisy and crowded setting, a strong wireless LAN architecture must guarantee dependable data transfer and offer some level of eavesdropping protection.
- **Collocated network operation**: As wireless LANs gain popularity, it's likely that two or more of them may run in the same space or in a location where LAN interference would occur. Such interference could prevent a MAC algorithm from operating normally and permit illegal access to a specific LAN. Due to widespread use of wireless LANs, overlapping networks in the same area become common, which may cause interference. This interference can disrupt the normal functioning of MAC protocols and leads to communication delays, data collisions, or loss of connectivity. Overlapping of signals may also increase security risks by enabling unauthorized access or eavesdropping. Effective management of frequency channels, power control, and enhanced security measures are essential to minimize interference and protect the integrity and privacy of each wireless LAN. Hence, effective management of WLANs are essential to minimize their privacy, security and to reduce their interferences.
- **Handoff or roaming:** Mobile stations should be allowed to move seamlessly between wireless LAN cells using MAC protocol without losing their connections.
- **Dynamic configuration:** A wireless LAN should support dynamic configuration of MAC addressing and LAN network management. This will ensure automatic and dynamic addition, removal, and relocation of end systems seamlessly. Such flexibility is crucial for WLANs for

efficient resource management and reducing manual configuration efforts.

5.5 WIRELESS LAN TECHNOLOGY

Various transmission techniques are used in Wireless LANs. Bases on these techniques, WLAN products are generally categorized in to *Infrared LANs*, *Spread Spectrum* and *Narrowband micro waves* (Stallings, 2004) as shown in Figure 5.2. All current wireless LAN products fall into one of the following categories:

- **Infrared LAN:** In this wireless technology, infrared light (IR) is used to connect the devices. Data transmission between the devices is possible transmit within a small area typically in a room. It is similar to remote control communication used for television.

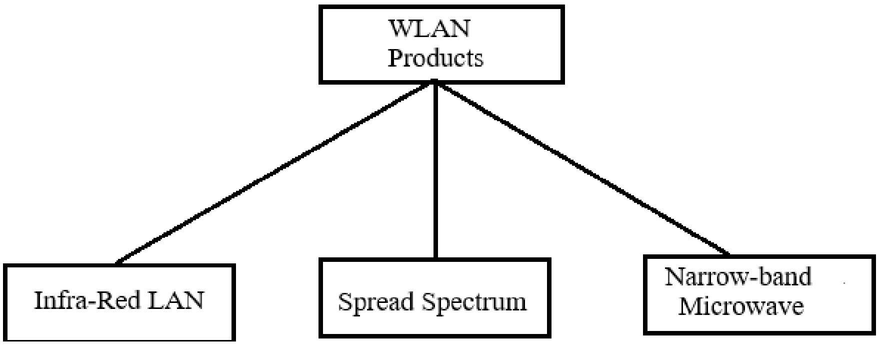


Figure 5.2 Category of WLAN products

- **Spread spectrum:** Spread spectrum is a communication technique in which information signals are transmitted over a much broader frequency band than is strictly necessary for the transmission of the signals. Spread spectrum provides robustness against interference, enhances security, increase privacy and, supports multiple users for sharing the same frequency range efficiently. Wireless LANs, viz., Wi-Fi and Bluetooth technologies utilizes it.
- **Narrowband microwave LAN:** Narrowband microwave LANs is a type of wireless technology which uses a microwave radio frequency band for signal processing in a relatively narrow bandwidth to establish communication over a LAN. This narrow bandwidth is just wide enough to accommodate the input signal.

5.6 INFRARED LANs

Infrared light cannot penetrate opaque walls. So, an individual cell of an infrared LAN (IR LAN) is limited to a single room and it is suitable for an indoor communication. Infrared LAN offers high security because it does not pass through walls which makes it difficult for unauthorized access to breeze the security.IR LAN has low interference with other devices used in various wireless communication technologies such as Wi-Fi and Bluetooth.

5.6.1Transmission Technologies of Infrared LANs

There are various transmission technologies available for data transmission in Infrared LANs. Three most widely used techniques are: *Directed Beam Infrared*, *Omnidirectional* and *Diffused*.

- **Directed Beam Infrared:** Directed beam infrared technology is used to establish point-to-point communication links. The coverage range of the communication mainly depends on precise focusing of the IR beams and on the emitted power. With a well-focused beam, IR LAN communications can be able to cover distances of several kilometres. Directed beam IR is generally ideal for creating cross-building connections. Figure 5.3 shows a Token Ring LAN Using Point-to-Point Infrared Links.

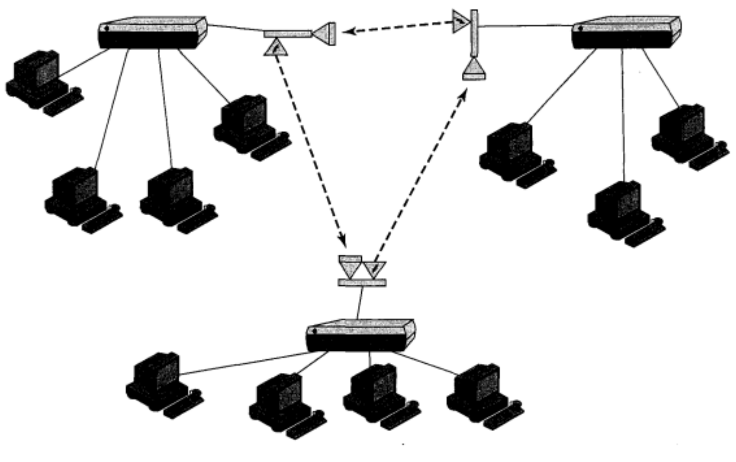


Figure 5.3Point-to-Point Infrared Links [1]

- **Omnidirectional:** In an omnidirectional infrared configuration, a single base station is used. This single base station is typically mounted on the ceiling and it is made available within the line of sight of all other stations in the LAN. This base station functions as a multiport repeater and it manages communication among various connected devices. It broadcasts omnidirectional infrared signals, which can be received by all IR transceivers in the coverage area. This setup enables centralized communication while maintaining good coverage within the room.
- **Diffused:** In a diffused infrared configuration, all infrared transmitters are aligned and focused at a specific point on a diffusely reflecting ceiling surface. IR radiation hitting the ceiling is scattered omnidirectionally and allows the signal to be received by all the receivers in the room regardless of their orientation. The diffused setup provides the user mobility and device positioning, making it well-suited for environments where direct aiming is impractical.

5.6.2Advantages of Infrared LANs

Infrared LANs have many advantages over Spread Spectrum and Narrowband Microwaves LANS. Followings are few of them.

- **Unlimited Spectrum:** The infrared spectrum is virtually unlimited. This unlimited bandwidth allows the possibility of achieving extremely high data rates that enables faster and efficient data transmission.

- **Less regulation:** In microwave spectrum, certain microwave frequency bands require licensing and strict regulations. In contrast to this, the infrared spectrum is unregulated worldwide. This license free regulation encourages innovation in communication technologies, making infrared an attractive option for various wireless applications without any regulatory constraints.

- **Coverage:** Infrared shares some common properties of visible light. Infrared light is diffusely reflected by light-coloured objects that makes the possibility of using ceiling reflection to achieve coverage of an entire room.

- **Security:** As Infrared light are unable to penetrate through walls or other opaque objects, making communication more secure against eavesdropping than microwave. In addition to that, a separate infrared installation can be operated in every room in a building without interference. This enabling the construction of very large infrared LANs.

5.6.3 Disadvantages of Infrared LANs

Infrared LANs have many disadvantages too. Followings are few of them.

- **Line of Sight**: Effective communication in an Infrared LAN requires clear line of sight between the transmitter and receiver for effective communication. Otherwise, the communication will face interruptions or complete loss of connection.

- **Speed and Range:** Compared to modern Wi-Fi and other RF based LAN technologies the Infrared LAN has less speed.

- **Higher Power Consumption**: Infrared communication faces intense indoor background radiation indoors causing ambient infrared noise. That reduces the signal clarity at infrared receivers. To overcome noise, higher transmitter power is needed in infrared communication.

5.7 SPREAD SPECTRUM LANs

- In Spread spectrum, the original signal is passed over a larger bandwidth than the required bandwidth. Because of border bandwidth it improves the security, increased resistance to interference and privacy. To allow redundancy it is necessary to use a larger spectrum than the required bandwidth for the original signal. This method is useful for secure transmission of data. A "Spread Code" is used to original signals bandwidth which is patterned series of numbers. A pictorial view of spread spectrum technique is shown in Figure 5.4.

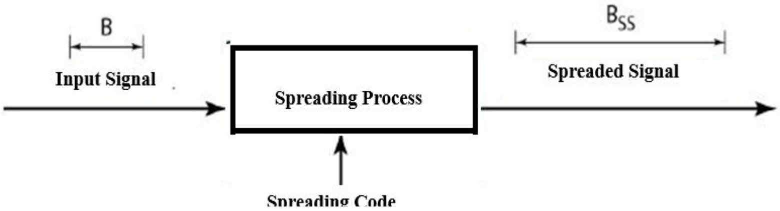


Figure 5.4 Spread spectrum techniques

5.7.1 Techniques of Spread Spectrum LANs

There are various techniques used in spread spectrum LANs. They are namely: *Frequency-Hopping Spread Spectrum (FHSS), Time-Hopping Spread Spectrum (THSS)* and *Chirp Spread Spectrum (CSS).* These techniques are discussed below.

- **Frequency-Hopping Spread Spectrum (FHSS):** In FHSS signals, data is transmitted in short bursts over one frequency, then hops to another frequency based on the hopping pattern. The changing of hops is controlled by a code known to both transmitter and receiver. FHSS uses code-division multiple access (CDMA) protocol to avoid interference, and stop eavesdropping.
- **Direct-Sequence Spread Spectrum (DSSS):** In DSSS it uses a pseudo random noise code which is multiplied with the data signals over a wider frequency band. DSSS is mainly used in IEEE 802.11b standards. Some practical and effective uses of DSSS include the code-division multiple access (CDMA) method, the IEEE 802.11b specification used in Wi-Fi networks and the Global Positioning System.
- **Time-Hopping Spread Spectrum (THSS):**In Time-Hopping Spread Spectrum (THSS), time is divided into discrete intervals or slots. The data is transmitted in a time slot is based on a pseudo-random time-hopping sequence. Unlike FHSS, which changes frequency, THSS changes the timing of signal transmission. THSS can be used in ultra-wideband (UWB) communications for achieving precise and low-power data transmission.
- **Chirp Spread Spectrum (CSS):** Chirp Spread Spectrum (CSS) uses chirp signals to transmit data. It is a modulation

technique in which frequency increases or decreases over time. Each chirp sweeps across a wide frequency range, which spreads the signal energy over time and frequency.

5.7.2 Advantages of Spread Spectrum LANs

Spread Spectrum LANs have many advantages too. Followings are few of them.

- **Interference Resistance**: As signals are spread over a wide frequency range, devices are less vulnerability to narrowband interferences. This ensures more reliable communication, even in noisy environments.
- **Security:** Spreading of signals reduces the chances of jamming or intercepting the transmitted signals. Spreading techniques like FHSS and DSSS are difficult to access from unauthorized users and hence are provides enhanced security.
- **Multipath Mitigation**: In WLAN, signals often reflect off walls or other opaque obstacles, causing signal fading and data errors at the receiving end. Spread spectrum techniques can be used to minimize the impact of such reflections. This in turn improves signal clarity and reduces errors in data transmission.
- **Shared Spectrum**: Shared spectrum permits multiple users to operate on the same frequency band with minimal interference. This makes spread spectrum LANs practically suitable for densely populated locations or multi-user environments, where multiple devices need to communicate simultaneously with reliable performances.

5.7.3 Disadvantages of Spread Spectrum LANs

Spread Spectrum LANs have many disadvantages too. Followings are few of them.

- **Lower Data Rates**: In spread spectrum, a significant portion of the available bandwidth is used for spreading the signal rather than carrying actual user data. This results in lower data transmission rate compared to narrowband systems operating in the same frequency range.

- **Complex Hardware**: The hardware used in spread spectrum required to support complex modulation and demodulation techniques. Design and maintenance of such complex systems are always difficult.

- **Higher Costs**: Compare to narrowband system equipment and implementation is costly in terms of designing, deployment, and maintenance.

- **Power Consumption**: Comparatively uses more power consumptions which may reduce efficiency in portable devices.

5.8 NARROWBAND MICROWAVE LANs

Narrowband microwave LANs is a type of wireless technology which uses a microwave radio frequency band for signal processing in a relatively narrow bandwidth to establish communication over a LAN. Narrowband Microwave signals operated both licensed and unlicensed microwave bands. Key concepts of this techniques include: *narrowband* and *microwave*. Narrowband microwave radio frequencies are usable for voice, text and video data transmission.

- **Narrowband:** Narrowband means a communication channel is consists of relatively small range of frequencies. Narrowband systems are useful for long range and low data-rate communication as compared to broadband communication systems.
- **Microwave:** It is a radio frequency generally used between 1GHz to 30 GHz. It is useful for high-speed point to point communication. This can be passed in a Narrowband communication channel.

5.8.1 Types of Narrowband RF

Narrowband microwave radio frequencies are either licensed or unlicensed.

- **Licensed Narrowband RF**: Microware RFs used for voice, data, and video transmission are licensed and coordinated within specific geographic locations to prevent them from potential data transmission interferences. Licensed spectrum gives the license holder a legal right to an interference-free data communications channel.
- **Unlicensed Narrowband RF**: Narrowband RF such as ISM bands (industrial, scientific and medical) are parts of the RF (radio-frequency) spectrum. They are unlicensed and users ISM-band LAN are at risk of interference disrupting their communications, for which they may not have a legal remedy.

5.8.2 Advantages of Narrowband Microwave LANs

Narrowband microwave has many advantages. Following are few merits of microwave LANs.

- **Large Bandwidth:** The microwave transmission offers a wider bandwidth for data communication at a fast rate. This is good for the applications that require teleconferencing, video streaming, and high-speed internet connectivity.
- **Speed:** Microwave signals travel at the speed of light, resulting fast data transmission
- **Reduced Power Consumption**: microwave frequencies exhibit low power consumptions. Hence, it is ideal for IoT and other energy-efficient applications.
- **Reliability:** Narrowband microwave offers a reliable communication and ensures uninterrupted connectivity. This is because , they are less prone to damage from natural disasters, such as earthquakes or floods, compared to physical cables.
- **Line of Sight Communication:** Microwave communication uses a Line of Sight (LOS) communication method requiring

a clear line of sight between the transmitting and receiving antennas. This makes it suitable for point-to-point communication over long distances where wired communication infrastructure is difficult to install.

5.8.3 Disadvantages of Narrowband Microwave LANs

Narrowband microwave has many disadvantages also. Following are few demerits of microwave LANs.

- **Line-of-Sight limitations:** As microwave signals use Line of Sight (LOS) communication method, they can be hampered by obstacles like trees, walls, buildings or hills. This can cause signal degradation or complete loss of communication.
- **Susceptible to Environmental Factors**: Microwave signals can be susceptible to interference from bas weather conditions like rain and storm resulting signal degradation or interruptions in communication.
- **Security threats:** As Microwave signals are wireless, they are more susceptible to potential interception and unauthorized access compared to wired communication systems. Proper encryption and authentication protocols need to be implemented to ensure the privacy and integrity of transmitted data.

Stop to Consider

Wireless LAN is used for wireless communication. Base on the use of transmission techniques, WLAN products fall into three broad categories, viz., *infrared LANs, Spread spectrum LANs* and *Narrowband microwave LANs*. Most widely used techniques in infrared LANS are namely, *Directed Beam Infrared*, *Omnidirectional* and *Diffused*. Narrowband microwave LANs may be either licensed or unlicensed. Licensed Narrowband microwave LANs are free from potential data transmission interferences.

5.9 IEEE 802 LAN STANDARDS

IEEE 802 defines a family of networking standards defined for various types of wired and wireless networks (e.g., Ethernet, Wi-Fi, Bluetooth) developed by Institute of Electrical and Electronics Engineers (IEEE) in February, 1985. IEEE 802.11 standard focuses on wireless networking. We look first at the overall architecture of IEEE 802standards and then at the specifics of IEEE 802.11.In this section, we will first discuss the overall architecture of IEEE 802 standard and finally we will discuss the specific IEEE 802.11 standard, dedicated for wireless LAN communication.

5.9.1 IEEE 802 Protocol Architecture

Protocols specifically designed for LAN and MAN (metropolitan area network) are responsible for the task of transmitting blocks of data over the network. We know that there are seven layers in OSI (Open Systems Interconnection) model and they are-*Physical layer*, *Data Linklayer*, *Network layer*, *Transport layer*, *Session layer*, *Presentation layer* and *Application layer*. In this model, higher-layer protocols (Network layer and above) are independent to underlying network architecture, and are applicable to LANs, MANs and WANs. The protocols and services defined in IEEE 802 standard corresponds to the lower two layers, viz., *data link layer* and *physical layer* in OSI model as shown in Figure 5.5.The bottom layer in IEEE 802 reference model is the physical layer, and is responsible for reliable the transmission and reception of data over various physical media. This layer performs various functions. Followings are few of them.

- Perform encoding and decoding of signals for reliable transmission.
- Establish connection between the devices to communicating medium and perform required synchronization of transmitted bits between sender and receiver.
- The physical layer is responsible establishing for the connection of devices to the medium and defining data transmission rate.

- Specifies transmission medium, transmission modes (Simplex, half-duplex and full-duplex) and physical topology for the communication.

The data link layer in IEEE 802 is responsible for providing service to LAN users. The functions of the data link layer include:

- Assemble the transmitted data into a frame with address and error detection
- Disassemble the received data frames, address recognitions and error detection.
- Managing access to the LAN transmission medium, providing interfaces to higher layers, and performing flow and error control.
- Establish connection between the devices to communicating medium and perform required synchronization of transmitted bits between sender and receiver.

The physical layer is responsible establishing for the connection of devices to the medium and defining data transmission rate

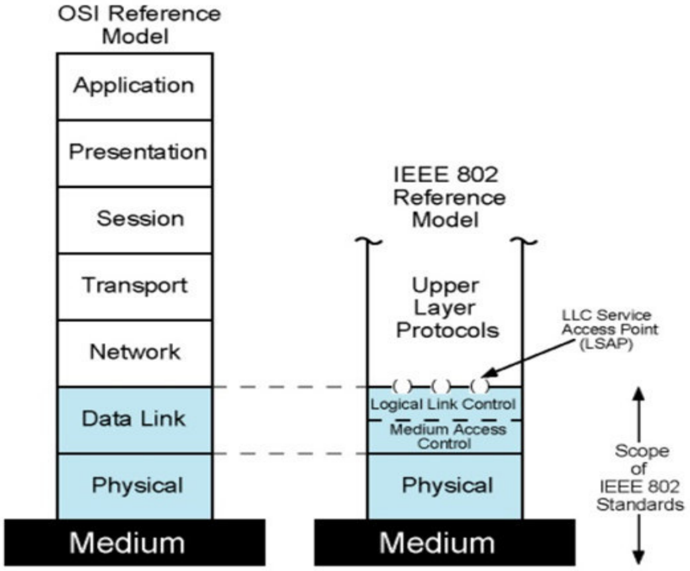


Figure 5.5IEEE 802 Protocol Layers Compared to OSI Model [Stallings, 2004]

The Data Link layer in 802 reference model is divided into two sub layers, viz., *Logical Link Control (LLC)* and *Medium Access Control (MAC)*.The main purpose of dividing the data link layer is because the logic required to manage access to a shared-access medium is not found in traditional data link layer and for the same LLC, several MAC options may be possible. This division enhances the conventional data link layer provides mechanism for accessing shared communication medium. Additionally, it provides flexibility to LLC to work with different MAC sub layers.

5.9.2 Logical Link Control Sublayer

Logical Link Control (LLC) sublayer is defined by 802.2 standards. This layer acts as an interface between the Network Layer and MAC sublayer. LLC multiplexes different network protocols such as (e.g. IP and IPX), making it possible to co-exist several network protocols within a multipoint shared communication environment. LLC is also controls flow control, frame synchronization, error checking, and providing services.

In IEEE 802, when data (e.g. IP packet) from higher-level arrives at data link layer, the LLC sublayer creates an LLC Protocol Data Unit (LPDU) by appends control information as a header. The LLC header control information may be DSAP, SSAP, and Control field. This combined frame is now called LPDU packet, and it is forwarder to the MAC sublayer. The MAC layer constructs a MAC frame by appending MAC control information, viz., *MAC header*, *MAC Trailer* at the front and back of LPDU. The MAC header contains MAC source/destination addresses and control bits. The MAC trailer contains Cyclic Redundancy Check (CRC) for error detection. The final MAC frame is now forwarded for the operation of MAC protocol.

5.9.2.1 Logical Link Control Protocol

The basic LLC protocol is designed after High Level Data Link Control (HDLC). The protocol data unit (PDU) in LLC is shown in Figure 5.6. The PDU has four fields, viz, Destination Service Access Point (DSAP), Source Service Access Point (SSAP), Control, and Information (i.e. user data). Let us discuss these fields in details.

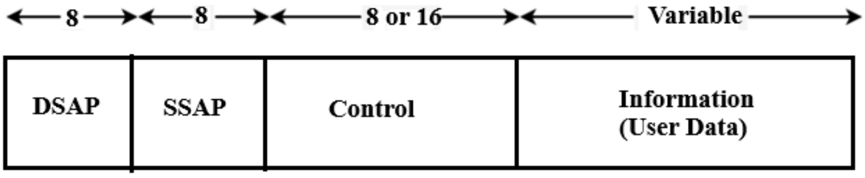


Figure 5.6 Protocol Data Unit (PDU) format

- **Destination Service Access Point (DSAP):** This field is generally 1 byte long, used to represent the address of destination SAP to which LPDU is sent. Six bits in DASP is dedicated to signifies the destination address, a use bit (U), and an Individual/Group (I/G) bit.
- **Source Service Access Point (SSAP):** This field is also 1 byte long, used to represent the address of source SAP form which the LPDU is generated. Six bits in SASP is dedicated to signifies the source address, a use bit (U), and a Command/Response (C/R) bit. On receiving the LPDU, C/R ignored, because Command/Response bit is used only to identify whether the receiving LPDU is a command or response.
- **Control field:** This field is consists of control, response, and sequence number information of LPDU.
- **Information field:** This field generally contains user data or information.

5.9.2.2 Logical Link Control Protocol Services

LLC specifies mechanisms for addressing the communicating devices i.e. SAPs and controls data exchange between the devices. LLC provides following three alternative services for the attached devices.

- **Unacknowledged connectionless service:** This is a datagram-style service also called **type-1** services. This service does not contain any data flow and error-controlling mechanism. Hence, delivery of data is not be guaranteed in this service.

- **Connection-Oriented service:** This service is similar to TCP, where, a logical connection is set up between two users before exchanging the data. Flow control and error control mechanism are offered in this service and is also known as **type-2** services.

- **Acknowledged connectionless service:** This service is a hybrid of type 1 and type-2 services known as type-3 services. It provides that user datagrams are to be acknowledged, but no prior logical connection is established.

5.9.3 Medium Access Control Sublayer

After receiving a block of data from the LLC layer, the MAC layer handles medium access tasks for shared communication and encapsulates frames so that they are suitable for transmission over the physical medium. MAC resolves the addressing of the devices required for the reliable communication. It determines the channel access methods for transmission, and also performed collision resolutions or initiating retransmission in case of occurring collision, viz., Carrier Sense Multiple Access with Collision Avoidance(CSMA/CA) and Carrier Sense Multiple Access/Collision Detection(CSMA/CD).Similar to other protocol layers, MAC uses a protocol data unit at its layer to carry out these responsibilities. This PDU is called a MAC frame in this layer. MAC frame is a crucial part of the MAC sublayer in IEEE 802 standards. The MAC frame format may vary slightly depending on the specific standard, but it generally contains key fields that control data transfer, ensure error checking, and provide addressing etc. Figure 5.7. shows the fields present in across all the IEEE 802 standards. They are namely, *MAC Control, destination address, source address, information,* and *CRC*.

- **MAC Control**: This field specifies the frame type, protocol version, and control information (e.g., retry, power management).

- **Destination MAC Address**: This field specifies destination address to which the MAC frame is intended i.e. it identifies the receiver of the MAC frame.

- **Source MAC Address:** This field represents source address from which the MAC frame is sent i.e. it identifies the sender of the MAC frame.

- **Information (user data):** This is called the body of the MAC frame. This may be LLC data from the next higher layer (e.g., IP packets) or control information relevant to the operation of the MAC protocol.

- **CRC:** The cyclic redundancy check (CRC) also known as Frame Check Sequence (FCS), present across in all standards. This is an error-detecting code used to detect transmission errors.

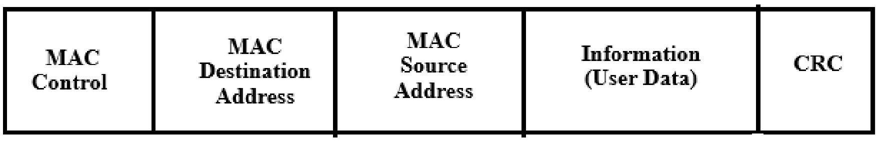


Figure 5.7 MAC Frame

5.10 COMMON IEEE 802 STANDARDS

There are many variations of IEEE 802 standards defined for handling specific network types, technologies, and protocols. Followings are example of some of the common IEEE 802 standards used.

- **IEEE 802.1:** This standard is defined for bridging and Network Management such as network switching, traffic prioritization etc. it is generally used for construction of data centres and enterprise LANs. Some of the popular protocols used are, viz.,*802.1Q* (VLAN tagging for network segmentation) and *802.1p* (QoS prioritization)

- **IEEE 802.2:** This standard ensures standardized communication across different 802 standards and provides services like acknowledgment, flow control, and error control.LLC (Logical Link Control) protocol is used in this standard.

- **IEEE 802.3:** Defines Ethernet, the dominant standard for wired LANs used for home/office/industrial networks. Protocols like CSMA/CD and Ethernet MAC are defined in this standard.

- **IEEE 802.11**: This standard defines the Wireless LAN popularly known as Wi-Fi), enabling wireless connectivity between devices using access points (AP) or Ad-hoc in homes, businesses, and any public hotspots. There are many variants of this standard is available such as 802.11a, 802.11b, 802.11g, 802.11i,802.11e, 802.11g(Wi-Fi 4), 802.11ac(Wi-Fi 5) and 802.11ax (Wi-Fi 6). Famous protocols used in these standards are CSMA/CA and Wi-Fi Protected Access protocols (WPA, WPA2, WPA3).

- **IEEE 802.15**: defines short-range, low-power Wireless Personal Area Networks (WPANs) usable for wearables, smart devices and IoT (Internet of Things). Protocols like 802.15.1(Bluetooth) and 802.15.4 (ZigBee) defined in this standard.

- **IEEE 802.16:** Defines protocols for broadband wireless access over metropolitan areas. It is also popularly known as (WiMAX). Protocols like, Orthogonal Frequency Division Multiplexing (OFDM) and Orthogonal Frequency Division Multiple Access (OFDMA) are used in this standard. Some variants of this standard include 802.16e (Mobile WiMAX) and 802.16m (WiMAX 2.0).

Some other IEEE 802 standard are, viz., IEEE 802.17 (Resilient Packet Ring (RPR)), IEEE 802.20 (Mobile Broadband Wireless Access), IEEE 802.22 (Wireless Regional Area Network (WRAN)), and 802.24 (Vertical Application TAG). (*See Figure 7.1 in Unit-7 to understand the relationship between the components of 802 family*).

Stop to Consider

IEEE 802 standards covering the physical and data link layers of OSI model. It includes two sublayers like LLC (Logical Link Control) for error handling and MAC (Medium Access Control).IEEE 802 standards have many variations. Some of the widely used standards include IEEE 802.3 (Ethernet), 802.11 (Wi-Fi), 802.15 (Bluetooth/ZigBee) and 802.16 (WiMAX), supporting both wired and wireless communications.

5.11 IEEE 802.11 STANDARDS

In 1990, a group named, 802.11 was formed to develop MAC protocols and physical specifications for wireless LAN applications. This group, initially targeted industrial, scientific, and medical bands, eventually developed Wi-Fi (IEEE 802.11 standard), which uses high-frequency radio waves instead of cables. This IEEE 802.11 standard defines the architecture and services of wireless local area networks (WLANs) supporting mobile devices, enabling seamless network access and integration with cellular technologies like 2G, 3G, 4G, and 5G.The major components of IEEE 802.11 are discussed in Unit-7. Let us discuss the architecture and the various services provided by IEEE 802.11 in this unit.

5.11.1 IEEE 802.11 Architecture

IEEE 802.11 LAN is based on a cellular architecture that connects multiple devices though wireless communication. Devices connected to a WLAN is known as *stations.* Two types of stations, viz., *Wireless Access Point (WAPs)* simply *Access Points (APs)*, and *clients* are connected to a WLAN. *Clients* are simple user devices such as Laptops, PCs, printers, cell phones etc. IEEE 802.11 LAN architecture supports three basic topologies, viz., *Basic service set (BSS)*, *Independent basic service set (IBSS)*, and *Extended service set (ESS).*The smallest building blocks in IEEE 802.11 architecture is the *Basic Service Set (BSS)*, and are also known as *cells*. Each BSS contains a group of wireless stations that uses the same MAC protocol, and access to the same shared wireless communication medium. A BSS may be isolated or interconnected to other BSSs trough some backbones, called *Distribution System (DS)*. The DS can be a switch, a wired network, or a wireless network. Two types of operational modes are supported by a BSS, viz., *infrastructure* and *independent* mode (Figure 5.2). In case of *infrastructure mode,* stations within a *Basic Service Set (BSS)* do not communicate with each other directly. Instead, all communication goes through the Access Point (AP).A station intending to send data to another station within the same BSS, first transmits its MAC frame to the AP to which it is connected, and it is then forwarded to the targeted station. Similarly, if the destination belongs to other BSS, the MAC frame is sent from the station to the AP, and then the AP relays it over the DS towards the final destination. When all the stations in the BSS are mobile stations, with no connection to other BSSs, the BSS is called an *Independent basic service set* (IBSS). An IBSS operates in *ad-hoc mode*, and communication among the stations within an IBSS happens directly without the involvement of any AP. A simple configuration of WLAN with IBSSs is shown in Figure 5.8, in which each station belongs to a single BSS.

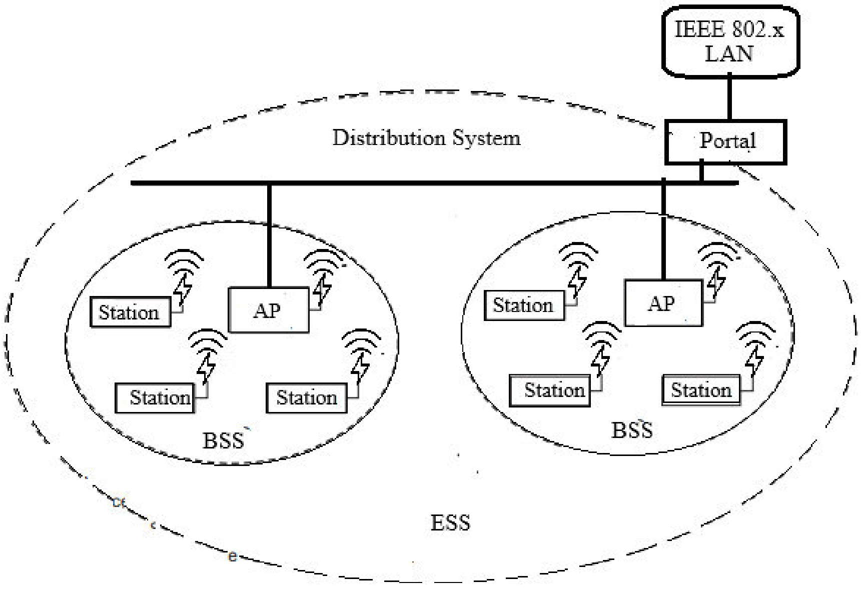


Figure 5.8 IEEE 802.11 Architecture

In WLAN, two BSSs may also overlap geographically, allowing a station to participate in more than one BSS. Additionally, the association between a station and a BSS is not fixed. At any moment, a station may turn off, come within range, and go out of range of a BSS. An *Extended Service Set (ESS)* can be formed by interconnecting a group of BSSs. In an ESS, each BSS has its own AP, and all APs are connected through the DS. Network consisting of ESSs provides mobility from one BSS to another while maintaining a continuous network connection. IEEE 802.11 infrastructure also supports the concept called, *portal* which is used to integrate an IEEE 802.11 architecture with a traditional wired LAN. The *portal* is a logic typically implemented in a bridge or router, which connects the DS to external wired networks. It facilitates interpretability and seamless communication between wireless stations and wired LAN devices. IEEE 802.11 supports both fixed and mobile wireless networks. It enables scalability, flexibility, and seamless integration with wired infrastructures accommodating dynamic network conditions and user mobility.

5.11.2 IEEE 802.11 Services

IEEE 802.11 defines nine services that provides equivalents to that which is inherent to wired LANs. These services are categorized as either *station services* or *distribution services*. *Station services* are implemented by every 802.11 station, including access point (AP) stations, whereas distribution services are provided between basic service sets (BSSs) by distribution system through APs. There are four station services viz., IEEE 802.11 station services are *authentication*, *de-authentication*, *MSDU delivery*, and *privacy* whereas there are a total of six distribution services provided in IEEE 802.11 service specifications. These distribution services are *association*, *reassociation*, *disassociation*, *distribution*, *integration*, and *MSDU* delivery. Three services, *authentication*, *de-authentication* and *privacy* are used to control IEEE 802.11 LAN access and confidentiality. The remaining six services are used to support the delivery of MAC service data units (MSDUs) between stations.

Station Services:

- **Authentication**: This service is used to verify the identity of the stations to each other before allowing to access the network. It is required for establishing a secure connection between a station and an AP.
- **De-authentication**: This service is used to terminate an existing authentication relationship. It is required on leaving a station from the network or when security policies require the disconnection of a station.
- **Privacy**: Also known as the confidentiality service, used to prevent the contents of messages from being read by other than the intended recipient.it ensures that transmitted data is protected from eavesdropping. This service provides for the optional use of encryption protocols such as WEP, WPA, or WPA2, WPA3to ensure privacy.

Distribution Services:

- **Association**: This service initiates the initial connection between a station to connect and an access point (AP) to an access the network for sending and receiving data.

- **Reassociation**: Enables a mobile station to switch its connection from one AP, to another, allowing it to move from one BSS to another maintaining network sessions.

- **Disassociation**: This service terminates an existing connection between a station and an AP. Disassociation may happen voluntarily or due to network conditions.

- **Distribution**: This service handles the transfer of data frames between stations between stations in the same or different basic service sets (BSS) through the distribution system.

- **Integration**: Enables communication between the 802.11 wireless network and and a station on an integrated IEEE 802.x LAN to allow transfer of data between them.

- **MSDU Delivery** – This service is used to ensure the reliable delivery of MAC Service Data Units (MSDUs) between the stations within a wireless LAN.

5.12 RELIABLE DATA DELIVERY IN 802.11

- Reliable data delivery in LAN using 802.11 is not an easy task, as the physical and MAC layers faces many challenges such as noise, interference, and signal fading. This result in the loss of a significant number of MAC frames. Even with error-correction codes, a number of MAC frames may not successfully be received. This can be handled by using the reliability mechanisms available at a higher layer, such as TCP. But, the retransmission rate at higher layers is relatively slow. Therefore, it is effective to deal with the errors at the MAC layer. IEEE 802.11 handles this issue using a frame exchange protocol. When a station receives a data frame, it sends back an acknowledgment (ACK). If the sender does not receive the ACK within a short period, it assumes the failure and retransmits the frame. This basic two-frame exchange approach ensures timely recovery from the errors. To enhance reliability, a four-frame exchange can also be used using four messages, viz., Request to Send (RTS), Clear to Send (CTS), Data, and ACK. RTS and CTS messages, help to prevent collisions from collision by notifying nearby stations to hold off transmissions, ensuring channel efficiency and reduces interference. RTS/CTS exchange is part of the MAC protocol, but it can be optionally disabled based on network requirements. The details of 802.11 MAC layer, MAC frame format and other physical layers of MAC is discussed in next UNITs.

5.13 WiMAX (IEEE 802.16 Standards)

- WiMAX (Worldwide Interoperability for Microwave Access)isa broadband internet technology developed by IEEE 802 group, also known as IEEE 802.16 standards. It has a long coverage up to 50 km.WiMAX technology is fast, convenient, and cost-effective. WiMAX has been replaced by new technologies like LTE and 5G. IEEE 802.16-2017 is the latest edition under IEEE 802.16, published on March 2, 2018.All earlier versions like 802.16e, 802.16m, 802.16s, etc. were merged, and was replaced by IEEE 802.16-2017.

5.13.1 IEEE 802.16 Protocol Architecture

The IEEE 802.16 protocol architecture maps to two layers in OSI model, viz., data link layer and physical layer. There are four layers in WiMAX and they are, *physical layer, transmission layer, MAC (Medium Access Control) layer,* and *convergence layer*. Let us discuss these layers.

Physical Layer: This is lowest layer from the bottom of 802.16 protocol. This layer corresponds to the physical layer of the OSI reference model. This layer performs following core functions:

- **Encoding/Decoding of Signals**: Responsible for the conversion of digital data into radio signals for transmission.

- **Preamble Generation and Removal:** Defines preambles at the beginning of a transmission for synchronization between the sender and receiver.
- **Bit Transmission and Reception:** Provide mechanism for actual transfer of bits over the air. Techniques like OFDM (Orthogonal Frequency Division Multiplexing), modulation (QPSK, 16-QAM, etc.), and error correction coding (FEC) are used for this purpose.

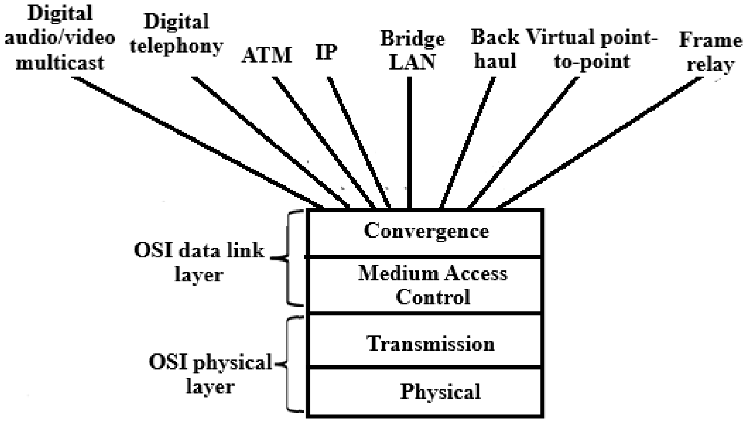


Figure 5.9 802.16 Protocol Architecture [6]

Transmission layer: This layer specifies the transmission medium and frequency bands for the communication. It also deals with error handling at bit-level, synchronization and framing of data at hardware level.

Medium Access control (MAC) layer: MAC Layer is a crucial part of the WiMAX protocol architecture, acts as an interface between the convergence layer and the physical layer. This level transmits data by converting into MAC frames using point-to-multipoint communication and relies on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

Convergence: Above the MAC layer is the convergence layer which is responsible for interfacing the WiMAX network with various external or higher-layer protocols such as IP and Ethernet. This layer is responsible for transforming higher-layer PDUs into required MAC format, managing QoS and traffic prioritization, enabling interoperability with other network technologies.

Check Your Progress

Q.1. Choose the Correct Option:

i) Which of the following is an advantage of using Spread Spectrum LANs?

(a) Higher cost of deployment
(b) Limited user support
(c) Interference resistance and improved security
(d) Requires clear line of sight

ii) In the IEEE 802.16 protocol architecture, which layer is responsible for converting higher-layer PDUs into MAC format and managing QoS?

(a) Physical Layer
(b) Transmission Layer
(c) Medium Access Control (MAC) Layer
(d) Convergence Layer

iii) What is the purpose of RTS/CTS messages in IEEE 802.11?

(a) To boost signal strength
(b) To prevent frame corruption Layer
(c) To increase bandwidth
(d) To avoid data collisions and improve channel efficiency

iv) Which of the following is the latest published standard in the IEEE 802.16 family?

(a) IEEE 802.16e
(b) IEEE 802.16-2017
(c) IEEE 802.16m
(d) IEEE 802.16s

v) Which of the following IEEE 802 standards defines Wireless LAN (Wi-Fi)?

(a) IEEE 802.3
(b) IEEE 802.2
(c) IEEE 802.11
(d) IEEE 802.16

5.13.2 IEEE 802.16 Protocol Services

The IEEE 802.16 standards provide following services:

- **Digital audio/video multicast:** Support one-way (e.g. digital broadcast cable TV) and two-way digital audio/video streaming (e.g. teleconferencing) to its users. Two-way streaming is special case of this service, and faces low latency and minimal jitter due to interactivity.

- **Digital telephony**: Supports multiplexed digital voice streams. A key application is the use of Wireless Local Loop (WLL) systems where fixed-line infrastructure is lacking.

- **ATM:** This service supports the transmission of ATM cells over a wireless medium.
- **Internet protocol:** This service provide supports the transfer of IP data grams using various QoS standards.

- **Bridged LAN:**This service enables MAC-layer bridging for transferring data between two LANs.

- **Back-haul:** This service is responsible for providing wireless trunking or backhaul for other networks. It is useful in connecting cellular or digital wireless telephone networks such as 3G, 4G and 5G.

Frame relay: Provides support for transmitting frame relay traffics. In contrast to ATMs, frame relay uses variable-length frames and are more flexible.

5.14 SUMMING UP

Wireless LAN technology or WLAN is the extension of wired local area networks. Based on the uses of the underlying techniques, WLAN products can be categorized in to *Infrared LANs*, *Spread Spectrum* and *Narrowband Microwaves*. IEEE 802 standards provide protocols for LAN and MAN (metropolitan area network) transmitting blocks of data over the network. IEEE 802 standards basically map the Physical layer and the Data Link layer of OSI reference model. The Data Link layer is divided into two sublayers, viz., Logical Link Control (LLC) sublayer and Medium Access Control (MAC) sublayers. IEEE 802.11 was formed to develop MAC protocols and physical specifications for wireless LAN applications. Two popular standards, viz., IEEE 802.11 (Wi-Fi) and IEEE 802.16 (WiMAX) have been discussed in this unit. The protocol structure and the system architecture of these standards have also been discussed in details.

5.15ANSWERS TO CHECK YOUR PROGRESS

1.(i) c (ii)d (iii) d (iv) b (v)c

5.16 POSSIBLE QUESTIONS

Short Answer Type Questions:

1. Define Wireless LAN. Write any four applications of wireless LAN.
2. State the types of wireless LAN based on the use of transmission Technology.
3. What is infrared (IR) LAN?
4. Differentiate between Direct beam infrared, Omnidirectional IR and Diffuse IR.
5. What is Spread spectrum? State the merits and demerits of Spread spectrum LANs.
6. What is Narrowband RF? State the advantages and disadvantages Narrowband Microwave LANs.

Long Answer Type Questions:

7. Describe briefly the different requirements for wireless LANs.
8. State the different variations of 802 standards.
9. Explain the architecture of the 802.11 standard.
10. Describe the various services supported in 802.11 standards.
11. Explain the various services provided by IEEE 802.16 standards.

5.17REFERENCES AND SUGGESTED READINGS

[1] Stallings, William. (2009). *Wireless Communications and Networks*. (2nd ed.). Prentice Hall. ISBN: 0-13-191835-4

[2] Hagen, Jon B. (2009). *Radio-Frequency Electronics: Circuits and applications* (2nd ed.). Leiden: Cambridge University Press. ISBN 978-0-511-58012-3.

[3] https://www.ni.com

[4] https://www.geeksforgeeks.org

***

UNIT- 6

ADVANCED WIRELESS TECHNOLOGIES

Unit Structure:

6. 1 INTRODUCTION

In the previous unit, we discussed about some popular wireless communication technologies specified in IEEE standards, viz., IEEE 802.11(Wi-Fi) and IEEE 802.16 (WiMAX). Though the technologies available to provide high-speed, reliable communication, but they are able to provide true user mobility. In the era of globalization, wireless technologies needed to be designed to support users' mobility during commutation, called as mobile communication technology. Mobile communications is an advanced wireless communication technology, and have gone through a rapid advancement in the past few decades. This progression has significantly improved the means of global connectivity, and enables users to communicate in much faster, efficient, and reliable ways. Mobile technologies have evolved through multiple generations. Each generation brought new capabilities and broader access to digital services. Inception of GSM (Global System for Mobile Communications) was a major breakthrough in wireless communication system. GSM is a family of standards to describe the protocols for second-generation (2G) digital cellular network. GSM introduced digital voice communication and SMS, and used by mobile devices such as mobile phones and mobile broadband modems. As data services became more essential, GPRS (General Packet Radio Service) emerged. It is an enhanced version of GSM architecture often referred to as 2.5G technology. As GPRS transmits data in packets using 2G infrastructure, it was only suitable for basic email and internet browsing, but it suffered from slower speeds and higher latency. To overcome this, 3G (Third Generation) was introduced, provides a major advancement over GPRS. 3G utilized advanced packet-switching and a dedicated network infrastructure for data transmission. This, results in lower latency, faster data rates, and more reliable connections. Inception of 3G technology, enabled support for data-intensive applications such as video calling, online gaming, and media streaming. 4G (Fourth Generation) is an enhancement over 3G, designed to support all-IP communications and broadband services with lower latency. Alongside these developments, WLL (Wireless in Local Loop) is also a wireless alternative to fixed-line telephone services, especially in rural or infrastructure-limited regions. Modern mobile communication has enough possibilities of future advancements and technology like 5G has evolved. In this unit, we will discuss above mentioned technologies in details.

6.2 OBJECTIVES

After going through this unit, you will be able to

- *understand* the GSM technology and its significance.
- *explain* the architecture and components of the GSM network.
- *describe* the concept of handoff and various GSM services.
- *understand* the architecture and different characteristics of GPRS.

- *state* various key features and standards of 3G network.
- *to evaluate* the advantages and limitations of 3G technology.
- *understand* the core concepts and the architecture of 4G network.
- *explain* the architectural components in 5G network.
- *describe* the concept and architecture of WLL.

6.3 SECOND GENERATION CELLULAR SYSTEM (2G TECHNOLOGY)

The starting technology of cellular mobile communication is termed as First-Generation Mobile Technology. They began mobile telephony using analog technology. 1G was launched in Japan by Nippon Telegraph and Telephone (NTT) in 1779. It enabled voice communication through analog signals and laid the foundation for other higher generation mobile connectivity. Nordic Mobile Telephone (NMT) and Advanced Mobile Phone System (AMPS) are such 1G standards that used FDMA (Frequency Division Multiple Access) mechanism for signal transmission. The bandwidth used in signal transmission in 2G is between 30 and 200 KHz. As digital technology advanced, the inherent advantages of digital systems over analog led to the eventual replacement of 1G by 2G networks. Second-generation (2G) cellular system digital telephony, like CDMA (Code Division Multiple Access) and TDMA (Time Division Multiple Access).One example of popular 2G mobile communication standard is GSM (Global System for Mobile).

6.3.1 GSM (GLOBAL SYSTEM for MOBILE)

The Global System for Mobile Communication (GSM) was introduced in the year, 1991. It was developed by the European Telecommunications Standards Institute (ETSI) for digital communication, it replaced 1G (First Generation) standard as1G technology uses incompatible analog data transmission system, causing fragmentation during handoffs. That caused international roaming difficult. To overcome this, GSM was introduced, which also unified mobile communication under a single digital standard. GSM uses TDMA digital wireless telephony technique. There are many variants of GSM. Some of the popular GSM variants are:

- **GSM-900:** Operating around 900 MHz. Frequency band 890MHz to 915 MHzis used for uplink (or reverse channel) and frequency band 935MHz to 960MHz is used for downlink (or forward channel). It is widely used GSM variant mostly used in Europe, Asia, and Africa
- **GSM-1800:** This variant is also called as Digital Communication Network (DCN), operating around 1800 MHz. Frequency band 1710MHz to 1785 MHz is used for uplink (or reverse channel) whereas, frequency band 1805 MHz to 1880 MHz is used for downlink (or forward channel). It is widely used GSM variant mostly used in Europe, Asia, and Middle East countries.
- **GSM-1900:** This variant operates around 1900 MHz and can also be used in Personal Communication system (PCS)bands. Here, the downlink frequency band is 1930 MHz to 1990 MHz, and uplink frequency band is 1850 MHz and 1910MHz. it mostly operates in U. S. A.

6.3.2 GSM System Architecture

The architecture of a GSM system has four main interconnected subsystems, viz., *Mobile Station (MS), Base station subsystem (BSS), Network and switching subsystem (NSS,* and *operation support subsystem (OSS)*. Figure 6.1 shows the system architecture of GSM. These subsystems are connected among themselves. They are connected with the users of GSM through some particular network interfaces such as Public Switched Telephone Network (PSTN), Integrated Services digital Network (ISDN), Circuit-Switched Public Data Network (CSPDN), and packet-switched public data network (PSPDN). Let us discuss theses subsystems.

- **Mobile Station (MS):** Mobile Station (MS) represents the end-user mobile equipment (ME) such as mobile phone, which includes GSM mobile devices containing key components like, Digital Signal Processor (DSP), the Radio Frequency (RF) chip, and the Subscriber Identity Module (SIM). The SIM card is implemented as a smart card that stores user's identity and authentication credentials. It is essential for accessing GSM network services.

- **Base station subsystem (BSS):** The BSS is the radio subsystem that forms the cell structure of GSM network. It manages the radio communication between the Mobile Station (MS) and the Network Switching Subsystem (NSS).BSS includes a transmission component, *Base Transceiver Station (BTS)*, and a managing component, *Base Station Controller (BSC).*The BTS carries out radio signal transmission and reception. It also does signal processing, voice encoding/decoding, and transmission rate modifications. The BSC is responsible the management of the Um, where Um is air interface between MS and the BTS in GSM. Functions like channel allocation and deallocation, handover, power control, and timing of radio signals are performed by a BSC. Ab is interface is used to link BTS to BSC, provides means for both user data transmission and control signals for controlling multiples BTSs by BSC using LAPD (Link Access Protocol on D channel) protocol. Another interface, called A interface connects the BSC to MSC. This interface manages services like call setup, location updates, user authentication, and inter-BSC handoffs. Various protocols used in this interface are, viz., Signaling Connection Control Part (SCCP), BSSAP (Base Station Subsystem Application Part), and Base Station Subsystem Management Application Part (BSSMAP) which are used as a part of SS7 (Signaling System No. 7) protocol.

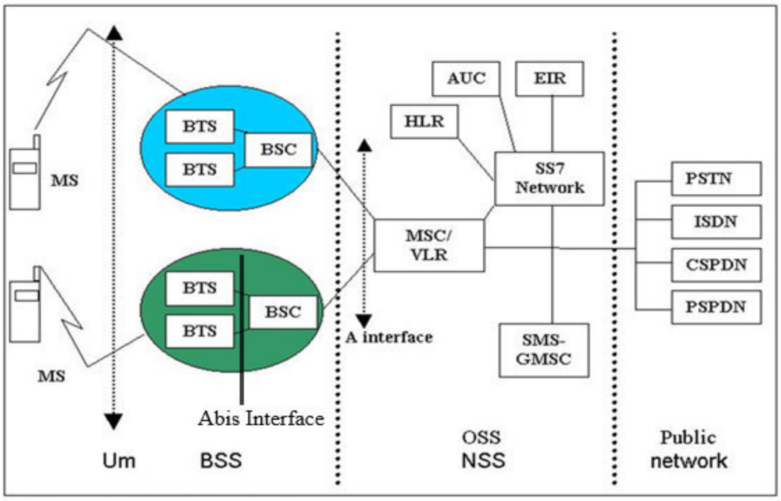


Figure 6.1 GSM System Architecture (*Source: https://mobiletelecommunicationarchitecture.blogspot.com/2010/07/ gsm-system-architecture-gsm-system.html*)

- **Network and switching subsystem (NSS):** The NSS is the core component the GSM network. It controls the main switching functions of GSM, enabling the MSCs to communicate other public networks like PSTN and ISDN. The Mobile Switching Center (MSC) is the core of the NSS, and it handles roaming, mobility, interfacing with other MSCs, and external network. NSS contains the databases, Home Location Register (HLR), Visitor Location Register (VLR), Authentication Center (AUC), and Equipment Identity Register (EIR) for managing call setup, routing, billing, mobility management, and subscriber data storage. The HLR, is a central database that stores permanent subscriber data, viz., IMSI (International Mobile Subscriber Identity), Mobile phone number (MSISDN), Subscribed services, and Current location (MSC/VLR area). The VLR database is linked to MSC that temporarily stores the visitor's information about currently serving by the MSC. When user roams into an area under a new MSC, it retrieves the user's information from the HLR. AUC stores all the security credentials of user to verify the users, ensuring data confidentiality using encryption protocols. The EIR keeps records of IMEI (International Mobile Equipment Identity) numbers of all user devices to identify whether a device is allowed, stolen, unauthorized or under observation.

- **Operation support subsystem (OSS):** OSS subsystem is responsible for supporting the GSM system to manage the configuration, performance, fault and, also to monitor the network.

6.3.3 GSM Services

GSM provides wide range of services. These services are broadly categorized into three main categories of services, *Bearer services, Teleservice,* and *Supplementary services*. Let us discuss these services.

- **Bearer Services:** Bearer Services, also known as data services, are the fundamental data transmission services provided by GSM, enables the subscribers to send and receive data to/from remote computers or mobile phones. The necessary bandwidth and data transfer mechanisms are supported by this service.
- **Telephone services:** This is an end-user communication services that transmit voice or text, supporting services, viz., emergency calling, text emoji, smiley including videotext and teletext.GSM provides both the voice-oriented teleservices and the non-voice teleservices.
- **Supplementary Services:** These services include additional features provided on top of basic voice and messaging service such as call forwarding, call barring, call waiting. Call hold, and multiparty communication call conferencing etc.

6.3.4 GSM Protocol Architecture

GSM Network has its own protocol architecture which is designed to handle the complexity of mobile communication. This protocol stack has three main layers, viz., *physical layer (layer 1), data Link Layer (Layer 2)*and *network layer*.

- **Physical layer (layer 1)**: It is the lowest layer of the GSM protocol architecture. This layer performs actual transmission of data over Um-Interface (air interface), This layer deals with radio frequency (RF) signaling, modulation using Gaussian Minimum Shift Keying (GMSK), channel allocation (e.g. FDMA, TDMA), synchronization, and other physical transmission parameters.
- **Data Link layer (layer 2)**: The Data Link Layer exists above the physical layer, and it operates between the MS and the BSS. It uses LAPDm(Link Access Protocol on the Dm channel) protocol, a derivative of LAPD and perform various task like framing, error-detection, error correction, flow control, re-transmission and link management. to a achieve reliable communication.
- **Network layer (layer 3)**: This is the topmost layer in GMS protocol stack. It has three sublayers, viz., Radio Resource (RR) Management, Mobility Management (MM), Connection Management (CM). RR sublayer provided functionalities like, channel allocation, power control, handoff management etc.MM sublayer deals with location tracking, user identification, authentication and security management. CM sublayer takes the responsibility of call-session management, SMS handling, and other supplementary services (call barring, call forwarding, call waiting etc.)

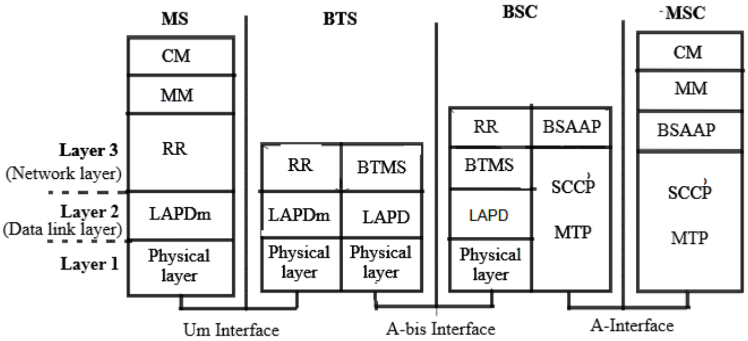


Figure 6.2 GSMProtocol Stack

Stop to Consider

GSM is a 2G digital mobile communication standard provides digital voice and SMS services. GSM has many popular and widely used variants like GSM-900, GSM-1800 and GSM-1900. GSM system has four major subsystems, Mobile Station (MS), Base Station Subsystem (BSS), Network and Switching Subsystem (NSS), and Operation Support Subsystem (OSS). Three major categories of services, viz., Bearer Services, Teleservices, and supplementary services are provided in GSM.

6.3.5 GSM Handover

The procedures of transferring an ongoing call (or data) session from one base station to another without interrupting the service is called *handover* (or *handoff*). GSM service often requires handover, as single cells do not cover the whole service area. Handover is also required to provide user mobility, quality maintenance, load balancing, and network optimization. In GSM, four possible handover scenarios are supported (Figure 6.3). Let us discuss them.

- **Intra-cell handover:** This type of handover occurs within a cell itself (scenario). Usually happened because of interference or degradation of signal quality on the current channel. It is resolved by the BSC, by changing the carrier frequency (Scenario 1).

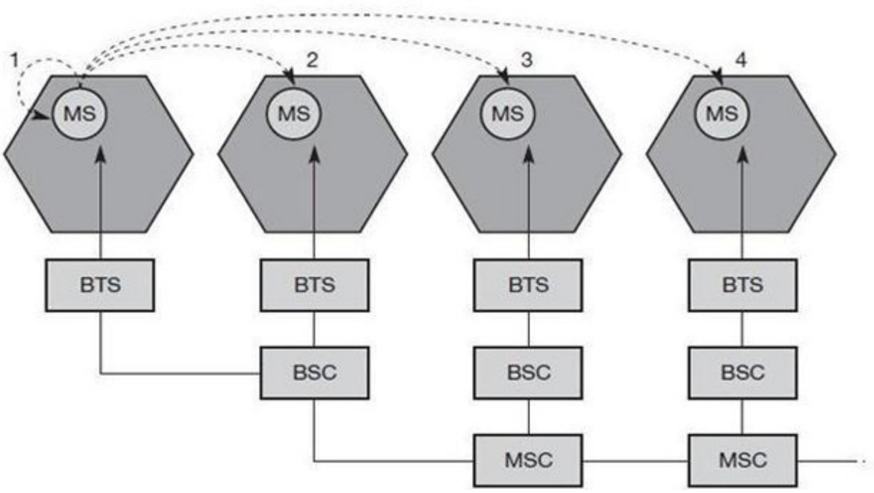


Figure 6.3 Handoff scenarios in GSM (source: [4])

- **Inter-cell, intra-BSC handover**: This is a typical handover occurs when a mobile station moves from one cell to another, and both cells stays within the control of the same BSC. The BSC handles this type of handover directly, assigning a new radio channel in the new cell and releases the old one (scenario 2).
- **Inter-BSC, intra-MSC handover**: This type of handoff triggered when, when a MS moves between cells controlled by different BSCs which are controlled by same Mobile Switching Center (MSC). in this case, handoff between the BSCs is coordinated by the controlling MSC (scenario 3)
- **Inter MSC handover:** This is a complex handover scenario occurred, when a mobile station (MS) moves to a cell to different MSCs. In this case, both MSCs perform the handover together. For this coordination between the serving MSC and the target MSC is needed (scenario 4).

6.3.6Advantages of GSM

- **Compatibility with other technology**: GSM is widely used all over the world with different communication network technologies as it is easily compatible with many different networks and devices.

- **Efficient use of bandwidth:** GSM uses time division multiplexing (TDM) technique for data transferring that enables different users to share the same frequency channel at different times. This method ensures efficient use of the available frequency spectrum, reducing congestion, also enhance network performance.

- **Security:** GSM protocol supports various kinds of security features, viz., authentication, encryption and confidentiality, which helps to protect the user's data and privacy.

- **Handoff or Roaming:** Roaming features of GSM allows users to roam different places of the world. This facilitates global mobility with seamless connectivity.

6.3.7 Disadvantages of GSM

- **Limited coverage:** In some remote geographical regions, it may not be feasible to build GSM infrastructure. In such case, GSM networks may have limited or no coverage.

- **Network congestion:** Too many GSM users at a place may lead to network congestion during peak hours of use, which can lead to dropped calls or poor call quality and network for the internet.

- **Security vulnerabilities:** Snooping, and spoofing are some kinds of network attacks, which are still vulnerable for GSM, though GSM offers enhanced security features.

- **Data transfer speed:** Compared to other new technologies such as 3G, 4G and 5G GSM networks offer relatively slow data transfer speeds.

- **Limited capacity:** As the size of data has increased dramatically data by day, user requires high-speed internet access or other data-intensive applications. The capacity of GSM is limited as compared to 3G, 4G, 5G GSM networks as it is unable to handle huge data volume.

6.3.8 Other 2G Technologies

Several other important 2G technologies were also developed alongside. These standards were particularly in North America, some parts of Asia, and Latin America. These include IS-95 (cdmaOne), PDC (Personal Digital Cellular), D-AMPS (IS-136), and iDEN (Integrated Digital Enhanced Network). Later on, these technologies were phased out by more advanced communication standards like 3G and 4Gs.

Check Your Progress-1

Q.1. Choose the Correct Option:

i) What generation of mobile communication does GSM represent?
   (a) 1G
   (b) 2G
   (c) 3G
   (d) 4G

ii) What protocol is used in the data link layer of GSM for reliable communication?
   (a) GMSK
   (b) CDMA
   (c) LAPDm
   (d) TCP

iii) What type of handover occurs when a mobile device moves between two BSCs controlled by the same MSC?
   (a) Inter-BSC, intra-MSC handover
   (b) Intra-cell handover
   (c) Inter-cell, intra-BSC handover
   (d) -MSC handover

iv) Which of the following services is classified as a Supplementary Service in GSM?
   (a) Emergency calling
   (b) SMS
   (c) Call forwarding
   (d) Voice calling

v) Which interface connects the Base Station Controller (BSC) to the Mobile Switching Center (MSC)?
   (a) Um-Interface

(b) Abis-Interface
(c) A-Interface
(d) F-interface

6.4 SECOND AND A HALF GENERATION CELLULAR SYSTEMS (2.5G TECHNOLOGY)

2.5G (also known as the second-and-a-half generation) technology, is a transitional intermediate technology that bridge 2G and 3G cellular networks. It was introduced in the late 1990s to early 2000s to packet-switching data capabilities to the overusing existing 2G infrastructure, allowing faster mobile internet access, email, and MMS (Multimedia Messaging Service). GPRS(General Packet Radio Service) is the core of 2.5G family.

6.4.1 GPRS (GENERAL PACKET RADIO SERVICE)

General Packet Radio Service, in short GPRS was standardized by European Telecommunications Standard Institute (ETSI). It is based on packet mobile data service. The main aim of GPRS is to enhance existing 2G cellular systems to provide efficient and flexible data transmission with higher rates. GPRS was introduced in early 2000, and it is the core of 2.5G cellular technology. GPRS uses existing GSM infrastructure but introduces new network elements and protocols to support unicast, multicast, and broadcast services. This enables GPRS to facilitates mobile internet access, email, and MMS (Multimedia Messaging Service) with existing GSM services. This leads a significant step towards3G technology.

6.4.2Characteristics of GPRS

GPS has many characteristics and some of them are discussed below:

- **Packet-Switching Operation:** GPRS operates with packet switching technology compared to GSM which uses circuit switching technology. So, the bandwidth used for the transmission of data can be efficiently utilized in data transmission. The packet switching scheme is more utilized effectively in GPRS network.

- **Always-On Connectivity:** Unlike traditional dial-up connections, GPRS allows for always-on internet connectivity. Users don't need to dial up to establish a data session each time. Users using GPRS connectivity are charged based on data usage rather than connection duration.
- **Security:** GPRS also provides different security services, viz., authentication, user identity confidentiality, user information confidentiality and access control which makes GPRS more secured than GSM.
- **Compatibility:** GPRS supports IP Protocol which makes it suitable for browsing, email surfing, MMS, and other internet services. As GPRS works alongside existing GSM networks, making it possible for the devices to switch between GSM (for voice) and GPRS (for data).
- **Data Transmission:** Use packet switching method in GPRS, allows users to and receive data in bursts. This makes GPRS more efficient than continuous circuit-switched transmission.
- **Quality of Service (QoS):** GPRS guarantees good Quality of Service (QoS) by providing different priority levels and performance guarantees for different classes of user traffics based on level of service required by the users such as faster speed, lower delay or higher reliability.

6.4.3 GPRS System Architecture

The GPRS system architecture is almost similar to GSM. The various components of GSM are also contained in GPRS architecture such as Mobile Station (MS), Base Station Subsystem (BSS), Mobile Switching Center (MSC) and storage facilities, viz., Home Location Register (HLR), Visitor Location Register (VLR), and Equipment Identity Register (EI). Two new components, viz., GSN (GPRS Support Nodes) and SGSN (Serving GPRS Support Nodes) are added to the GPRS architecture along external packet data network (PDN), gateway GPRS support node (GGSN) and Packet Control Unit (PCU). A pictorial view of GPRS architecture is depicted in Figure 6.4. The functionalities of MS, BSS, MSC, HLR, VLR, and EI are same as GSM, and have been already discussed in section 6.3.1.GSN and SGSN are in fact routers and new additional interfaces are defined in GPRS. Gateway GPRS Support Node (GGSN) is a key component in GPRS network. It interconnects GPRS network to external packet data networks (PDN) like IP and x.25 through G_i interface. This node contains routing information for GPRS users and transfers packets to the SGSN via an IP-based GPRS backbone network (called as G_n interface), The GGSN is connected to external networks (e.g., IP or X.25) via the Gi interface. GGSN performs functions like address conversion, packet forwarding, and encapsulate and decapsulate data packets (called data tunneling), QoS management, security handling. Serving GPRS Support Node (SGSN) supports the mobile stations (MS) using Gb interface. It is connected to the Base Station Controller (BSC) through Frame Relay. SGSN operates at the level of Mobile Switching Center (MSC). The SGSN performs several essential functions such as mobility management, user address management using GPRS Register (GR), tracking locations of individual mobile stations, collecting billing information for user data usage, and enforcing security. The GPRS Register is contained within the Home Location Register (HLR), stores about data relevant services.

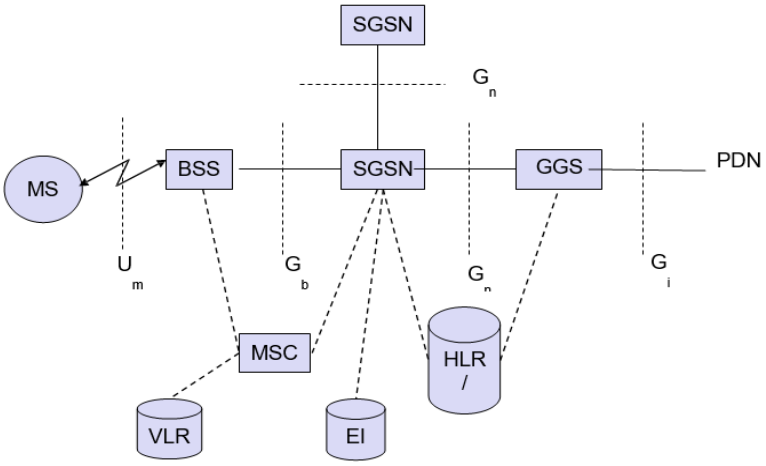


Figure 6.4 Architecture of GPRS

(Source: https://ebooks.inflibnet.ac.in/itp12/chapter/gprs/)

6.4.4 Other 2.5G Technologies

Alongside 2.5G, other communication technologies were also developed using the core of 2.5G mechanism. High-Speed Circuit Switched Data (HSCSD), Enhanced Data rates for GSM Evolution (EDGE). HSCSD is a circuit switched protocol that enables transmission large data and multimedia files. EDGE (also known as 2.75G), an enhanced technology over GSM that facilitates higher rate of data transmission compared to conventional GSM.

Stop to Consider

2.5G is bridging communication technology between 2G and 3G based on packet-switched data that uses existing GSM infrastructure. GPRS (General Packet Radio Service) is core standard of 2.5G technology. Other 2.5G technologies includes HSCSD (circuit-switched for larger data files) and EDGE (Enhanced Data rates for GSM Evolution)

Third Generation, in short 3G is a cellular wireless communication technology. It is more advanced than its predecessors, 2G and 2.5G technologies. There were different 2G standards adopted in America, Europe and Japan at same time, making the incompatible roaming situations. So, the basic idea behind 3G technology development was to unify these 2G standards by bringing them under a single umbrella. For this purpose, in early 2000s, International Telecommunication Union (ITU) established a set of standards, called International Mobile Telecommunications-2000 (IMT-2000). Any network that complies with IMT-2000 is termed as 3G technology, that provides high-speed data transfer, more effective internet connectivity, and multimedia services. 3Gtechnology uses Circuit switching for voice communication, and Packet switching for data transmission. It supports maximum data transfer rates of 2.05 Mbps, 384 Kbps, and 128 Kbps for stationary devices, devices moving at a slow pace, devices moving at high speed, respectively. The first 3G technology was commercial launched by NTT DoCoMo in Japan on 1 October 2001.

6.5.1 IMT-2000 Standards

IMT-2000 specified five standards for 3G, viz., W-CDMA (Wideband Code Division Multiple Access), CDMA2000, TD-SCDMA (Time Division Synchronous CDMA), UWC-136 (Universal Wireless Communications), and Digital Enhanced Cordless Telecommunications (DECT).

- **W-CDMA (Wideband Code Division Multiple Access):** W-CDMA is a 3G technology developed by 3GPP (3rd Generation Partnership Project) that enables simultaneous voice, data, and multimedia services. W-CDMA supports circuit-switched and packet-switched data, glob roaming, and high network capacity. It supports high speed data transmission, and broadband Internet access
- **CDMA2000:** CDMA2000, developed by 3GPP2, is a 3G evolution of the 2G cdmaOne standard. It provides spectrum-efficiency and backward compatibility with 2G CDMA.
- **TD-SCDMA (Time Division Synchronous CDMA):**TD-SCDMA is 3G standard, jointly developed by the Chinese Academy of Telecommunications Technology and Datang Telecom. It uses Time Division Duplexing (TDD) to transmit data on the same frequency at different times.
- **UWC-136 (Universal Wireless Communications-136)**:UWC-136 is also referred to as EDGE. It was developed by 3GG that enhanced the existing GSM/GPRS infrastructure, enabling data speeds of up to 384 Kbps.
- **DECT (Digital Enhanced Cordless Telecommunications):** DECT is a European standard developed by ETSI. It was designed for cordless telephony in residential and business environments. DECT supports high-quality voice and low-speed data over short distances.

6.5.2Key Features of 3G Technology

3G technology has many key features that distinguish it from existing1G and 2G technologies. Following are few key features of 3G.

- **Higher Data Rates:** Compared to 2G, 3G networks provide more data speeds ranging from 128 Kbps to up to 2.05 Mbps.
- **Voice and Data Integration:** Users can simultaneously make voice calls and access data services. Users can also browse internet, send/receive emails while entertaining on a call. The quality of voice also improved with reduced call drops.
- **Seamless Global Roaming:** Global roaming is also supported by 3G networks, enabling interoperability with seamless service access across various networks and geographical boundaries.
- **Enhanced Multimedia Services:** It supports different kinds of multimedia services such as video calling, streaming, mobile TV, and online gaming.
- **Better Security:** 3G services are more secured compared to other predecessors. It implements encryption, authentication, and data protection algorithms to make the communication reliable and secure.
- Improved Battery Life The 3G technology has a more efficient power management system, which improves the battery life of mobile devices.

6.5.3 3G Network Architecture

The 3G network enables voice calls, data, and multimedia services. It is designed to support both circuit-switched and packet-switched services. It has three major components, viz., User Equipment (UE), Radio Access Network (RAN), and Core Network (CN) as shown in Figure 6.5.

- **User Equipment (UE**): UEs are the mobile devices such as smart-phones, tablets, and data cards used by the subscriber/users.
- **RAN (Radio Access Network):**This part consists of base stations (BTS) and radio access (RAC) controller, acts as bridges between Mobile Station and Core Network. It also controls and manages the air interface (Um) for the whole network. RAN in 3G network is also termed as UTRAN (Universal Terrestrial Radio Access Network).

- **CN (Core Network):** It is the main processing part of the network. It is responsible for Switching and Routing, user mobility management, connection management. Security handing, and maintaining subscriber information, providing QoS. It has two sub-domains, viz., Circuit Switched Domain and Packet-switched domain. The circuit switched domain handles voice calls and real-time services. Whereas packet-switched domain takes care of data services like internet browsing, email, and multimedia messaging. IMS (IP Multimedia Subsystem) is a part of CN which provides IP multimedia services.

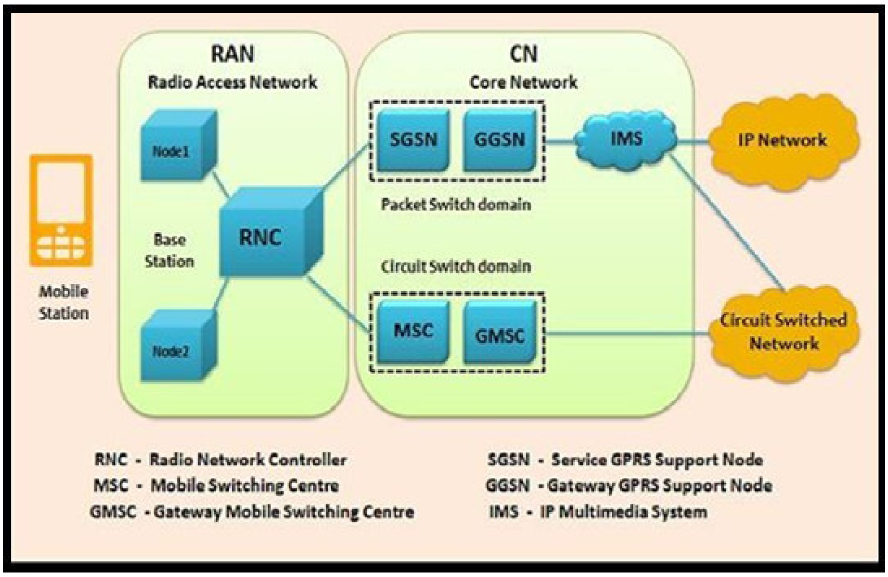

RAN
Radio Access Network
CN
Core Network
Node1
Base Station
RNC
Node2
Mobile Station
SGSN
GGSN
Packet Switch domain
Circuit Switch domain
MSC
GMSC
IMS
IP Network
Circuit Switched Network
RNC - Radio Network Controller
MSC - Mobile Switching Centre
GMSC - Gateway Mobile Switching Centre
SGSN - Service GPRS Support Node
GGSN - Gateway GPRS Support Node
IMS - IP Multimedia System

Figure 6.5 3G Newtok Architecture
(Source: https://techdifferences.com/difference-between-3g-and-4g-technology.html)

6.5.3 Advantages of 3G Technology

3G technology has many advantages over other existing networks. Followings are few notable advantages of 3G networks.

- **High speed data transfer:** 3G networks has higher bandwidth. This allows its subscribers to stream music and videos, download files, and access web pages quickly and efficiently

- **Support for Multimedia Applications:** 3G technology supports fast and efficient multimedia services, like mobile TV, live video calling, mobile gaming, MMS (Multimedia Messaging Service).

- **Standardized Global Roaming:** 3G networks enabled standardized global interoperability and international roaming, which allows users to travel across countries while continuing to access mobile services.

- **Enhanced Security Features:** As communication technology for mobile devices evolved from voice-only services to multimedia, multifunctional security has become a major concern. 3G technologies uses reliable security protocols to protect user information and prevent unauthorized access.

6.5.4 Disadvantages of 3G

Though 3G technology has many advantages, it has few limitations also over other existing networks. Followings are few limitations associated with 3G technology.

- **Limited Coverage**: Though, 3G is expected to offer higher speeds and better coverage, in actual it was often inconsistent. The network coverage was limited for users living in rural or remote areas as they had difficulty in accessing high-speed data transfer rates and multimedia services.
- **Device Incompatibility:** When 3G was launched, most of the devices are not compatible to adhere the 3G technology. Users had to upgrade their existing mobile devices or had to buy new 3G supporting devices to get the benefits of 3G technology, which an added additional cost on the users.
- **Network Congestion**: As 3G technology offered high-speed data transfer and has increased network capacity with multimedia services. This may sometimes increase network congestion that reduced the overall network performance.
- **Security Vulnerabilities:** Although, 3G technology provides enhanced security measures, it may still but possess to security vulnerabilities. Unauthorized access to users' data is still possible.

Stop to Consider

Third Generation, in short 3G is a cellular wireless communication technology. It is more advanced than its predecessors, 2G and 2.5G technologies. 3G technology uses Circuit switching for voice communication, and Packet switching for data transmission. It supports maximum data transfer rates of 2.05 Mbps, 384 Kbps, and 128 Kbps for stationary devices, devices moving at a slow pace, devices moving at high speed, respectively. The first 3G technology was commercial launched by NTT DoCoMo in Japan on 1 October 2001.

6.6 FOURTH GENERATION CELLULAR SYSTEMS (4G TECHNOLOGY)

Fourth-generation mobile telecommunications technology, known as 4Gis an enhancement of 3G mobile networks developed in late 2000s to offer more offer faster data speeds, enhanced multimedia services, HD video streaming, improved reliability, than 3G. 4G technology is entirely based on packet-switched mechanism that uses IP-based architecture including voice over IP (VoIP). 4G uses Long Term Evolution (LTE) technology for its implementation, hence also called as 4G-LTE network.

6.6.1 Architecture of 4G Networks

The 4G LTE architecture is the evidence to the evolution of recent mobile networks. The 4G Architecture provides many advantages compared to its predecessors, 2G and 3G architecture. These advantages include routing techniques, sharing frequency band, increases mobility and increased bandwidth capacity (Hicham et. al, 2015). The 4G network architecture has three main components, viz., User Equipment (UE), Evolved Universal Terrestrial Radio Access Network (E-UTRAN), and Evolved Packet Core (EPC) as shown in Figure 6.6.

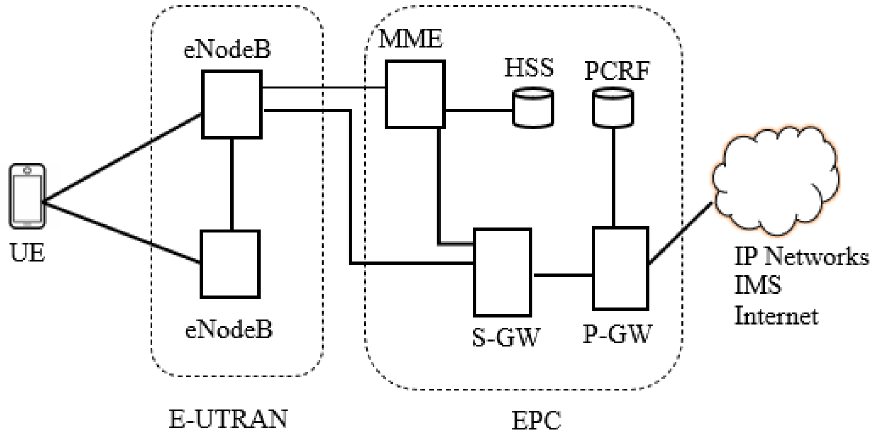


Figure 6.6 Architecture of 4G-LTE Network

User Equipment (UE) are the 4G-LTE compatible mobile devices such as laptops, tablets, and smartphones. *Universal Terrestrial Radio Access Network (E-UTRAN)* is the radio access network (RAN) used in 4G LTE (Long Term Evolution) systems which is the evolved version of the UTRAN in 3G network. E-UTRAN contains Evolved Node B (eNodeB). Each eNodeB is the base station that connects directly to User Equipment (UE), and to the Evolved Packet Core (EPC). The eNodeB acts as network controller also, integrating the services of RNC and BSC in 3G network. It performs key operations like allocation and release of radio resources, packet scheduling, and mobility management. The *Evolved Packet Core (EPC)* has four key components, *Mobility Management Entity (MME), Serving Gateway (S-GW), Packet Data Network Gateway (P-GW), Home Subscriber Server (HSS),* and Policy and *Charging Rules Function (PCRF)*.The MME is responsible for managing the signaling exchanges between the UEs and the EPC, as well as those between the eNodeBs and the EPC. It manages handovers, session control, and user authentications. The S-GW acts routes user data packets from eNodeBs to external network via P-GW. The P-GW ensures connectivity of UEs to external packet data networks (PDN), providing IP address. The Home Subscriber Server (HSS) is a central database that contains user profiles, authentication credentials etc. The Policy and Charging Enforcement Function (PCEF) is a key component located within the P-GW. It enforces policy rules, manages QoS, and detects service data flows, supporting both charging and traffic control in LTE networks.

6.6.2 Advantages of 4G

The network architecture of 4G LTE is has many advantages. Some of the key advantages are as follows.

- **Faster Data Speeds:** 4G-LTE Supports high speed data rates of compared to 3G, enabling HD video streaming, mobile TV, and large multimedia file downloads.

- **Low Latency:** Reduces delays in data transmission, making it suitable for real-time gaming applications, and video calls.

- **IP-Based Architecture**: 4G-LTE transmits data entirely on packet-switched mechanisms, contrast to 3G which uses both circuit-switched (voice) and packet-switched (data) domains. This enables the integration of internet services and VoIP (e.g., VoLTE).

- **Improved Spectrum Efficiency:** Optimized for handling more users and higher data demands.

- **Seamless Mobility:** Ensures fast and smooth handovers between cells and across different networks without dropping connections which make it more convenient for international compatibility and roaming services.

6.6.3 Disadvantages of 4G

Although 4G-LTE network is superior than other networks like, 2G and 3G, has many drawbacks. Let us discuss some of them.

- **High Deployment Costs:** Network providers face significant costs in upgrading infrastructure and deploying new base stations. Most of the existing 2G and 3G devices are incompatible with 4G LTE. This needs the 4G network providers to upgrade existing infrastructure and requires to install new base stations that supports LTE, suffering high network deployment cost.

- **High Battery Consumption:** High-speed data transmission always consumes battery power which leads to faster battery depletion in mobile devices.

- **Limited Network Coverage:** As 4G coverage is still not universal, subscribers living in rural and remote areas may experience slower connection and limited network availability.
- **High Network Congestion:** 4G users have always has high demand data services. This can create high chances of network congestion during the peak and users can experiences slower network speed.

6.7 FIFTH GENERATION CELLULAR SYSTEMS (5G TECHNOLOGY)

The fifth-generation cellular technology, called 5G is the latest generation of mobile networks, brought significant improvements over 4G. It offers very high-speed internet and lower latency. The peak speed of mobile internet in 5G is up to 20 Gbps and on average it is over 100 Mbps. 5G uses OFDM (Orthogonal Frequency-Division Multiplexing) technology. 5G is also designed to support all types of communication including voice, non-voice, IoT (Internet of Things) and other regular services. The 5G core system architecture is a cloud-based system called service-based architecture (SBA) that is designed to increase scalability and flexibility.

6.7.1 5G Network Architecture

The major components of 5G architecture are, viz., *User Equipment (UE),Radio Access Network (RAN)*, and *5G Core Network (5GC).* UEs are the 5G like smartphones, laptops, tablets, autonomous vehicles, IoT sensors etc. The UE connects to the Core network via NR (New Radio) interface, replacing the LTE interface used in 4G. Radio Access Network (RAN), one of the core components of the 5G network connects the UEs to the 5G Core Network. The RAN in 5G is more advanced than that 4G which provides high speed data transmission with ultra-low latency, and to connect a massive number of devices. The RAN uses the base station called gNodeB, replacing eNodeB in 4G. These bases stations support a wider range of frequency spectrums for faster and reliable communication. The 5GC is developed to provide scalable, flexible, and cloud-native operations. There are many key components in 5GC as given below:

- *Access and Mobility Management Function (AMF):* It is responsible for management of user registration, connection, and mobility, also acts as the control point for UE authentication and handovers

- *User Plane Function (UPF):* It handles the data traffic, packet routing, forwarding, traffic inspection, and policy enforcement.

- *Session Management Function (SMF):* It is responsible for session management, IP address allocations to UEs. It also handles QoS and interacts with policy control.

- *Authentication Server Function (AUSF)*: It does user authentications based on available user subscription credentials in UDM.

- *Unified Data Management (UDM)*): It is a centralized database that keeps credentials for subscriber data. it has replaced the existing HLR/HSS used in 3G/4G.

- *Network Slice Selection Function (NSSF)*: It allocates user equipments (UEs) to the suitable network slice depending on the service being accessed by the subscribers.

- *Network Exposure Function (NEF)*: Major duty of it is to allows external applications to interact with the 5G core securely using specific APIs.

- *Policy Control Function (PCF)*: Manages all policies required for QoS, billings, and access control.
- *Application Function (AF)*: It performs responsibilities like hosting service logic for third-party applications, requesting policy decisions and interacting with other core functions via the NEF

6.7.2 Advantages of 5G Network

There many advantages of 5G Network. The 5G network offers ultra-fast, and seamless video streaming with high data rates transmissions. The network in 5G is highly scalable. It can connect up to 1 million devices per square kilometer which makes it ideal for many real time IoT applications, like smart city development. Another advantage of 5G is that the latency in 5G is quite low. 5G network is also energy efficient. It provides enhanced reliability, and better spectral utilization which improves the overall network performance. Finally, the network slicing techniques offered in 5G allows operators to create multiple VNs (Virtual networks) on a single physical infrastructure.

Stop to Consider

4G is an enhancement of 3G mobile networks developed in late 2000s. It is designed to offer more offer faster data speeds, enhanced multimedia services, HD video streaming, improved reliability, than 3G. 4G technology is entirely based on packet-switched mechanism that uses IP-based architecture including voice over IP (VoIP). 4G uses Long Term Evolution (LTE) technology for its implementation, hence also called as 4G-LTE network. The 5G network offers ultra-fast, and seamless video streaming with high data rates transmissions. network slicing techniques offered in 5G allows operators to create multiple VNs (Virtual networks) on a single physical infrastructure.

6.8 WIRELESS LOCAL LOOP (WLL)

WLL (Wireless Local Loop) is a telecommunication technology which uses wireless technologies to connect users to the govt. or public switched telephone network (PSTN) or any other telecommunication networks for the use of following services such as voice, data, and internet services. The main objective of WLL is provide an alternative to conventional copper wired connection. WLL offers a communication alternative for the areas where laying cables is difficult, expensive, or time-consuming for building physical wired infrastructure.

6.8.1 Architecture of WLL

The architecture of WLL (Wireless Local Loop) can be separated into three major segments, viz., the subscriber segment, the access network segment, and the core network segment. Each of these segments performs distinct role in the overall WLL system. The subscriber segment consists of number of Subscriber Premises Equipments (SPEs). Each SPE is a telecommunication device such as landline phones, modems, fax machines, and computers. SPEs are connected to the access segment called, Wireless Access Subscriber Unit (WASU). WASU acts as a gateway between the users and the wireless network. WASU converts the wired signals from the telephone or computer into wireless signals suitable for wireless data transmission. Other functionalities of WASU may also include, management of protocols, ensuring of synchronization, user authentication. The converted wireless signals form WASU are transmitted to a nearby Base Station (BS), which is the part of WLL core network. it is also known as the Base Transceiver Station (BTS). The BTS is consisting of transceivers and antennas which handle communication over unlicensed or licensed radio frequency bands. The BTS are responsible to handling modulation, signal encoding, signal amplification, and also controls radio resources. Each BTS is connected to the Base Station Controller (BSC). The BSC controls and manages multiple base stations and perfume tasks like handoff management, frequency allocation, power control, and load balancing. Another core component of WLL architecture is the Switch Function (SF) which interfaces the PSTN to the WANUs. This provides a switching mechanism between MSC (Mobile Switching Center), and an Internet Gateway, depending on whether the WLL system is circuit-switched or packet-switched. SF is also responsible for management of Quality of Service (QoS) control, traffic, and interfacing with available service providers. The Public Switched Telephone Network (PSTN) or the Internet Backbone is connected to WLL through trunk lines or leased fiber links, which carries traffic over long distances. PSTN complete the call or data transmission path from one user to another. The other supporting components of WLL includes, viz., the Home Location Register (HLR) and Authentication Centers (AUC). HLR stores user subscription data, whereas AUC sores user credentials that is to be used to verify user identities and secure communication channels. Some WLL systems may also include Operation and Maintenance Centers (OMC) which is used for managing and monitoring of the WLL infrastructure. In modern WLL deployments, the architecture has also evolved to support Fixed Wireless Access (FWA) using 4G LTE or 5G technology. In such systems, the WASU is replaced by a 4G/5G Customer Premises Equipment (CPE) units. The base stations are also enhanced to eNodeBs (for4G- LTE) or gNodeBs (for 5G). The core network in such architectures, follows a fully IP-based architecture, including IMS (IP Multimedia Subsystem) and virtualized network functions. This allows for cloud-based scalability and dynamic resource allocation in data transmission.

Check Your Progress-2

Q.1. Choose the Correct Option:

i) What key technology is used for implementing 4G networks?

(a) WiMAX
(b) CDMA
(c) LTE
(d) GSM

ii) Which component of the 4G LTE architecture directly connects User Equipment (UE) to the Evolved Packet Core (EPC)?

(a) Mobility Management Entity (MME)
(b) Home Subscriber Server (HSS)
(c) Evolved Node B (eNodeB)
(d) Packet Gateway (P-GW)

iii) Which organization defined the IMT-2000 standards for 3G?

(a) IEEE
(b) ITU
(c) 3GPP
(d) ETSI

iv) Which 3G standard uses Time Division Duplexing (TDD)?

(a) W-CDMA
(b) DECT
(c) CDMA2000
(d) TD-SCDMA

v) Which component of the 5G Core replaces the HLR/HSS used in 3G/4G?

(a) UDM
(b) AUSF
(c) UPF
(d) NEF

6.9 SUMMING UP

In the earlier unit, we explored wireless communication technologies like IEEE 802.16 (WiMAX) and IEEE 802.11 (Wi-Fi). These technologies, despite of its offerings like high-speed and reliable communication, are still lacking in providing true mobility support. To address this, mobile communication technologies emerged to enable seamless connectivity together with user mobility. Inception of GSM marked a milestone in digital communication by offering digital voice and SMS services. GPRS, or 2.5G, improved GSM which is based on packet-switched mechanism, but had limitations in speed. The development of 3G enhanced the services provided by GSM, and GPRS.3G introduces very fast data transmission capability and supported services, viz., video calls, streaming etc. 3G is designed to unify various 2G standards developed under ITU's IMT-2000, offering higher speeds, multimedia support, and global roaming. Key technologies in 3G includes W-CDMA, CDMA2000, and TD-SCDMA. 3G is further enhanced to 4G technology. The 4G technology based on LTE, used an all-IP architecture to support HD streaming and VoIP with significantly faster speeds. 5G, the latest generation, offers ultra-high-speed internet, low latency, and supports IoT. It uses OFDM and a cloud-based architecture for scalability. Additionally, WLL (Wireless Local Loop) provides wireless connectivity in areas lacking physical infrastructure, offering voice and internet services as an alternative to wired connections. This unit covered a detailed discussion on the above-mentioned mobile technologies.

6.10 ANSWERS TO CHECK YOUR PROGRESS

Check Your Progress-1

1. (i) b (ii) c (iii) a (iv) c (v) c

Check Your Progress-2

1. (i) c (ii) c (iii) b (iv) d (v) a

6.11 POSSIBLE QUESTIONS

Short Answer Type Questions:

1. What is GSM? Differentiate between GSM-900, GSM-1800, and GSM-1900 based on their frequency bands and regions of use.
2. What is the role of the Base Station Controller (BSC) in the GSM architecture?
3. State three limitations of GSM.
4. State few characteristics of GPRS.
5. What is 4G? how it is differ from 3G?
6. Differentiate between 4G and 5G networks.
7. What is WLL?
8. What is eNodeB? State few responsibilities of eNodeB.
9. What are the major components in a WLL architecture.

Long Answer Type Questions:

10. Describe briefly the three categories of GSM services.
11. Explain the purpose of the Authentication Center (AUC) and Equipment Identity Register (EIR) in GSM.
12. Explain the GSM system architecture with suitable diagram.
13. Describe the different handover scenarios in GSM.
14. Explain the various layers present in a GSM protocol stack.
15. Explain the architecture of 4G-LTE network.
16. Describe the 5G network architecture.
17. Explain the details of WLL architecture.

6.12 REFERENCES AND SUGGESTED READINGS

[1] Stallings, William. (2009). *Wireless Communications and Networks*. (2nd ed.). Prentice Hall. ISBN: 0-13-191835-4

[2] Murthy, R.S. M., and Manoj, B. S. (2004). *Ad Hoc Wireless Networks*. (1st ed.). Pearson Education. ISBN: 81-317-0688-5

[3] https://mobiletelecommunicationarchitecture.blogspot.com/2010/07/gsm-system-architecture-gsm-system.html

[4] https://www.jeppiaarinstitute.org/pdf/lectures/902.pdf

[5] https://ebooks.inflibnet.ac.in/itp12/chapter/gprs/

[6] https://www.telecomtrainer.com/3g-third-generation-of-mobile-communication-technologies/

[7] https://techdifferences.com/difference-between-3g-and-4g-technology.html

[8] Hicham, M., Abghour, N., &Ouzzif, M. (2015). 4G system: network architecture and performance. Int. J. Innov. Res. Adv. Eng.(IJIRAE), 2, 215-220.

***

UNIT- 7

802.11

Unit Structure:

7.1 INTRODUCTION

802.11 is a member of the IEEE 802 family, which is a series of specifications for local area network (LAN) technologies. Figure 7.1 shows the relationship among various components of the 802 family and their place in the OSI model.

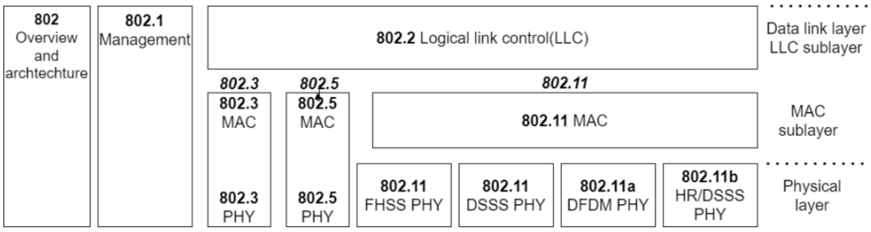


Figure 7.1 Components of the 802 family and their place in the OSI model

IEEE 802 specifications focus on the two lowest layers of the OSI model, because they incorporate physical and data link components. All 802 networks have a MAC and a Physical (PHY) component. The MAC is a set of rules to determine how to access the medium and send data, but the details of transmission and reception are left to the PHY.

7.2 OBJECTIVES

After going through this unit learner will able to

- *understand* the authentication mechanisms in IEEE 802.11 networks, including open-system, shared-key, and pre-authentication processes.
- *analyse* the importance of timing synchronization in wireless networks and describe how beacon frames and TSF maintain coordinated communication.
- *learn* the concept of the association process in infrastructure networks and assess its role in mobility and power-saving mechanisms.
- *understand* the concept o f 802.11 hardware integration and configuration in Linux environments, including PCMCIA support and driver management.

7.3 COMPONENTS OF 802.11

802.11 networks consist of four major physical components as depicted in Figure 7.2. They are:

- Distribution System
- Access Points
- Wireless Medium
- Stations

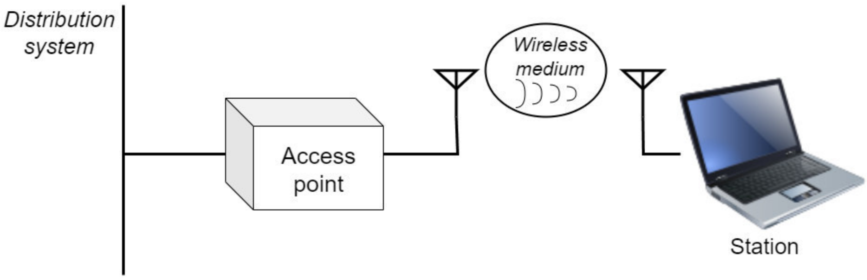


Figure 7.2 Physical Components of 802.11

- ***Distribution System***

When several access points are connected to form a large coverage area, they must communicate with each other to track the movements of mobile stations. The distribution system is the logical component of 802.11 used to forward frames to their destination. 802.11 does not specify any particular technology for the distribution system. In most commercial products, the distribution system is implemented as a combination of a bridging engine and a distribution system medium, which is the backbone network used to relay frames between access points; it is often called simply the backbone network. In nearly all commercially successful products, Ethernet is used as the backbone network technology.

- ***Access Points***

Frames on an 802.11 network must be converted to another type of frame for delivery to the rest of the world. Devices called access points perform the wireless-to-wired bridging function. Access points perform a number of other functions, but bridging is by far the most important.

- ***Wireless Medium***

To move frames from station to station, the standard uses a wireless medium. Several different physical layers are defined; the architecture allows multiple physical layers to be developed to support the 802.11 MAC. Initially, two radiofrequency (RF) physical layers and one infrared physical layer were standardized, though the RF layers have proven far more popular.

- ***Stations***

Networks are built to transfer data between stations. Stations are computing devices with wireless network interfaces. Typically, stations are battery-operated laptop or handheld computers. There is no reason why stations must be portable computing devices, though. In some environments, wireless networking is used to avoid pulling new cable, and desktops are connected by wireless LANs.

7.3.1 Types of Networks

The basic building block of an 802.11 network is the basic service set (BSS), which is simply a group of stations that communicate with each other. Communications take place within a somewhat fuzzy area, called the basic service area, defined by the propagation characteristics of the wireless medium.[1] When a station is in the basic service area, it can communicate with the other members of the BSS. BSSs come in two flavours, both of which are illustrated in Figure 7.3.

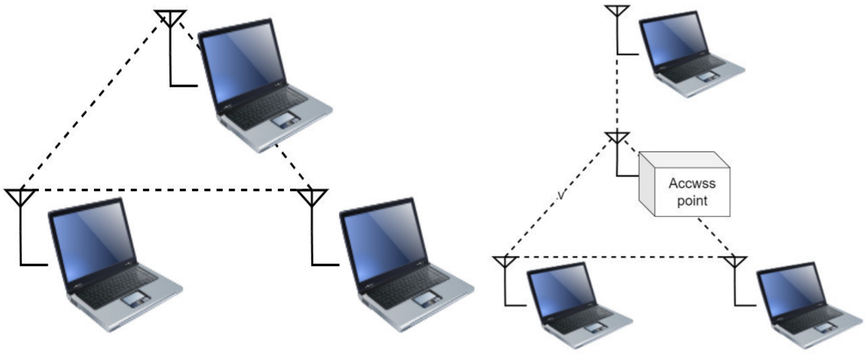


Figure 7.3 Independent and Infrastructure BSS

On the left is an independent BSS (IBSS). Stations in an IBSS communicate directly with each other and thus must be within direct communication range. The smallest possible802.11 network is an IBSS with two stations. Typically, IBSSs are composed of a small number of stations set up for a specific purpose and for a short period of time. One common use is to create a short-lived network to support a single meeting in a conference room. As the meeting begins, the participants create an IBSS to share data. When the meeting ends, the IBSS is dissolved.[2] Due to their short duration, small size, and focused purpose, IBSSs are sometimes referred to as ad hoc BSSs or ad hoc networks.

On the right side of Figure 7.3 is an infrastructure BSS (never called an IBSS).Infrastructure networks are distinguished by the use of an access point. Access points are used for all communications in infrastructure networks, including communication between mobile nodes in the same service area. If one mobile station in an infrastructure BSS needs to communicate with a second mobile station, the communication must take two hops. First, the originating mobile station transfers the frame to the access point. Second, the access point transfers the frame to the destination station. With all communications relayed through an access point, the basic service area corresponding to an infrastructure BSS is defined by the points in which transmissions from the access point can be received.

7.3.2 Network Operations

From the outset, 802.11 was designed to be just another link layer to higher-layer protocols. Network administrators familiar with Ethernet will be immediately comfortable with 802.11. The shared heritage is deep enough that 802.11 is sometimes referred to as "wireless Ethernet."The core elements present in Ethernet are present in 802.11. Stations are identified by 48-bit IEEE 802 MAC addresses. Conceptually, frames are delivered based on the MAC address. Frame delivery is unreliable, though 802.11 incorporates some basic reliability mechanisms to overcome the inherently poor qualities of the radio channels it uses [4]. One way to define a network technology is to define the services it offers and allow equipment vendors to implement those services in whatever way they see fit. 802.11 provide nine services. Only three of the services are used for moving data; the remaining six are management operations that allow the network to keep track of the mobile nodes and deliver frames accordingly. The services are described and summarized in Table 7-1:

Table 7.1 Summary of services

Service	**Station or Distribution Service**	**Description**
Distribution	Distribution	Service used in frame delivery to determine destination address in infrastructure networks
Integration	Distribution	Frame delivery to an IEEE 802 LAN outside the wireless network
Association	Distribution	Used to establish the AP which serves as the gateway to a particular mobile station
Reassociation	Distribution	Used to change the AP which serves as the gateway to a particular mobile station
Disassociation	Distribution	Removes the wireless station from the network
Authentication	Station	Establishes identity prior to establishing association
De-authentication	Station	Used to terminate authentication, and by extension, association
Privacy	Station	Provides protection against eavesdropping
MSDU Delivery	Station	Delivers data to the recipient

Station Services

Station services are part of every 802.11-compliant station and must be incorporated by any product claiming 802.11 compliance. Both mobile stations and the wireless interface on access points provide station services. Stations provide frame delivery services to allow message delivery, and, in support of this task, they may need to use the authentication services to establish associations. Stations may also wish to take advantage of privacy functions to protect messages as they traverse the vulnerable wireless link.

Distribution System Services

Distribution system services connect access points to the distribution system. The major role of access points is to extend the services on the wired network to the wireless network; this is done by providing the distribution and integration services to the wireless side. Managing mobile station associations is the other major role of the distribution system. To maintain association data and station location information, the distribution system provides the association, reassociation, and disassociation services.

7.4 802.11 MAC

The key to the 802.11 specification is the MAC. It rides on every physical layer and controls the transmission of user data into the air. It provides the core framing operations and the interaction with a wired network backbone. Different physical layers may provide different transmission speeds, all of which are supposed to interoperate.802.11 does not depart from the previous IEEE 802 standards in any radical way. The standard successfully adapts Ethernet-style networking to radio links. Like Ethernet,802.11 uses a carrier sense multiple access (CSMA) scheme to control access to the transmission medium. However, collisions waste valuable transmission capacity, So, rather than employing the collision detection (CSMA/CD) by Ethernet, 802.11 uses collision avoidance (CSMA/CA). Also like Ethernet, 802.11 uses a distributed access scheme with no centralized controller. Each 802.11 station uses the same method to gain access to the medium. The major differences between 802.11 and Ethernet stem from the differences in the underlying medium.

MAC Access Modes and Timing:

Coordination functions control access to the wireless medium. Ethernet-like CSMA/CA access is provided by the distributed coordination function (DCF). If contention-free service is required, it can be provided by the point coordination function (PCF), which is built on top of the DCF. Contention-free services are provided only in infrastructure networks. The coordination functions are described in the following list and illustrated in Figure 7.4:

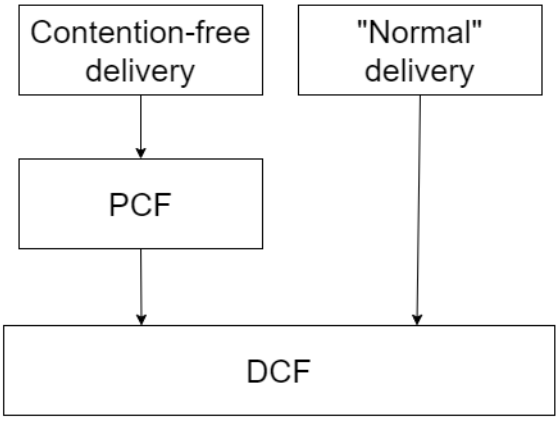


Figure 7.4 MAC Access Modes

The DCF is the basis of the standard CSMA/CA access mechanism. Like Ethernet, it first checks to see that the radio link is clear before transmitting. To avoid collisions, stations use a random back off after each frame, with the first transmitter seizing the channel. In some circumstances, the DCF may use the CTS/RTS clearing technique to further reduce the possibility of collisions.

The PCF provides contention-free services. Special stations called point coordinators are used to ensure that the medium is provided without contention. Point coordinators reside in access points, so the PCF is restricted to infrastructure networks. To gain priority over standard contention-based services, the PCF allows stations to transmit frames after a shorter interval.

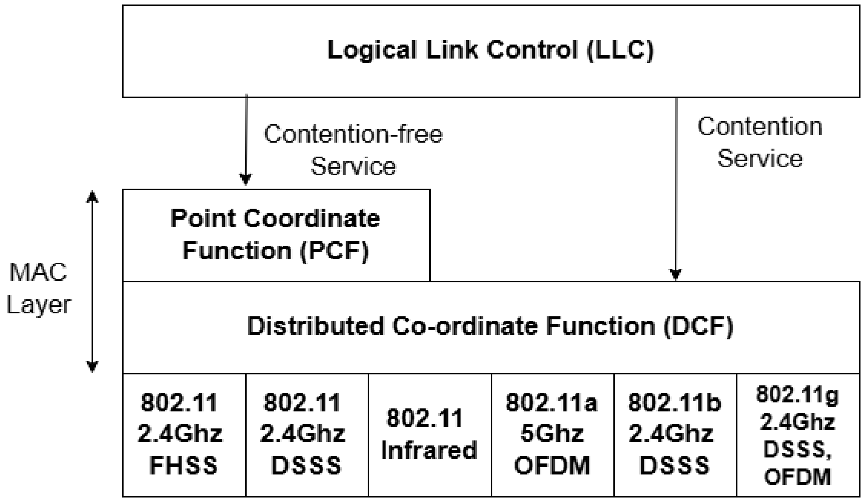


Figure 7.5 IEEE 802.11 Protocol Architecture

Figure 7.5 illustrates the architecture. The lower sublayer of the MAC layer is the distributed coordination function (DCF). DCF uses a contention algorithm to provide access to all traffic.

Ordinary asynchronous traffic directly uses DCE The point coordination function (PCF) is a centralized MAC algorithm used to provide contention-free service. PCF is built on top of DCF and exploits features of DCF to assure access for its users.

7.4.1 Distributed Coordination Function (DCF):

The DCF sublayer makes use of a simple CSMA (carrier sense multiple access) algorithm, which functions as follows. If a station has a MAC frame to transmit, it listens to the medium. If the medium is idle , the station may transmit; otherwise the station must wait until the current transmission is complete before transmitting. The DCF does not include a collision detection function (i.e., CSMA/CD) because collision detection is not practical on a wireless network. The dynamic range of the signals on the medium is very large, so that a transmitting station cannot effectively distinguish incoming weak signals from noise and the effects of its own transmission.

To ensure the smooth and fair functioning of this algorithm, DCF includes a set of delays that amounts to a priority scheme. Let us start by considering a single delay known as an inter frame space (IFS). In fact, there are three different IFS values, but the algorithm is best explained by initially ignoring this detail.

Using an IFS, the rules for CSMA access are as follows:

1. A station with a frame to transmit senses the medium. If the medium is idle, it waits to see if the medium remains idle for a time equal to IFS. If so, the station may transmit immediately.
2. If the medium is busy (either because the station initially finds the medium busy or because the medium becomes busy during the IFS idle time), the station defers transmission and continues to monitor the medium until the current transmission is over.
3. Once the current transmission is over, the station delays another IFS. If the· medium remains idle for this period, then the station backs off a random amount of time and again senses the medium. If the medium is still idle, the station may transmit. During the backoff time, if the medium becomes busy, the backoff timer is halted and resumes when the medium becomes idle.
4. If the transmission is unsuccessful, which is determined by the absence of an acknowledgement, then it is assumed that a collision has occurred.

To ensure that backoff maintains stability, a technique known as binary exponential backoff is used. A station will attempt to transmit repeatedly in the face of repeated collisions, but after each collision, the mean value of the random delay is doubled up to some maximum value. The binary exponential backoff provides a means of handling a heavy load. Repeated failed attempts to transmit result in longer and longer backoff times, which helps to smooth out the load. Without such a backoff, the following situation could occur. Two or more stations attempt to transmit at the same time, causing a collision. These stations then immediately attempt to retransmit, causing a new collision.

7.4.2 Point Coordination Function (PCF):

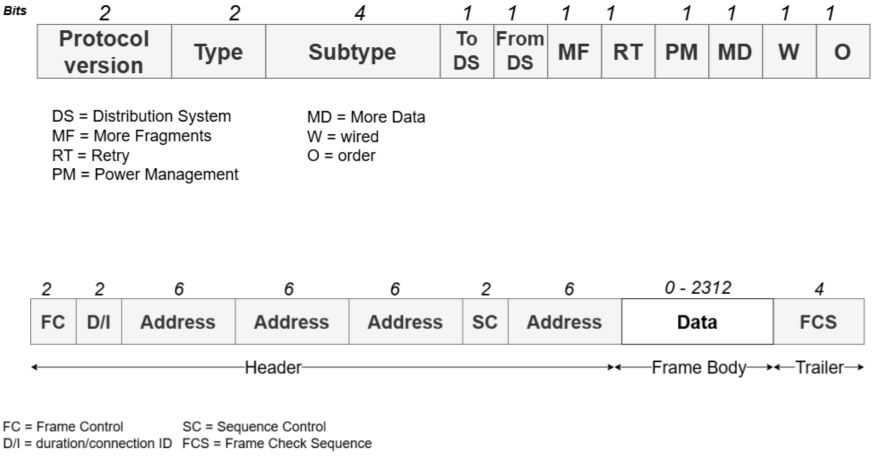
PCF is an alternative access method implemented on top of the Distributed Co-ordination Function (DCF). The operation consists of polling by the centralize polling master (point coordinator). The point coordinator makes use of PIFS when issuing polls. Because PIFS is smaller than DIFS, the point coordinator can seize the medium and lock out all asynchronous traffic while it issues polls and receives responses. As an extreme, consider the following possible scenario. A wireless network is configured so that a number of stations with time-sensitive traffic are controlled by the point coordinator while remaining traffic contends for access using CSMA. The point coordinator could issue polls in a round-robin fashion to all stations configured for polling. When a poll is issued, the polled station may respond using SIFS. If the point coordinator receives a response, it issues another poll using PIFS. If no response is received during the expected turnaround time, the coordinator issues a poll. If the discipline of the preceding paragraph were implemented, the point coordinator would lock out all asynchronous traffic by repeatedly issuing polls. To prevent this, an interval known as the super frame is defined. During the first part of this interval, the point coordinator issues polls in a round-robin fashion to all stations configured for polling. The point coordinator then idles for the remainder of the super frame, allowing a contention period for asynchronous access.

At the beginning of a super frame, the point coordinator may optionally seize control and issues polls for a given period of time. This interval varies because of the variable frame size issued by responding stations. The remainder of the super frame is available for contention-based access. At the end of the super frame interval, the point coordinator contends for access to the medium using PIFS. If the medium is idle, the point coordinator gains immediate access and a full super frame period follows. However, the medium may be busy at the end of a super frame. In this case, the point coordinator must wait until the medium is idle to gain access; this results in a foreshortened super frame period for the next cycle.

Check Your Progress -I

1. **State True or False**
   - **(i)** Access points perform the wireless-to-wired bridging function.
   - **(ii)** Stations are computing devices with wireless network interfaces.
   - **(iii)** Stations cannot provide frame delivery services to allow message delivery.
   - **(iv)** The basic building block of an 802.11 network is the basic service set (BSS).
   - **(v)** The DCF include a collision detection function.

7.5 802.11 FRAMMING



Bits	2	2	4	1	1	1	1	1	1	1	1
	Protocol version	Type	Subtype	To DS	From DS	MF	RT	PM	MD	W	O

DS = Distribution System
MF = More Fragments
RT = Retry
PM = Power Management
MD = More Data
W = wired
O = order

2	2	6	6	6	2	6	0 - 2312	4
FC	D/I	Address	Address	Address	SC	Address	Data	FCS

FC = Frame Control
D/I = duration/connection ID
SC = Sequence Control
FCS = Frame Check Sequence

Figure 7.6 IEEE 802.11 MAC Frame Format

Figure 7.6 shows the 802.11 frame format when no security features are used. This general format is used for all data and control frames, but not all fields are used in all contexts. The fields are as follows:

- **Frame Control**: Indicates the type of frame and provides control information.
- **Duration/Connection ID**: If used as a duration field, indicates the time (in microseconds) the channel will be allocated for successful transmission of a MAC frame. In some control frames, this field contains an association, or connection, identifier.
- **Addresses**: The number and meaning of the 48-bit address fields depend on context. The transmitter address and receiver address are the MAC addresses of stations joined to the BSS that are transmitting and receiving frames over the wireless LAN. The service set ID (SSID) identifies the wireless LAN over which a frame is transmitted. For an IBSS, the SSID is a random number generated at the time the network is formed. For a wireless LAN that is part of a larger configuration the SSID identifies the BSS over which the frame is transmitted; specifically, the SSID is the MAC-level address of the AP for this BSS (Figure 14.4). Finally the source address and destination address are the MAC addresses of stations, wireless or otherwise, that are the ultimate source and destination of this frame. The source address may be identical to the transmitter address and the destination address may be identical to the receiver address.
- **Sequence Control**: Contains a 4-bit fragment number subfield used for fragmentation and reassembly, and a 12-bit sequence number used to number frames sent between a given transmitter and receiver.
- **Frame Body**: Contains an MSDU or a fragment of an MSDU The MSDU is a LLC protocol data unit or MAC control information.
- **Frame Check Sequence**: A 32-bit cyclic redundancy check. The frame control field, shown in Figure 14.8b, consists of the following fields:
- **Protocol Version**: 802.11 version, currently version O.
- **Type**: Identifies the frame as control, management, or data.

- **Subtype**: Further identifies the function of frame.
- **To DS**: The MAC coordination sets this bit to 1 in a frame destined to the distribution system.
- **From DS**: The MAC coordination sets this bit to 1 in a frame leaving the distribution system.
- **More Fragments**: Set to 1 if more fragments follow this one.
- **Retry**: Set to 1 if this is a retransmission of a previous frame.
- **Power Management**: Set to 1 if the transmitting station is in a sleep mode.
- **More Data**: Indicates that a station has additional data to send. Each block of data may be sent as one frame or a group of fragments in multiple frames.
- **WEP**: Set to 1 if the optional Wired Equivalent Privacy Protocol is implemented. WEP is used in the exchange of encryption keys for secure data exchange.
- **Order**: Set to 1 in any data frame sent using the Strictly Ordered service, which tells the receiving station that frames must be processed in order.

Control Frames:

Control frames assist in the reliable delivery of data frames. There are six control frame subtypes:

- **Power Save-Poll (PS-Poll)**: This frame is sent by any station to the station that includes the AP (access point). Its purpose is to request that the AP transmit a frame that has been buffered for this station while the station was in power-saving mode.
- **Request to Send (RTS)**: This is the first frame in the four-way frame exchange. The station sending this message is alerting a potential destination, and all other stations within reception range, that it intends to send a data frame to that destination.
- **Clear to Send (CTS)**: This is the second frame in the four-way exchange. It is sent by the destination station to the source station to grant permission to send a data frame.
- **Acknowledgment:** Provides an acknowledgment from the destination to the source that the immediately preceding data, management, or PS-Poll frame was received correctly.

- **Contention-Free (CF)-End**: Announces the end of a contention-free period that is part of the point coordination function.
- **CF-End + CF-Ack**: Acknowledges the CF-end. This frame ends the contention-free period and releases stations from the restrictions associated with that period.

Data Frames:

There are eight data frame subtypes, organized into two groups. The first four subtypes define frames that carry upper-level data from the source station to the destination station. The four data-carrying frames are as follows:

- **Data**: This is the simplest data frame. It may be used in both a contention period and a contention-free period.
- **Data + CF-Ack**: May only be sent during a contention-free period. In addition to carrying data, this frame acknowledges previously received data.
- **Data + CF-Poll**: Used by a point coordinator to deliver data to a mobile station and also to request that the mobile station send a data frame that it may have buffered.
- **Data + CF-Ack + CF-Poll**: Combines the functions of the Data + CF-Ack and Data + CF-Poll into a single frame.

The remaining four subtypes of data frames do not in fact carry any user data. The Null Function data frame carries no data, polls, or acknowledgments. It is used only to carry the power management bit in the frame control field to the AP, to indicate that the station is changing to a low-power operating state. The remaining three frames (CF-Ack, CF-Poll, CF-Ack + CF-Poll) have the same functionality as the corresponding data frame subtypes in the preceding list (Data + CF-Ack, Data + CF-Poll, Data + CF-Ack + CF-Poll) but without the data.

Management Frames:

They are used to manage communications between stations and APs. The following subtypes are included:

- **Association Request**: Sent by a station to an AP to request an association with this BSS. This frame includes capability information, such as whether encryption is to be used and whether this station is pollable.
- **Association Response**: Returned by the AP to the station to indicate whether it is accepting this association request.
- **Reassociation Request**: Sent by a station when it moves from one BSS to another and needs to make an association with the AP in the new BSS. The station uses reassociation rather than simply association so that the new AP knows to negotiate with the old AP for the forwarding of data frames.
- **Reassociation Response**: Returned by the AP to the station to indicate whether it is accepting this reassociation request.
- **Probe Request**: Used by a station to obtain information from another station or AP. This frame is used to locate an IEEE 802.11 BSS.
- **Probe Response**: Response to a probe request.
- **Beacon**: Transmitted periodically to allow mobile stations to locate and identify a BSS.
- **Announcement Traffic Indication Message**: Sent by a mobile station to alert other mobile stations that may have been in low power mode that this station has frames buffered and waiting to be delivered to the station addressed in this frame.
- **Dissociation**: Used by a station to terminate an association.
- Authentication: Multiple authentication frames are used in an exchange to authenticate one station to another.
- **De-authentication**: Sent by a station to another station or AP to indicate that it is terminating secure communications.

7.6 WIRED EQUIVALENT PRIVACY (WEP)

In wireless networks, the word "broadcast" takes on an entirely new meaning. Security concerns have haunted 802.11 deployments since the standardization effort began. IEEE's attempt to address snooping concerns culminated in the optional Wired Equivalent Privacy (WEP) standard, which is found in clause 8.2 of 802.11. WEP can be used by stations to protect data as it traverses the wireless medium, but it provides no protection past the access point.

7.6.1 WEP Cryptographic Operations

Communications security has three major objectives. Any protocol that attempts to secure data as it travels across a network must help network managers to achieve these goals. Confidentiality is the term used to describe data that is protected against interception by unauthorized parties. Integrity means that the data has not been modified. Authentication underpins any security strategy because part of the reliability of data is based on its origin. Users must ensure that data comes from the source it purports to come from. Systems must use authentication to protect data appropriately. Authorization and access control are both implemented on top of authentication. Before granting access to a piece of data, systems must find out who the user is (authentication) and whether the access operation is allowed (authorization).

WEP provides operations that attempt to help meet these objectives. Frame body encryption supports confidentiality. An integrity check sequence protects data in transit and allows receivers to validate that the received data was not altered in transit.

7.6.2 WEP Data Processing

Confidentiality and integrity are handled simultaneously, as illustrated in Figure 7.7. Before encryption, the frame is run through an integrity check algorithm, generating a hash called an integrity check value (ICV). The ICV protects the contents against tampering by ensuring that the frame has not changed in transit. The frame and the ICV are both encrypted, so the ICV is not available to casual attackers.

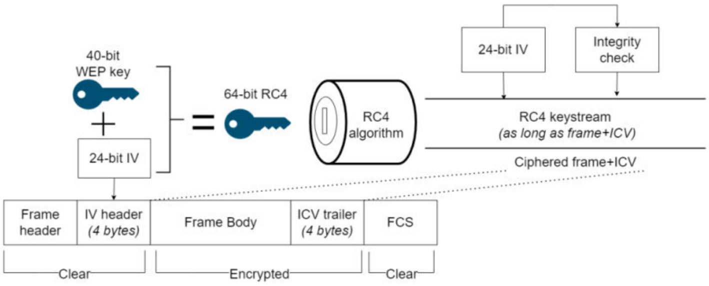


Figure 7.7 WEP Operations

WEP specifies the use of a 40-bit secret key. The secret WEP key is combined with a 24-bit initialization vector (IV) to create a 64-bit RC4 key; the first 24 bits of the RC4 key are the IV, followed by the 40-bit WEP key. RC4 takes the 64 input bits and generates a keystream equal to the length of the frame body plus the IV. The keystream is then XO Red with the frame body and the IV to cipher it. To enable the receiver to decrypt the frame, the IV is placed in the header of the frame

WEP Key Lengths:

Standardized WEP implementations use 64-bit shared RC4 keys. Of the 64 bits, 40 are a shared secret. Vendors use a variety of names for the standard WEP mode: "standard WEP," "802.11-compliant WEP," "40-bit WEP," "40+24-bitWEP," or even "64-bit WEP."

WEP Keying:

To protect traffic from brute-force decryption attacks, WEP uses a set of up to four default keys, and it may also employ pair wise keys, called mapped keys, when allowed. Default keys are shared among all stations in a service set. Once a station has obtained the default keys for its service set, it may communicate using WEP.

Key reuse is often a weakness of cryptographic protocols. For this reason, WEP has a second class of keys used for pair wise communications. These keys are shared only between the two stations communicating. The two stations sharing a key have a key mapping relationship; the key mapping relationship is part of the 802.11 MIB.

WEP Framing:

When WEP is in use, the frame body expands by eight bytes. Four bytes are used for a frame body IV header, and four are used for the ICV trailer.

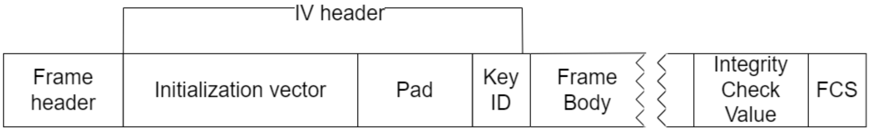


Figure 7.8 WEP Frame extensions

Cryptographic Properties:

The IV header uses 3 bytes for the 24-bit IV, with the fourth byte used for padding and key identification. When a default key is used, the Key ID subfield identifies the default key that was used to encrypt the frame. If a key mapping relationship is used, the Key ID subfield is 0. The 6 padding bits of the last byte must be 0. The integrity check is a 32-bitCRC of the data frame; it is appended to the frame body and protected by RC4.

Like so many other cryptographic protocols based on symmetric keys, WEP suffers from the Achilles heel of key distribution. The secret bits of the WEP key must be distributed to all stations participating in an 802.11 service set secured by WEP. The 802.11standard, however, fails to specify the key distribution mechanism. The result is that vendors haven't done anything; you typically type keys into your device drivers or access points by hand. Unfortunately, manual configuration by the system administrator is the most non-scalable "protocol" in use.

Setting aside the system management headaches for a minute, consider the difficulties inherent in a cryptographic system requiring manual key distribution:

- Keys cannot be considered secret: all keys must be statically entered into either the driver software or the firmware on the wireless card. Either way, the key cannot be protected from a local user who wants to discover it.[2]
- If keys are accessible to users, then all keys must be changed whenever staff members leave the organization. Knowledge of WEP keys allows a user to set up an 802.11 station and passively monitor and decrypt traffic using the secret key for the network. WEP cannot protect against authorized insiders who also have the key.
- Organizations with large numbers of authorized users must publish the key to the user population, which effectively prevents it from being a secret.

7.7 AUTHENTICATION:

Security is a common thread linking many of the wireless LAN stories in the news throughout the past year, and several polls have shown that network managers consider security to be a significant obstacle to wider deployment of wireless LANs. Many of the security problems that have prevented stronger acceptance of 802.11 are caused by flaws in the design of WEP. WEP attempts to serve as both an authentication mechanism and a privacy mechanism.

To address the shortcomings of WEP for authentication, the industry is working towards solutions based on the 802.1x specification, which is itself based on the IETF's Extensible Authentication Protocol (EAP). EAP was designed with flexibility in mind, and it has been used as the basis for a number of network authentication extensions. (Cisco's lightweight EAP, LEAP, also is based on EAP.)802.1x is not without its problems, however. A recent research report identified several problems with the specification.[1]

The first major problem is that 802.11 does not provide a way to guarantee the authenticity and integrity of any frames on the wireless network. Frames on wireless networks can easily be tampered with or forged outright, and the protocol does not provide a way to easily stop or even detect such attacks. The second major problem is that 802.1x was designed to allow the network to authenticate the user. Implicit in the protocol design is the assumption that users will connect to only the "right" network. On wireline networks, connecting to the right network can be as simple as following the wires. Access to the wiring helps the users identify the "right" network.

On a wireless network, clear physical connections do not exist, so other mechanism must be designed for networks to prove their identity (or, more precisely, the identity of their owners) to users. 802.1x was designed to collect authentication information from users and grant or deny access based on that information. It was not designed to help net works provide credentials to users, so that function is not addressed by the 802.1x. The spectre for rogue access points will not be put to rest by 802.1x.

7.7.1 The Extensible Authentication Protocol

802.1x is based on EAP. EAP is formally specified in RFC 2284 and was initially developed for use with PPP. When PPP was first introduced, there were two protocols available to authenticate users, each of which required the use of a PPP protocol number. Authentication is not a "one size fits all" problem, and it was an active area of research at the time. Rather than burn up PPP protocol numbers for authentication protocols that might become obsolete, the IETF standardized EAP. EAP used a single PPP protocol number while supporting a wide variety of authentication mechanisms. EAP is a simple encapsulation that can run over any link layer, but it has been most widely deployed on PPP links. Figure 6-1 shows the basic EAP architecture, which is designed to run over any link layer and use any number of authentication methods.

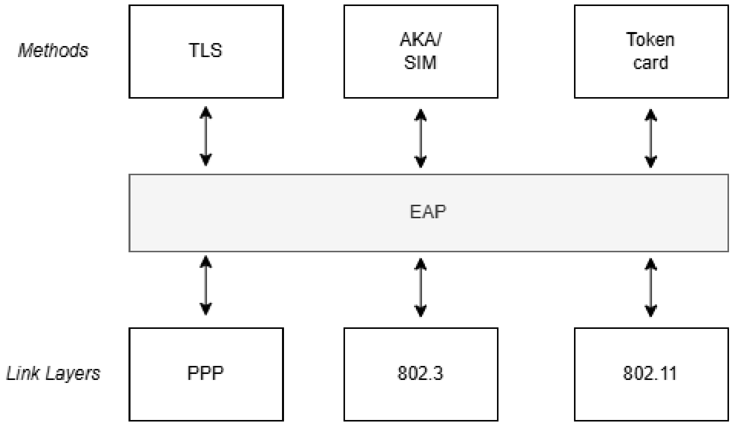


Figure 7.9 EAP architecture

- EAP Packet Format

Figure 7.10 shows the format of an EAP packet. When used on PPP links, EAP is carried in PPP frames with a protocol number of 0xC227. There is no strict requirement that EAP run on PPP; the packet shown in Figure 7.10 can be carried in any type of frame. The fields in an EAP packet are:

- **Code**: The Code field, the first field in the packet, is one byte long and identifies the type of EAP packet. It is used to interpret the Data field of the packet.
- **Identifier**: The Identifier field is one byte long. It contains an unsigned integer used to match requests with responses to them. Retransmissions reuse the same identifier numbers, but new transmissions use new identifier numbers.

- **Length**: The Length field is two bytes long. It is the number of bytes in the entire packet, which includes the Code, Identifier, Length, and Data fields. On some link layer protocols, padding may be required. EAP assumes that any data in excess of the Length field is link-layer padding and can be ignored.
- **Data**: The last field is the variable-length Data field. Depending on the type of packet, the Data field may be zero bytes long. Interpretation of the Data field is based on the value of the Code field.

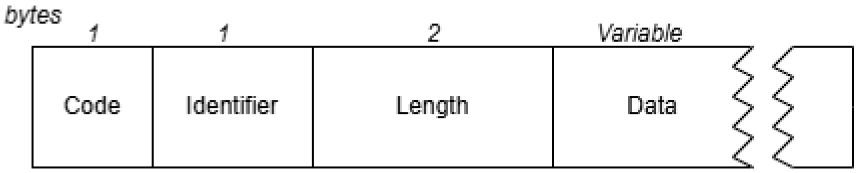


Figure 7.10 EAP packet format

- **EAP Requests and Responses**

EAP exchanges are composed of requests and responses. The authenticator sends requests to the system seeking access, and based on the responses, access may be granted or denied. The format of request and response packets is shown in Figure 7.11.

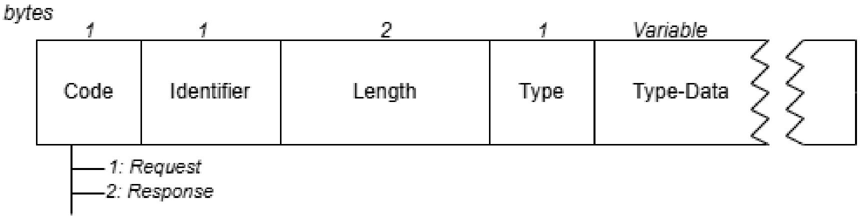


Figure 7.11 EAP Request and EAP Response packets

The Code field is set to 1 for requests and 2 for responses. The Identifier and Length fields are used as described in the previous section on the generic format. The Data field carries the data used in requests and responses. Each Data field carries one type of data, broken down into a type identifier code and the associated data:

- **Type**: The Type field is a one-byte field that indicates the type of request or response. Only one type is used in each packet. With one exception, the Type field of the response matches the corresponding request. That exception is that when a request is unacceptable, the peer may send a NAK to suggest an alternative type. Types greater than or equal to 4 indicate authentication methods.

- **Type-Data**: The Type-Data field is a variable field that must be interpreted according to the rules for each type.

- **EAP Success and Failure**

At the conclusion of an EAP exchange, the user has either authenticated successfully or has failed to authenticate (Figure 7.12). Once the authenticator determines that the exchange is complete, it can issue a Success (code 3) or Failure (code 4) frame to end the EAP exchange. Implementations are allowed to send multiple requests before failing the authentication to allow a user to get the correct authentication data.

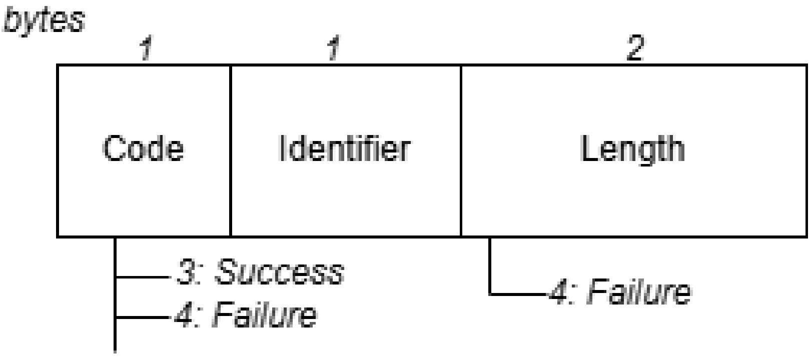


Figure 7.12 EAP Success and Failure Frames

CASE STUDY: A Sample EAP Exchange

A sample EAP exchange is shown in Figure 7.13. It is unnecessarily complex to illustrate several features of the protocol. The EAP exchange is a series of steps beginning with are quest for identity and ending with a success or failure message:

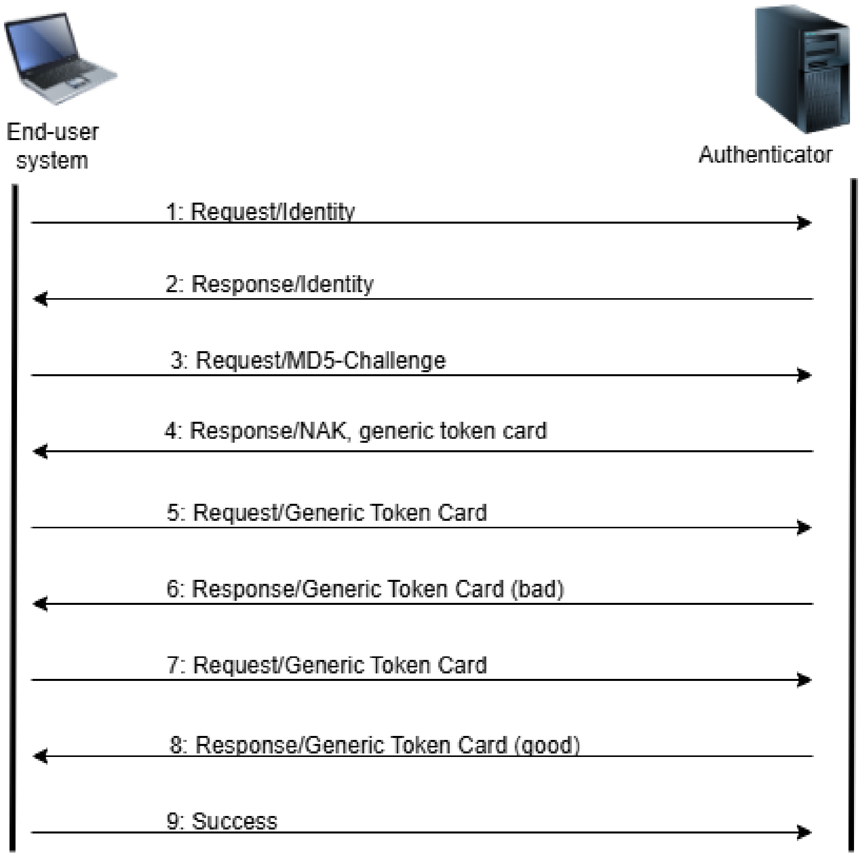

End-user system
Authenticator
1: Request/Identity
2: Response/Identity
3: Request/MD5-Challenge
4: Response/NAK, generic token card
5: Request/Generic Token Card
6: Response/Generic Token Card (bad)
7: Request/Generic Token Card
8: Response/Generic Token Card (good)
9: Success

Figure 7.13 Sample EAP exchange

1. The authenticator issues a Request/Identity packet to identify the user.
2. The end user system prompts for input, collects the user identifier and sends the user identifier in a Response/Identity message.
3. With the user identified, the authenticator can issue authentication challenges. In step 3 in the figure, the

authenticator issues an MD-5 Challenge to the user with a Request/MD-5 Challenge packet.

4. The user system is configured to use a token card for authentication, so it replies with a Response/NAK, suggesting the use of Generic Token Card authentication.
5. The authenticator issues a Request/Generic Token Card challenge, prompting for the numerical sequence on the card.
6. The user types a response, which is passed along in a Response/Generic Token Card.
7. The user response was not correct, so authentication is not possible. However, the authenticator EAP implementation allows for multiple authentication Requests, so a second Request/Generic Token Card is issued.
8. Once again, the user types a response, which is passed along in a Response/Generic Token Card.
9. On the second try, the response is correct, so the authenticator issues a Success message.

7.8 MANAGEMENT OPERATIONS

While being untethered from a wired network can be an advantage, it can lead to problems: the medium is unreliable, unauthorized users can take advantage of the lack of physical boundaries, and power consumption is critical when devices are running on batteries. The management features of the 802.11 protocol were designed to reduce the effect of these problems.

7.8.1 Management Architecture

Conceptually, the 802.11 management architecture is composed of three components: the MAC layer management entity (MLME), a physical-layer management entity (PLME), and a system management entity (SME). The relation between the different management entities and the related parts of 802.11 is shown in Figure 7.14.

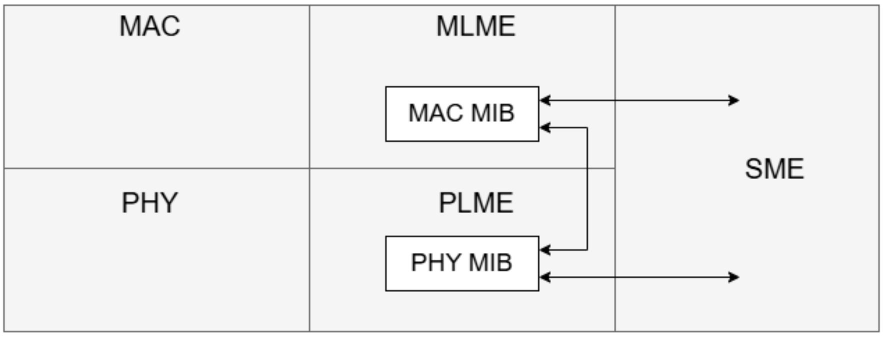


Figure 7.14 Relationship between management entities and components of the 802.11 specification

802.11 does not formally specify the SME. It is the method by which users and device drivers interact with the 802.11 network interface and gather information about its status. Both the MAC and PHY layers have access to a management information base (MIB).The MIB has objects that can be queried to gain status information, as well as objects that can cause certain actions to take place.

There are three defined interfaces between the management components. The station management entity may alter both the MAC and PHY MIBs through the MLME and PLME service interfaces. Additionally, changes to the MAC may require corresponding changes in the PHY, so an additional interface between the MLME and PLME allows the MAC to make changes to the PHY.

7.8.2 Scanning

Before using any network, first task is to find it. With wired networks, finding the network is easy: look for the cable or a jack on the wall. In the wireless world, stations must identify a compatible network before joining it. The process of identifying existing networks in the area is called scanning.

Several parameters are used in the scanning procedure. The user may specify these parameters; many implementations have default values for these parameters in the driver.

- **BSS Type** (independent, infrastructure, or both): Scanning can specify whether to seek out independent ad hoc networks, infrastructure networks, or all networks.
- **BSSID** (individual or broadcast): The device can scan for a specific network to join (individual) or for any network that is willing to allow it to join (broadcast). When 802.11 devices are moving, setting the BSSID to broadcast is a good idea because the scan results will include all BSSs in the area.
- **SSID** ("network name"): The SSID assigns a string of bits to an extended service set. Most products refer to the SSID as the network name because the string of bits is commonly set to a human-readable string. Clients wishing to find any network should set this to the broadcast SSID.
- **Scan Type** (active or passive): Active scanning uses the transmission of Probe Request frames to identify networks in the area. Passive scanning saves battery power by listening for Beacon frames.
- **Channel List**: Scans must either transmit a Probe Request or listen on a channel for the existence of a network. 802.11 allows stations to specify a list of channels to try. Products allow configuration of the channel list in different ways. What exactly constitutes a channel depends on the physical layer in use. With direct-sequence products, it is a list of channels. With frequency-hopping products, it is a hop pattern.
- **Probe Delay**: This is the delay, in microseconds, before the procedure to probe a channel in active scanning begins. This delay ensures that an empty or lightly loaded channel does not completely block the scan.
- **Min Channel Time** and **Max Channel Time** These values, specified in time units (TUs), specify the minimum and maximum amount of time that the scan works with any particular channel.

Also, there are two basic types of scanning:

Passive Scanning:

Passive scanning saves battery power because it does not require transmitting. In passive scanning, a station moves to each channel on the channel list and waits for Beacon frames. Any Beacons received are buffered to extract information about the BSS that sent them.

In the passive scanning procedure, the station sweeps from channel to channel and records information from any Beacons it receives. Beacons are designed to allow a station to find out everything it needs to match parameters with the basic service set(BSS) and begin communications. In Figure 7.15, the mobile station uses a passive scan to find BSSs in its area; it hears Beacon frames from the first three access points. If it does not hear Beacons from the fourth access point, it reports that only three BSSs were found.

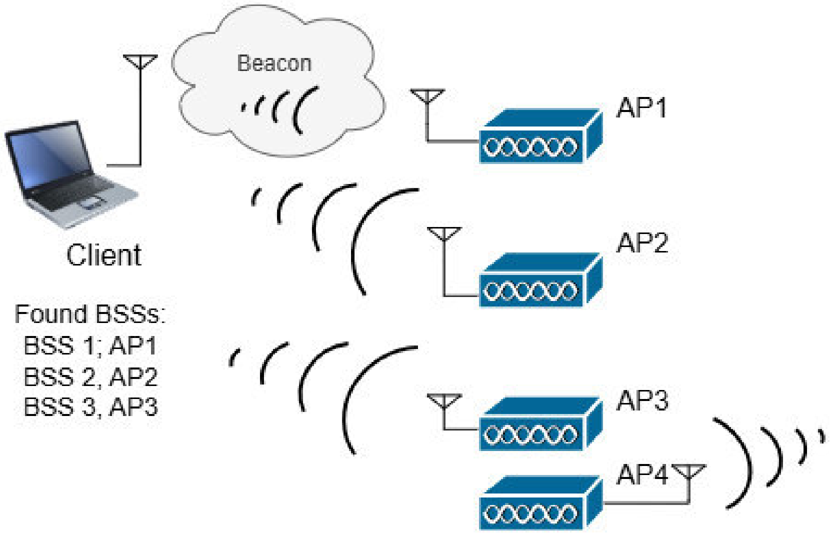


Figure 7.15 Passive Scanning

Active Scanning:

In active scanning, a station takes a more assertive role. On each channel, Probe Request frames are used to solicit responses from a network with a given name. Rather than listening for that network to announce itself, an active scan attempts to find the network. Stations using active scanning employ the following procedure for each channel in the channel list:

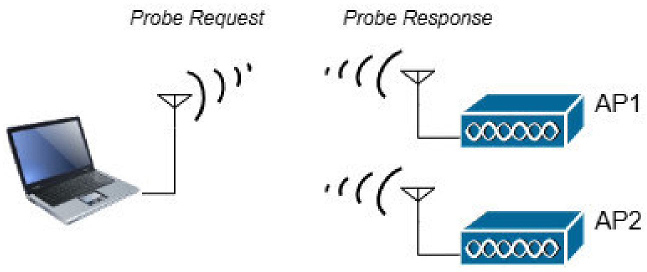
1. Move to the channel and wait for either an indication of an incoming frame or for the Probe Delay timer to expire. If an incoming frame is detected, the channel is in use and can be

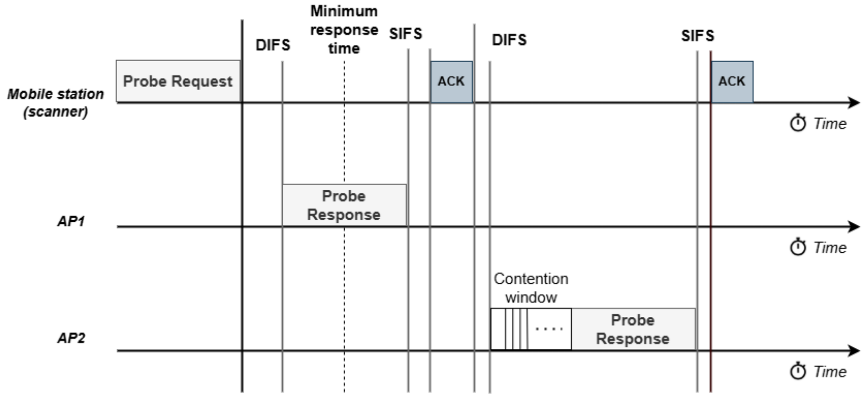
probed. The timer prevents an empty channel from blocking the entire procedure; the station won't wait indefinitely for incoming frames.

2. Gain access to the medium using the basic DCF access procedure and send a Probe Request frame.
3. Wait for the minimum channel time, Min Channel Time, to elapse.
    a. If the medium was never busy, there is no network. Move to the next channel.
    b. If the medium was busy during the Min Channel Time interval, wait until the maximum time, Max Channel Time, and process any Probe Response frames

One station in each BSS is responsible for responding to Probe Requests. The station that transmitted the last Beacon frame is also responsible for transmitting any necessary Probe Response frames. In infrastructure networks, the access points transmit Beacons and thus are also responsible for responding to itinerant stations searching the area with Probe Requests. IBSSs may pass around the responsibility of sending Beacon frames, so the station that transmits Probe Response frames may vary. Probe Responses are unicast management frames and are therefore subject to the positive acknowledgment requirement of the MAC. It is common for multiple Probe Responses to be transmitted as a result of a single Probe Request. The purpose of the scanning procedure is to find every basic service area that the scanning station can join, so a broadcast Probe Request results in a response from every access point within range. Any overlapping independent BSSs may also respond.

(a)





(b)

Figure 7.16 Active Scanning

Figure 7.16 shows the relationship between the transmission of Probe frames and the various timing intervals that can be configured as part of a scan. In Figure 7.16(a), a mobile station transmits a probe request to which two access points respond. The activity on the medium is shown in Figure 7.16 (b). The scanning station transmits the Probe Request after gaining access to the medium. Both access points respond with a Probe Response that reports their network's parameters.

7.8.3 Authentication

On a wired network, authentication is implicitly provided by physical access; if you're close enough to the network to plug in a cable, you must have gotten by the receptionist at the front door. While this is a weak definition of authentication, and one that is clearly inappropriate for high-security environments, it works reasonably well as long as the physical access control procedures are strong. Wireless networks are attractive in large part because physical access is not required to use network resources. Therefore, a major component of maintaining network security is ensuring that stations attempting to associate with the network are allowed to do so. Two major approaches are specified by802.11: open-system authentication and shared-key authentication. Shared-key authentication is based on WEP and requires that both stations implement WEP.

802.11 does not restrict authentication to any particular scenario. Any station can authenticate with any other station. In practice, authentication is most useful in infrastructure networks. The usefulness of authentication for infrastructure networks is due in part to the design of the authentication methods, which do not really result in mutual authentication. As a matter of design, the authentication process really only proves the identity of one station. 802.11 implicitly assumes that access points are in a privileged position by virtue of the fact that they are typically under control of network administrators. Network administrators may wish to authenticate mobile stations to ensure that only authorized users access the 802.11 network, but mobile stations can't authenticate the access point. For this reason, the examples in this section assume that a mobile station such as an 802.11-equipped PC is attempting to authenticate to an access point. The standard, however, does not restrict authentication to infrastructure networks.

802.11 authentications is currently a one-way street. Stations wishing to join a network must authenticate to it, but networks are under no obligation to authenticate themselves to a station. The designers of 802.11 probably felt that access points were part of the network infrastructure and thus in a more privileged position, but this curious omission makes a man-in-the-middle attack possible. A rogue access point could certainly send Beacon frames for a network, it is not a part of, and attempt to steal authentication credentials.

7.8.3.1 Open-System Authentication

Open-system authentication is the only method required by 802.11. Calling it authentication is stretching the meaning of the term a great deal. In open-system authentication, the access point accepts the mobile station at face value without verifying its identity. (Imagine a world where similar authentication applied to bank withdrawals!)

An open-system authentication exchange consists of two frames, shown in Figure 7.17.

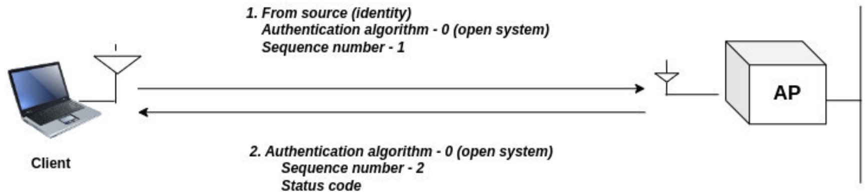

1. From source (identity)
Authentication algorithm - 0 (open system)
Sequence number - 1
AP
Client
2. Authentication algorithm - 0 (open system)
Sequence number - 2
Status code

Figure 7.17 Open-system Authentication exchange

The first frame from the mobile station is a management frame of subtype authentication.802.11 does not formally refer to this frame as an authentication request, but that is its practical purpose. In 802.11, the identity of any station is its MAC address. Like Ethernet networks, MAC addresses must be unique throughout the network and can readily double as station identifiers. Access points use the source address of frames as the identity of the sender; no fields within the frame are used to further identify the sender.

There are two information elements in the body of the authentication request. First, the Authentication Algorithm Identification is set to 0 to indicate that the open-system method is in use. Second, the Authentication Transaction Sequence number is set to 1 to indicate that the first frame is in fact the first frame in the sequence.

The access point then processes the authentication request and returns its response. Like the first frame, the response frame is a management frame of subtype authentication.

Three information elements are present: the Authentication Algorithm Identification field is set to 0 to indicate open-system authentication, the Sequence Number is 2, and a Status Code indicates the outcome of the authentication request.

7.8.3.2 Shared-Key Authentication

Shared-key authentication makes use of WEP and therefore can be used only on products that implement WEP. Furthermore, 802.11 requires that any stations implementing WEP also implement shared-key authentication. Shared-key authentication, as its name implies, requires that a shared key be distributed to stations before attempting authentication. A shared-key authentication exchange consists of four management frames of subtype authentication, shown in Figure 7.18.

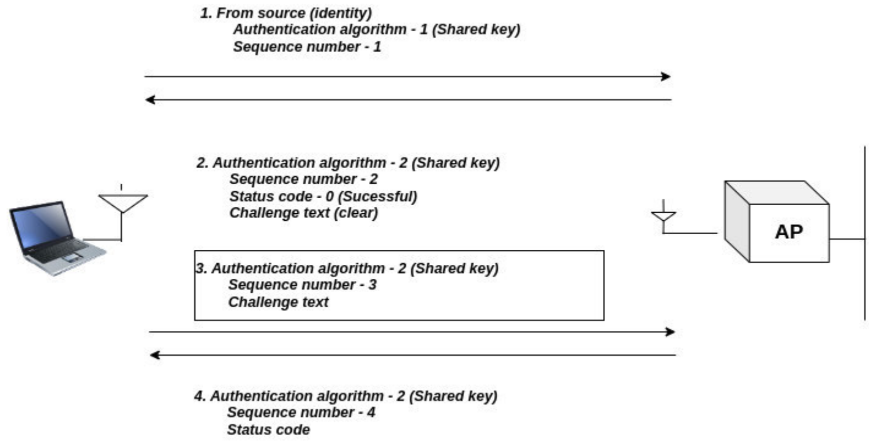

1. From source (identity)
Authentication algorithm - 1 (Shared key)
Sequence number - 1
2. Authentication algorithm - 2 (Shared key)
Sequence number - 2
Status code - 0 (Sucessful)
Challenge text (clear)
3. Authentication algorithm - 2 (Shared key)
Sequence number - 3
Challenge text
4. Authentication algorithm - 2 (Shared key)
Sequence number - 4
Status code
AP

Figure 7.18 Shared-key authentication exchange

The first frame is nearly identical to the first frame in the open-system authentication exchange. Like the open-system frame, it has information elements to identify the authentication algorithm and the sequence number; the Authentication Algorithm Identification is set to 1 to indicate shared-key authentication.

Instead of blindly allowing admission to the network, the second frame in a shared-key exchange serves as a challenge. Up to four information elements may be present in the second frame. Naturally, the Authentication Algorithm Identification, Sequence Number, and Status Code are present. The access point may deny an authentication request in the second frame, ending the transaction. To proceed, however, the Status Code should be set to 0 (success), as shown in Figure 7.18. When the Status Code is successful, the frame also includes a fourth information element, the Challenge Text. The Challenge Text is composed of 128 bytes generated using the WEP key stream generator with a random key and initialization vector. The third frame is the mobile station's response to the challenge. To prove that it is allowed on the network, the mobile station constructs a management frame with three information elements: the Authentication Algorithm Identifier, a Sequence

Number of 3,and the Challenge Text. Before transmitting the frame, the mobile station processes the frame with WEP. The header identifying the frame as an authentication frame is preserved, but the information elements are hidden by WEP.

After receiving the third frame, the access point attempts to decrypt it and verify the WEP integrity check. If the frame decrypts to the Challenge Text, and the integrity check is verified, the access point will respond with a status code of successful. Successful decryption of the challenge text proves that the mobile station has been configured with the WEP key for the network and should be granted access. If any problems occur, the access point returns an unsuccessful status code.

7.8.3.3 Pre-authentication

Stations must authenticate with an access point before associating with it, but nothing in802.11 requires that authentication take place immediately before association. Station scan authenticate with several access points during the scanning process so that when association is required, the station is already authenticated. This is called pre-authentication. As a result of pre-authentication, stations can re associate with access points immediately upon moving into their coverage area, rather than having to wait for the authentication exchange. In both parts of Figure 7.19, there is an extended service set composed of two access points. Only one mobile station is shown for simplicity. Assume the mobile station starts off associated with AP1 at the left side of the diagram because it was powered on inAP1's coverage area. As the mobile station moves towards the right, it must eventually associate with AP2 as it leaves AP1's coverage area.

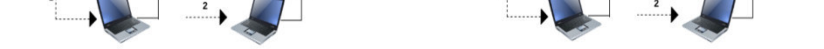


Figure 7.19 Time savings of pre-authentication

7.8.4 Association

Once authentication has completed, stations can associate with an access point (or reassociate with a new access point) to gain full access to the network. Association is a recordkeeping procedure that allows the distribution system to track the location of each mobile station, so frames destined for the mobile station can be forwarded to the correct access point. After association completes, an access point must register the mobile station on the network so frames for the mobile station are delivered to the access point. One method of registering is to send a gratuitous ARP so the station's MAC address is associated with the switch port connected to the access point. Association is restricted to infrastructure networks and is logically equivalent to plugging into a wired network. Once the procedure is complete, a wireless station can use the distribution system to reach out to the world, and the world can respond through the distribution system. 802.11 explicitly forbids associating with more than one access point.

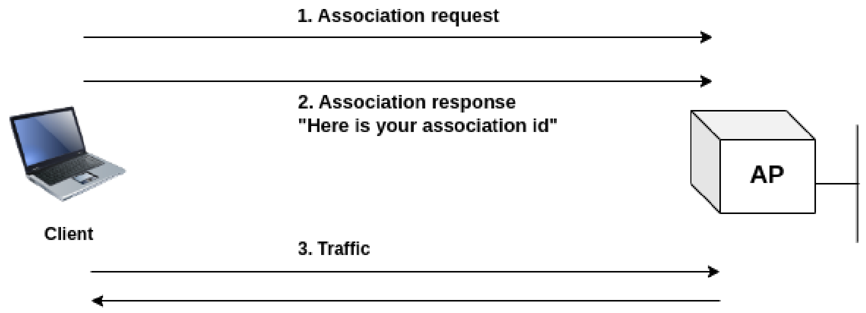


Figure 7.20Association procedure

The basic association procedure is shown in Figure 7.20.Like authentication, association is initiated by the mobile station. No sequence numbers are needed because the association process is a three-step exchange. The two frames are management frame subtypes defined by the specification. As unicast management frames, both steps in the association procedure are composed of an association frame and the required link-layer acknowledgment:

1. Once a mobile station has authenticated to an access point, it can issue an Association Request frame. Stations that have not yet authenticated receive a De-authentication frame from the access point in response.
2. The access point then processes the association request. 802.11 does not specify how to determine whether an association should be granted; it is specific to the access point implementation. One common consideration is the amount of space required for frame buffering. Rough estimates are possible based on the Listen Interval in the Association Request frame.
    a. When the association request is granted, the access point responds with a status code of 0 (successful) and the Association ID (AID). The AID is a numerical identifier used to logically identify the mobile station to which buffered frames need to be delivered.
    b. Unsuccessful association requests include only a status code, and the procedure ends.
3. The access point begins processing frames for the mobile station. In all commonly used products, the distribution system medium is Ethernet. When an access point receives a frame destined for an associated mobile station, that frame can be bridged from the Ethernet to the wireless medium or buffered if the mobile station is in a power-saving state. In shared Ethernets, the frame will be sent to all the access points and will be bridged by the correct one. In switched Ethernets, the station's MAC address will be associated with a particular switch port. That switch port is, of course, connected to the access point currently providing service for the station.

7.8.5 Timer Synchronization

Like other wireless network technologies, 802.11 depends a great deal on the distribution of timing information to all the nodes. It is especially important in frequency-hopping networks because all stations on the network must change frequency channels in a coordinated pattern. Timing information is also used by the medium reservation mechanisms.

In addition to local station timing, each station in a basic service area maintains a copy of the timing synchronization function (TSF), which is a local timer synchronized with the TSF of every other station in the basic service area. The TSF is based on a 1-MHz clock and "ticks" in microseconds. Beacon frames are used to periodically announce the value of the TSF to other stations in the network. The "now" in a timestamp is when the first bit of the timestamp hits the PHY for transmission.

7.8.5.1 Infrastructure Timing Synchronization

The ease of power management in an infrastructure network is based on the use of access points as central coordinators for data distribution and power management functions. Timing in infrastructure networks is quite similar. Access points are responsible for maintaining the TSF time, and any stations associated with an access point must simply accept the access point's TSF as valid. When access points prepare to transmit a Beacon frame, the access point timer is

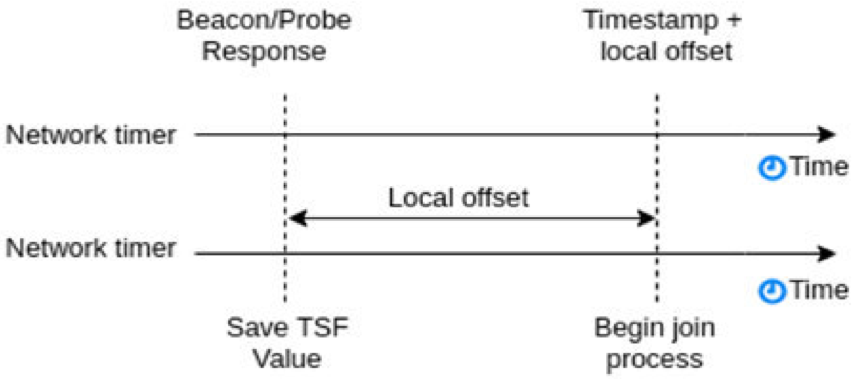


Figure 7.21Infrastructure Timing Synchronization

copied into the Beacon's timestamp field. Stations associated with an access point accept the timing value in any received Beacons, but they may add a small offset to the received timing value to account for local processing by the antenna and transceiver. Associated stations maintain local TSF timers so they can miss a Beacon frame and still remain roughly synchronized with the global TSF. The wireless medium is expected to be noisy, and Beacon frames are unacknowledged. Therefore, missing a Beacon here and there is to be expected, and the local TSF timer mitigates against the occasional loss of Beacon frames. To assist active scanning stations in matching parameters with the BSS, timing values are also distributed in Probe Response frames. When a station finds a network by scanning, it saves the timestamp from the Beacon or Probe Response and the value of the local timer when it was received. To match the local timer to the network timer, a station then takes the timestamp in the received network advertisement and adds the number of microseconds since it was received. Figure 7.21 illustrates this process.

7.8.5.2 IBSS Timing Synchronization

IBSSs lack a central coordination point, so the Beacon process is distributed. TSF maintenance is a subset of the Beacon generation process. Time is divided into segments equivalent to the inter beacon timing period. Beacon frames are supposed to be transmitted exactly as the beacon interval ends, at the so-called target Beacon transmission time (TBTT). Independent networks take the TBTT as a guideline.

All stations in the IBSS prepare to transmit a Beacon frame at the target time. As it approaches, all other traffic is suspended. Timers for the transmission of frames other than Beacon frames or ATIM frames are stopped and held to clear the medium for the important management traffic. All stations in the IBSS generate a backoff timer for Beacon transmission; the backoff timer is a random delay between 0 and twice the minimum contention window for the medium. After the target beacon interval, all stations begin to count the Beacon backoff timer down to 0. If a Beacon is received before the station's transmission time, the pending Beacon transmission is cancelled.

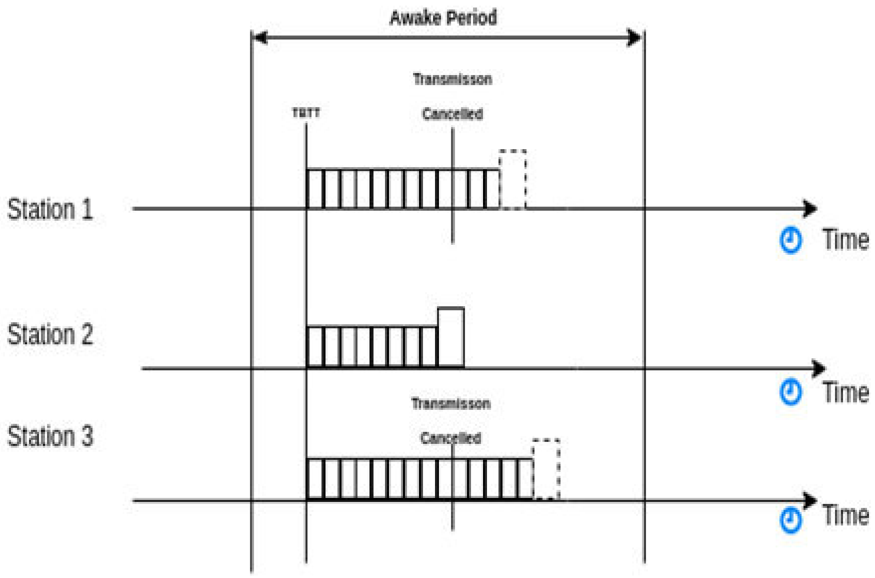


Figure 7.22Distributed Beacon generation

In Figure 7.22, each station selects a random delay; station 2 has randomly generated the shortest delay. When station 2's timer expires, it transmits a Beacon, which is received by stations 1 and 3. Both stations 1 and 3 cancel their Beacon transmissions as a result. Because timer synchronization ensures that all stations have synchronized timers, multiple Beacon frames do not pose a problem. Receivers simply process multiple Beacon frames and perform multiple updates to the TSF timer.

7.9 802.11 IN LINUX

Of the operating systems currently in wide use and active development, Unix environments offer the flexibility and stability required by power users and network administrators. When new hardware hits the market, the technical staff responsible for making purchase recommendations often asks about Linux support because of the additional functionality that can frequently be gained from the environment.

7.9.1 802.11 Hardware

Only a handful of 802.11 chipset manufacturers exist. Most vendor suse chipsets produced by Intersil (http://www.intersil.com, formerly known as Harris Semiconductor). Intersil's industry-leading position is the result of the success of its PRISM chipset. The initial PRISM, whose name is an acronym for Programmable Radioin the ISM band, was a common solution for vendors seeking a 2-Mbps DSSS 802.11solution. When 802.11b was standardized in 1999, Intersil brought out the PRISM-2chipset, which supported the 5.5-Mbps and 11-Mbps data rates. Linksys, Nortel/Netgear, D-Link, and SMC for interface use, Intersil's chipsets cards.

In addition to the radio chipset, cards must have a MAC controller. Most cards on the market use an Intersil MAC controller. Several first-generation cards used an AMDAm930 MAC controller but have switched to the integrated MAC controller in thePRISM-2 chipset. Cisco's Aironet product line uses an Aironet-developed MAC controller with a PRISM-2 radio chipset.

7.9.2 PCMCIA Support on Linux

Most add-on 802.11 solutions for laptop computers are based on the PCMCIA form factor. Adding 802.11 support to Linux requires an understanding of how the PCMCIA subsystem in Linux is put together and how it works to enable drivers for PCMCIA cards.

PCMCIA Card Services:

Card Services grew out of an attempt to simplify system configuration. Rather than dedicating system resources to individual devices, the host system maintained a pool of resources for PC Cards and allocated resources as necessary. Figure 7.23 shows the procedure by which cards are configured on Linux.

When a card is inserted, the cardmgr process orchestrates the configuration of the device, as shown in Figure 7.23. The orchestration pulls together system resources, kernel components, and kernel driver modules through the configuration files stored in/etc/pcmcia. Roughly speaking, the host takes the following steps:

1. A card is inserted into an empty PC Card socket, and cardmgr is notified of this event. In addition to performing any hardware operations (such as supplying power to the socket), cardmgr queries the card information structure (CIS) to determine the type of card inserted and the resources it needs. For more information on the CIS, see the sidebar Card Information Structure.
2. cardmgr consults the card database stored in /etc/pcmcia/config to identify which card was inserted. Part of the configuration involves associating cards with a class. For configuring network cards, it's important to note that items in the network class undergo additional network configuration operations later. The card is identified by the CIS data from the previous step, and the class setting is specified in the main system configuration file. At this point, cardmgr beeps once. Successful identification produces a high-pitched beep, while unsuccessful identifications are indicated by a lower-pitched beep.

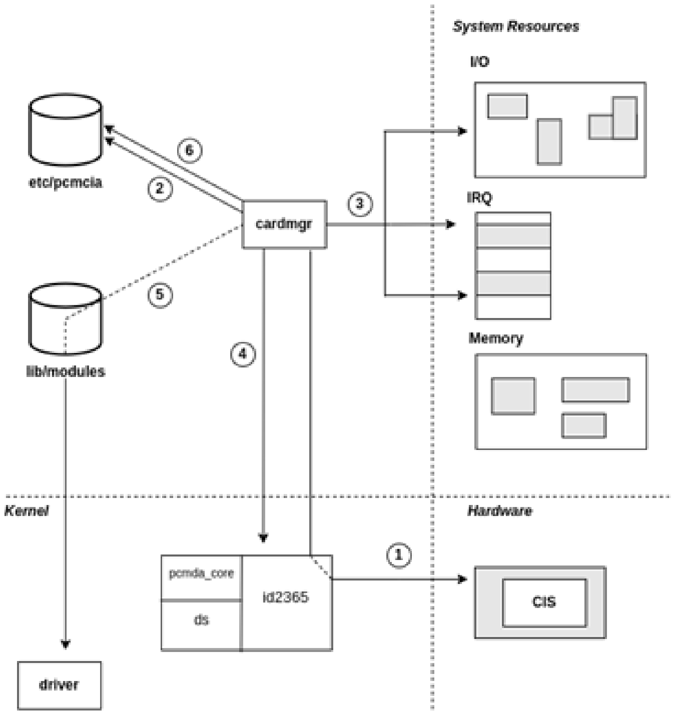


Figure 7.23 Linuc PCMCIA configuration System

1. cardmgr determines which resources are available to allocate to the card. Blocks of system resources are reserved for PCMCIA card use in the main configuration file, and cardmgr allocates resources to cards as needed. The number of I/O ports and the size of the memory window are obtained from the CIS.
2. Resources allocated by cardmgr are programmed into the PCMCIA controller, depicted in Figure 7.23 as interaction with the device driver. PCMCIA controllers implement resource steering to map the resources required by the card onto available system resources. A card may request an interrupt; however, the actual assigned interrupt is not relevant. During operation, the card simply asks the PCMCIA controller to raise an interrupt, and the controller is responsible for looking up the interrupt assigned to the socket and activating the correct interrupt line.
3. Part of the configuration information obtained from the lookup in the previous step is the name of the device driver that should be loaded to use the newly inserted card. Drivers for PCMCIA cards are implemented as kernel modules. During the insertion process, the driver is informed of the resources allocated in the prior step. With proper module dependencies, module stacking can be used to load multiple modules.
4. Further user-space configuration is performed based on the class of the device. For instance, network cards require additional configuration performed by the /etc/pcmcia/network script, which is configured by editing /etc/pcmcia/network.opts. Successful configuration at this stage generates a second high beep, while failure is reported with a low beep.

Check Your Progress –II

2. State True or False

(i) The Association ID is a numerical identifier used to physically identify the mobile station.

(ii) Most add-on 802.11 solutions for laptop computers are based on the PCMCIA form factor.

(iii) The Null Function data frame carries no data, polls, or acknowledgments.

(iv) Open-system authentication is the only method required by 802.11.

(v) ICV(Integrated Check Value) is always available for the casual attackers.

7.10 SUMMING UP

The 802.11 wireless networking protocol includes several key processes that ensure that devices can connect to and communicate within a wireless network. Authentication is one of the initial steps in this process, with two primary methods: open-system and shared-key authentication. Open-system authentication is the simpler of the two, where the access point (AP) accepts a mobile station (MS) based solely on its MAC address without verifying its identity. This method is quick but offers no real security. In contrast, shared-key authentication uses a pre-shared key (WEP) for a more secure process. It involves a four-frame exchange in which the access point challenges the mobile station to prove that it knows the shared key and the station responds accordingly. If the access point can successfully decrypt the response, then the station is authenticated.

Another concept related to authentication is pre-authentication, which allows a station to authenticate with multiple access points during its scanning process. This pre-emptive authentication ensures that when a station moves between APs, it can quickly reassociate without waiting for a full authentication cycle, thereby reducing connection delays and improving user experience.

Once authenticated, the next stage is association. In this phase, the mobile station requests to associate with an AP to gain full access to the network. The association process helps the AP maintain a record of which station is connected and where to route its data. This process is critical for infrastructure networks, which use APs as intermediaries between stations and the broader network. The AP assigns an Association ID (AID) to the station, ensuring proper routing of frames.

Timing synchronization is also vital in 802.11 networks, especially in infrastructure setups. Access points are responsible for maintaining the timing synchronization function (TSF), a local timer shared by all stations within its basic service set (BSS). APs periodically broadcast the TSF in Beacon frames, allowing all stations to stay synchronized. This synchronization is critical for coordinated medium access, power management, and frequency hopping, particularly in frequency-hopping networks. In infrastructure networks, stations synchronize to the AP's TSF, while in independent basic service sets (IBSS), stations share responsibility for maintaining the TSF and take turns transmitting Beacon frames.

The 802.11 standard also ensures that network devices are compatible with Linux operating systems. Linux-based systems rely on open-source drivers and utilities to support a variety of 802.11 hardware, often through the PCMCIA interface. This support enables flexible and stable wireless networking for laptop users and power users who rely on Linux for network administration. The configuration process for wireless cards on Linux involves several steps, including the identification of the card, resource allocation, and driver loading. The PCMCIA Card Services framework manages these tasks, ensuring smooth integration of wireless devices into Linux-based systems.

In summary, the 802.11 protocol provides a structured approach for wireless authentication, association and synchronization, with essential mechanisms in place for power management and seamless integration with Linux systems.

7.11 ANSWER TO CHECK YOUR PROGRESS

1. (i) True (ii)True (iii) False (iv) True (v) False

2. (i) False (ii) True (iii) True (iv) True (v) false

7.12 POSSIBLE QUESTIONS

1. What is the role of the distribution system in an 802.11 network?
2. Besides bridging, what other functions might an access point perform?
3. Why have RF physical layers become more popular than infrared layers?
4. Why might wireless networking be used for desktop computers in some environments?
5. What is the difference between an Independent BSS (IBSS) and an Infrastructure BSS?
6. How does 802.11 ensure reliable frame delivery despite the unreliability of radio channels?
7. Which 802.11 services are used specifically for data movement and which are used for network management?
8. How do distribution system services assist in managing mobile stations?
9. How does CSMA/CA differ from CSMA/CD, and why is it used in wireless networks?
10. What are the two coordination functions used in 802.11 MAC access and what is the key difference between them?
11. What are the basic steps a station follows under DCF to transmit a frame?
12. How does PCF enable contention-free access to the wireless medium?
13. What are the major fields in an 802.11 MAC frame and what is the function of each?

14. How the SSID is used in different BSS types (IBSS vs infrastructure)?
15. What are the type and subtype fields used for in the Frame Control section?
16. What is the purpose of the RTS/CTS frame exchange?
17. Which data frame subtypes actually carry user data?
18. What is the purpose of the Association Request and Association Response frames?
19. How does a Reassociation Request differ from an Association Request?
20. What is the role of a Probe Request and Probe Response in wireless communication?
21. What are the three primary objectives of communication security that WEP attempts to address?
22. What does the Integrity Check Value (ICV) do and how is it protected during transmission?
23. How the RC4 is key generated in WEP and what is its total length?
24. What is the purpose of the Initialization Vector (IV), and how is it transmitted?
25. Why key reuse is considered vulnerability in WEP?
26. What dual roles did WEP attempt to fulfil in 802.11 networks?
27. Why WEP is considered inadequate as an authentication mechanism?
28. What two main problems limit the effectiveness of 802.1X in wireless networks?
29. How are request and response packets distinguished in EAP exchanges?
30. What happens if a client receives an EAP request type it does not support?
31. What are the code values for EAP Success and Failure and what do they signify?

32. How are request and response packets distinguished in EAP exchanges?
33. What happens if a client receives an EAP request type it does not support?
34. What are the code values for EAP Success and Failure and what do they signify?
35. How are request and response packets distinguished in EAP exchanges?
36. What happens if a client receives an EAP request type it does not support?
37. What are the code values for EAP success and failure and what do they signify?

7.13 REFERENCES AND SUGGESTED READINGS

1. Gast, M. S. (2005). *802.11 Wireless Networks: The definitive guide* (2nd ed.). O'Reilly Media. ISBN: 9780596100520
2. Lin, Y.-B. (2009). *Wireless and mobile network architectures*. Wiley India Pvt. Ltd. ISBN: 978-81-265-1560-8
3. Rappaport, T. S. (2005). *Wireless communications: Principles and practice* (2nd ed.). Pearson Education. ISBN: 978-81-317-3186-4
4. Singal, T. L. (2010). *Wireless communications*. Tata McGraw-Hill Education. ISBN: 978-0-07-068178-1

***

BLOCK- III

MOBILE IP AND WIRELESS APPLICATION PROTOCOL

Unit 1: Mobile IP

Unit 2: WAP (Wireless Application Protocol)

UNIT- 1

MOBILE IP

Unit Structure:

1.1 INTRODUCTION

Mobile IP is a communication protocol that enables users to change their location from one network to another with the same IP address. It is developed through the extension of Internet Protocol (IP) to boosts mobile communication. It is designed to make sure that the communication will proceed uninterrupted without dropping the user's sessions or connections while moving across different networks. Mobile IP operates like a phone number that never changes regardless of the location of the owner of the phone number. Devices like Wi-Fi and cellular often changes network location. To handle such kind of devices, Mobile IP is especially useful. Mobile IP ensures seamless, stable, consistent internet connectivity maintaining user mobility. In this unit, we will discuss how need of Mobile IP, how it operates and its capabilities.

1.2 OBJECTIVES

After going through this unit, learner will be able to

- *explain* the concepts of mobile IP;
- *describe* the different key components of Mobile IP;
- understand various encapsulation and route optimization in IP Header;
- *understand* the concepts of mobility binding;
- *understand* the concepts of cellular IP;
- *understand* the mobile IP with IPV6;
- *understand* various concepts of IP Security.

1.3 NEED FOR MOBILE IP

The Internet Protocol (IP) enables the mobile devices to communicate over networks by assigning fixed IP address using an ISP (Internet Service Provider) based on the device's current network. Whenever a device moves from one network to another, its IP address changes. This causes the break to its ongoing sessions and disrupts the communication. For example, suppose you are on a video call from your laptop which is connected to your home Wi-Fi (with a specific IP). Now, if you move to a nearby café and there you connect to the Wi-Fi (which gives a different IP) there, the call would automatically drop because the IP has changed. Besides, applications involving Remote login, remote printing, and file transfers require interrupted communications while an individual roams across network boundaries. Mobile IP is needed to solve this issue. This means we need connection such that the device keeps on operating with the same existing IP address even when switching between the networks.

1.4 COMPONENTS OF MOBILE IP

Mobile IP is a communication standard, which was developed by the IETF (Internet Engineering Task Force). There are three major components associated to a Mobile IP, viz., Mobile Node (MN), Home Agent (HA), and Foreign Agent (FA) as shown in Figure 1.1. Let us look into these components.

- **Mobile Node (MN):** A mobile node is a device such as a cell phone, laptop, personal digital assistant, or laptop. The software in a MN continuously monitors the device’s mobility, enabling its network roaming capabilities.   whose software enables network roaming capabilities.
- **Home Agent (HA):** It is a router on the home network that serves as the point of communication with the Mobile Node. It maintains the information about the current location of the mobile note and tunnels packets to the Care-of Address (CoA) of the mobile node to the roaming Mobile Node. The CoA is a temporary IP address assigned to the mobile node when it is visiting a foreign network.
- **Foreign Agent (FA):**A FA is router on the network the mobile node visits called as the foreign network. It assigns Care-of Address (CoA) to the mobile node for delivering tunneled packets from the Home Agent to the Mobile Node.

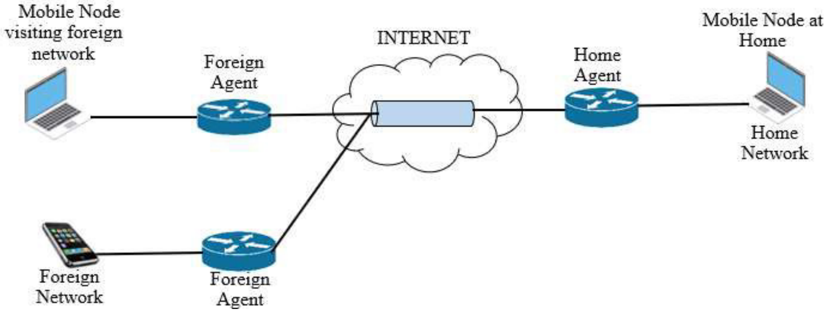


Figure 1.1 Components of Mobile IP

Stop to Consider

Mobile IP is a communication protocol that ensures uninterrupted internet connectivity when a device moves across different networks, whereas the conventional IP is not capable of. The key components of Mobile IP are *Mobile Node (MN), Home Agent (HA) and Foreign Agent (FA)*.

1.5 WORKING PRINCIPLE OF MOBILE IP

The workflow of Mobile IP has three key phases, viz., Agent Discovery, Registration and Tunneling. Let us discuss these phases in details.

- ***Agent Discovery*****:** Agent Discovery is the initial step in Mobile IP that enables a Mobile Node (MN) to determine whether it is on its home or a foreign network. For this, both the agents, viz., Home Agents (HA) and Foreign Agents (FA) periodically broadcast Agent Advertisements (Figure 1.2) using the ICMP Router Discovery Protocol (IRDP). These advertisements include Mobile IP extensions that identify the agent type (Home or Foreign), available Care-of Address (CoA), supported services (e.g., reverse tunneling and GRE), and the allowed lifetime registration or roaming period for visiting mobile devices. Instead of waiting for these broadcasts, a Mobile Node can also send an Agent Solicitation to prompt immediate responses from nearby agents. When the Mobile Node receives an advertisement, it checks if it's connected to a foreign network. If so, it will acquire a Care-of Address to maintain communication while away from its home network. Two types of Care-of Addresses are available, one provided by the Foreign Agent, which can be shared by multiple Mobile Nodes, and a Colocated Care-of Address, which is a temporary address assigned directly to the Mobile Node and is unique to it. The Colocated address gives the Mobile Node more control and direct connectivity but typically requires support like DHCP. Upon confirming its location in a foreign network and acquiring a suitable Care-of Address, the Mobile Node initiates the registration process to update its current location.

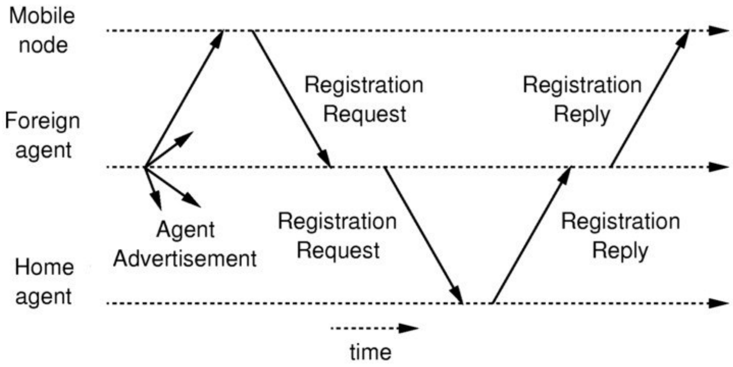


Figure 1.2 Request Registration in Mobile IP

- ***Registration*:** Once the Mobile Node (MN) detects it is no longer in its home network through Agent Discovery, it acquires a CoA either from a Foreign Agent (FA) or by assigning itself a temporary address (Colocated CoA) via services like DHCP. If the MN is using a Foreign Agent CoA, the request is first sent a request message to the FA, which forwards it to the HA after appending its own identification and authentication data. This request message includes key information, viz., the Mobile Node's home address, newly acquired CoA, the IP address of its HA, registration lifetime (how long the binding should remain active), and a unique identifier (UID). If the MN uses a Colocated CoA, it can directly communicate with the Home Agent without the help of a Foreign Agent. The registration process is now authenticated by the HA using Mobile IP Authentication. This ensures that whether the request has not been forged or tampered with. After successful verification, HA updates its binding table to associate the MN’s home address with its current CoA. This enables the Home Agent to intercept any data packets sent to the Mobile Node’s permanent IP address and forward them through tunneling to the current location of the Mobile Node. Finally, the Home Agent sends a Registration Reply back to the Mobile Node (via the Foreign Agent if involved), indicating whether the registration was successful or denied. If successful, the Mobile Node can now continue its communication sessions uninterrupted, despite being away from its home network.

- ***Tunneling*****:** Once the Mobile Node successfully registered its presence in a foreign network, the data packets addressed to the destination IP address are intercepted by the HA. The Home Agent encapsulates each packet, called *tunneling* process. Tunneling ensures that packets are properly routed to the FA, which will be then decapsulated and delivered to the MN. Two types of tunneling are used in Mobile IP, viz., *direct tunneling* and *indirect* tunneling.
    - *Direct Tunneling*: In this tunneling, HA encapsulates the incoming data packets and then sends them directly to the FA. The Foreign Agent decapsulates these packets and forwards them to the Mobile Node.
    - *Reverse Tunneling*: Reverse tunneling is used when the Mobile Node needs to send data back to the
    - Correspondent Node. Here, the data packets are first sent to the FA. The FA encapsulates the received data packets and forwards them to the HA, which are then forwarded to the Correspondent Node.

After all these three major phases, the actual *data delivery* starts. Once the tunneling process gets finished, FA delivers the decapsulated data packets to the MN. The Mobile Node processes the data and, if necessary, sends a response back to the Correspondent Node.

Check Your Progress-1

Q.1. Choose the Correct Option:

i) What is the main issue caused by IP address change during network roaming?

(a) Increased bandwidth
(b) Faster communication3G
(c) Disruption of ongoing sessions
(d) Duplicate IPs in the network

ii) Which protocol enables devices to maintain the same IP address while moving between networks?

(a) TCP
(b) DNS

(c) DHCP
(d) Mobile IP

iii) What does the Foreign Agent provide to a visiting Mobile Node?
(a) Home address
(b) Care-of Address (CoA)
(c) Authentication key
(d) IP address

iv) Which of the following protocols is used by the agents to broadcast their presence in Agent Discovery?
(a) ICMP Router Discovery Protocol
(b) DHCP
(c) TCP
(d) DNS

v) The purpose of the Tunnelling phase in Mobile IP is
(a) to authenticate users
(b) to compress packets
(c) to disconnect inactive Mobile Nodes
(d) to encapsulate and forward packets to the mobile node

1.6 FORMAT OF REGISTRATION MESSAGES

As we discussed earlier, the registration operation uses two types of messages, viz., Registration Request message (Figure 1.3), and Registration Reply message (Figure 1.4).

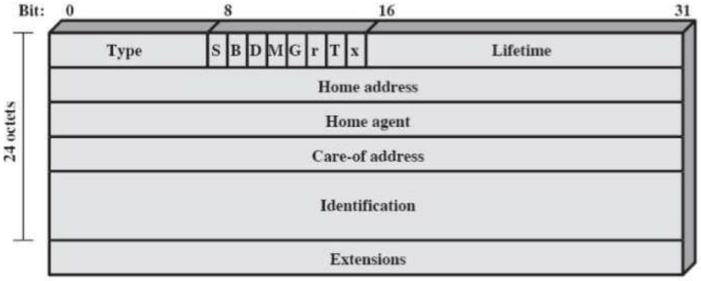


Figure 1.3 Format of Registration Request message

(Source: https://www.slideserve.com/vinson/mobile-ip-and-wireless-application-protocol)

1.6.1 Key Fields in Registration Request Message

The key fields in the Registration Request message are as follows:

- **Type**: Specifies the message type (e.g., 1 for Registration Request).
- **Flags**: Various bits indicating options, viz., S, B, D, M, G, r, T, x.
  - S (Simultaneous bindings): Allow multiple care-of addresses.
  - B (Broadcast): Request to use broadcast registration.
  - D (Decapsulation by FA): Indicates if Foreign Agent should decapsulate.
  - M (Minimal encapsulation): Use minimal encapsulation.
  - G (GRE encapsulation): Use GRE encapsulation.
  - r (Reserved)
  - T (Reverse tunneling requested)
  - x (Reserved)
- **Lifetime**: The desired lifetime (in seconds) for the registration (how long the registration should be valid).
- **Home Address**: The permanent IP address of the Mobile Node (its address in the home network).
- **Care-of Address**: The current IP address of the Mobile Node (typically the address assigned in the foreign network).
- **Identification:** A unique identifier for the registration request. Used to match the request and reply.
- **Extensions**: Various optional extensions can be included, such as, Authentication extensions (for security), additional IP addresses for simultaneous bindings, and other vendor-specific or protocol-specific extensions.

1.6.2 Key Fields in Reply Request Message

The key fields in the Registration Request message are as follows:

- **Type:** Specifies the message type. Here it is 3, which indicates that this is a registration reply.
- **Code:** Indicates result of the registration request. Different code values for a Mobile IP Registration Reply are defined. Followings are some of them.

  - 0 (registration accepted)
  - 1 (registration accepted, but simultaneous mobility bindings unsupported)
  - 128 (reason unspecified)
  - 129 (administratively prohibited)
- Lifetime: If the code field indicates that the registration was accepted, the number of seconds before the registration is considered expired. A value of zero indicates that the mobile node has been de-registered.
- Home Address: The home IP address of the mobile node.
- Home Agent: The IP address of the mobile node's home agent.

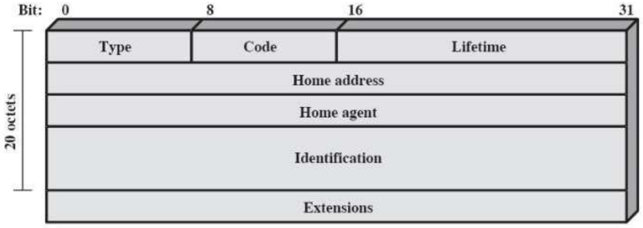


Figure 1.4 Format of Registration Reply message

(Source: https://www.slideserve.com/vinson/mobile-ip-and-wireless-application-protocol)

Check Your Progress-2

Q.1. Choose the Correct Option:

i) What is the value in message type for a Mobile IP Registration Request?

(a) 1
(b) 2
(c) 3
(d) 4

ii) Which flag in the Registration Request message indicates that the Foreign Agent should decapsulate the packet?

(a) S
(b) D
(c) M
(d) B

iii) In the Registration Reply message, what does the Code value 0 indicate?

(a) Registration rejected
(b) Registration expired
(c) Registration accepted, but Simultaneous mobility bindings unsupported
(d) Administration prohibited

iv) What is the message type value for a Registration Reply?

(a) 1
(b) 2
(c) 3
(d) 4

v) The Lifetime field in the Registration Request message specifies how long the registration should be valid. (State True or False)

1.7 SUMMING UP

Mobile IP is a communication protocol that allows devices to maintain the same IP address while moving across different networks. This ensures uninterrupted communication and it solves the problem of changing IP addresses during network transitions. Mobile IP involves three key components: Mobile Node, Home Agent and Foreign Agent. The Mobile Node detects its current location using Agent Discovery message, and registers its current address with the Home Agent and communicates through tunneling mechanisms. This unit covers a thorough discussion on Mobile IP, its operation process and its details of various registration messages formats.

1.8 ANSWERS TO CHECK YOUR PROGRESS

Check Your Progress-1

1.(i) c (ii)d (iii) b (iv) a (v) d

Check Your Progress-2

1.(i) a (ii) b (iii) c (iv) c (v) True

1.9 POSSIBLE QUESTIONS

Short Answer Type Questions:

1. What is Mobile IP? What is the importance of Mobile IP?
2. State the key components of Mobile IP?
3. Define the Home Address in the context of Mobile IP Registration.
4. What is the purpose of the Identification field in a Registration Request message?
5. What are the various types of messages used in registration process?
6. What is the purpose of the Lifetime field in the Registration Request and Registration Reply messages? How does it impact the registration process?

Long Answer Type Questions:

1. Describe briefly the three categories of GSM services.
2. Explain how a mobile IP operates.
3. Explain the significance of the Flags field in the Mobile IP Registration Request message.
4. Describe the role of the Lifetime field in both Registration Request and Registration Reply messages. How does it affect the registration process?
5. Discuss the different Code values in the Registration Reply message and their implications for the mobile node.
6. Explain the importance of the Home Address and Care-of Address fields in Mobile IP registration.
7. What are extensions in the Registration Request message? Discuss their role and provide examples of extensions used in Mobile IP.

1.10 REFERENCES AND SUGGESTED READINGS

[1] Stallings, William. (2009). *Wireless Communications and Networks*. (2nd ed.). Prentice Hall. ISBN: 0-13-191835-4

[2] https://egyankosh.ac.in/bitstream/123456789/94403/1/Unit-6.pdf

[3] https://binaryterms.com/mobile-ip.html

[4] https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/mobile_ip/mobil_ip.html

[5] https://pdfcookie.com/documents/seminar-report-on-mobile-ip-4k2pkwy49dl9

***

UNIT- 2

WAP (WIRELESS APPLICATION PROTOCOL)

Unit Structure:

2.1 INTRODUCTION

The Wireless Application Protocol (WAP) is a universal open standard created by the WAP Forum to provide mobile users with access to telephony and information services, such as the Internet and the Web, through wireless devices like mobile phones, pagers, and personal digital assistants (PDAs). WAP is designed to be compatible with a range of wireless network technologies, including GSM, CDMA, and TDMA. It is built upon established Internet standards like IP, XML, HTML, and HTTP, while also incorporating security features. The WAP Forum was founded in 1997 by the initiatives taken by companies like Ericsson, Motorola, Nokia and Phone.com.

The use of mobile phones and terminals for data services is significantly affected by the limitations of both the devices and the networks that connect them. These devices typically have limited processing power, memory and battery life. Their user interfaces are also restricted, and the displays are small. Additionally, wireless networks usually have lower bandwidth, higher latency, and less stable connectivity than wired connections. These characteristics can vary widely between different terminal devices and networks. Furthermore, mobile wireless users often have different expectations and needs compared to users of traditional information systems. For example, mobile terminals must be extremely easy to use, even more so than workstations or personal computers. WAP is designed to address these challenges effectively.

The WAP specification consists of several different protocols and modules, whose relationship is depicted in Figure 2.1
The WAP (Wireless Application Protocol) specification includes:

1. A programming model based on the World Wide Web Programming Model.
2. A markup language called Wireless Markup Language, which adheres to XML standards.
3. Specifications for a small browser designed for use on mobile, wireless devices.
4. A lightweight communications protocol stack.
5. A framework for Wireless Telephony Applications (WTAs).

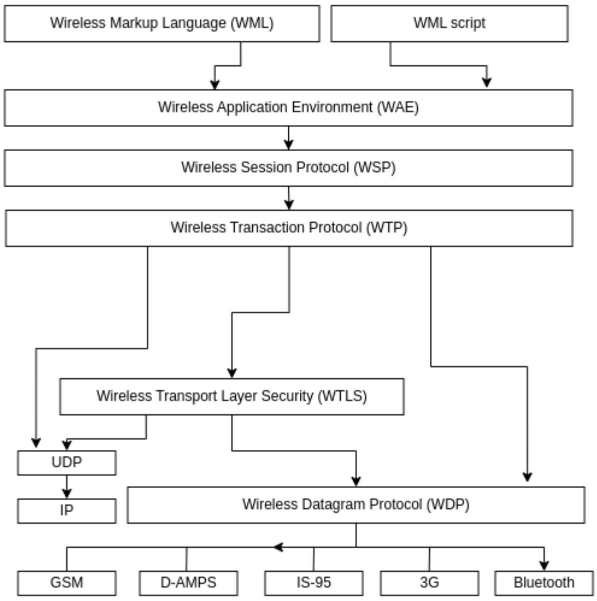

Wireless Markup Language (WML)
WML script
Wireless Application Environment (WAE)
Wireless Session Protocol (WSP)
Wireless Transaction Protocol (WTP)
Wireless Transport Layer Security (WTLS)
UDP
IP
Wireless Datagram Protocol (WDP)
GSM
D-AMPS
IS-95
3G
Bluetooth

Figure 2.1 WAP Protocol stack

2.2 OBJECTIVES:

After going through this unit learner will able to

- Understand the concept of the components and layers of the WAP architecture and its protocol stack.
- Learn the role of WML, WML Script, and WAE in delivering mobile web content and interactivity.
- Learn the concept of the development of simple mobile applications using WML and scripting with WML Script.
- Analyze the functions of WSP, WTP, WTLS, and WDP in enabling secure, reliable communication in mobile networks.
- Evaluate the limitations of mobile devices and wireless networks, and how WAP addresses these challenges.

2.3 WAP ARCHITECTURE:

The WAP Programming Model consists of three main components: the client, the gateway, and the original server as depicted in Figure 2.2. HTTP is used for content transfer between the gateway and the original server. The gateway acts as a proxy server within the wireless domain and performs several tasks to accommodate the limited capabilities of handheld wireless devices.

For example, the gateway provides DNS services and facilitates the conversion between the WAP protocol stack and the World Wide Web stack (including HTTP and TCP/IP). It also compresses web content to reduce the amount of data transmitted over wireless connections. The gateway then decodes this compressed information back into standard web formats. Additionally, it caches frequently requested content to enhance access speed.

Figure 2.3 shows the key components of a WAP environment. By using a WAP gateway, a mobile user can access web content hosted on a standard web server. The web server delivers content in HTML format, transmitted via the standard web protocol stack (HTTP/TCP/IP). This HTML content must pass through an HTML filter, which can either be integrated with the WAP proxy or be a separate module. The filter is responsible for converting HTML into WML (Wireless Markup Language). If the filter is separate, HTTP/TCP/IP is used to send the WML to the proxy.

Once the WAP proxy receives the WML, it converts the content into a more compact format called binary WML. The proxy then transmits the binary WML to the mobile user over a wireless network using the WAP protocol stack.

STOP TO CONSIDER

The separation of client, gateway, and server in the WAP model ensures optimized data processing and transmission. The gateway handles tasks like compression, protocol translation, and caching, reducing the burden on mobile devices and improving performance over low-bandwidth networks.

If the web server is capable of directly generating WML content, it sends the WML to the proxy over HTTP/TCP/IP, where it is converted to binary WML and transmitted to the mobile device using WAP protocols.

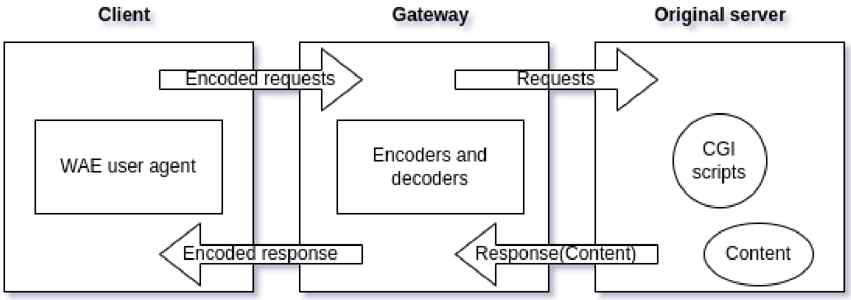


Figure 2.2 The WAP Programming Model

The WAP architecture is designed to overcome two primary challenges of wireless web access: the limitations of mobile devices, such as small screen sizes and restricted input capabilities, and the low data rates of wireless digital networks. Even with the introduction of 3G wireless networks offering higher data speeds, handheld mobile devices will continue to face constraints in terms of input and display capabilities. As a result, WAP or a similar technology will remain essential for the foreseeable future.

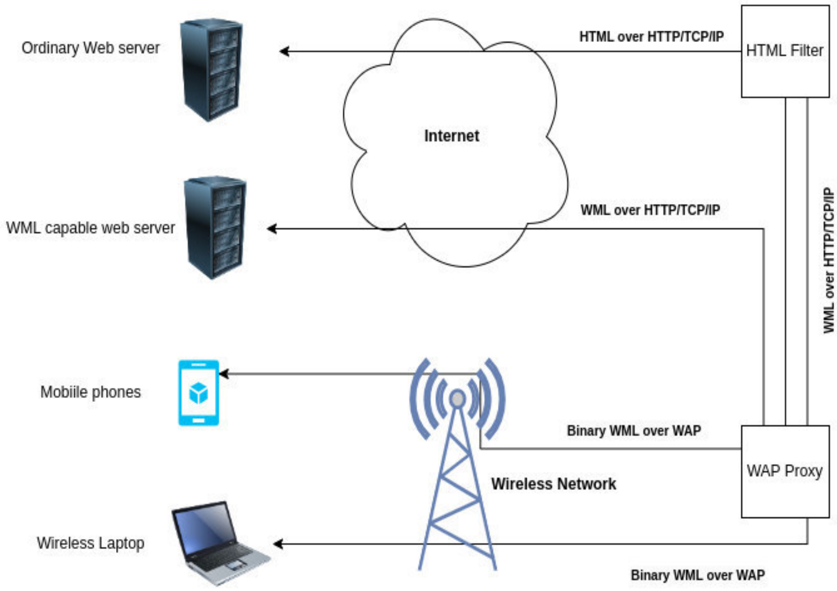


Figure 2.3 WAP Infrastructure

CHECK YOUR PROGRESS-I

1. True or False: The WAP gateway does not perform any data compression.
2. Fill in the Blank: The WAP gateway acts as a ___________ server within the wireless domain.
3. MCQ: What role does the WAP gateway play?
   a) It stores all mobile content
   b) It provides DNS services and protocol translation
   c) It directly interacts with end-users
   d) It replaces web servers

2.4 WIRELESS MARKUP LANGUAGE

WML (Wireless Markup Language) was created to define content and formatting for devices with limited bandwidth, small screen sizes, and restricted input capabilities. It is designed to work with telephone keypads, styluses, and other common input methods used in mobile and wireless communication. WML supports display scaling, making it adaptable to both the small two-line screens of basic devices and the larger screens of smartphones.

On a standard PC, a web browser renders content from web pages written in HTML (Hypertext Markup Language). To make an HTML page suitable for wireless devices, much of the content, particularly graphics and animations, must be stripped away. WML focuses primarily on presenting text-based information that retains the core message of the original web page while ensuring usability on mobile devices. Some important features of WML include:

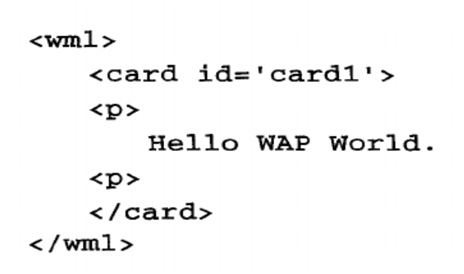
1. Text and Image Support: WML provides formatting and layout commands for both text and limited image capabilities.

2. Deck/Card Organizational Metaphor: WML documents are organized into small, distinct units of user interaction called cards. Users can navigate through these cards by moving back and forth. Each card defines one or more interaction elements, such as a menu, a text screen, or a text-entry field. A WML deck, similar to an HTML page, is identified by a web address (URL) and functions as the unit of content transmission.

3. Navigation Support among Cards and Decks: WML includes features for event handling, which facilitate navigation or the execution of scripts.

In an HTML-based web browser, users navigate by clicking on links. In contrast, a WML-capable mobile device allows users to interact with cards, enabling them to move forward and backward through the deck.

WML (Wireless Markup Language) is a tagged language that resembles HTML, where individual elements are defined by lowercase tags enclosed in angle brackets. Typically, a WML card starts with a non-visible section containing executable elements, followed by the content that is displayed. For example, consider the following:



```
<wml>
    <card id='card1'>
    <p>
        Hello WAP World.
    <p>
    </card>
</wml>
```

The tags `<wml>`, `<card>` and `<p>` are used to enclose the deck, card and paragraph respectively. Similar to HTML, most elements end with a closing tag, which is identical to the opening tag but includes a forward slash (`/`). When a wireless device receives this code, it will display the message "Hello WAP World" on the screen of the terminal.

Table 2.1 below lists the full set of WML tags, which are divided into eight functional groups.

Table 2.1 WML tags

Groups/Tag	**Description**
Deck Structure	
<access>	Access control
<card>	Card definition
<head>	Deck-level information (meta, access, template)
<meta>	Meta information
<template>	Deck-level event bindings
<wml>	Deck definition
Content	
<img>	Image
<p>	Paragraph, visible content
<table>	Table
<td>	Table data
<tr>	Table row
Formatting	
<b>	Bold
<big>	Large font
<br>	Line break

<em>	Emphasis
<i>	Italic
<small>	Small font
<strong>	Strong font
<u>	Underline

Groups/Tag	**Description**
Deck Structure	
<access>	Access control
<card>	Card definition
<head>	Deck-level information (meta, access, template)
<meta>	Meta information
<template>	Deck-level event bindings
<wml>	Deck definition
Content	
<img>	Image
<p>	Paragraph, visible content
<table>	Table
<td>	Table data
<tr>	Table row
Formatting	
<b>	Bold
<big>	Large font
<br>	Line break
<em>	Emphasis
<i>	Italic
<small>	Small font
<strong>	Strong font
<u>	Underline

Self Asking Questions

Q.1 How does the gateway simplify data access for mobile devices?

……………………………………………………………………………

Q.2 How does WML differ from HTML in handling content?

…………………………………………………………………………..

Check Your Progress-II

1. True or False: WMLScript cannot be compiled to bytecode.
2. Fill in the Blank: WMLScript is based on a subset of __________.
3. MCQ: What is the main function of WMLScript?
   a) Create graphics
   b) Validate input and handle logic
   c) Display videos
   d) Store large datasets

2.5 WML SCRIPT

WMLScript is a scripting language similar to JavaScript, designed for creating script-type programs on user devices with limited processing power and memory. Table 2.2 below shows valid WMLScript statements. Key capabilities of WMLScript include the following:

Table 2.2 WML Script statements

Statement	**Description**
=	Assignment
break	Terminate the current loop
continue	Current loop iteration
for	Indexed loop
function	Function declaration
if,else	Conditional test
return	Exit the current function
var	Variable declaration
while	Boolean-controlled loop

- Check the validity of user input before it is sent to the content server.
- Access device facilities and peripherals.
- Interact with the user without introducing round trips to the origin server(e.g., display an error message).

Key WMLScript features include the following:

- **JavaScript-based scripting language:** WMLScript is a subset of JavaScript, with some extensions.
- **Procedural logic:** WMLScript adds the power of procedural logic to the Wireless Application Environment (WAE), discussed subsequently.
- **Event based**: WMLScript may be invoked in response to certain user or environmental events.
- **Compiled implementation:** WMLScript can be compiled down to a more efficient byte code that is transported to the client.
- **Integrated into WAE:** WMLScript is fully integrated with the WML browser.

This allows authors to construct their service using both WML and WMLScript.

• **Efficient extensible library support:** WMLScript can be used to expose and

Extend device functionality without changes to the device software.

Stop to Consider

WMLScript's use of bytecode reduces the data size transmitted to devices, conserving bandwidth and processing power. Its integration with WML allows dynamic interaction without needing continuous communication with the server.

Check Your Progress-III

1. WMLScript is a full implementation of JavaScript. State whether the statement is true or false.
2. Which of the following is not a feature of WMLScript?
   a) Compiled to bytecode
   b) Client-side validation
   c) Complex animations
   d) Integrated with WML browser

2.6 WIRELESS APPLICATION ENVIRONMENT

The Wireless Application Environment (WAE) outlines an application framework designed for wireless devices, including mobile phones, pagers, and PDAs. Essentially, the WAE provides tools and formats that streamline the development of applications and devices compatible with the Wireless Application Protocol (WAP). The key components of the WAE model include the following (Figure 2.4):

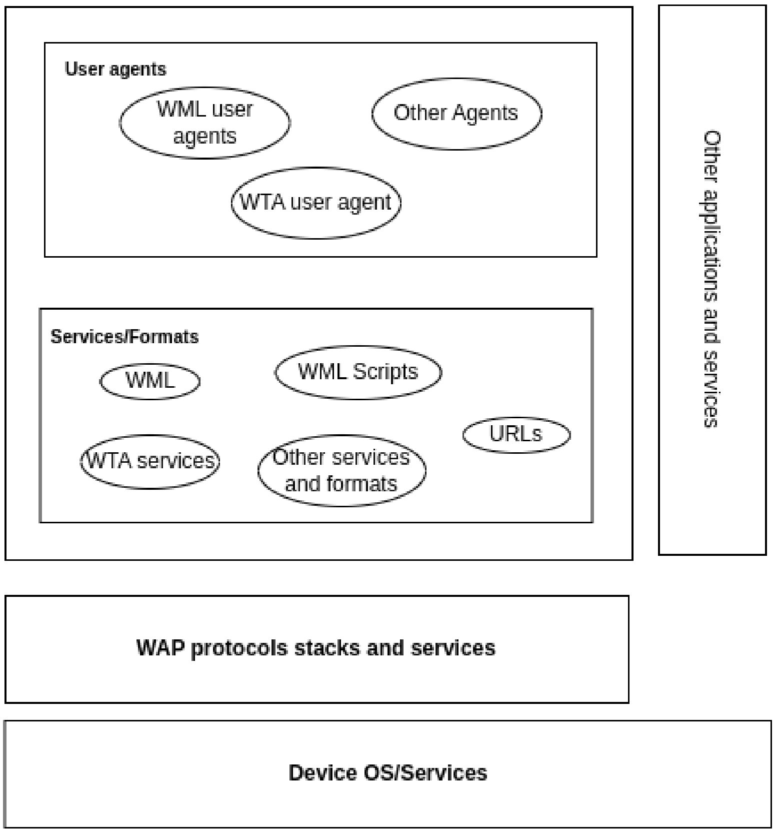


Figure 2.4 WAE Client Components

- **WAE user agents** are software applications that run on a user's wireless device and provide specific functionalities, such as displaying content to the end user.
- **Content generators** are applications or services located on origin servers (for example, CGI scripts) that produce standard content formats in response to requests made by user agents on mobile

devices. WAE does not define any specific content generators but anticipates that a variety of them will be available, operating on typical HTTP origin servers that are commonly used on the World Wide Web today.

- **Standard Content Encoding**: This is designed to enable a Wireless Application Environment (WAE) user agent, such as a web browser, to easily navigate web content.
- **Wireless Telephony Applications (WTA):** This is a set of telephony-specific extensions that offer advanced control mechanisms for calls and features, allowing authors to access mobile network services. With WTA, application developers can utilize the micro browser to initiate telephone calls and respond to events from the telephone network.

2.7 WIRELESS SESSION PROTOCOL

The Wireless Session Protocol (WSP) provides applications with an interface for two types of session services. The connection-oriented session service operates above the reliable transport protocol (WTP), while the connectionless session service works above the unreliable transport protocol (WDP). WSP is built on HTTP, with several modifications and enhancements designed to optimize its performance over wireless channels.

WSP addresses key challenges such as low data rates and the potential for connection loss due to poor coverage or network congestion. It follows a transaction-oriented, request-and-reply model. Each WSP Protocol Data Unit (PDU) includes a body that may contain Wireless Markup Language (WML), WMLScript, or images, along with a header that provides information about the data and the transaction itself.

Additionally, WSP defines a server push operation that allows the server to send unsolicited content to a client device. This feature can be utilized for broadcasting messages or providing tailored services, such as news headlines or stock quotes customized for each client.

In general, a connection-mode WSP offers the following services:

1. Establishes a reliable session from the client to the server and releases that session in an orderly manner.
2. Agrees on a common level of protocol functionality through capability negotiation.
3. Exchanges content between the client and server using compact encoding.
4. Suspends and resumes a session.

Pushes content from the server to the client in an unsynchronized manner.

At the service level, WSP is defined as a set of service primitives, each with corresponding parameters. These service primitives form the interface between WSP and its users within the Wireless Application Environment (WAE). At the protocol level, the WSP specification details the format of the Protocol Data Unit (PDU) used for data exchange between peer WSP entities.

Self Asking Questions

1. How does WAE support application flexibility?
   ……………………………………………………………
   ……………………………………………………………
   ……………………………………………………………
2. What problem does WSP solve in mobile communication?
   ……………………………………………………………
   ……………………………………………………………
   ……………………………………………………………

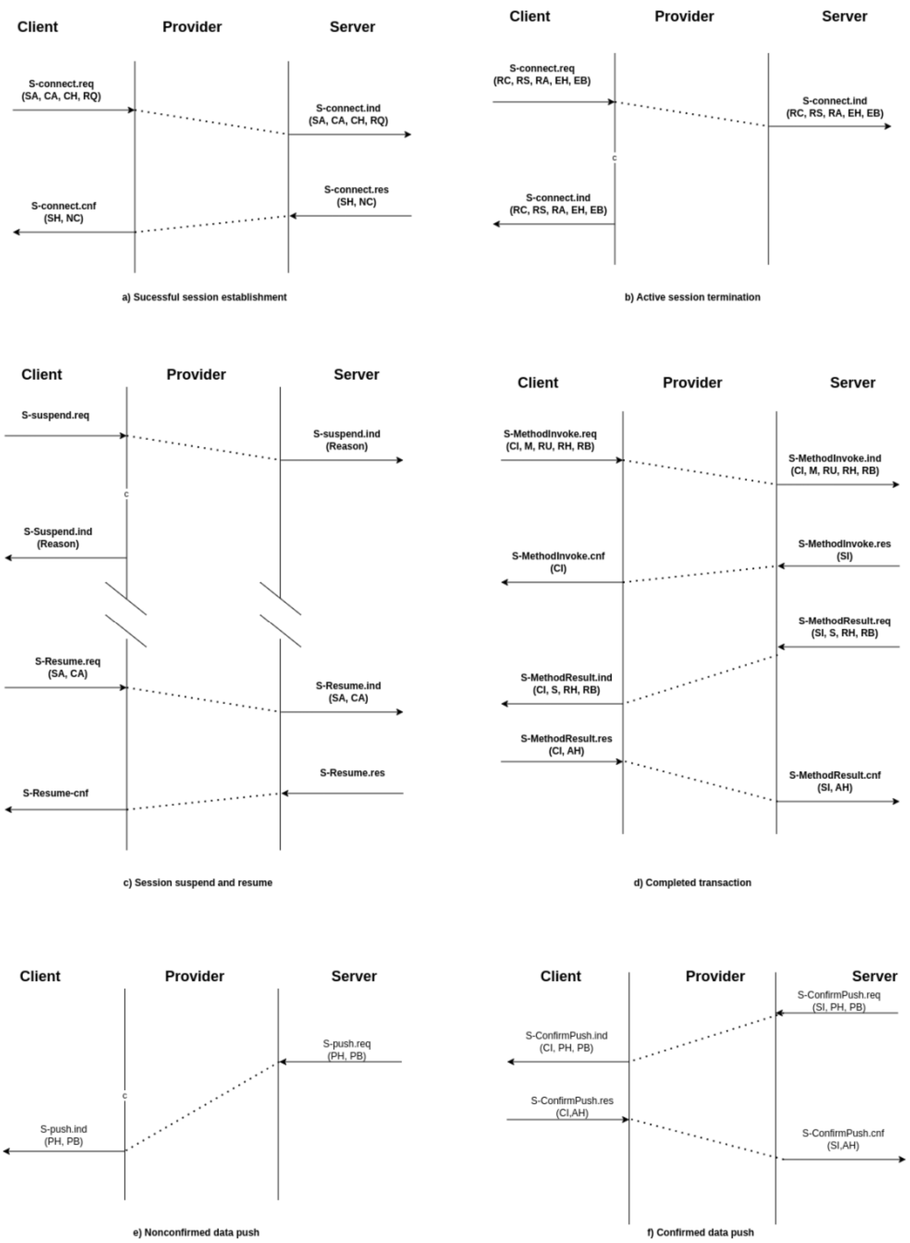


Figure 2.5 Wireless Session Protocol Primitives and Parameters

The figure 2.5 above illustrates the key WSP transaction types, highlighting the primitives and parameters exchanged. While there are additional transaction types, these are enough to provide a general understanding of how WSP operates. Session establishment involves the exchange of S-Connect primitives (Figure 2.5 a). In this process, a WSP user acting as a client (on the mobile node side) requests a session with a WSP user acting as a server (the Web Server) on a remote system by sending an S-Connect.req to WSP. The request includes four parameters:

- **Server address:** The peer with which the session will be established.
- **Client address:** The originator of the session.
- **Client headers:** Contain attribute information that can be used for application-level parameters to communicate with the peer. This information is passed by WSP without modification and is not processed by WSP.
- **Requested capabilities:** A set of capabilities requested by the client for this session, as outlined in Table 2.3.

STOP TO CONSIDER

Session suspension and resumption in WSP are essential for maintaining application continuity in environments where network connectivity is unstable. This feature enhances user experience by preserving state across temporary disconnections.

The client's Wireless Session Protocol (WSP) prepares a WSP Protocol Data Unit (PDU) containing the necessary parameters to send a request to the peer WSP on the server. The server address, client address, and client headers remain unchanged. However, either the WSP service provider on the client side, the WSP service provider on the server side, or both may modify the requested capabilities to ensure they do not exceed the functionality the provider can support.

Table 2.3 Wireless Session Protocol Capabilities

Name	Class	Type	Description
Aliases	I	List of addresses	Indicates which alternative addresses the peer may use to access this session service user. Can be used to facilitate a switch to a news bearer when a session is resumed.
Client SDU size	N	Positive integer	The size of the largest transaction service data unit that may be sent to the client during the session.
Extended methods	N	Set of method names	The set of extended methods that are supported by both client server peers.
Header code pages	N	Set of code page names	The set of extension header code pages that are supported by both client and server peers.
Maximum outstanding method requests	N	Positive integer	The maximum number of method invocations that can be active at the same time during the session.
Maximum outstanding push requests	N	Positive integer	The maximum number of confirmed Push the invocations that can be active at the same time during the session.
Protocol options	N	Set of facilities and features	Includes Push, Confirmed Push, Session Resume, and Acknowledgment Headers.
Server SDU size	N	Positive integer	The size of the largest transaction SDU that may be sent to the server during the session.

After any modifications, an S-Connect.ind message—containing the same parameters as the original request—is sent to the WSP user on the server side. If the WSP user at the server accepts the session request, they respond by invoking WSP with an S-Connect.rsp message. This message includes server headers and any negotiated capabilities. The negotiated capabilities parameter is optional; if it is not included, the server agrees to the set of capabilities proposed in the S-Connect.ind message. If included, it specifies the level of functionality the server is willing to accept.

Finally, an S-Connect.ind message is sent back to the original requester, which contains the server headers and the final set of negotiated capabilities. To terminate the session, the S-Disconnect primitive is used. If the client WSP user initiates the termination, the request primitive includes the following parameters:

- **Reason code**: Indicates the cause of disconnection. If the disconnection is due to the client being redirected to a new server address, the following two parameters must also be included.
- **Redirect security**: Specifies whether the client can reuse the current secure session during the redirection.
- **Redirect addresses**: Lists alternate addresses to be used for establishing a new session.
- **Error headers and error body**: If the termination is due to an error, these parameters may be included to provide the server WSP user with information about the error.

WSP acknowledges receipt of a request by sending an S-Disconnect.ind message to both the client WSP user and the server WSP user. The WAP Session Protocol (WSP) supports session suspension and resumption, a feature particularly useful when the client anticipates being temporarily unavailable, such as during roaming or when the client device disconnects and reconnects to the network.

When a session is suspended, the session state is saved on both the client and server sides, though any in-transit data is lost. To request a suspension, the only required parameter is a reason code included in the S-Suspend.ind primitive. In contrast, when issuing a resume request, both the server address and the client address must be included in the request and indication primitives.

A transaction involves the exchange of data between a client and a server using the S-Method Invoke and S-Method Result primitives. The S-Method Invoke primitive is used to request the server to execute a specific operation. This request includes the following parameters:

- Client Transaction ID: Used to distinguish between pending transactions.
- Method: Identifies the operation being requested.
- Request URI (Uniform Resource Identifier): Specifies the entity to which the operation should be applied.
- Request headers and body: Contain attribute information and data associated with the request.

The indication sent to the server includes the same parameters, except that the client Transaction ID is replaced by a server Transaction ID. The response and confirm primitives are used to verify that the request has been delivered, and they include transaction IDs.

The S-Method Result is used to provide a response to an operation request from the server. It includes the server Transaction ID, the status of the response, and response headers and body containing related attribute information and data. The response and confirm primitives are again used to confirm the delivery of the request, including transaction IDs. Additionally, these primitives may contain acknowledgment headers that provide feedback to the server.

The non-confirmed data push method is used to send unsolicited information from the server to the client. The only parameters associated with these primitives are push headers and a push body, which contain attributes and the information being communicated. In contrast, with a confirmed data push, the server receives confirmation that the push data has successfully reached the client. Along with push headers and a push body, confirmed data push primitives include a push ID. The response and confirm primitives may also contain acknowledgment headers.

The connectionless session service provides a non-confirmed capability for exchanging content entities between WSP users. In this context, only method invocation and push facilities are available.

WSP conveys service requests and responses in WSP PDUs, which are passed down to the transport layer to be included as the body of a transport-level PDU. At the highest level, the WSP PDU consists of three fields.

Check Your Progress-IV

1. True or False: WSP is based entirely on FTP.
2. Fill in the Blank: WSP supports both __________ and connectionless session services.
3. MCQ: What feature does WSP provide to support temporary disconnections?
   a) Session lock
   b) Session suspend/resume
   c) Constant reconnect
   d) Session duplication

2.8 WIRELESS TRANSACTION PROTOCOL

WTP (Wireless Transport Protocol) manages transactions by facilitating communication between a user agent, such as a WAP browser, and an application server. This communication supports activities like web browsing and e-commerce transactions. WTP offers a reliable transport service but minimizes the overhead associated with TCP, making it a lightweight protocol. This makes it ideal for implementation in "thin" clients, such as mobile devices, and for use over low-bandwidth wireless connections. The features of WTP include:

Three classes of transaction service.

- **Optional user-to-user reliability**: The WTP user triggers the confirmation for each received message.

- **Optional out-of-band data on acknowledgments**: Allows additional data to be included with acknowledgment messages.
- **PDU concatenation and delayed acknowledgment**: Reduces the number of messages sent by combining multiple PDUs and delaying acknowledgments.
- **Asynchronous transactions**: Supports transactions that do not require immediate response or synchronization between the client and server.

WTP is transaction oriented rather than connection oriented. With WTp, there is no explicit connection setup or teardown but rather a reliable connectionless service.WTP Transaction Classes WTP provides three transaction classes that may be invoked by WSP or another higher layer protocol:

- **Class 0**: Unreliable invoke message with no result message
- **Class 1:** Reliable invoke message with no result message
- **Class 2:** Unreliable invoke message with one reliable result message

Class 0 provides an unreliable datagram service, ideal for unreliable push operations. In this class, data from a WTP user is encapsulated by the WTP (the initiator or client) in an Invoke PDU and transmitted to the target WTP (the responder or server) without any acknowledgment. The responder WTP then delivers the data to the target WTP user.

Class 1 offers a reliable datagram service, suitable for reliable push operations. Here, data from the initiator is encapsulated in an Invoke PDU and sent to the responder. The responder delivers the data to the target WTP user and acknowledges receipt by sending an ACK PDU back to the WTP entity on the initiator side. This ACK confirms the transaction to the source WTP user. Additionally, the responder WTP retains state information for a certain period after sending the ACK, allowing for retransmissions if the ACK is lost or if the initiator retransmits the Invoke PDU.

Class 2 provides a request/response transaction service and supports multiple transactions within a single WSP session. In this case, data from the initiator is encapsulated in an Invoke PDU and sent to the responder, which passes the data to the target WTP user. The target WTP user then prepares the response data, which is sent back to the local WTP entity. The responder WTP sends these data back in a Result PDU. If there is a delay in generating the response data that exceeds a specified timer threshold, the responder may send an ACK PDU before transmitting the Result PDU. This prevents the initiator from unnecessarily retransmitting the Invoke message.

WTP (Wireless Transaction Protocol) utilizes six types of Protocol Data Units (PDUs). Each PDU begins with a fixed header, as illustrated in Figure 2.6, and may be followed by a variable header that contains additional control information. This supplementary information is presented as one or more Transaction Protocol Items (TPIs).

The Invoke PDU is specifically designed to transmit a request from an initiator to a responder. It is four bytes long and includes the following fixed header fields:

Continue Flag: When set, this flag indicates that there are one or more TPIs following the fixed header. Each TPI also begins with a continue flag bit to specify whether additional TPIs will follow or if this is the last one.

PDU Type: This field indicates that the PDU is an Invoke PDU.

Group Trailer Flag: Used when segmentation and reassembly are involved, as explained later.

Transmission Trailer Flag: Similar to the Group Trailer Flag, this is also used in segmentation and reassembly.

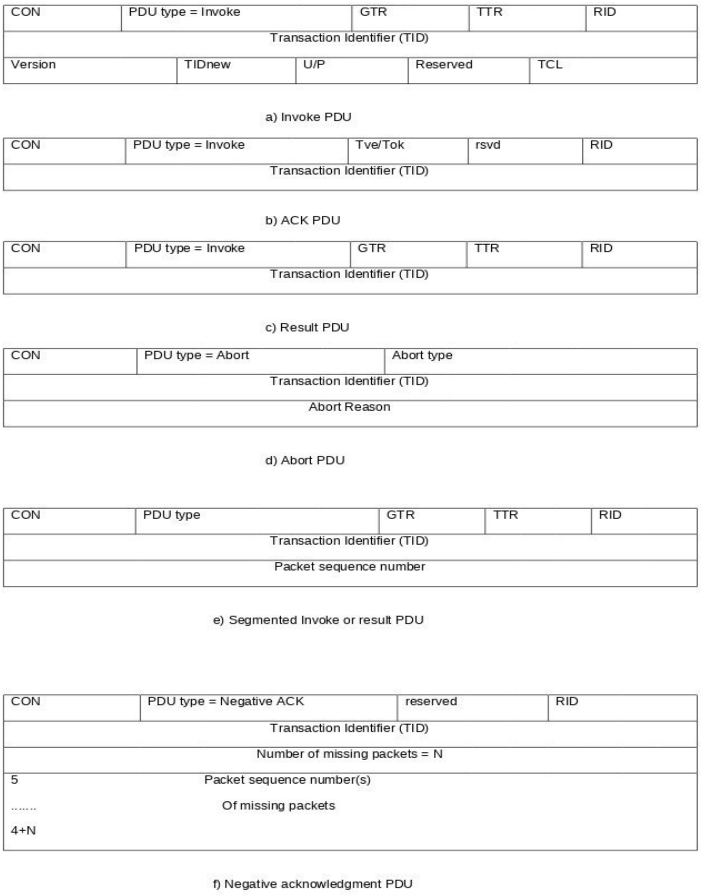
Retransmission Indicator: Specifies whether the current transmission is a retransmission. If the initiator does not receive an acknowledgment within a specified time, it will resend the Invoke PDU.

Transaction Identifier: Used to associate the PDU with a specific transaction.

Version: Specifies the version of WTP being used.

TID New Flag: Set when the initiator has "wrapped" the Transaction ID (TID) value, meaning the next TID will be lower than the previous one.

U/P Flag: When set, it indicates that the initiator requires a user acknowledgment from the server WTP user. In this case, the WTP user must confirm every received message. If the flag is clear, the responding WTP entity can acknowledge an incoming PDU without needing confirmation from its user.



CON	PDU type = Invoke	GTR	TTR	RID
Transaction Identifier (TID)				
Version	TIDnew	U/P	Reserved	TCL

a) Invoke PDU

CON	PDU type = Invoke	Tve/Tok	rsvd	RID
Transaction Identifier (TID)				

b) ACK PDU

CON	PDU type = Invoke	GTR	TTR	RID
Transaction Identifier (TID)				

c) Result PDU

CON	PDU type = Abort	Abort type
Transaction Identifier (TID)		
Abort Reason		

d) Abort PDU

CON	PDU type	GTR	TTR	RID
Transaction Identifier (TID)				
Packet sequence number				

e) Segmented Invoke or result PDU

CON	PDU type = Negative ACK	reserved	RID
Transaction Identifier (TID)			
Number of missing packets = N			
5 .... 4+N	Packet sequence number(s) Of missing packets		

f) Negative acknowledgment PDU

Figure 2.6 WTP PDU Fixed Header Formats

Here,

CON =continue flag TIDnew = TIDnew flag

GTR = group trailer U/P = user/provider acknowledgment flag

TTR = transmission trailer TCL = transaction class

RID = retransaction indicator Tve/Tok = TID verify/TID OK flag

Transaction Class: This field specifies the desired transaction class for processing the Invoke PDU.

If the message from WTP (i.e., the data block from WSP) exceeds the capacity of the current bearer, WTP may segment the message and send it across multiple packets, with each packet contained in a separate Invoke PDU. When a message is divided into smaller packets, these packets can be transmitted and acknowledged in groups. Table 2.4 illustrates how the Group Trailer (GTR) and Transmission Trailer (TTR) flags are used to manage this process.

Table 2.4 Group Trailer (GTR) and Transmission Trailer (TTR) Combinations

GTR	**TTR**	**Description**
0	0	Not last packet
0	1	Last packet message
1	0	Last packet of packet group
1	1	Segmentation and reassembly not supported

The ACK PDU is a three-byte unit used to acknowledge either an Invoke or Result PDU. It contains a Tverrok flag, which has different meanings depending on the direction of the communication. When this PDU is sent from the responder to the initiator, it is known as the Tve flag. If the Tve flag is set, it indicates, "Do you have an outstanding transaction with this Transaction ID (TID)?" Conversely, when the PDU is sent in the opposite direction, if the Tok flag is set, it signifies, "I have an outstanding transaction with this TID."

The Result PDU is also three bytes long and conveys the server's response to the client.

The Abort PDU is used to terminate a transaction and has two defined types: user abort and provider abort.

- If the abort is initiated by the WTP user (e.g., WSP), the user's reason for the abort is included in the body of the PDU and sent to the intended WTP user at the destination.
- If the abort is initiated by the WTP provider (the entity sending the Abort PDU), the reason for the abort in the PDU can indicate one of the following issues:
- Unknown: An unexplained error occurred.
- Protocol error: The received PDU could not be interpreted correctly.
- Invalid TID: Indicates a negative result during Transaction ID (TID) verification by the initiator.

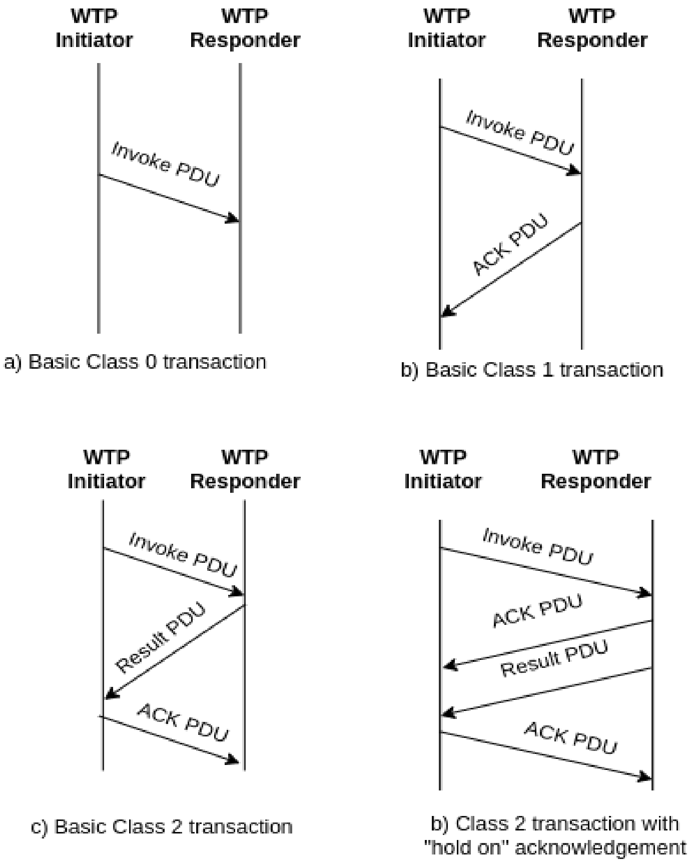
- Not implemented Class 2: The responder does not support Class 2, as requested.
- Not implemented SAR: The responder does not support segmentation and reassembly (SAR).
- Not implemented user acknowledgment: The responder does not support user acknowledgment.
- WTP version 1: The initiator requested a WTP version that is not supported; the current version is 1.
- Capacity temporarily exceeded: The transaction cannot be completed due to an overload situation.

The WTP (Wireless Transaction Protocol) service is defined by three main primitives:

1. TR-Invoke: This primitive is used to initiate a new transaction.
2. TR-Result: This primitive is used to send back the result of a transaction that was previously initiated.
3. TR-Abort: This primitive is used to terminate an existing transaction.

Figure 2.8 illustrates the relationship between these primitives and a Class 2 transaction that uses "hold on" acknowledgment. For comparison, refer to Figure 2.7d.

Additionally, Figure 2.8 demonstrates how the WTP service supports the WSP (Wireless Session Protocol) service. The sequence of WSP service primitives facilitates a completed transaction and is identical to the sequence depicted in Figure 2.5 d.



a) Basic Class 0 transaction

b) Basic Class 1 transaction

c) Basic Class 2 transaction

b) Class 2 transaction with "hold on" acknowledgement

Figure 2.7 Examples of WTP Operation

Wireless Transport Layer Security:

WTLS (Wireless Transport Layer Security) provides security services between mobile devices (clients) and WAP (Wireless Application Protocol) gateways. It is based on the industry-standard

Transport Layer Security (TLS) protocol, which evolved from the secure sockets layer (SSL). TLS is the standard protocol for securing communication between web browsers and web servers.

WTLS is more efficient than TLS because it requires fewer message exchanges. To ensure end-to-end security, WTLS is implemented between the client and the gateway, while TLS is used between the gateway and the target server. The WAP systems manage the conversion between WTLS and TLS within the gateway, which serves as a potential point of vulnerability. Consequently, the gateway must be thoroughly secured against external threats.

WTLS provides the following features:

Data integrity: Ensures that data sent between the client and the gateway remains unaltered, using message authentication.

Privacy: Protects the confidentiality of the data, ensuring it cannot be read by unauthorized third parties, through encryption.

Authentication: Verifies the identity of both parties, using digital certificates.

Denial-of-service protection: Detects and rejects messages that are either replayed or fail verification.

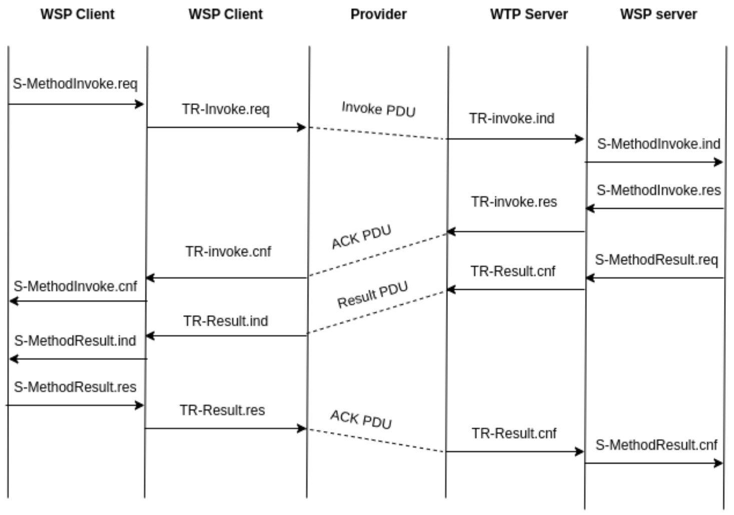


Figure 2.8 WSP-WTP Timing Diagram

WTLS is not a single protocol but rather a combination of two layers of protocols, as shown in Figure 2.9. The WTLS Record Protocol delivers basic security services to various higher-layer protocols. Specifically, the Hypertext Transfer Protocol (HTTP), as defined in RFC 2068, which facilitates Web client/server interaction, can operate on top of WTLS. Three higher-layer protocols are defined within WTLS: the Handshake Protocol, the Change Cipher Spec Protocol, and the Alert Protocol.

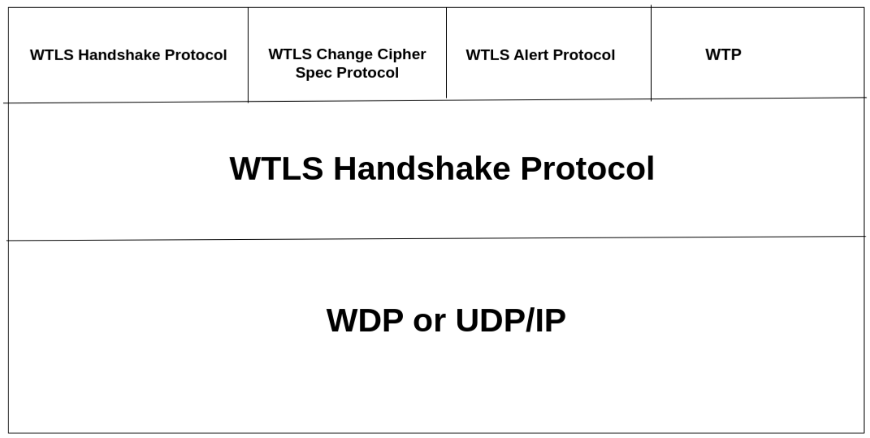


Figure 2.9 WTLS Protocol Stack

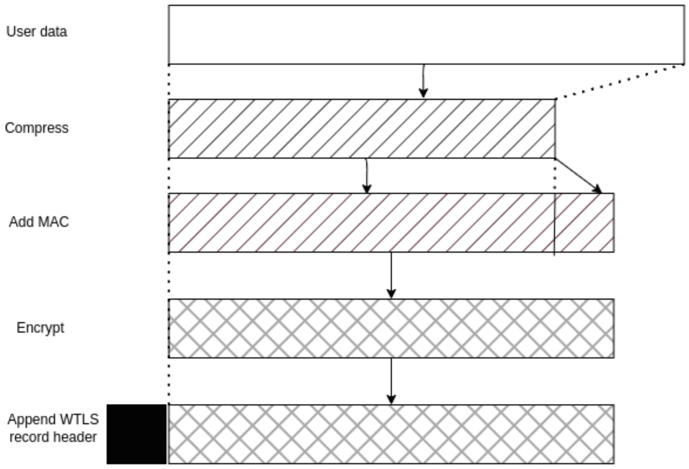


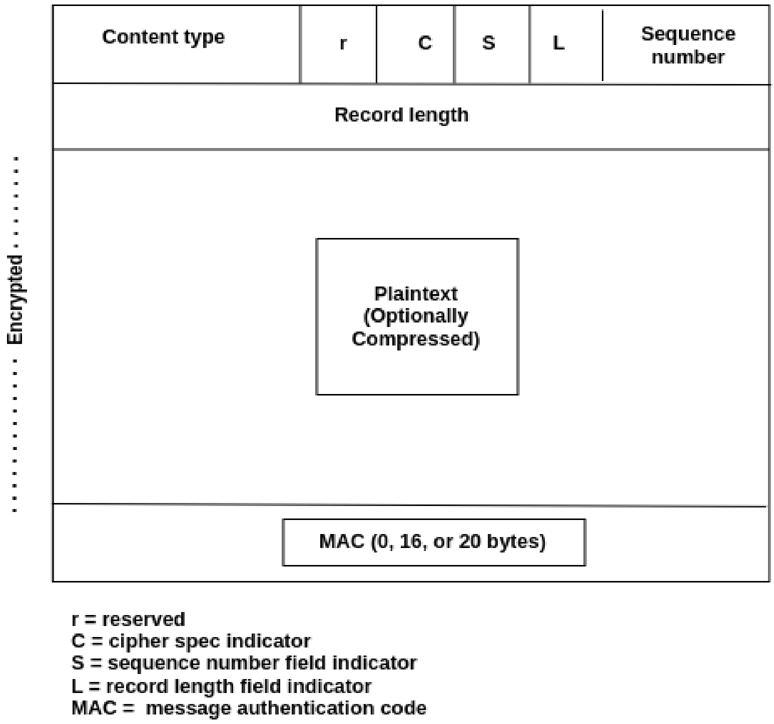
Figure 2.10 WTLS Record Protocol Operation

WTLS Record Protocol: The WTLS Record Protocol takes user data from the next higher layer (such as WTP, WTLS handshake protocol, WTLS alert protocol, or WTLS change cipher spec protocol) and encapsulates this data into a PDU. The following steps occur as depicted in the Figure 2.10 above.

1. The payload is compressed using a lossless compression algorithm.
2. A message authentication code (MAC) is computed over the compressed data using HMAC. HMAC is a keyed hash code, similar to but more complex than the one described in Appendix 12B. Several hash algorithms can be used with HMAC, including MD-5 and SHA-1. The hash code length can be 0, 5, or 10 bytes. The MAC is added after the compressed data.
3. The compressed message along with the MAC code is encrypted using a symmetric encryption algorithm. The allowable encryption algorithms include DES, triple DES, RC5, and IDEA.
4. The Record Protocol prepends a header to the encrypted payload.

The Record Protocol header consists of the following fields as shown in Figure 2.11.

- **Content Type (8 bits):** Indicates the higher-layer protocol above the WTLS Record Protocol.
- **Cipher Spec Indicator (1 bit):** If this bit is zero, it indicates that no compression, MAC protection, or encryption is used.
- **Sequence Number Field Indicator (1 bit):** Indicates whether a sequence number field is present.
- **Record Length Field Indicator (1 bit):** Indicates whether a record length field is present.
- **Sequence Number (16 bits):** A sequence number associated with this PDU, providing reliability over an unreliable transport service.
- **Record Length (32 bits):** The length in bytes of the plaintext data (or compressed data if compression is used).



Content type
r
C
S
L
Sequence number
Record length
Plaintext (Optionally Compressed)
MAC (0, 16, or 20 bytes)
Encrypted
r = reserved
C = cipher spec indicator
S = sequence number field indicator
L = record length field indicator
MAC = message authentication code

Figure 2.11 WTLS Record Format

The Change Cipher Spec Protocol is associated with the current transaction and defines the encryption algorithm, hash algorithm for HMAC, and various cryptographic attributes such as the MAC code size. Each session has two states: the current operating state for both reading (receiving) and writing (sending). During the Handshake Protocol, there are also pending read and write states that are created.

The Change Cipher Spec Protocol is one of the three WTLS-specific protocols that use the WTLS Record Protocol, and it is the simplest of them. This protocol consists of a single message, which is just one byte with the value of 1. The main purpose of this message is to transfer the pending state to the current state, thus updating the cipher suite that will be used for this connection.

Self Asking Question

Q.1: Why is the gateway a critical point in WTLS?

…………………………………………………………………………...

…………………………………………………………………………...

The Alert Protocol is used to communicate WTLS-related alerts to a peer entity. Like other WTLS applications, alert messages are compressed and encrypted according to the current state. Each message in this protocol consists of two bytes. The first byte represents the severity level of the message, which can be one of the following: warning (1), critical (2), or fatal (3). If the severity level is fatal, WTLS will immediately terminate the connection. Although other connections within the same session may continue, no new connections can be established for that session. The second byte contains a code indicating the specific alert. Examples of fatal alerts include:

- **unexpected_message:** An inappropriate message was received.
- **bad_record_mac**: An incorrect MAC was received.
- **decompression_failure**: The decompression function received improper input (e.g., unable to decompress or decompress to greater than the maximum allowable length).
- **handshake_failure**: The sender was unable to negotiate an acceptable set of security parameters given the options available.
- **illegal_parameter**: A field in a handshake message was out of range or inconsistent with other fields.

Examples of nonfatal alerts include:

- **bad_certificate:** A received certificate was corrupt (e.g., contained a signature that did not verify).
- **unsupported_certificate:** The type of the received certificate is not supported.
- **certificate_revoked:** A certificate has been revoked by its signer.
- **certificate_expired:** A certificate has expired.
- **certificate_unknown:** Some other unspecified issue arose in processing the certificate, rendering it unacceptable.

The Handshake Protocol is the most complex part of WTLS. It enables the server and client to authenticate each other and negotiate encryption and MAC algorithms as well as cryptographic keys used to protect data sent in a WTLS record. The Handshake Protocol is used before any application data are transmitted.

Stop to Consider

WTLS provides end-to-gateway encryption, ensuring secure communication over the wireless link. While this protects data in transit between the client and gateway, the gateway itself must be highly secure to prevent vulnerabilities during protocol handover.

The Handshake Protocol consists of a series of messages exchanged between the client and the server shown in figure 2.12. The initial exchange needed to establish a logical connection between client and server can be viewed in four phases:

The first phase establishes a logical connection and determines the security capabilities associated with it. It starts with the client sending a "client_hello" message, which includes a session ID and a list of supported cryptographic and compression algorithms, ordered by preference. After sending this message, the client waits for the "server_hello" message, which indicates which cryptographic and compression algorithms will be used for the exchange.

The second phase focuses on server authentication and key exchange. The server begins by sending its public key certificate for authentication, if required. Following this, the server may send a `server_key_exchange` message if necessary. This message is vital for certain public key algorithms used for symmetric key exchange. The server can then request a public key certificate from the client by sending a `certificate_request` message. The final message in this phase is the `server_hello_done` message, signaling the conclusion of the server hello and its associated messages. The server waits for a response from the client after sending this message, and no parameters are included.

The third phase centers on client authentication and key exchange. Upon receiving the `server_hello_done` message, the client verifies that the server has provided a valid certificate (if required) and checks that the server hello parameters are acceptable. If everything is satisfactory, the client sends one or more messages back to the server. If the server has requested a certificate, the client sends a certificate message. The next step is the `client_key_exchange` message, which is mandatory. The content of this message depends on the type of key exchange being used. Finally, the client may also send a `certificate_verify` message to explicitly verify the client certificate.

The fourth phase finalizes the establishment of a secure connection. The client sends a `change_cipher_spec` message, updating the current CipherSpec with the pending one. This message is transmitted using the Change Cipher Spec Protocol, not the Handshake Protocol. The client then immediately sends a `finished` message using the new algorithms, keys, and secrets. This message confirms that the key exchange and authentication processes were successful.

In response, the server sends its own `change_cipher_spec` message, updates the current CipherSpec with the pending one, and then sends its own `finished` message. At this point, the handshake is complete, and both the client and server can begin exchanging application layer data.

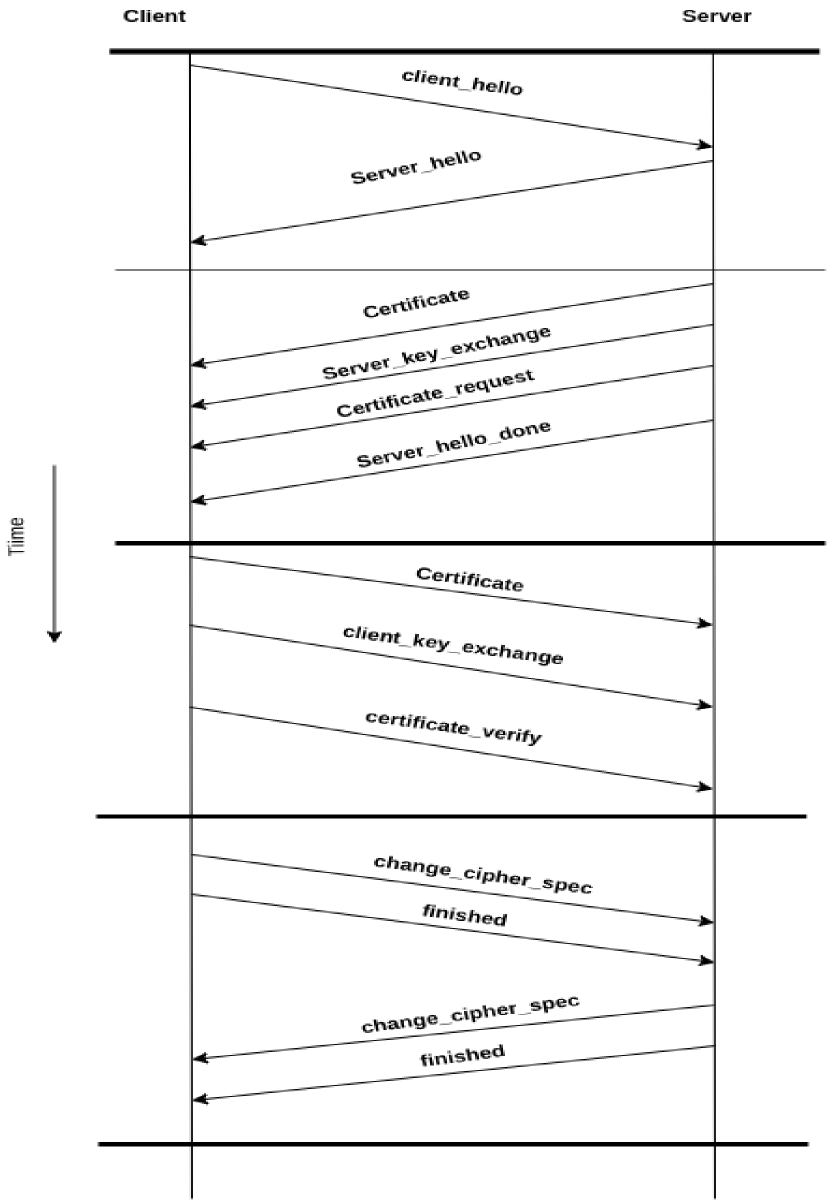


Figure 2.12 WTLS Handshake Protocol Action

Check Your Progress-V

1. True or False: WTLS is less efficient than TLS.
2. Fill in the Blank: WTLS is implemented between the client and the __________.
3. MCQ: Which WTLS protocol is used to update encryption settings?
   a) Alert
   b) Record
   c) Change Cipher Spec
   d) Handshake

2.9 WIRELESS DATAGRAM PROTOCOL

WDP (Wireless Datagram Protocol) is designed to adapt a higher-layer WAP (Wireless Application Protocol) to the communication mechanism, or bearer, used between the mobile node and the WAP gateway. This adaptation may include segmenting data into appropriately sized pieces for the bearer and managing the interaction with the bearer network. WDP hides the complexities of different bearer networks from the other layers of WAP. In certain scenarios, WAP is implemented over IP (Internet Protocol).The WDP service is defined by two service primitives: T-D Unit-data primitive and T-Derror.ind primitive.

The T-DUnit-data primitive provides a non confirmed service with the following parameters:

- **Source address**: Address of the device making a request to the WDP layer
- **Source port**: Application address associated with the source address
- **Destination address:** Destination address for the data submitted to WDP

• **Destination port:** Application address associated with the destination address

• **User data:** User data from the next higher layer, submitted to WDP for transmission to the destination port

The T-Derror.ind primitive is designed to notify a WDP user when there is a failure in delivering a WDP datagram. Along with the source address, source port, destination address, and destination port parameters, the T-Derror.ind also includes an error code parameter that holds local significance.

The following fields are necessary in a WDP PDU:

- Destination Port
- Source Port

If the underlying bearer does not provide segmentation and reassembly, this feature is implemented in the Wireless Datagram Protocol (WDP) in a way that is independent of the bearer.

For instance, GSM (Global System for Mobile Communications) specifies a format for a user data header. This header consists of a sequence of information elements, with each element defined by an identifier, a length, and one or more bytes of value. The structure of the WDP Protocol Data Unit (PDU) for GSM is as follows:

- **Header length (1 byte)**: Length of header.
- **Port numbers identifier (1 byte):** The value 5 indicates that this information element consists of two port numbers.
- **Port numbers length (1 byte):** The value 4 indicates that the value portion of this information element is 4 bytes long.
- **Destination port (2 bytes)**
- **Source port (2 bytes)**
- **SAR identifier (1 byte):** The value 0 indicates that this information element consists of information for segmentation and reassembly.
- **SAR length (1 byte):** The value 3 indicates that the value portion of this information element is 3 bytes long.

- **Datagram reference number (1 bytes):** An identifier assigned to all of the segments that make up a block of user data.
- **Number of segments (1 byte):** The total number of segments that need to be reassembled.
- **Segment count:** A sequence number that identifies this segment within the sequence of all segments that need to be reassembled to form the block of user data.
- **User data (1 to n bytes)**

The Wireless Control Message Protocol (WCMP) serves a function similar to that of the Internet Control Message Protocol (ICMP) for the Wireless Datagram Protocol (WDP). WCMP is utilized in environments that do not have an IP bearer, making the use of ICMP impractical. It is employed by wireless nodes and Wireless Application Protocol (WAP) gateways to report errors encountered when processing WDP datagrams. Additionally, WCMP can be used for informational and diagnostic purposes.

Table 2.5 details the various WCMP messages along with their corresponding error codes.

WCMP Message	WCMP Type	WCMP Code	WCMP Node	WAP Gateway
Destination Unreachable	51			
No route to destination		0	N/A	O
Communication administratively prohibited		1	N/A	O
Address unreachable		3	N/A	O
Port unreachable		4	M	N/A
Parameter Problem	54			
Erroneous header field		0	O	O
Message Too Big	60	0	M	N/A
Reassembly Failure	61			
Reassembly time exceeded		1	O	N/A
Buffer overflow		2	O	N/A
Echo Request	178	0	O	N/A
Echo Reply	179	0	M	N/A

M = mandatory
O = optional
N/A = not applicable

Check Your Progress-VI

1. True or False: WDP provides confirmed delivery of datagrams.
2. MCQ: What is the function of the SAR field in WDP headers?
   a) Store port numbers
   b) Indicate encryption
   c) Support segmentation and reassembly
   d) Transmit debug logs

2.10 SUMMING UP

The Wireless Application Protocol (WAP) provides a comprehensive solution for enabling mobile devices to access the web by introducing a stack of lightweight and optimized protocols. The WAP architecture is designed to handle the limitations of mobile devices, such as small screens, limited processing power, and intermittent connectivity. At the content level, Wireless Markup Language (WML) allows the creation of text-oriented, navigable content suitable for mobile interfaces, while WMLScript enhances interactivity without the need for constant communication with the server. The protocol layers such as Wireless Session Protocol (WSP) and Wireless Transaction Protocol (WTP) provide efficient data exchange and transaction management, ensuring minimal latency and low bandwidth usage. Security is addressed through Wireless Transport Layer Security (WTLS), which ensures authentication, privacy and data integrity in the wireless environment. Lastly, the Wireless Datagram Protocol (WDP) serves as an adaptation layer that makes WAP versatile across various bearer networks. Altogether, these elements form a robust framework for delivering web-like services to mobile users efficiently and securely.

2.11 ANSWER TO CHECK YOUR PROGRESS

Check Your Progress-I

1. False 2. Translator or intermediary

3.b) It provides DNS services and protocol translation

Check Your progress-II

1. False 2. ECMA Script (formerly JavaScript)

3. b)Validate input and handle logic

Check Your progress-III

1. False 2. C) Complex animation

Check Your progress-IV

1.False 2. Connection-oriented

3 b) Session suspend/resume

Check Your progress-V

1. False 2. WAP gateway 3. c) Change Cipher Spec

Check Your progress-VI

1. False 2. a) Stores port numbers

2.12 POSSIBLE QUESTIONS

1. Define Wireless Application Protocol (WAP) and explain its need in mobile communication.
2. Describe the WAP architecture with the help of a diagram.
3. What roles do the gateway and client play?
4. What are the limitations of mobile devices that WAP addresses? Compare WML and HTML.
5. How is WML better suited for wireless communication?
6. Explain the structure of a WML deck and card. Provide a simple example.

7. What are the major features of WML Script? How does it differ from JavaScript?
8. Discuss the significance of the Wireless Application Environment (WAE). How does it support mobile applications?
9. Explain the role of the WSP (Wireless Session Protocol) in the WAP architecture. How does it manage session control?
10. Describe the three transaction classes of WTP (Wireless Transaction Protocol) with examples.
11. What is the role of WTLS in ensuring security in wireless communication? Mention its key features.
12. How does WDP (Wireless Datagram Protocol) handle bearer diversity in WAP?
13. Why is content compression important in WAP gateways? Explain with a suitable scenario.
14. Write a note on the role and structure of the WAP stack.
15. Differentiate between connection-oriented and connectionless services in WSP.
16. How does the WAP model ensure backward compatibility with existing web technologies?

2.13 REFERENCES AND SUGGESTED READINGS:

- Imielinski, T. & Badrinath, B. R. (1994). Mobile wireless computing: Challenges in data management.*Communications of the ACM, 37*(10), 18–28. https://doi.org/10.1145/194313.194316

- Kumar, K. (2013). *Mobile computing* (2nd ed.). Oxford University Press.

- Perkins, C. E. (1998). *Mobile IP: Design principles and practices*. Addison-Wesley.

- Pont, M. J. (2001). *Patterns for time-triggered embedded systems (PTTES)*. Addison-Wesley.

- Schiller, J. (2003). *Mobile communications* (2nd ed.). Pearson Education.

- Stallings, W. (2005). *Wireless communications and networks* (2nd ed.). Pearson Education.

- WAP Forum. (2001). *Wireless application protocol architecture specification* (WAP-210-WAPArch-20010712-a). Open Mobile Alliance. https://www.openmobilealliance.org

***