PNS SCHOOL OF ENGINEERING AND TECHNOLOGY
NISHAMANI VIHAR, MARSHAGHAI, KENDRAPARA

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

LECTURER’S NOTES

Semester: 5th Semester

Subject: MOBILE COMPUTING

Prepared By:

Er. AMARENDRA SAHOO

HOD DEPT. OF ETC

Chapter- 1

INTRODUCTION TO WIRELESS NETWORKS & MOBILE COMPUTING

Networks

Wireless Networks3Mobile
Computing
Mobile Computing Characteristics
Application of Mobile Computing
Networks

A network is two or more computers (or other electronic devices) that are connected together, usually by cables or Wi-Fi. Some computer networks will have a server. A server is a powerful computer that often acts as a central hub for services in a network e.g. e-mails, internet access and file storage.

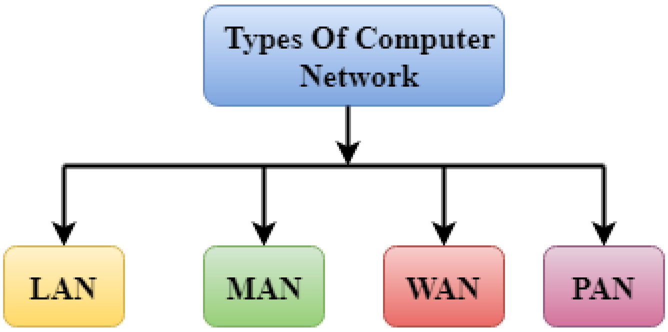
An example of networking is sharing and acquiring information between different divisions of the same company to share information and solve business problems. An example of networking is linking the entire network of computers to a print server to allow each workstation to have the ability to print documents.

A Controller Area Network (CAN bus) is a robust vehicle bus standard designed to allow microcontrollers and devices to communicate with each other's applications without a host computer.

Types of Networks

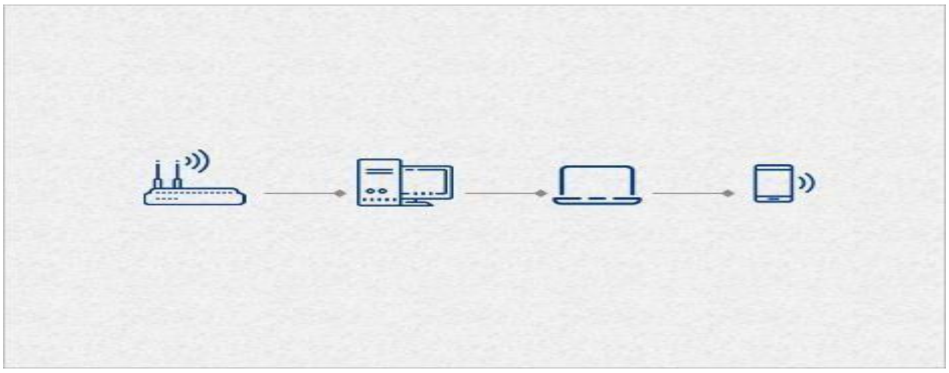
A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

A computer network can be categorized by their size. A computer network is mainly of four types:



LAN (Local Area
Network) PAN (Personal
Area Network)
MAN (Metropolitan Area
Network) WAN (Wide Area
Network) Wireless Networks

In recent years, however, wireless technologies have grown and become much more popular. Wi-Fi and other wireless technologies have become the favourite option for building computer networks. One of the reasons for this is that wireless networks can easily support different types of wireless gadgets that have become popular over the years, such as smartphones and tablets. Mobile networking is now an important thing to consider because it's not going to go away anytime soon.



A wireless network is a computer network that uses wireless data connections between network nodes.

Wireless networking is a method by which homes, telecommunications networks and business installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure.Examples of wireless networks include cell phone networks, wireless local area networks (WLANs), wireless sensor networks, satellite communication networks, and terrestrial microwave networks.

IEEE Standard	Frequency/ Medium	Speed	Topology	Transmission Range	Access Method	Spread Spectrum
802.11	2.4GHz RF	1 to 2Mbps	Ad hoc infrastructure	20 feet indoors.	CSMA/CA	DSSS/FHSS
802.11a	5GHz	Up to 54Mbps	Ad hoc infrastructure	25 to 75 feet indoors; range can be affected by building materials.	CSMA/CA	OFDM
802.11b	2.4GHz	Up to 11Mbps	Ad hoc infrastructure	Up to 150 feet indoors; range can be affected by building materials.	CSMA/CA	DSSS
802.11g	2.4GHz	Up to 54Mbps	Ad hoc infrastructure	Up to 150 feet indoors; range can be affected by building materials.	CSMA/CA	DSSS
802.11n	2.4GHz/5GHz	Up to 600Mbps	Ad hoc infrastructure	175+ feet indoors; range can be affected by building materials.	CSMA/CA	OFDM

Table 7.5. 802.11 Wireless Standards

Introduction to Mobile Computing

The rapidly expanding technology of cellular communication, wireless LANs, and satellite services will make information accessible anywhere and at any time. Regardless of size, most mobile computers will be equipped with a wireless connection to the fixed part of the network, and, perhaps, to other mobile computers. The resulting computing environment, which is often referred to as mobile or nomadic computing, no longer requires users to maintain a fixed and universally known positionin the network and enables almost unrestricted mobility. Mobility and portability will create an entire new class of applications and, possibly, new massive markets combining personal computing and consumer electronics.

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

Mobile Computing

A technology that is capable of providing an environment which enables users to transmit data from one device to other device without the use of any physical link/cables is known as Mobile Computing.

It means, data transmission is done wireless-ly with the help of wireless devices such as mobiles, laptops etc.

Whenever any device is connected to a network without being connected physically over a link or cable, data transmission such as messages, voice recording, videos etc. can be done be done by using the concept of mobile computing.

Mobile Computing technology helps users to access and transmit data from any remote locations without being present there physically.

Thus, having such a big coverage diameter, it is one of the fastest and most reliable sectors of computing technology field.

Mobile computing is used in different contexts with different names. The most common names are:

- Mobile Computing
- Nomadic Computing
- Ubiquitous Computing
- Pervasive Computing
- Invisible Computing

–Mobile Computing:

The computing environment is mobile and moves along with the user.

This is similar to the telephone number of a GSM (Global System for Mobile communication) phone, which moves with the phone.

The offline (local) and real-time (remote) computing environment will move with the
user.In real-time mode user will be able to use all his remote data and services online.

– Ubiquitous Computing:

This is the generic definition of ubiquity, where the information is available anywhere, all the time.

– Virtual Home Environment:

(VHE) is defined as an environment in a foreign network such that the mobile users can experience the same computing experience as they have in their home or corporate computing environment.

For example, one would like to put one's room heater on when one is about 15 minutes away from home.

Nomadic Computing:

The computing environment is nomadic and moves along with the mobile
user.This is true for both local and remote services.

Pervasive Computing:

A computing environment, which is pervasive in nature and can be made available in any environment.

Invisible Computing:

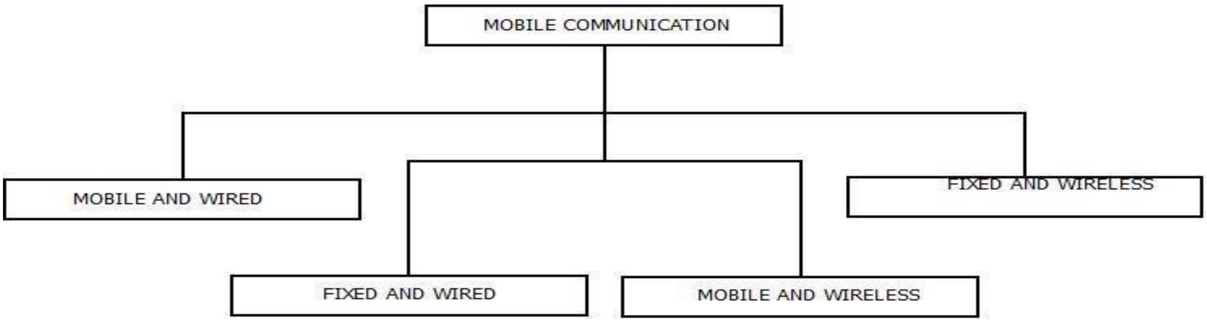
A disappearing (nobody will notice its presence) everyplace computing environment. User will be able to use both local and remote services.

Mobile Communication

Mobile Communication is the framework that is responsible behind the working of mobile computing technology.It ensures the consistency and reliability of communication process through this framework.

Mobile communication framework includes communication devices such as mobiles, laptops, as rules of conduct, fitness etc. They are responsible for delivering of smooth communication process.

Mobile communication can be of one of the following forms as mentioned below.



Characteristics of Mobile Computing

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

Fixed and wired: This configuration describes the typical desktop computer in an office. Neither weight nor power consumption of the devices allow for mobile usage. The devices use fixed networks for performance reasons.

Mobile and wired: Many of today's laptops fall into this category; users carry the laptop from one hotel to the next, reconnecting to the company's network via the telephone network and a modem.

Fixed and wireless: This mode is used for installing networks, e.g., in historical buildings to avoid damage by installing wires, or at trade shows to ensure fast network setup.

Mobile and wireless: This is the most interesting case. No cable restricts the user, who can roam between different wireless networks. Most technologies discussed in this book deal with this type of device and the networks supporting them. Today's most successful example for this category is GSM with more than 800 million users.

Or

Ubiquity - Ability of a user to perform computations from anywhere and at any time.

Location Awareness- Can provide information about the current location of a user to a tracking station.

Adaptation- GPS Implies the ability of a system to adjust bandwidth fluctuation without inconveniencing the user.Broadcast- Efficient delivery of data can be made simultaneously to hand reads of mobile users.

Personalization- Services in a mobile environment can be easily personalized according to a user's profile.

Functions of Mobile Computing

We can define a computing environment as mobile if it supports one or more of the following characteristics:User Mobility:

User should be able to move from one physical location to another location and use the same service.The service could be in the home network or a remote network.

Example could be a user moves from London to New York and uses Internet to access the corporate application the same way the user uses in the home office.

Network Mobility:

User should be able to move from one network to another network and use the same service.

Example could be a user moves from Hong Kong to New Delhi and uses the same GSM phone to access the corporate application through WAP (Wireless Application Protocol). In home network he uses this service over GPRS (General Packet Radio Service) whereas in Delhi he accesses it over the GSM network.Bearer Mobility:

User should be able to move from one bearer to another and use the same service.

Example could be a user was using a service through WAP bearer in his home network in Bangalore. He moves to Coimbatore, where WAP is not supported, he switches over to voice or SMS (Short Message Service) bearer to access the same application. Device Mobility:

User should be able to move from one device to another and use the same service.

–Example could be sales representatives using their desktop computer in home office. During the day while they are on the streets, they would like to use their Palmtop to access the application.

Session Mobility:

A user session should be able to move from one user-agent environment to another.

Example could be a user was using his service through a CDMA (Code Division Multiple Access) IX network. The user entered into the basement to park the car and got disconnected from his CDMA network. User goes to home office and starts using the desktop. The unfinished session in the CDMA device moves from the mobile device to the desktop computer.

Service Mobility:

User should be able to move from one service to another.

Example could be a user is writing a mail. To complete the mail user needs to refer to some other information. In a desktop PC, user simply opens another service (browser) and moves between them using the task bar. User should be able to switch amongst services in small footprint wireless devices like in the desktop.

Host Mobility:

–The user device can be either a client or server.

–When it is a server or host, some of the complexities change.

In case of host mobility, the mobility of IP needs to be taken care of.

Applications of Mobile Computing

Some of the major field in which mobile computing can be applied are:

- Web or Internet access.
- Global Positioning System (GPS).
- Emergency services.
- Entertainment services
- Educational services.
- Limitations of Mobile Computing

Resource constraints: Battery

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

Bandwidth: Although they are continuously increasing, transmission rates are still very low for wireless devices compared to desktop systems. Researchers look for more efficient communication protocols with low overhead.

Dynamic changes in communication environment: variations in signal power within a region, thus link delays and connection losses

Network Issues: discovery of the connection-service to destination and connection stabilityInteroperability issues: the varying protocol standards

Security constraints: Not only can portable devices be stolen more easily, but the radio interface is also prone to the dangers of eavesdropping. Wireless access must always include encryption, authentication, and other security mechanisms that must be efficient and simple to use.

****

Chapter- 2

INTRODUCTION TO MOBILE DEVELOPMENT FRAMEWORK

C/S architecture
n-tier architecture
n-tier architecture and
www Peer-to Peer
architecture Mobile
agent architecture

What is mobile development framework?

A mobile development framework is a software framework that is designed to support mobile app development. It is a software library that provides a fundamental structure to support the development of applications for a specific environment. Frameworks can be in three categories: native frameworks for platform-specific development, mobile web app frameworks, and hybrid apps, which combine the features of both native and mobile web app frameworks.

CLIENT-SERVER ARCHITECTURE

The Client-server architecture is a distributed application structure that partitions task or workload between the providers of a resource or service, called servers, and service requesters called clients. In the client-server architecture, when the client computer sends a request for data to the server through the internet, the server accepts the requested process and deliver the data packets requested back to the client. Clients do not share any of their resources. Examples of Client-Server Architecture are Email, World Wide Web, etc.

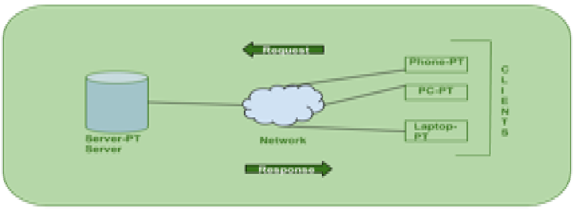
How the Client-Server Architecture works

Client- Server architecture and have a look at how the Internet works via, web browsers. This article will help us in having a solid foundation of the WEB and help in working with WEB technologies with ease.

Client: When we talk the word Client, it means to talk of a person or an organization using a particular service. Similarly, in the digital world a Client is a computer (Host) i.e. capable of receiving information or using a particular service from the service providers (Servers).

Servers: Similarly, when we talk the word Servers, It mean a person or medium that serves something. Similarly, in this digital world a Server is a remote computer which provides information (data) or access to particular services.

So, it is basically the Client requesting something and the Server serving it as long as its present in the database.



How the browser interacts with the servers

There are few steps to follow to interacts with the servers a client.

User enters the URL(Uniform Resource Locator) of the website or file. The Browser then requests the DNS(DOMAINNAME SYSTEM) Server.

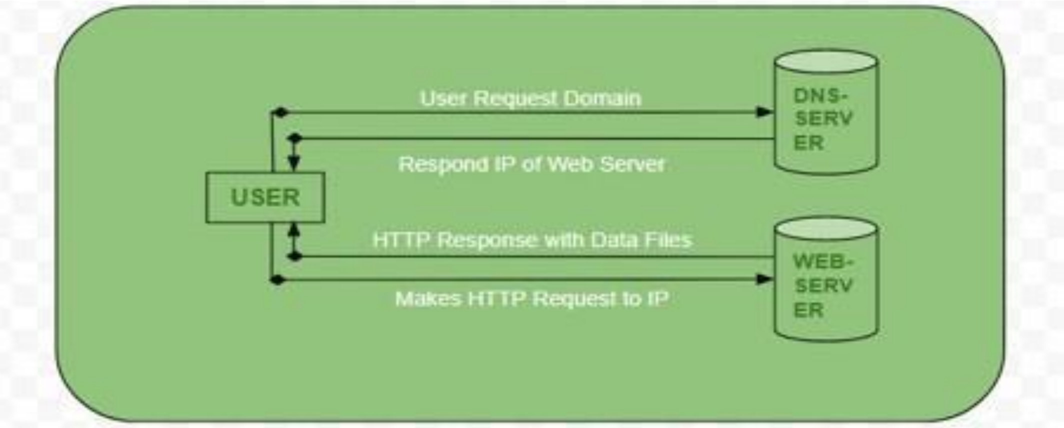
DNS Server lookup for the address of the WEB Server.

DNS Server responds with the IP address of the WEB Server.

Browser sends over an HTTP/HTTPS request to WEB Server’s IP (provided by DNS server).

Server sends over the necessary files of the website.

Browser then renders the files and the website is displayed. This rendering is done with the help of DOM (Document Object Architecture) interpreter, CSS interpreter and JS Engine collectively known as the JIT or (Just in Time) Compilers.



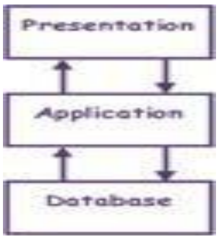
Advantages of Client-Server architecture:
Centralized system with all data in a single place.
Cost efficient requires less maintenance cost and Data recovery is possible. The capacity of the Client and Servers can be changed separately.

Disadvantages of Client-Server architecture:
Clients are prone to viruses, Trojans and worms if present in the Server or uploaded into the Server.
Server are prone to Denial of Service (DOS) attacks.
Data packets may be spoofed or modified during transmission.
Phishing or capturing login credentials or other useful information of the user are common and MITM (Man in theMiddle) attacks are common.

N-TIER ARCHITECTURE

What is N-Tier?

An N-Tier Application program is one that is distributed among three or more separate computers in a distributed network.The most common form of n-tier is the 3-tier Application, and it is classified into three categories.
User interface programming in the user's computer/presentation layer Application logic in a more centralized computer, and/application layerRequired data in a computer that manages a database. /database layer
This architecture model provides Software Developers to create Reusable application/systems with maximum flexibility.
In N-tier, "N" refers to a number of tiers or layers are being used like – 2-tier, 3-tier or 4-tier, etc. It is also called "Multi-Tier Architecture".
The n-tier architecture is an industry-proven software architecture model. It is suitable to support enterprise level client-server applications by providing solutions to scalability, security, fault tolerance, reusability, and maintainability. It helps developers to create flexible and reusable applications.
N-Tier Architecture



A diagrammatic representation of an n-tier system depicts here – presentation, application, and database layers.
N Tier Architecture Diagram given below.These three layers can be further subdivided into different sub-layers depending on the requirements.
Some of the popular sites who have applied this architecture are:MakeMyTrip.com

Sales Force enterprise application Indian Railways – IRCTC Amazon.com, etc.

Some common terms to remember, so as to understand the concept more clearly:

Distributed Network: It is a network architecture, where the components located at network computers coordinate and communicate their actions only by-passing messages. It is a collection of multiple systems situated at different nodes but appears to the user as a single system.

It provides a single data communication network which can be managed separately by different networks.

An example of Distributed Network – where different clients are connected within LAN architecture on one side and on the other side they are connected to high-speed switches along with a rack of servers containing service nodes.

Client-Server Architecture: It is an architecture model where the client (one program) requests a service from a server (another program) i.e. It is a request-response service provided over the internet or through an intranet.

In this model, Client will serve as one set of program/code which executes a set of actions over the network. While Server, on the other hand, is a set of another program, which sends the result sets to the client system as requested.

In this, client computer provides an interface to an end user to request a service or a resource from a server and on the other hand server then processes the request and displays the result to the end user.

An example of Client-Server Model– an ATM machine. A bank is the server for processing the application within the large customer databases and ATM machine is the client having a user interface with some simple application processing.

Platform: In computer science or software industry, a platform is a system on which applications program can run. It consists of a combination of hardware and software that have a built-in instruction for a processors/ microprocessor toperform specific operations.

In more simple words, the platform is a system or a base where any applications can run and execute to obtain a specific task.

An example of Platform – A personal machine loaded with Windows 2000 or Mac OS X as examples of 2 different platforms.

Database: It is a collection of information in an organized way so that it can be easily accessed, managed and updated.Examples of Database – MySQL, SQL Server, and Oracle Database are some common Db's.

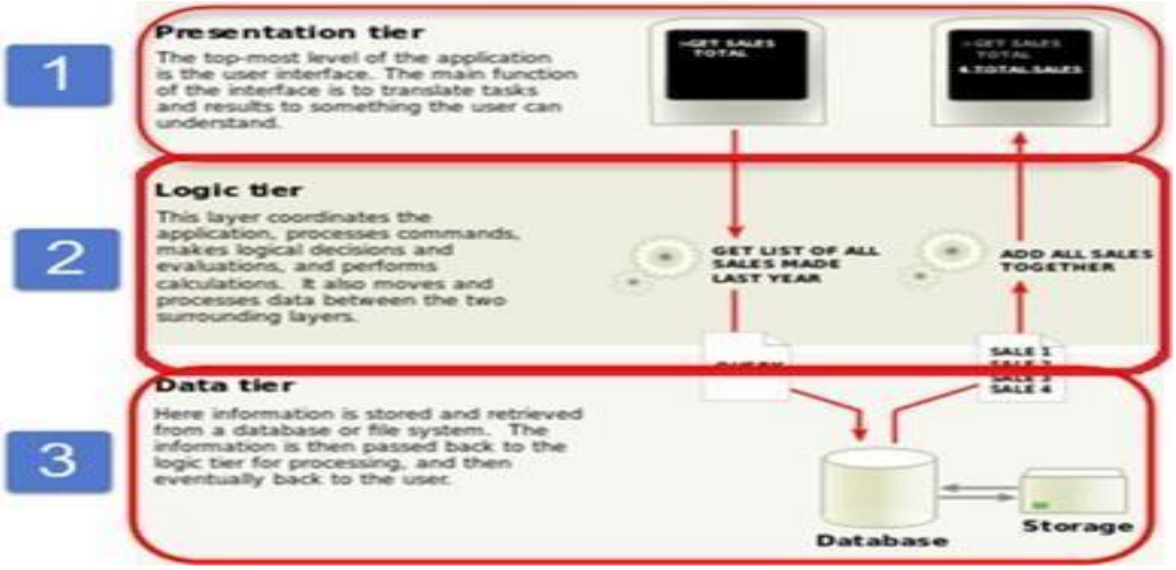
Types of N-Tier Architectures

There are different types of N-Tier Architectures, like 3-tier Architecture, 2-Tier Architecture and 1- Tier Architecture.First, we will see 3-tier Architecture, which is very important.

3-Tier Architecture

By looking at the below diagram, you can easily identify that 3-tier architecture has three different layers.

- Presentation layer
- Application Logic layer
- Database layer



The top-most level of the application is the user interface. The main function of the interface is to translate tasks and results to something the user can understand.

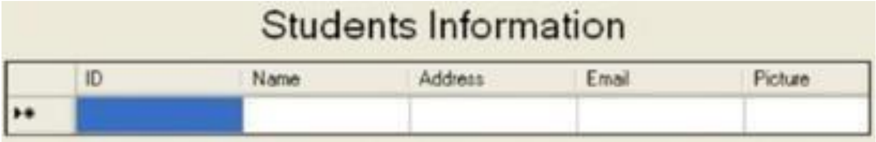
This layer coordinates the application, processes commands, makes logical decisions and evaluations, and performs calculations. It also moves and processes data between the two surrounding layers.

Here information is stored and retrieved from a database or file system. The information is then passed back to the logic tier for processing, and then eventually back to the user.

3 Tier Architecture Diagram

User Interface Layer or Presentation Layer

Here we have taken a simple example of student form to understand all these three layers. It has information about a student like – Name, Address, Email, and Picture.



Students Information

	ID	Name	Address	Email	Picture
▸*					

Application Access Layer -

This is the function of the application layer which accepts the data from the presentation layer and passes it to thedata layer.

Application logic acts as an interface between Client layer and Data Access Layer

All application logic – like validation of data, calculations, data insertion/modification are written under application logic layer.

It makes communication faster and easier between the client and data layer

Defines a proper workflow activity that is necessary to complete a task

Data Access Layer

This is the data layer function, which receives the data from the application layer and performs the necessary operation into the database.

2-Tier Architecture:

It is like Client-Server architecture, where communication takes place between client and server.

In this type of software architecture, the presentation layer or user interface layer runs on the client side while dataset layer gets executed and stored on server side.

There is no Application logic layer or immediate layer in between client and server.

Single Tier or 1-Tier Architecture:

It is the simplest one as it is equivalent to running the application on the personal computer. All of the required components for an application to run are on a single application or server.

Presentation layer, Application logic layer, and data layer are all located on a single machine.

Advantages and Disadvantages of Multi-Tier Architectures

Advantages	Disadvantages
Scalability	Increase in Effort
Data Integrity	Increase in Complexity
Reusability	
Reduced Distribution	
Improved Security	
Improved Availability	

Hence, it is a part of a program which encrypts real-world application problems and determines how data can be updated, created, stored, or changed to get the complete task done.

Summary:

The N-tier architecture helps to manage all the components (application layer, presentation layer, and database layer) of an application under one roof.

Applications that use small numbers of users on a local area network can benefit from n-tier architecture.

Such architectural design ascertains maintaining, scaling up and deploying an application on the Internet efficiently.

N-TIER ARCHITECTURE and www

WWW stands for World Wide Web. A technical definition of the World Wide Web is : all the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP).

The World Wide Web is the universe of network-accessible information, an embodiment of human knowledge.

In simple terms, The World Wide Web is a way of exchanging information between computers on the Internet, tying them together into a vast collection of interactive multimedia resources.

Internet and Web is not the same thing: Web uses internet to pass over the information.

Components of Web

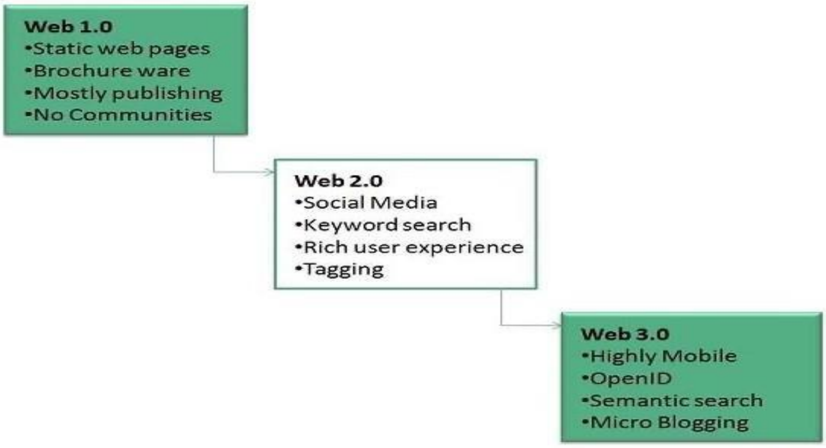
There are 3 components of web:

- Uniform Resource Locator (URL): serves as system for resources on web.
- HyperText Transfer Protocol (HTTP): specifies communication of browser and server.
- Hyper Text Markup Language (HTML): defines structure, organisation and content of webpage

EVOLUTION

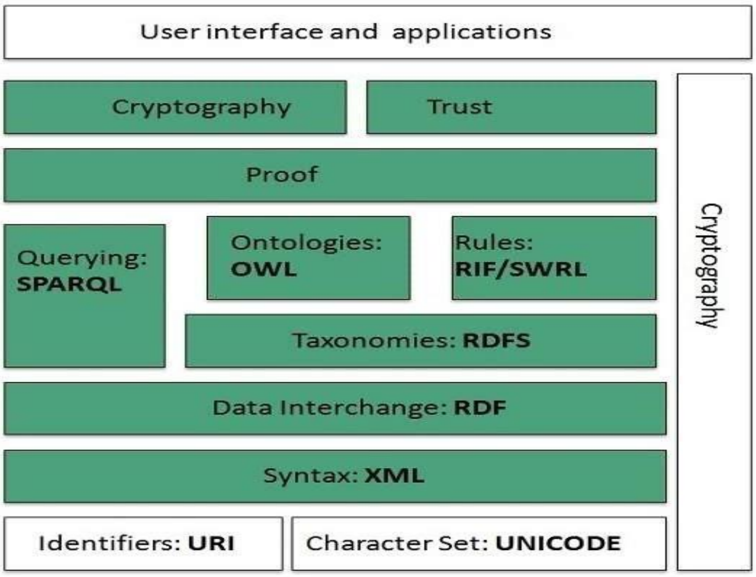
World Wide Web was created by Timothy Berners Lee in 1989 at CERN in Geneva. World Wide Web came into existence as a proposal by him, to allow researchers to work together effectively and efficiently at CERN. Eventually it became World Wide Web.

The following diagram briefly defines evolution of World Wide Web:



WWW ARCHITECTURE

WWW architecture is divided into several layers as shown in the following diagram:



Identifiers and Character Set

Uniform Resource Identifier (URI) is used to uniquely identify resources on the web and UNICODE makes it possible to build web pages that can be read and write in human languages.

Syntax

XML (Extensible Markup Language) helps to define common syntax in semantic web.

Data Interchange

Resource Description Framework (RDF) framework helps in defining core representation of data for web. RDF represents data about resource in graph form.

Taxonomies

RDF Schema (RDFS) allows more standardized description of taxonomies and other ontological constructs.

Ontologies

Web Ontology Language (OWL) offers more constructs over RDFS. It comes in following three versions:

OWL Lite for taxonomies and simple constraints.

OWL DL for full description logic support.

OWL for more syntactic freedom of RDF

Rules

RIF and SWRL offers rules beyond the constructs that are available from RDFs and OWL. Simple Protocol and RDF Query Language (SPARQL) is SQL like language used for querying RDF data and OWL Ontologies.

Proof

All semantic and rules that are executed at layers below Proof and their result will be used to prove deductions.

Cryptography

Cryptography means such as digital signature for verification of the origin of sources is used.

User Interface and Applications

On the top of layer User interface and Applications layer is built for user interaction.

WWW OPERATION

WWW works on client- server approach. Following steps explains how the web works:

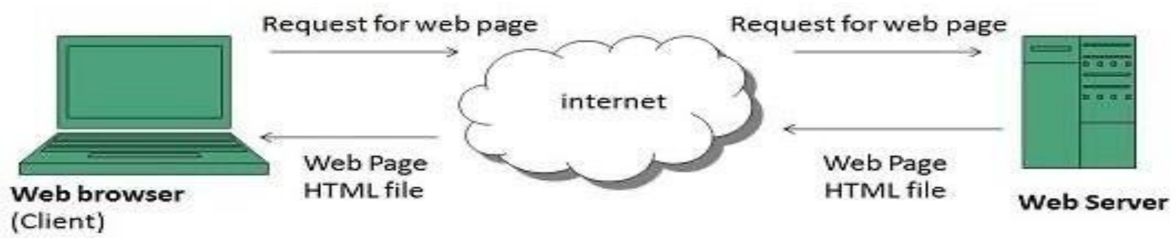
User enters the URL (say, http://www.facebook.com) of the web page in the address bar of web browser.

Then browser requests the Domain Name Server for the IP address corresponding to www.facebook.com.

After receiving IP address, browser sends the request for web page to the web server using HTTP protocol which specifies the way the browser and web server communicates.

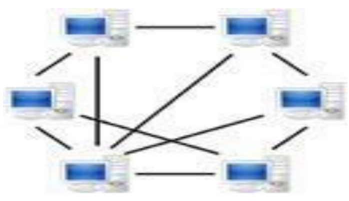
Then web server receives request using HTTP protocol and checks its search for the requested web page. If found it returns it back to the web browser and close the HTTP connection.

Now the web browser receives the web page, It interprets it and display the contents of web page in web browser's window.



PEER-TO-PEER ARCHITECTURE

In the common client-server architecture, multiple clients will communicate with a central server. A peer- to-peer (P2P) architecture consists of a decentralized network of peers - nodes that are both clients and servers. P2P networks distribute the workload between peers, and all peers contribute and consume resources within the network without the need for a centralized server. However, not all peers are necessarily equal. Super peers may have more resources and can contribute more than they consume. Edge peers do not contribute any resources, they only consume from the network. In its purest form, P2P architecture is completely decentralized. However, in application, sometimes there is a central tracking server layered on top of the P2P network to help peers find each other and manage the network.



Some uses of P2P architecture:

File sharing

Instant messaging

Voice Communication

Collaboration

High Performance Computing

Some examples of P2P architecture:

Napster - it was shut down in 2001 since they used a centralized tracking server

BitTorrent - popular P2P file-sharing protocol, usually associated with piracy

Skype - it used to use proprietary hybrid P2P protocol, now uses client-server model after Microsoft's acquisition
Bitcoin - P2P cryptocurrency without a central monetary authority

MOBILE AGENT ARCHITECHTURE

Mobile (transportable) agents: An agent is "an independent software program, which runs on behalf of a network user". A mobile agent is a program that, once it is launched by a user, can travel from node to node autonomously, and can continue to function even if the user is disconnected from the network.

What is mobile agent ?

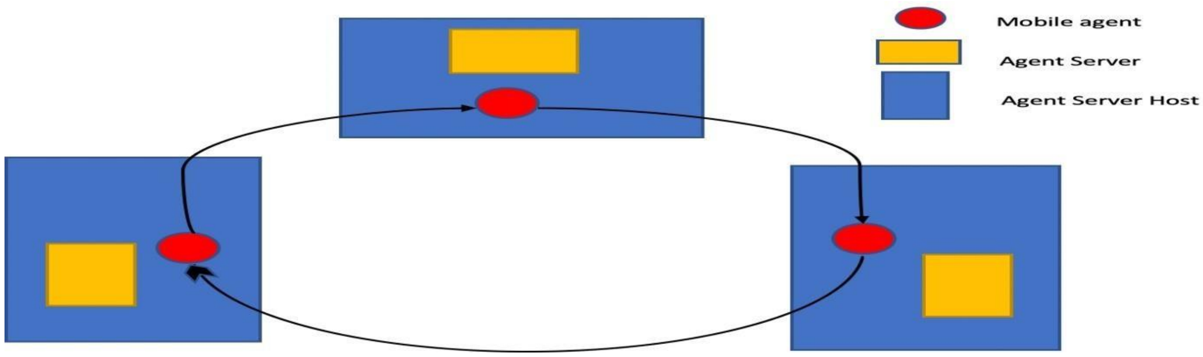
Program that can migrate and performs some processing at each host. Agent decides when and where to move next .

-How it Moves : (in just 3 steps)

Save state

Transport

Resume



Mobile Agent Architecture

An agent server process runs on each participating host. Participating hosts are networked through links that can be low-bandwidth and unreliable. An agent is a serializable object whose execution state can be frozen for transportation and reconstituted upon arrival at a remote site.

What's in the Agent?

An agent is an object, hence it contains state data and methods. Among the instance data is an itinerary of the sites to be visited, which may be dynamically constructed or adjusted. Other data may include an agent ID or other authentication data. The agent's behaviour at each stop can be pre- programmed and dynamically adjusted.

Events in Mobile Agent

Creation: a brand new agent is born and its state is initialized.

Cloning: a twin agent is born and the current state of the original is duplicated in the clone.

Dispatch: an agent travels to a new host.

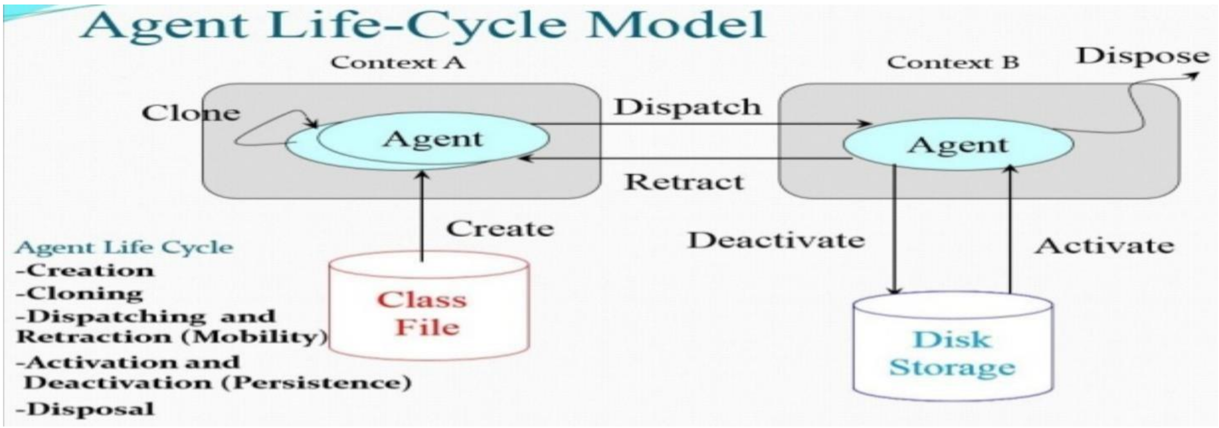
Deactivation: an agent is put to sleep and its state is saved in persistent storage.

Activation: a deactivated agent is brought back to life and its state is restored from persistent storage.

Retraction: an agent is brought back from a remote host along with its state to the home machine.

Disposal: an agent is terminated and its state is lost forever.

Communication: Notifies the agent to handle messages incoming from other agents , which is the primary means of inter-agent correspondence.



Agent Life Cycle
-Creation
-Cloning
-Dispatching and Retraction (Mobility)
-Activation and Deactivation (Persistence)
-Disposal

Why mobile agent ?

They reduce the network load
they overcome network latency
they encapsulate protocols
they adapt dynamically
they execute asynchronously and autonomously
they are natural heterogeneous
they are fault tolerance

Mobile-agent applications

Information retrieval
Monitoring
Virtual market-place/ meeting room
Shareware
Example:
Mobile Agents in Java A mobile agent in Java is called an “Aglet” – Lightweight agent Why use Java?
Platform independence!
Create once, go anywhere
Price FREE TOOLKITS (ASDK)
Hosts can provide an environment for the aglet to execute within
Types of agent mobility WEAK
-when moving a mobile agent Carrier (Code + Date State)
-global or instance variables
-on moving , execution starts from the beginning
STRONG
-when moving a mobile agent Carrier (Code + Date State + Execution State)
-global or instance variables
- Execution State :local variables and threads
-on moving : execution can be continued from the point it is stopped previously

Security in Mobile Agent Systems
Security concern is the primary deterrent of deploying the mobile-agent technology.
There are concerns for both the agent hosts and the mobile agents.
Agent host concerns: Malicious/unauthorized agents can misuse/destroy system resources (e.g., worms).
Agent concerns: Malicious hosts can destroy or alter an agent’s logic, (e.g., Mobile agent’s route can be altered.)

Security in Mobile Agent Systems Measures:

Authentication – an agent must authenticate itself to the host, and an agent server must authenticate itself to the agent.
Encryption – an agent encrypts its sensitive data

Resource access – a host enforces strict access control to its resources.

Current Areas of Work

mobile agent theories: Pi-calculus extensions, Mobile Ambient, Agent Itineraries

mobile agent model: component-based, AI- based

mobile agent infrastructure: environment supporting mobile agents - security, naming, domain crossing, etc

mobile agent programming: languages, toolkits, abstractions

mobile agent standards: OMG’s MASIF, FIPA

****

Chapter- 3

INTRODUCTION TO MOBILE DEVELOPMENT FRAMEWORK

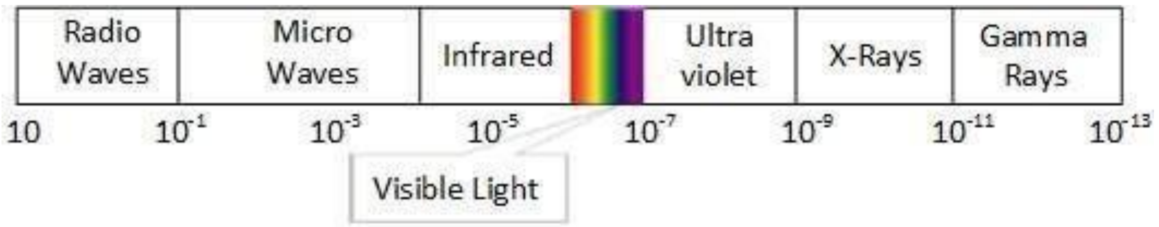
IntroductionSignals
Period, Frequency and
Bandwidth.Antennas
Signal Propagation
Multiplexing Modulation
Spread Spectrum Cellular System

INTRODUCTION

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

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

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



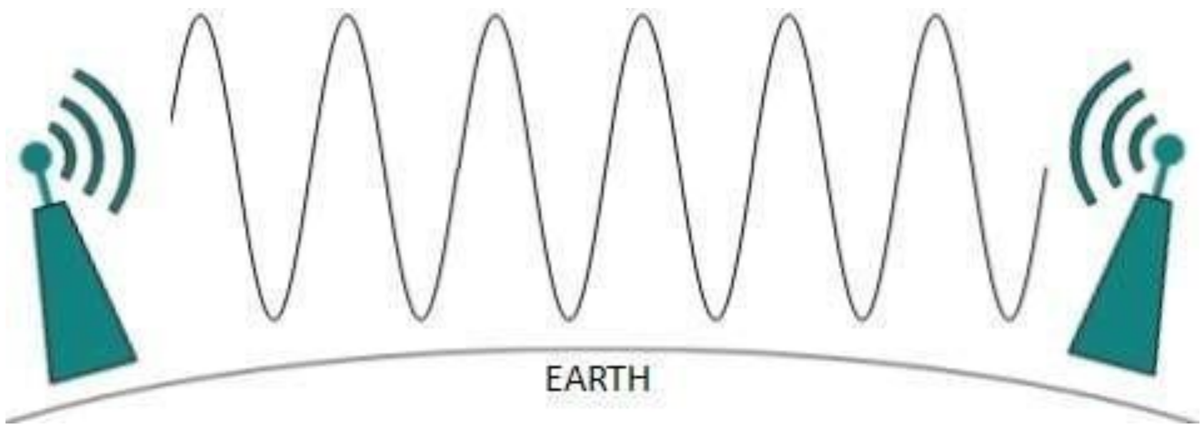
RADIO TRANSMISSION

Radio frequency is easier to generate and because of its large wavelength it can penetrate through walls and structures alike.Radio waves can have wavelength from

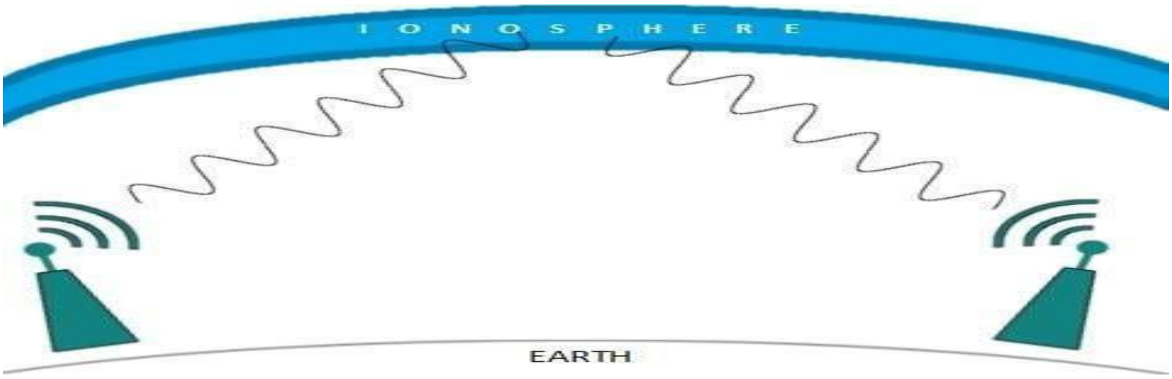
1 mm – 100,000 km and have frequency ranging from 3 Hz (Extremely Low Frequency) to 300 GHz (Extremely High Frequency). Radio frequencies are sub- divided into six bands.

Radio waves at lower frequencies can travel through walls whereas higher RF can travel in straight line and bounce back. The power of low frequency waves decreases sharply as they cover long distance. High frequency radio waves have more power.

Lower frequencies such as VLF, LF, MF bands can travel on the ground up to 1000km over the earth's surface.

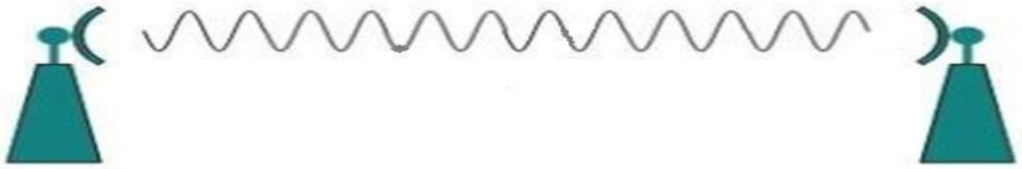


Radio waves of high frequencies are prone to be absorbed by rain and other obstacles. They use Ionosphere of earth atmosphere. Highfrequency radio waves such as HF and VHF bands are spread upwards. When they reach Ionosphere, they are refracted back to the earth.



MICROWAVE TRANSMISSION

Electromagnetic waves above 100 MHz tend to travel in a straight line and signals over them can be sent by beaming those waves towards one particular station. Because Microwaves travels in straight lines, both sender and receiver must be aligned to be strictly in line-of-sight. Microwaves can have wavelength ranging from 1 mm – 1 meter and frequency ranging from 300 MHz to 300 GHz.



Microwave antennas concentrate the waves making a beam of it. As shown in picture above, multiple antennas can be aligned to reach further. Microwaves have higher frequencies and do not penetrate wall like obstacles.

Microwave transmission depends highly upon the weather conditions, antenna size and the frequency it is using.

INFRARED TRANSMISSION

Infrared wave lies in between visible light spectrum and microwaves. It has wavelength of 700-nm to 1-mm and frequency ranges from 300-GHz to 430-THz.

Infrared wave is used for very short range communication purposes such as television and it's remote. Infrared travels in a straight line hence it is directional by nature. Because of high frequency range, Infrared cannot cross wall-like obstacles.

LIGHT TRANSMISSION

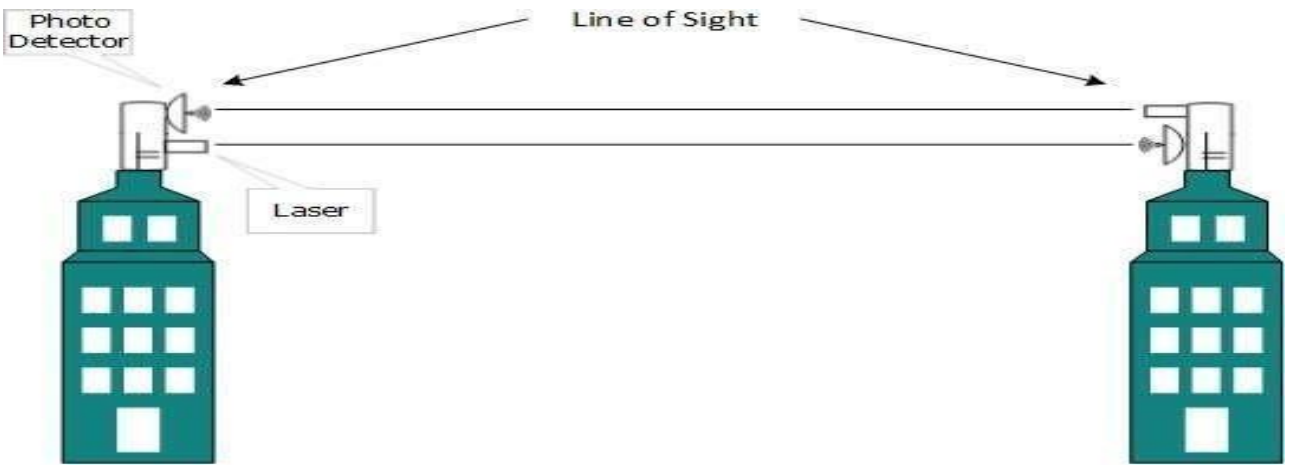
Highest most electromagnetic spectrum which can be used for data transmission is light or optical signaling. This is achieved by means of LASER.

Because of frequency light uses, it tends to travel strictly in straight line.Hence the sender and receiver must be in the line-of-sight. Becauselaser transmission is unidirectional, at both ends of communication the laser and the photo-detector needs to be installed. Laser beam is generally 1mm wide hence it is a work of precision to align two far receptors each pointing to lasers source.

Laser works as Tx (transmitter) and photo-detectors works as Rx (receiver).

Lasers cannot penetrate obstacles such as walls, rain, and thick fog. Additionally, laser beam is distorted by wind, atmosphere temperature,or variation in temperature in the path.

Laser is safe for data transmission as it is very difficult to tap 1mm wide laser without interrupting the communication channel.



SIGNALS

Signals are the physical representation of data.

Users of a communication system can only exchange data through the transmission of signals.

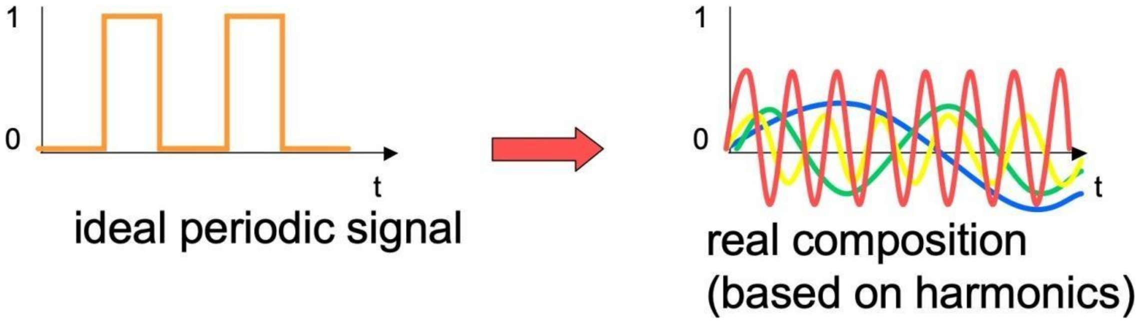
Layer 1 of the ISO/OSI basic reference model is responsible for the conversion of data, i.e., bits, into signals and vice versa.Signals are functions of time and location.

Signal parameters represent the data values.

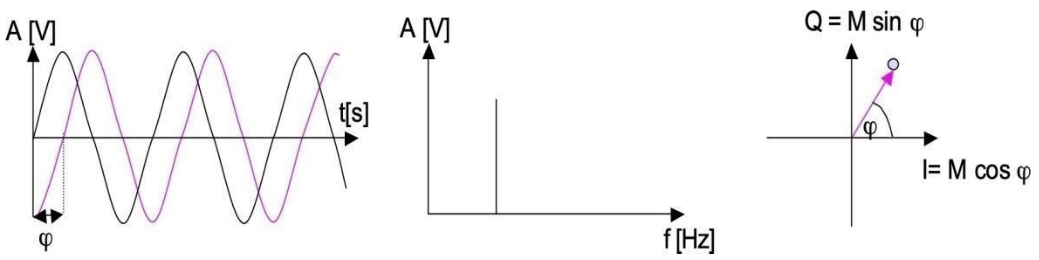
The most interesting types of signals for radio transmission are periodic signals, especially sine waves as carriers. The general function of a sine wave is, g(t) = At sin (2 πft t + ϕt)

Signal parameters are the amplitude A, the frequency f, time period t and the phase shift ϕ.Signals are of 2 types:

analog signal = continuous time and continuous values digital signal = discrete time and discrete values



Different representations of signals Amplitude (amplitude domain)
Frequency spectrum (frequency domain)
Phase state diagram (amplitude M and phase j in polar coordinates)



Composed signals transferred into frequency domain using Fourier transformationDigital signals need infinite frequencies for perfect transmission q modulation with a carrier frequency for transmission (analog signal)PERIOD, FREQUENCY AND BANDWIDTH

PERIOD

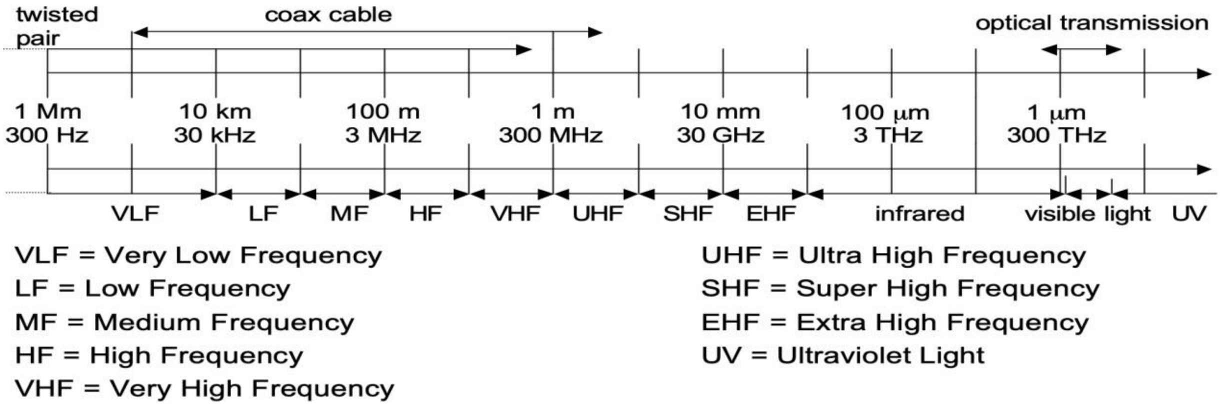
Period refers to the time that it takes to do something. When an event occurs repeatedly, then we say that the event is periodic and refer to the time for the event to repeat itself as the period.

The period of a wave is the time for a particle on a medium to make one complete vibrational cycle.A period (T) is the time required for one complete cycle of vibration to pass a given point.

Period equals the Total time divided by the Number of cycles. NOTE: Frequency and Period are in reciprocal relationships FREQUENCY

The frequency is the number of complete vibrational cycles of a medium per given amount of time.

It is reasonable that the quantity frequency would have units of cycles/second, waves/second, vibrations/second, or something/second. Unit for frequency is the Hertz (abbreviated Hz) where 1 Hz is equivalent to 1 cycle/second. If 2 vibrational cycles in one second, then thefrequency is 2 Hz. If 8 vibrational cycles in 4 seconds, then the frequency is 2 Hz (8 cycles/4 s = 2 cycles/s).



Frequency and wave length:

wave length l, speed of light c= 3x108m/s, frequency f

VLF, LF, MF HF not used for wireless

VHF-/UHF-ranges for mobile radio

simple, small antenna for cars

deterministic propagation characteristics, reliable connections

SHF and higher for directed radio links, satellite communication

small antenna, beam forming

large bandwidth available

Wireless LANs use frequencies in UHF to SHF range

some systems planned up to EHF

limitations due to absorption by water and oxygen molecules (resonance Frequencies)weather dependent fading. E.g. signal loss caused by heavy rain

BANDWIDTH

Bandwidth is the maximum amount of data transmitted over an internet connection in a given amount of time. Bandwidth measures how much data can be transferred along a communications channel. The more frequencies available to the communications channel, the more data that can be transferred at once.

Bandwidth is often mistaken for internet speed when it's actually the volume of information that can be sent over a connection.

While bandwidth is officially measured as a frequency (Hz), it is more generally reported in amount of time – calculated in megabits per second (Mbps).

ANTENNAS

Antenna is a device which can receive and radiate electromagnetic waves from one station to another.

Radiation and reception of electromagnetic waves, coupling of wires to space for radio transmission

In radio engineering, an antenna is the interface between radio waves propagating through space and electric currents moving in metal conductors, used with a transmitter or receiver.

In transmission, a radio transmitter supplies an electric current to the antenna's terminals, and the antenna radiates the energy from the current as electromagnetic waves (radio waves).

In reception, an antenna intercepts some of the power of a radio wave in order to produce an electric current at its terminals, that is applied to a receiver to be amplified. Antennas are essential components of all radio equipment.

Antenna is a metal rod or dish that catches radio waves and turns them into electrical signals feeding into something like a radio or television or a telephone system.

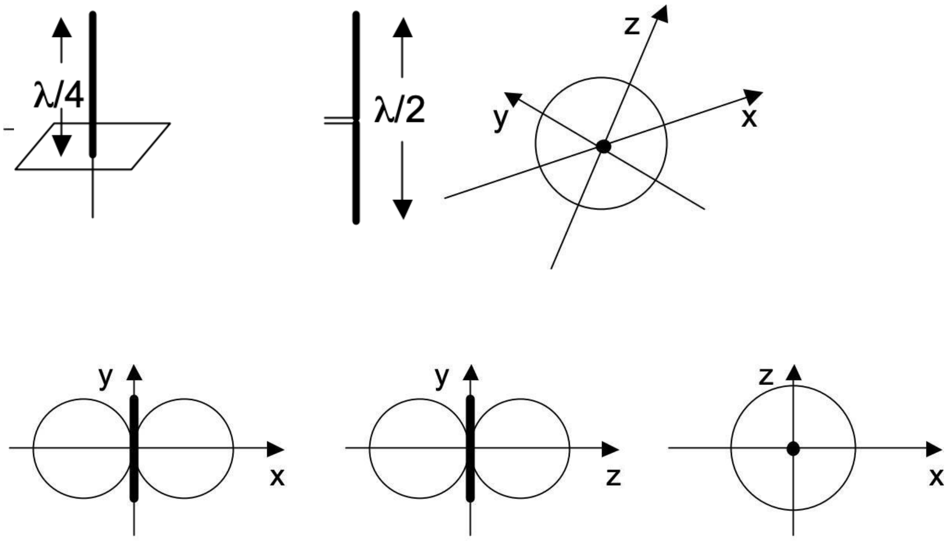
ANTENNAS: ISOTROPIC RADIATOR

Isotropic radiator: equal radiation in all directions (three dimensional) - only a theoretical reference antenna Real antennas always have directive effects (vertically and/or horizontally) Radiation pattern: measurement of radiation around an antennaideal isotropic antenna.

ANTENNAS: SIMPLE DIPOLES

Real antennas are not isotropic radiators but simple dipoles are real antennas, e.g., dipoles with lengths l/4 on car roofs or l/2 as Hertzian dipole Ë shape of antenna proportional to wavelength

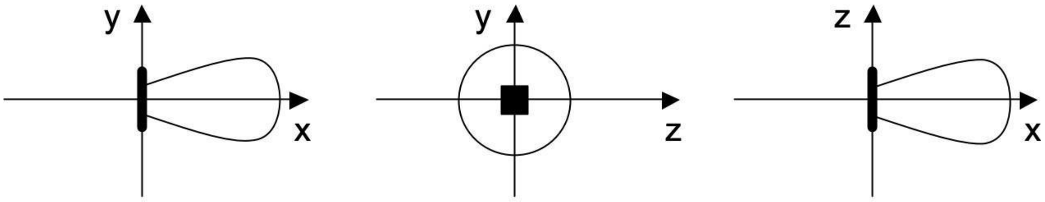
Example: Radiation pattern of a simple Hertzian dipole



side view (xy-plane) side view (yz-plane) top view (xz-plane)

ANTENNAS: DIRECTED ANTENNA

These are the antenna having particular direction specified for receiving the signal.

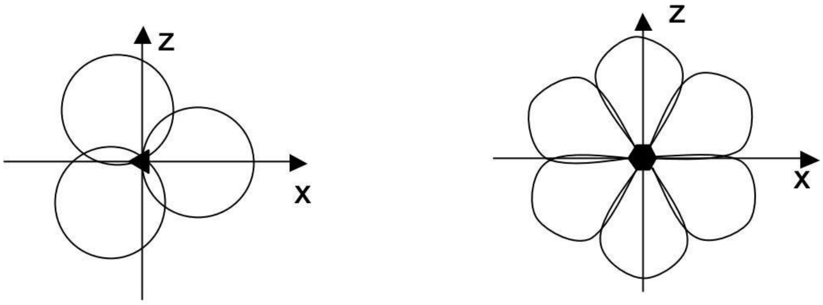


side view (xy-plane) side view (yz-plane) top view (xz-plane)

ANTENNAS: SECTORIZED ANTENNA

Antenna is divided in sectors to receive the particular signal from 3 or 6 different direction.

Often used for microwave connections or base stations for mobile phones (e.g., radio coverage of a valley)



top view, 3 sector top view, 6 sector

ANTENNAS: DIVERSITY ANTENNA

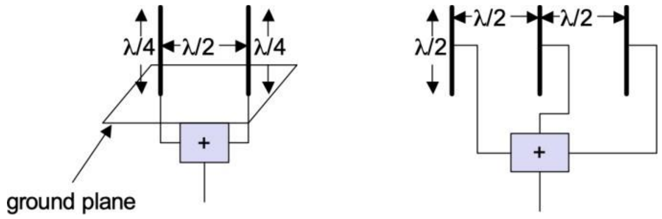
Grouping of 2 or more antennas together is known as diversity antenna.

It increases the strength of the receiving signal

Receiver can choose the largest output

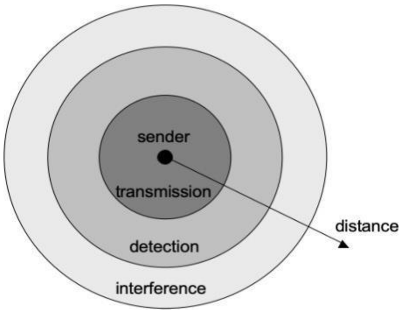
It can combine output power of antenna to produce gain.

Co-phasing needed to avoid cancellation

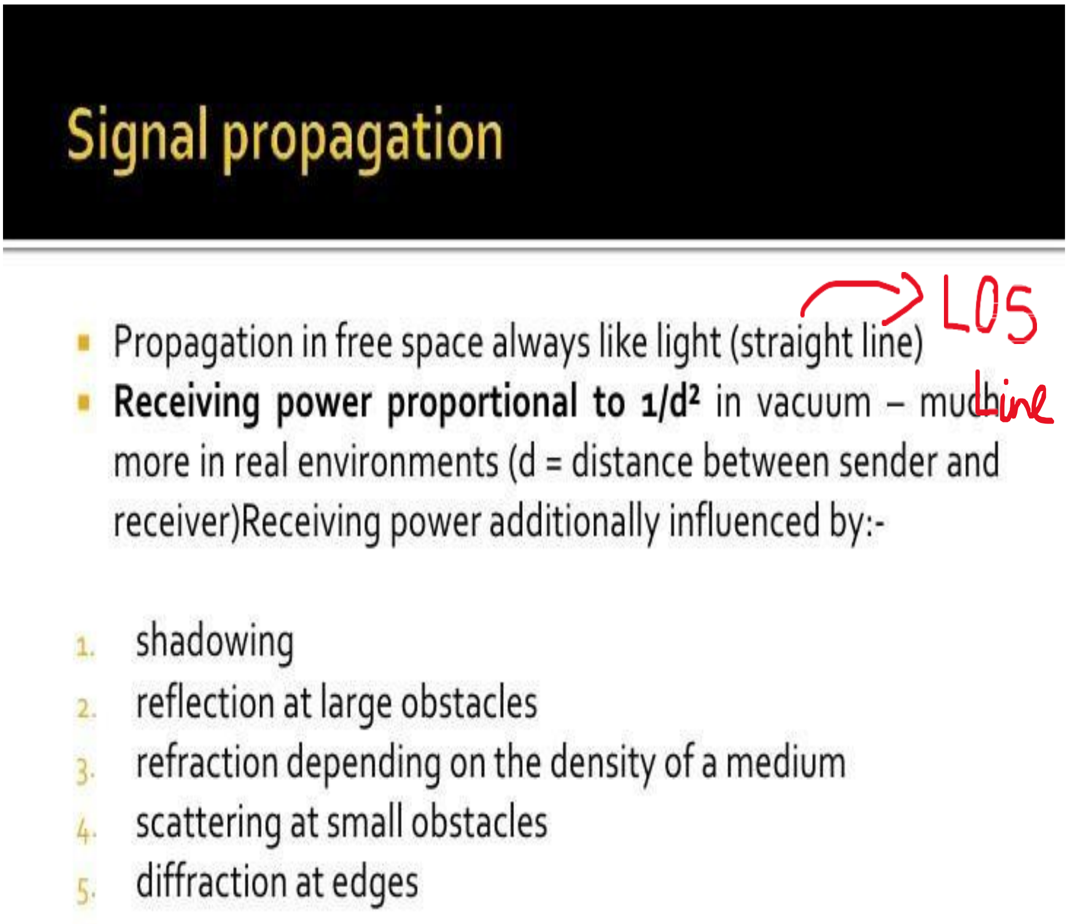


SIGNAL PROPAGATION

Transmission range
communication possible
low error rate
Detection range
detection of the signal possible
no communication possible
Interference range
signal may not be detected q
signal adds to the background noise



Signal propagation ranges



Signal propagation

- Propagation in free space always like light (straight line) LOS
- **Receiving power proportional to 1/d²** in vacuum – much Line more in real environments (d = distance between sender and receiver)Receiving power additionally influenced by:-

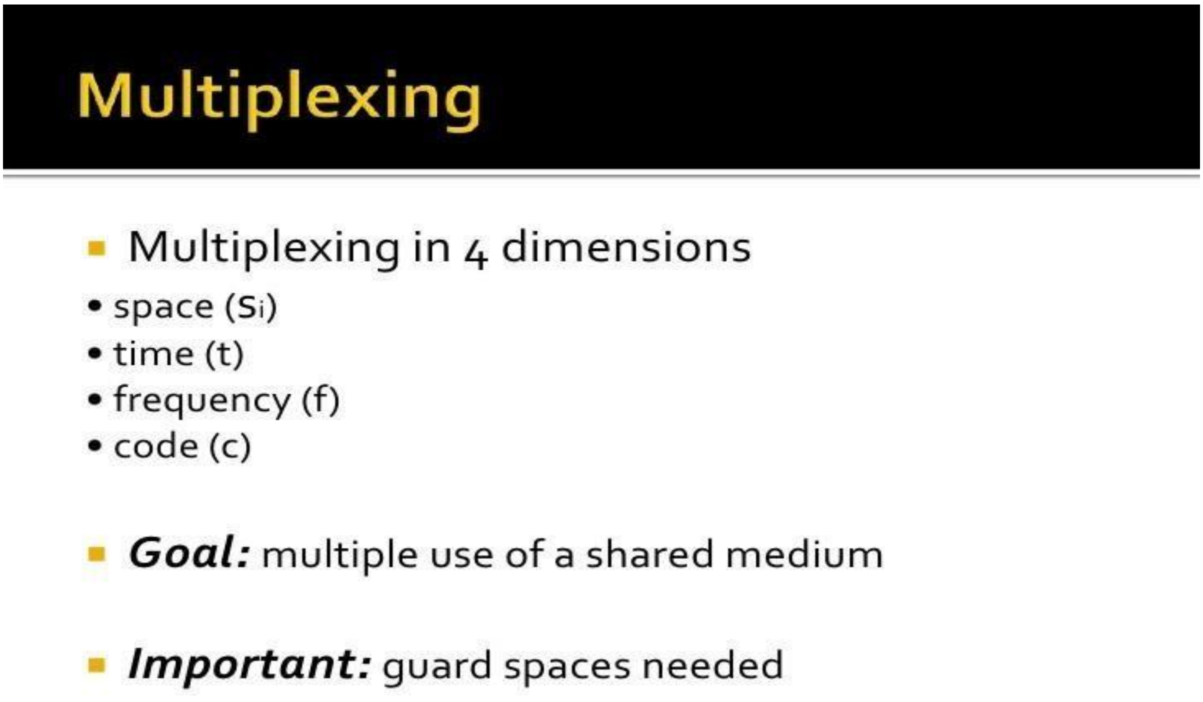
1. shadowing
2. reflection at large obstacles
3. refraction depending on the density of a medium
4. scattering at small obstacles
5. diffraction at edges

DELAY SPREAD- Signal travelling in diff. paths in diff lengths are received at diff times at reciever end.

MULTIPLEXING

It is a technique where two or more signals are combined and use the same channel for transmission.

Multiple access technique: application of multiplexing from user point to get data over a channel. Eg. Wifi



Multiplexing

- Multiplexing in 4 dimensions
  - space (S_i)
  - time (t)
  - frequency (f)
  - code (c)
- ***Goal:*** multiple use of a shared medium
- ***Important:*** guard spaces needed

MODULATION

Modulation is the process of varying one or more properties of a periodic waveform called the carrier signal, with a modulating signal typically contains information to be transmitted.

For digital modulation, digital data (0 and 1) is translated into an analog signal (baseband signal).

Digital modulation is required if digital data has to be transmitted over a medium that only allows for analog transmission.

One example for wired networks is the old analog telephone system. – to connect a computer to this system a modem is needed. The modem then performs the translation of digital data into analog signals and vice versa.

Need for Modulation

Reduction in the height of the antennaAvoids mixing of signals

Makes multiplexing possible

Increases the range of communication

In wireless networks, however, digital transmission cannot be used.Here, the binary bit-stream has to be translated into an analog signal first.The three basic methods for this translation are,

- amplitude shift keying (ASK)
- frequency shift keying (FSK) and
- phase shift keying (PSK)

Apart from the translation of digital data into analog signals, wireless transmission requires an additional modulation, an analog modulation.

Analog modulation shifts the center frequency of the baseband signal generated by the digital modulation up to the radio carrier.

Amplitude Shift Keying (ASK) Modulation

As the name suggests, in Amplitude Shift Key or ASKS Modulation, the amplitude is represented by "1," and if the amplitudedoes not exist, it is represented by "0".

Using Amplitude Shift Key Modulation is very simple, and it requires a very low bandwidth.

Amplitude Shift Key Modulation is vulnerable to inference or deduction.

Frequency Shift Key (FSK) Modulation

In Frequency Shift Key or FSK Modulation, different notations f1 and f2 are used for different frequencies.Here, f1 is used to represent bit "1," and f2 represents bit "0".

It is also a simple modulation technique but uses different frequencies for different bits; bandwidth requirement becomes high.

SPREAD SPECTRUM

A collective class of signaling techniques are employed before transmitting a signal to provide a secure communication, knownas the Spread Spectrum Modulation.

Spread spectrum technique is used for increasing the bandwidth of baseband message signal (when compared to original signal) with the help of pseudo random noise.

The main advantage of spread spectrum communication technique is to prevent “interference” whether it is intentional or unintentional.

These spread spectrum signals transmit at low power density and has a wide spread of signals.

The signals modulated with these techniques are hard to interfere and cannot be jammed. An intruder with no official access is never allowed to crack them. Hence, these techniques are used for military purposes.

A coded sequence of 1s and 0s with certain auto-correlation properties, called as Pseudo-Noise coding sequence is used in spread spectrum techniques.

It is a maximum-length sequence, which is a type of cyclic code(periodic) and deterministic.Pseudo-Noise code generation is done by linear feedback shift register.

NARROW-BAND AND SPREAD-SPECTRUM SIGNALS

Both the Narrow band and Spread spectrum signals can be understood easily by observing their frequency spectrum .Narrow-band / Baseband Message Signals

The Narrow-band signals have the signal strength concentrated as shown in the following frequency spectrum figure. Following are some of its features −

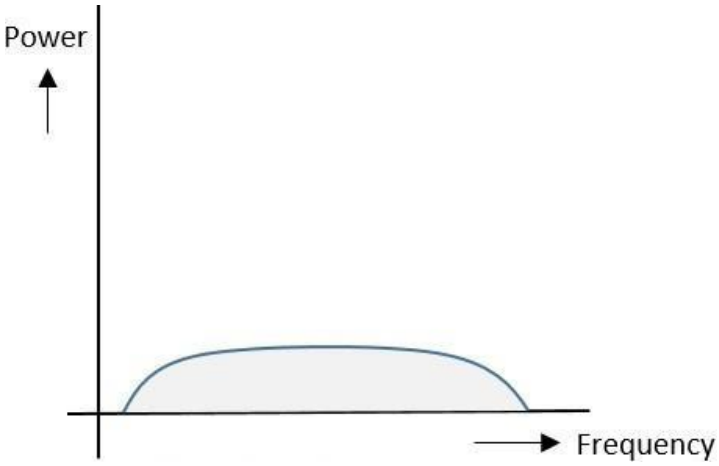
Band of signals occupy a narrow range of frequencies.Power density is high.

Spread of energy is low and concentrated.

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

Spread Spectrum Signals

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



Following are some of its features −

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

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

FHSS and DSSS / CDMA

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

These are of two types.

1. Frequency Hopped Spread Spectrum FHSS
2. Direct Sequence Spread Spectrum DSSS
3. Frequency Hopped Spread Spectrum FHSS

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

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

Direct Sequence Spread Spectrum DSSS

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

Comparison between FHSS and DSSS/CDMA

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

Advantages of Spread Spectrum

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

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

FHSS	DSSS / CDMA
Multiple frequencies are used	Single frequency is used

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

CELLULAR SYSTEM

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

Features of Cellular Systems

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

Offer very high capacity in a limited spectrum. Reuse of radio channel in different cells.

Enable a fixed number of channels to serve an arbitrarily large number of users by reusing the channel throughout the coverage region.

Communication is always between mobile and base station (not directly between mobiles).

Each cellular base station is allocated a group of radio channels within a small geographic area called a cell.Neighboring cells are assigned different channel groups.

By limiting the coverage area to within the boundary of the cell, the channel groups may be reused to cover different cells. Keep interference levels within tolerable limits.

Frequency reuse or frequency planning. Organization of Wireless Cellular Network.

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

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

The shape of cells can be either square or hexagon –Square

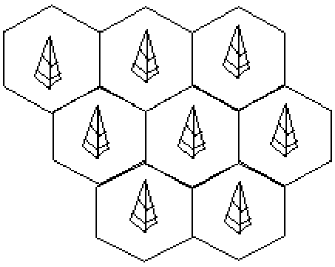
A square cell has four neighbors at distance d and four at distance Root 2 dBetter if all adjacent antennas equidistant

Simplifies choosing and switching to new antennaHexagon

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

Provides equidistant antennas

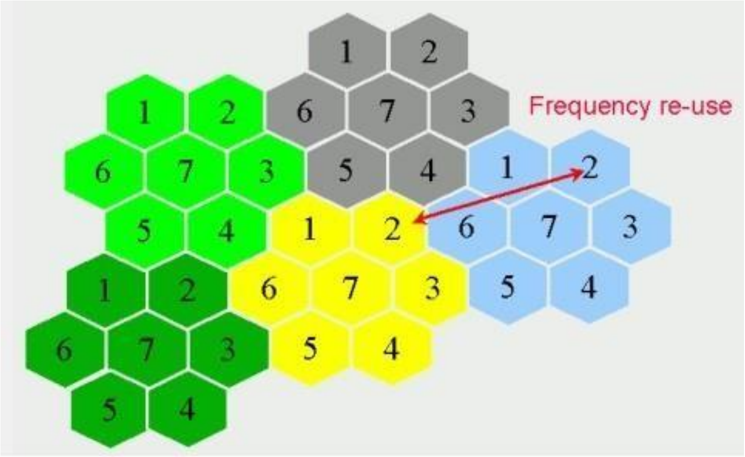
Distance from center to vertex equals length of side



Frequency Reuse

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

Frequency reuse offers the following benefits −



Allows communications within cell on a given frequencyLimits escaping power to adjacent cells

Allows re-use of frequencies in nearby cells

Uses same frequency for multiple conversations10 to 50 frequencies per cell

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

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

****

Chapter-4
MEDIUM ACCESS CONTROL

Introduction

Hidden/ Exposed Terminals

The basic Access Method

Near / Far Terminals

SDMA, FDMA,TDMA, CDMA

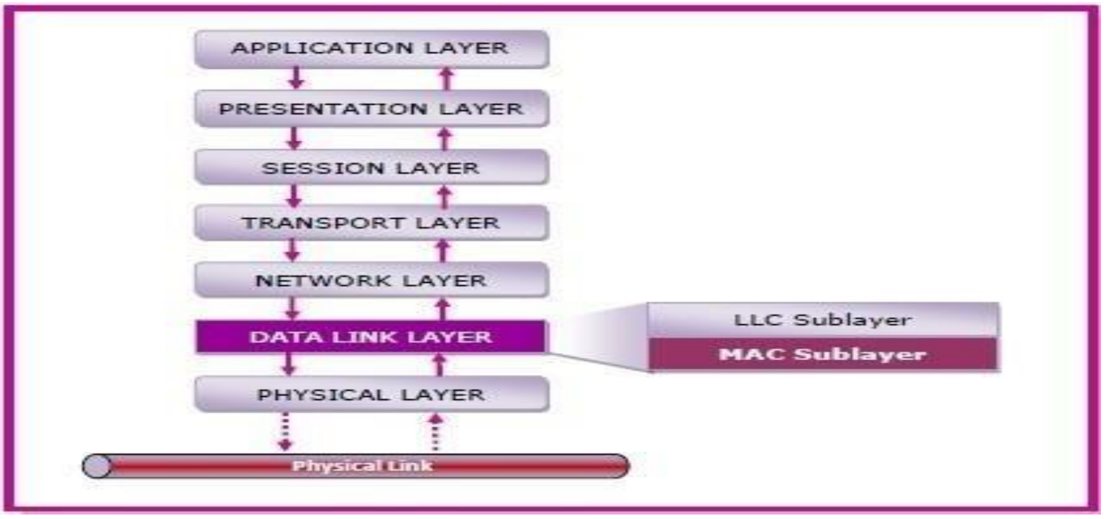
INTRODUCTION

A media access control is a network data transfer policy that determines how data is transmitted between two computer terminals through a network cable.

Or

The medium access control (MAC) is a sublayer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels. It sends data over the network interface card.

The following diagram depicts the position of the MAC layer –



Functions of MAC Layer

It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network.

It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.

It resolves the addressing of source station as well as the destination station, or groups of destination stations.

It performs multiple access resolutions when more than one data frame is to be transmitted. It determines the channel access methods for transmission.

It also performs collision resolution and initiating retransmission in case of collisions.

It generates the frame check sequences and thus contributes to protection against transmission errors.

MAC Addresses

MAC address or media access control address is a unique identifier allotted to a network interface controller (NIC) of a device. It is used as a network address for data transmission within a network segment like Ethernet, Wi-Fi, and Bluetooth.

MAC address is assigned to a network adapter at the time of manufacturing. It is hardwired or hard-coded in the network interface card (NIC). A MAC address comprises of six groups of two hexadecimal digits, separated by hyphens, colons, or no separators. An example of a MAC address is 00:0A:89:5B:F0:11.

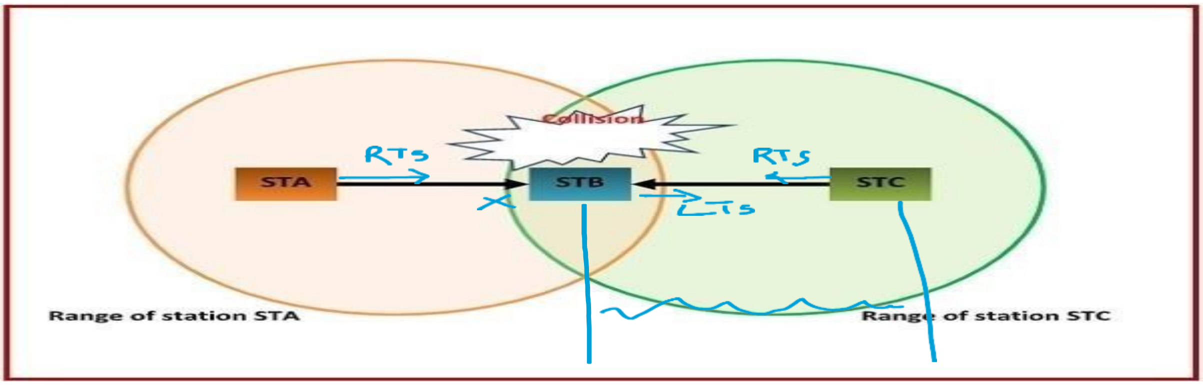
HIDDEN/ EXPOSED
TERMINALS HIDDEN
TERMINALS

In wireless LANs (wireless local area networks), the hidden terminal problem is a transmission problem that arises when two or more stations who are out of range of each other transmit simultaneously to a common recipient. This is prevalent in decentralised systems where there aren't any entity for controlling transmissions. This occurs when a station is visible from a wireless access point (AP), but is hidden from other stations that communicate with the AP.

Problem Illustration

Suppose that there are three stations labelled STA, STB, and STC, where STA and STC are transmitting while STB is receiving. The stations are in a configuration such that the two transmitters STA and STC are not in the radio range of each other. This is shown in the following figure –

•



The above diagram shows that station STA starts transmitting to station STB. Since station STC is out of radio range of STA, it perceives that the channel is free and starts transmitting to STB. The frames received by STC are garbled and collision occurs. This situation is known as the hidden terminal problem.

Solution

The exposed terminal problem is solved by the MAC (medium access control) layer protocol IEEE 802.11 RTS/CTS, with the condition that the stations are synchronized and frame sizes and data speed are the same. RTS stands for Request to Send andCTS stands for Clear to Send.

A transmitting station sends a RTS frame to the receiving station. The receiving station replies by sending a CTS frame. On receipt of CTS frame, the transmitting station begins transmission.

Any station hearing the RTS is close to the transmitting station and remains silent long enough for the CTS. Any station hearingthe CTS is close to the receiving station and remains silent during the data transmission.

In the above example, station STC hears does not hear RTS from station STA, but hears CTS frame from station STB. So, it understands that STB is busy defers its transmission thus avoiding collision.

EXPOSED TERMINALS

In wireless LANs (wireless local area networks), the exposed terminal problem is a transmission problem that arises when a transmitting station is prevented from sending frames due to interference with another transmitting station. This is prevalent in decentralised systems where there aren't any entity for controlling transmissions. This occurs when a station is visible from a wireless access point (AP), but not from other stations that communicate with the AP.

A transmitting station sends a RTS frame to the receiving station.The receiving station replies by sending a CTS frame. On receipt of CTS frame, the transmitting station begins transmission.

Any station hearing the RTS is close to the transmitting station and remains silent long enough for the CTS. Any station hearingthe CTS is close to the receiving station and remains silent during the data transmission.

In the above example, station STC hears RTS from station STB, but does not hear CTS from station STA. So, it is free to transmitto station STD.

NEAR AND FAR TERMINALS

The near–far problem or hearability problem is the effect of a strong signal from a near signal source in making it hard for a receiver to hear a weaker signal from a further source due to adjacent-channel interference, co-channel interference, distortion, capture effect, dynamic range limitation,etc. Such a situation is common in wireless communication systems, in particular CDMA.

SDMA, FDMA,TDMA, CDMA

SPACE DIVISION MULTIPLE ACCESS (SDMA)

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

All users can communicate at the same time using the same channel.SDMA is completely free from interference.

A single satellite can communicate with more satellites receivers of the same frequency.

The directional spot-beam antennas are used and hence the base station in SDMA, can track a moving user.Controls the radiated energy for each user in space.

SDMA is always used in combination with other scheme and not individually.

FREQUENCY DIVISION MULTIPLE ACCESS (FDMA)

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

FDMA allots a different sub-band of frequency to each different user to access the network.

If FDMA is not in use, the channel is left idle instead of allotting to the other users.FDMA is implemented in Narrowband systems and it is less complex than TDMA. Tight filtering is done here to reduce adjacent channel interference.

The base station BS and mobile station MS, transmit and receive simultaneously and continuously in FDMA.

TIME DIVISION MULTIPLE ACCESS (TDMA)

In the cases where continuous transmission is not required, there TDMA is used instead of FDMA. The features of TDMA include the following.TDMA shares a single carrier frequency with several users where each users makes use of non-overlapping time slots.

Data transmission in TDMA is not continuous, but occurs in bursts. Hence handsoff process is simpler. TDMA uses different time slots for transmission and reception thus duplexers are not required.

TDMA has an advantage that is possible to allocate different numbers of time slots per frame to different users.

Bandwidth can be supplied on demand to different users by concatenating or reassigning time slot based on priority.

CODE DIVISION MULTIPLE ACCESS (CDMA)

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

In CDMA every user uses the full available spectrum instead of getting allotted by separate frequency.CDMA is much recommended for voice and data communications.

While multiple codes occupy the same channel in CDMA, the users having same code can communicate with each other.

CDMA offers more air-space capacity than TDMA.

The hands-off between base stations is very well handled by CDMA.

****

Chapter-5

WIRELESS LANS Wireless LAN and communication

Infrared
Radio Frequency
IR Advantages and Disadvantages RF Advantages and Disadvantages
Wireless Network Architecture
LogicalType of WLAN
IEEE 802.11
MAC layer
Security
Synchroniza
tion
Power
Management
Roaming
Bluetooth Overview

WIRELESS LAN AND COMMUNICATION

Wireless Communication is a method of transmitting information from one point to other, without using any connection like wires, cables or any physical medium.

What is WLAN???

A wireless local area network(LAN) is a flexible data communications system implemented as an extension to, or as an alternative for, a wired LAN.Using radio frequency (RF) technology, wireless LANs transmit and receive data over the air, minimizing the need for wired connections.

Thus, combining data connectivity with user mobility.

Advantages of WLAN

- Productivity, convenience, and cost advantages
- Installation speed and simplicity.
- Installation flexibility.
- Reduced cost-of-ownership.
- Mobility.
- Scalability.

Disadvantages of WLAN

- Cost
- Wireless network cards cost 4 times more than wired network cards.
- The access points are more expensive than hubs and wires.
- Signal Bleed Over
- Access points pick up the signals of adjacent access points or overpower their signal.
- Environmental Conditions
- Susceptible to weather and solar activity.
- Constrained by buildings, trees, terrain.
- Less Capacity

- Slower bandwidth.
- Limit to how much data a carrier wave can transmit without lost packets impacting performance.

Wireless LAN Applications

Medical Professionals

Corporate

Education

Temporary Situations

Airlines

Security Staff

Emergency Centers

INFRARED COMMUNICATION (IR)

This is one of the earliest types of optical communication and is still very much in use today. It is found in remote controls for televisions, dvd players and most other entertainment devices.Dimmer lights and other facilities can be also be controlled using infrared. Infrared uses light that is invisible to us and is just above the red end of the colour spectrum.The key component of an infrared system is an infrared LED (Light Emitting Diode) to emit the light and a photo- diode in the television or equipment to receive the light.A digital code within the controller switches the light on and off, this is then picked up as a digital code at the other end. The communication standard is called 'IrDA' short for Infrared Digital Association and it allows wire-less communication between Mouse, keyboard, joysticks, gamepads etc and receiving equipment such as PC, Laptop, game console.Bandwidth is normally quite modest, around 115.2 kbps (IrDA serial infrared standard). Although IrDA does define a fast data transfer standard of up to 14 Mbps, this is rarely used.IR works only up to about 10 metres but that is fine for the type of applications it is mainly used for. It will only work line-of-sight.Technologies such as Bluetooth has largely supplanted infrared as a communication method for mobiles and computers.

5.4 IR ADVANTAGES AND DISADVANTAGES

Advantages	Disadvantages
Inexpensive compared to other technologies	Only works line-of-sight
Works over a moderate bandwidth 115 kbps	Short range - a few metres
Works well over a short distance	Low bandwidth

5.3 RADIO FREQUENCY

RF is the short form of radio frequency. RF is used in wireless communications of every kind. The medium of communication is popularly called as RF wave similar to cable for wired communication.

It is all around us when we use cell phone, when we use Bluetooth device, when we use remote control, when we watch TV, when we listen radio, when we USE microwave oven. It has many applications and day by day it is increasing.

The unit of radio frequency is Hertz (Hz) i.e. no of oscillations or cycles per second. There is one more term which is often used interchangeably to mention RF and is called 'wavelength'. The relationship between wavelength and radio frequency is mentioned below.

Wavelength=C/Frequency,

Where C is the speed of light and is 3 x 10^8 meter/second.

Radio frequency is allocated and administered by FCC (Federal Communications Commission) and many such frequencies will form electromagnetic spectrum. This spectrum is labeled with different names as below.

Designation	Frequency Range
Extremely Low Frequency (ELF)	3-30Hz
Super Low Frequency (SLF)	30-300Hz

Ultra Low Frequency (ULF)	300-3000Hz
Very Low Frequency (VLF)	3-30 KHz
Low Frequency (LF)	30-300 KHz
Medium Frequency (MF)	300KHz-3 MHz
High Frequency (HF)	3-30 MHz
Very High Frequency (VHF)	30 MHz-300 MHz
Ultra High Frequency (UHF)	300 MHz-3 GHz
Super High Frequency (SHF)	3-30 GHz
Extremely High Frequency (EHF)	30-300 GHz

Note:1000Hz=1KHz, 1000KHz=1MHz, 1000MHz=1GHz

The device which receives and transmits this radio frequency (RF) is called as antenna which everyone is familiar. There are different antennas designed to transmit and receive different RF frequencies as mentioned in the table.

RF ADVANTAGES AND DISADVANTAGES

Advantages of RF

Following are the advantages of RF:

=>It has different penetration through the walls of the buildings or houses based on the frequency. Hence used for radio and television transmission and for cellular mobile phone service.

=>Used in various medical applications. It is used in Diathermy instrument for surgery. It is used in MRI for taking images of human body. It is also used for skin tightening.

=>It is used in radar for object detection.

=>It is used for satellite communication.

=>It is used in microwave line of sight communication system.

Disadvantages of RF

Following are the disadvantages of RF:

=>Uncontrolled radiation of RF affects pre-adolescent childrens, pregnant women, elderly humans, patients with pace makers, small birds, flora and fauna, small insects etc.

=>The areas near RF cellular towers have been observed with more lightening compare to other areas.

=>It also affects some of the fruits grown near the RF tower areas.

=>As RF waves are available both in LOS and non LOS regions of transmitter, it can be easily intruded by the hackers and crucial personal/official data can be decoded for malicious motives. In order to avoid this situation, radio frequency wave based transmission is used with highly secured algorithms such as AES, WEP, WPA etc. RF signal can also be modulated either using frequency hopping or spread spectrum techniques to avoid this kind of eavesdropping.

WIRELESS NETWORK ARCHITECTURE LOGICAL

IEEE 802.11 Architecture

The components of an IEEE 802.11 architecture are as follows –

Stations (STA) − Stations comprises of all devices and equipment that are connected to the wireless LAN. A station can be oftwo types−

Wireless Access Point (WAP) − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.

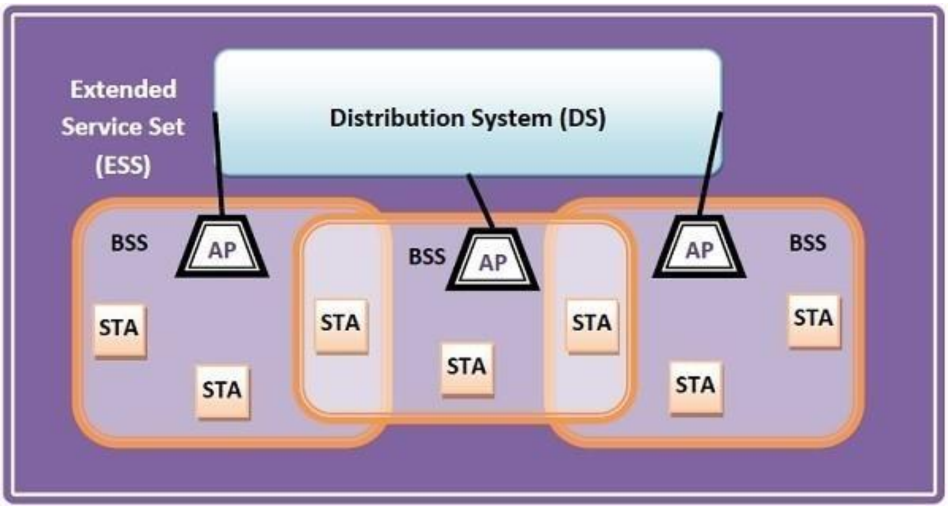
Client. Clients are workstations, computers, laptops, printers, smartphones, etc.Each station has a wireless network interface controller.

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

Infrastructure BSS − Here, the devices communicate with other devices through access points. Independent BSS − Here, the devices communicate in a peer-to-peer basis in an ad hoc manner.Extended Service Set (ESS) − It is a set of all connected BSS.

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

Portal- Logical entity where 802.11 network integrates with a non 802.11 network.



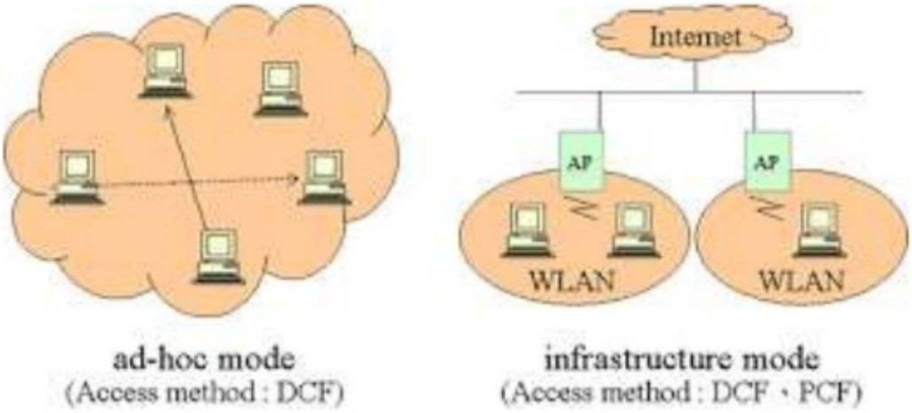
Types of WLAN

IEEE 802.11 Infrastructure

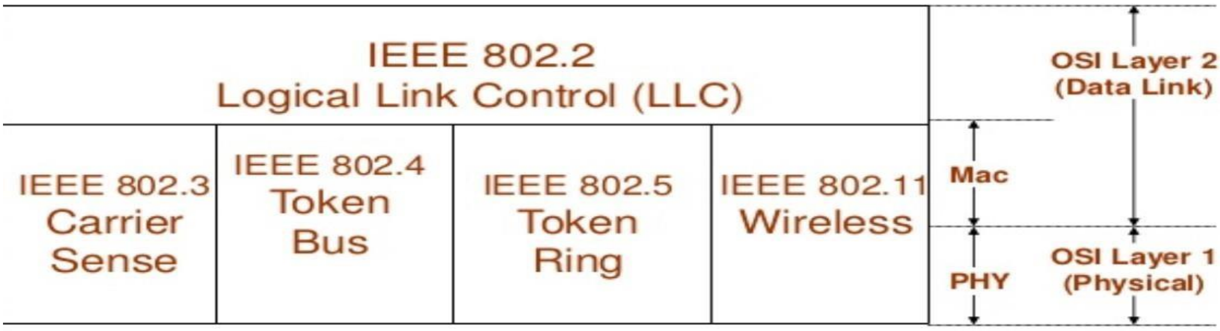
802.11 networks can be used in two modes: Infrastructure and Ad hoc Mode Infrastructure mode requires a central access point that all devices connect to.

Ad-hoc mode is also known as "peer-to-peer" mode. Ad-hoc networks don't require a centralized access point. Instead, devices on the wireless network connect directly to each other.

WLAN Topology Ad-Hoc Network and WLAN Topology Infrastructure



In infrastructure mode, each station computer (STA for short) connects to an access point via a wireless link. The set-up formed by the access point and the stations located within its coverage area are called the basic service set, or BSS for short. They form one cell.



Each BSS is identified by a BSSID, a 6-byte (48-bite) identifier. In infrastructure mode, the BSSID corresponds to the access point's MAC address.

- It is possible to link several access points together (or more precisely several BSS's) using a connection called a distribution system (DS for short) in order to form an extended service set or ESS. The distribution system can also be a wired network, a cable between two access points or even a wireless network.
- An ESS is identified with an ESSID (Extended Service Set Identifier), a 32-character identifier (in ASCII format) which acts as its name on the network. The ESSID, often shortened to SSID, shows the network's name, and in a way acts a firstlevel security measure, since it is necessary for a station to know the SSIDin order to connect to the extended network.
- In ad hoc mode, wireless client machines connect to one another in order to form a peer-to-peer network,i.e. a network in which every machine acts as both a client and an access point at the same time.
- The set-up formed by the stations is called the independent basic service set, or IBSS for short. An IBSS is a wireless network which has at least two stations and uses no access point. The IBSS therefore forms a temporary network which lets people in the same room exchange data. It is identified by an SSID, just like an ESS in infrastructure mode. In an ad hoc network, the range of the independent BSS is determined by each station's range. That means that if two of the stations on the network areoutside each other's range,they will not be able to communicate, even if they can "see" other stations. Unlike infrastructure mode, ad hoc mode has no distribution system that can send data frames from one station to another. An IBSS, then, is by definition a restricted wireless network.

5.8 IEEE 802.11

Wireless LAN Standard

In response to lacking standards, IEEE developed the first internationally recognized wireless LAN standard – IEEE 802.11 .IEEE published 802.11 in 1997, after seven years of work

Scope of IEEE 802.11 is limited to Physical and Data Link Layers.

IEEE 802.11 standard, popularly known as WiFi, lays down the architecture and specifications of wireless LANs (WLANs). WiFi or WLAN uses high frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage.

IEEE 802 LAN Standards Family:

MAC layer:

The 802.11 MAC sublayer provides an abstraction of the physical layer to the logical link control sublayer and upper layers of the OSI network. It is responsible for encapsulating frames and describing frame formats.

MAC Sublayer Frame Format of IEEE 802.11:

The main fields of a frame of wireless LANs as laid down by IEEE 802.11 are −

Frame Control − It is a 2 bytes starting field composed of 11 subfields. It contains control information of the frame.

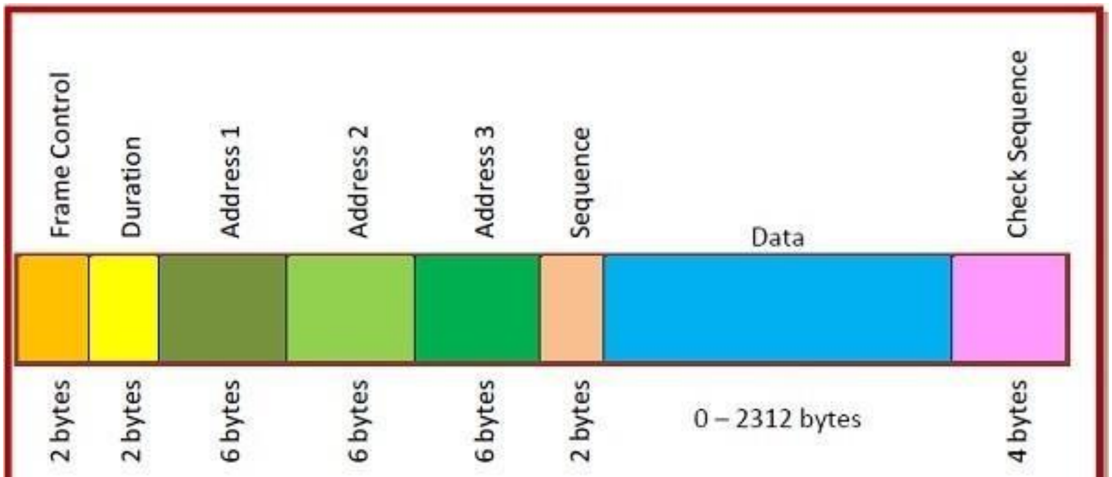
Duration − It is a 2-byte field that specifies the time period for which the frame and its acknowledgment occupy the channel.

Address fields − There are three 6-byte address fields containing addresses of source, immediate destination, and final endpoint respectively.

Sequence − It a 2 bytes field that stores the frame numbers.

Data − This is a variable-sized field that carries the data from the upper layers. The maximum size of the data field is 2312 bytes.

Check Sequence – It is a 4-byte field containing error detection information.



IEEE 802.11 Frame Format

Avoidance of Collisions by 802.11 MAC Sublayer

In wireless systems, the method of collision detection does not work. It uses a protocol calledcarrier sense multiple access with collision avoidance (CSMA/CA).

The method of CSMA/CA is –

When a frame is ready, the transmitting station checks whether the channel is idle or busy.If the channel is busy, the station waits until the channel becomes idle.

If the channel is idle, the station waits for an Inter-frame gap (IFG) amount of time and then sends the frame.After sending the frame, it sets a timer.

The station then waits for acknowledgement from the receiver. If it receives the acknowledgement before expiry of timer, it marks a successful transmission.

Otherwise, it waits for a back-off time period and restarts the algorithm.Co-ordination Functions in 802.11 MAC Sublayer

IEEE 802.11 MAC Sublayer uses two co-ordination functions for collision avoidance before transmission –

Distributed Coordination Function (DCF) –

It is a mandatory function used in CSMA/CA.

It is used in distributed contention-based channel access.

It is deployed in both Infrastructure BSS (basic service set) as well as Independent BSS.Point Coordination Function (PCF) –

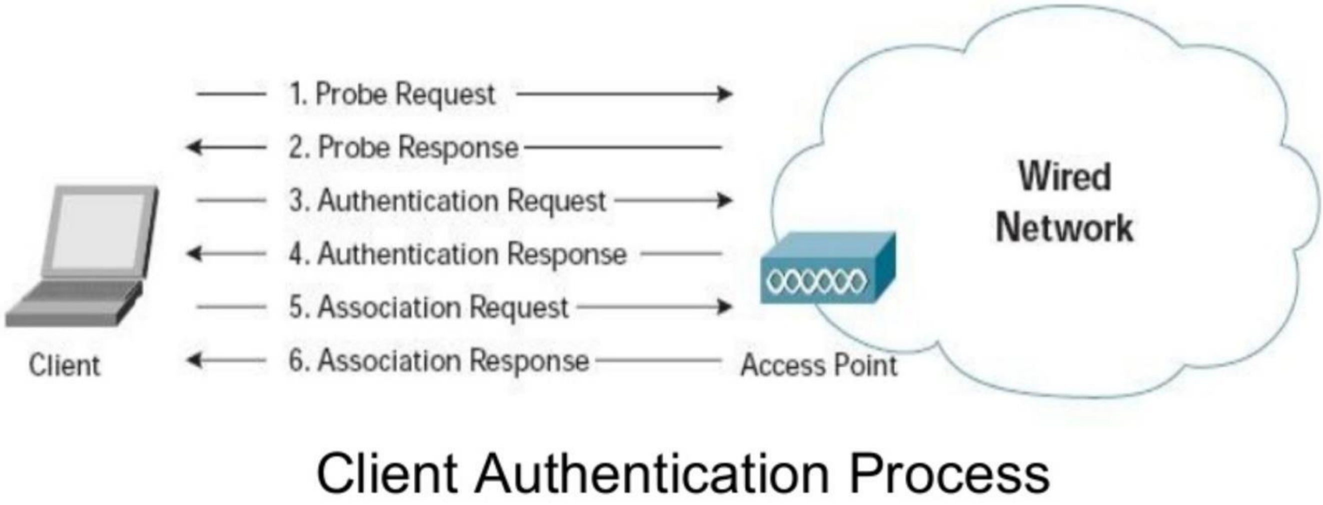
It is an optional function used by 802.11 MAC Sublayer. It is used in centralized contention-free channel access. It is deployed in Infrastructure BSS only.

IEEE 802.11 standard, popularly known as WiFi, lays down the architecture and specifications of wireless LANs (WLANs). WiFi or WLAN uses high-frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage.

SECURITY

Wireless local area network security (WLAN security) is a security system designed to protect networks from the security breaches(/leakage) to which wireless transmissions are susceptible. This type of security is necessary because WLAN signals have no physical boundary limitations, and are prone to illegitimate access over network resources, resulting in the vulnerability of private and confidential data. Network operations and availability can also be compromised in case of a WLAN security breach. To address these issues, various authentications, encryption, invisibility and other administrative controlling techniques are used in WLANs. Business and corporate WLANs in particular require adequate security measures to detect, prevent and block piggy backers, eavesdroppers and other intruders.

Security has remained a major concern in WLANs around the globe. While wireless networks provide convenience and flexibility, they also increase network vulnerability. Security threats such as unauthorized access, denial of service attacks, IP and MAC spoofing, session hijacking and eavesdropping can all be problems for WLANs. To counter these threats, various standard authentication and encryption techniques are combined with other access control mechanisms. These protocols, devices and techniques collectively secure the WLAN a level that equals and even exceeds wired LAN security.



Some of the technologies employed in WLAN security include:

Wired Equivalent Privacy (WEP): An old encryption standard used to overcome security threats. WEP provides security to WLAN by encrypting the information transmitted over the air so that only the receivers with the correct encryption key can decrypt the information.

WPA/WPA2 (WI-FI Protected Access): Improved on WEP by introducing Temporal Key Integrity Protocol (TKIP). While still using RC4 encryption, TKIP uses a temporal encryption key that is regularly renewed, making it more difficult to steal. In addition, data integrity was improved through the use of a more robust hashing mechanism.

Wireless Intrusion Prevention Systems/Intrusion Detection Systems: Intrusion detection and prevention focuses on radio frequency (RF) levels. This involves radio scanning to detect rogue access points or ad hoc networks to regulate network access. Advanced implementations are able to visually represent the network area along with potential threats, and have automatic classification capabilities so that threats can be easily identified.

SYNCHRONIZATION:

Timing synchronization function (TSF) is specified in IEEE 802.11 wireless local area network (WLAN) standard to fulfill timing synchronization among users. A TSF keeps the timers for all stations in the same basic service set (BSS) synchronized. All stations shall maintain a local TSF timer. Each mobile host maintains a TSF timer with modulus 264 counting in increments of microseconds. The TSF
is based on a 1-MHz clock and "ticks" in microseconds. On a commercial level, industry vendors assume the 802.11 TSF's synchronization to be within 25 microseconds.

Timing synchronization is achieved by stations periodically exchanging timing information through beacon frames. In (infra) BSS, the AP sends the TSF information in the beacons. In Independent Basic Service Set (IBSS, ad-hoc), each station competes to send the beacon.

Each station maintains a TSF timer counting in increments of microseconds (µs). Stations adopt a received timing if it is later than the station’s own TSF timer.

POWER MANAGEMENT

Power management is the feature that turns off the power or switches the system to a low power state when inactive.The basic idea to save power in WLAN is to switch off the transceiver whenever it is not needed.

Power management in infrastructure based network:

In infrastructure based network, an access point is responsible for the power management.Access point buffers data packet for all sleeping station.

Access point transmits a Traffic Indication Map (TIM) with a beacon frame.TIM consists of a list of destination of buffered data.

Additionally, the access point also maintains a Delivery Traffic Indication Map(DTIM)interval.

DTIM is used for sending broadcast/multicast frames. The DTIM interval is always a multiple of TIM interval. All station wakes up prior to an expected TIM and DTIM. Power management in Ad-hoc network

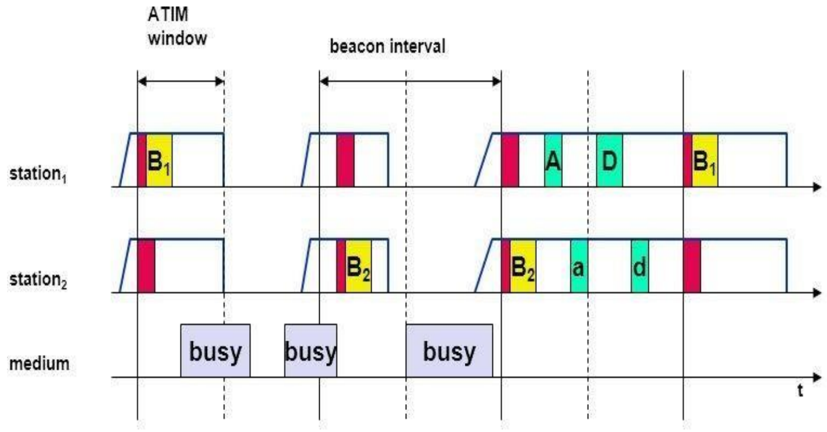
In ad-hoc network, each station buffers data packet that it wants to send to power saving station.

There is no access point.

In Ad-hoc network, all station announces a list of buffered frame during a period when they are all awake.

All station announce destination for which packets are buffered using Ad-hoc Traffic Indication Map (ATIM) during the ATM interval.

Figure shows Power Management in IEEE 802.11 Ad-hoc Network.



ROAMING:

Roaming refers to the ability for a cellular customer to automatically make and receive voice calls, send and receive data, or access other services, including home data services, when travelling outside the geographical coverage area of the home network, by means of using a visited network.

When a roaming user goes from one BSS to another while moving within the ESS, his or her machine's wireless network adapter is able to switch access points depending on the quality of the signal it receives from different access points. Access points communicate with one another using a distribution system in order to trade information about the stations and, if necessary, to transmit data from mobile stations. This feature which lets stations move "transparently" from one access point to another is called roaming.

BLUETOOTH OVERVIEW:

- Bluetooth technology is a short-range wireless communications technology to replace the cables connecting electronic devices, allowing a person to have a phone conversation via a headset, use a wireless mouse and synchronize information from a mobile phone to a PC, all using the same core system.

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

History of Bluetooth

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

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

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

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

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

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

- Bluetooth offers a uniform structure for a wide range of devices to connect and communicate with each other.

- Bluetooth technology has achieved global acceptance such that any Bluetooth enabled device, almost everywhere in the world, can be connected with Bluetooth enabled devices.

- Low power consumption of Bluetooth technology and an offered range of up to ten meters has paved the way for several usage models.

Bluetooth offers interactive conference by establishing an adhoc network of laptops.

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

Piconets and Scatternets:

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

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

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

The features of Piconets are as follows –

- Within a Piconet, the timing of various devices and the frequency hopping sequence of individual devices is determined by the clock and unique 48-bit address of master.

- Each device can communicate simultaneously with up to seven other devices within a single Piconet.

- Each device can communicate with several piconets simultaneously.

- Piconets are established dynamically and automatically as Bluetooth enabled devices enter and leave piconets.

- There is no direct connection between the slaves and all the connections are essentially master- to-slave or slave-to- master.Slaves are allowed to transmit once these have been polled by the master.Transmission starts in the slave-to-master time slot immediately following a polling packet from the master.A device can be a member of two or more piconets, jumping from one piconet to another by adjusting the transmission regime-timing and frequency hopping sequence dictated by the master device of the second piconet.

- It can be a slave in one piconet and master in another. It however cannot be a master in more than once piconet.

- Devices resident in adjacent piconets provide a bridge to support inner-piconet connections, allowing assemblies of linked piconets to form a physically extensible communication infrastructure known as Scatternet.

Spectrum:

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

Range:

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

Data rate:

- Bluetooth supports 1Mbps data rate for version 1.2 and 3Mbps data rate for Version 2.0 combined with Error Data Rate.

****

Chapter-6
UBIQUITOUS WIRELESS
COMMUNICATION

Mobile Communication Generations 1G to
3G 3rd Generation Mobile Communication
Network
Universal Mobile telecommunication System (UMTS)

INTRODUCTION:

Ubiquitous networking, also known as pervasive networking, is the distribution of communications infrastructure and wireless technologies throughout the environment to enable continuous connectivity.

Ubiquitous applications need to access relevant remote external information and tasks, anywhere and anytime.

Different applications require different combinations of network functions and services, e.g., data streaming, minimal jitter, specific media access control etc.

Different networks support different sets of communication functions in different ways.

SCENARIO OF MOBILE COMMUNICATION:

In order to tackle these challenges and target the right enabling technology components, the following five scenarios have been specified:

“Amazingly fast” focuses on providing very high data-rates for future mobile broadband users so as to experience instantaneous connectivity without delays.

“Great service in a crowd” focuses on providing reasonable mobile broadband experiences even in crowded areas such as stadiums, concerts or shopping malls.

“Best experience follows you” focuses on providing end-users on the move, e.g. in cars or trains, with high levels of service experience.

“Super real-time and reliable connections” focuses on new applications and use cases with very strict requirements on latency and reliability.

“Ubiquitous things communicating” focuses on the efficient handling of a very large number of devices (including e.g. machinetype of devices, and sensors) with widely varying requirements.

MOBILE COMMUNICATION GENERATIONS 1G TO 3G:

Since the introduction of first commercial mobile phone in 1983 by Motorola, mobile technology has come a long way. Be it technology, protocols, services offered or speed, the changes in mobile telephony have been recorded as generation of mobilecommunication. Here we will discuss the basic features of these generations that differentiate it from the previous generations.

1G Technology:

1G refers to the first generation of wireless mobile communication where analog signals were used to transmit data. It was introduced in the US in early 1980s and designed exclusively for voice communication. Some characteristics of 1G communication are –

Speeds up to 2.4
kbps Poor voice
quality
Large phones with limited
battery lifeNo data security

2G Technology:

2G refers to the second generation of mobile telephony which used digital signals for the first time. It was launched in Finland in1991 and used GSM technology. Some prominent characteristics of 2G communication are -

Data speeds up to 64 kbps
Text and multimedia messaging possible

Better quality than 1G

When GPRS technology was introduced, it enabled web browsing, e-mail services and fast upload/download speeds. 2G with GPRS is also referred as 2.5G, a step short of next mobile generation.

3G Technology:

Third generation (3G) of mobile telephony began with the start of the new millennium and offered major advancement over previous generations. Some of the characteristics of this generation are −

Data speeds of 144 kbps to 2 Mbps High speed web browsing

Running web based applications like video conferencing, multimedia e-mails, etc.Fast and easy transfer of audio and video files

3D gaming

Every coin has two sides. Here are some downsides of 3G technology −Expensive mobile phones

High infrastructure costs like licensing fees and mobile towers Trained personnel required for infrastructure set up

The intermediate generation, 3.5G grouped together dissimilar mobile telephony and data technologies and paved way for thenext generation of mobile communication.

3RD GENERATION MOBILE COMMUNICATION NETWORK:

Third generation mobile phones, or "3G Internet" mobile phones, is a set of standards for wireless mobile communication systems, that promises to deliver quality multimedia services along with high quality voice transmission.

Features

3G systems comply with the International Mobile Telecommunications-2000 (IMT- 2000) specifications by the International Telecommunication Union (ITU).

The first 3G services were available in 1998.

It provides high speed transmission having data transfer rate more than 0.2Mbps.

Global roaming services are available for both voice and data.

It offers advanced multimedia access like playing music, viewing videos, television services etc.

It provides access to all advanced Internet services, for example surfing webpages with audio and video.

It paved the way for the increased usage of smartphones with wide screens as they provided better viewing of mobile webpages, videos and mobile televisions.

Specifications for 3G:

3G specifications are laid down by two groups, 3GPP and 3GPP2.

3GPP (Third Generation Partnership Project) − These specifications are based upon Global System for Mobile (GSM) communications, and are known as Universal Mobile Telecommunications Systems (UMTS). The technologies are :

Universal Terrestrial Radio Access (UTRA) General Packet Radio Service (GPRS)

Enhanced Data rates for GSM Evolution (EDGE)

3GPP2 − These specifications are based upon Code Division Multiple Access (CDMA). Two main specifications under this are −Wideband CDMA (WCDMA)

CDMA2000:

Areas of Application

Wireless voice telephony

Fixed wireless Internet access Mobile Internet access

Video calls

Video
conferencing
Tele-medicine
Global Positioning System
(GPS) Location-based
services

UNIVERSAL MOBILE TELECOMMUNICATION SYSTEM (UMTS):

The Universal Mobile Telecommunications System (UMTS) is a broadband, packet- based, 3G mobile cellular system based upon GSM standards. The specifications of UMTS covers the entire network system, including the radio access network, the core network and user authentication.

Features

UMTS is a component of IMT-2000 standard of the International Telecommunications Union (ITU), developed by 3GPP. It uses wideband code division multiple access (W-CDMA) air interface.
It provides transmission of text, digitized voice, video and multimedia.It provides high bandwidth to mobile operators.

It gives a high data rate of 2Mbps. For High-Speed Downlink Packet Access (HSDPA) handsets, the data-rate is as high as 7.2 Mbps in the downlink connection.
It is also known as Freedom of Mobile Multimedia Access (FOMA).
It encompasses specifications for the entire mobile network system −
Radio access network specified by UTRAN (UMTS Terrestrial Radio Access Network)Core network specified by MAP (Mobile Application Part)

****

CHAPTER 8
WORLD WIDE WEB ARCHITECTURE

The WWW architecture provides a very flexible and powerful programming model. Applications and content are presented in standard data formats, and are browsed by applications known as web browsers. The web browser is a networked application, i.e., it sends requests for named data objects to a network server and the network server responds with the data encoded using the standard formats.

The WWW standards specify many of the mechanisms necessary to build a general-purpose application environment.All servers and content on the WWW are named with-an Internet-standard Uniform Resource Locator (URL). All content on the WWW is given specific type thereby allowing web browsers to correctly process the content based on its type. All web browsers support a set of standard content formats. These include the Hyper Text Mark up Language (HTML) scripting languages (JavaScript) and a large number of other formats. Standard networking protocols allow any web browser To communicate with any web server. The most commonly used protocol on the WWW is the Hyper Text Transport Protocol (HTTP), operating on top of the TCP/IP protocol Suite.

NEED OF WAP

THE WIRELESS APPLICATION PROTOCOL (WAP) One obvious approach for such a common platform seems to be the Internet. The prevailed communication protocol in the Internet is TCP/IP, which offers a unified interface for transmitting data, independent of the underlying network. This idea has several advantages: All Internet-based applications such as WWW or e- mail can be used, and the integration of new applications is very easy by using TCP/IP, e.g., telephony via Internet using Voice over IP [V5]. However, using the Internet has one main disadvantage: The protocols for communication are optimised for fixed networks with high reliability and low error rates. In mobile environments, this property is very disadvantageous and affects the behaviour of applications in several negative ways:

- TCP/IP works very ineffective in wireless environments. IP is based on a hierarchical addressing scheme; thus, supporting mobility is hard to achieve. A solution for this problem might be Mobile IP [6]; but the deployment of Mobile IP raises several other problems, e.g. in security support [6]. Compared to fixed networks, wireless links usually have higher delays and frequent transient interruptions. In those cases, TCP supposes congestion on the link and immediately slows down the data rate to its minimum. The slow-start-algorithm implemented in TCP prevents an increase in performance, thus the overall performance is by far lower than technically feasible.

- Security mechanisms in the Internet, such as SSL (Secure Socket Layer), are not sufficient for applications that handle personal information, such as online banking or electronic commerce. Mechanisms for the authentication of mobile devices are not provided, and meanwhile, further less expendable encryption algorithms exist.

- On the higher layers, HTTP that transports WWW content works stateless and does not perform any compression, which blows up the data volume that has to be transmitted. Additionally, HTML used for describing WWW pages contains a lot of information useless for today's mobile devices, such as colourful pictures or java applets. Those disadvantages show the need for an alternative architecture with standardised protocols that are optimised for the use in mobile and wireless environments. Thus, in 1997, the WAP Forum was founded by a few companies in order to create an open, global specification that empowers mobile users with wireless devices to easily access and interact with information and services instantly. This aspect makes it interesting for the use in vehicles. Meanwhile, over 200 companies joined the forum, representing over 90 % of the global handset market, carriers with more than 100 million subscribers, leading infrastructure providers, software developers and other organizations providing solutions to the wireless industry. Figure 2 gives an overview of a typical WAP infrastructure. A mobile device communicates with, e.g., a Web server via a WAP proxy. Thus, a set of new techniques can be used for the wireless network, such as protocols optimised for wireless links, or, as shown in figure 2, the use of the Wireless Markup Language (WML) instead of the unsuitable HTML for describing 4 the information. The WAP proxy is also integrated in the Internet environment, i.e., it can access Web Servers by simply using the Internet protocols, i.e., TCP/IP and HTTP. The basic communication interaction between mobile device and Web Server works in the following way. The mobile device sends an encoded request to the WAP Proxy, which decodes the request and translates it from the WAP protocol stack to the Internet protocol stack. The WAP Proxy passes the new request to the specified Web Server, which sendsthe requested information in a response back to the WAP Proxy. The information will be translated to the WAP protocols, encoded, and finally sent to the mobile device. There are two ways to create WML content. The first is to write raw WML code, which is stored directly on a Web Server. The WAP Proxy downloads this code via HTTP and sends it directly to the mobile device, using the protocols defined in the WAP architecture. Alternatively, the WAP Proxy requests common HTML code, and converts it to WML code using specific filters. From the outset, WAP integrates speech services for telephony using WTA Servers (Wireless Telephony Application). This empowers the WAP architecture as one common platform for supporting voice and data communication and, thus, takes the preceding integration of voice and data services into account.

The WAP Architecture Starting with version 1.0 in 1999, version 1.1 is currently implemented in common mobile devices. Meanwhile, the standardisation of version 1.2 has been finished. Basically, version 1.1 and version 1.2 of WAP describe the same architecture and protocols; version 1.2 can be seen as an extension in order to support more features. The WAP architecture comprises six layers as can be seen in figure 3. The stack on the left hand compares the protocols used in the Internet with the layers of the WAP architecture. One main idea of WAP is the independence of communication protocols from the employed bearer service used for transmitting data. WAP only specifies the adaptation to those different bearers. In WAP 1.2, the adaptation to the following bearers is specified: various GSM services (e.g., GSM-CSD, GSM-GPRS, GSM-SMS, etc.), IS-136, CDPD, CDMA, PDC, iDEN, FLEX and ReFLEX, PHS, DataTAC, TETRA, and DECT. The WAP architecture is open in a way, that services and applications can be implemented using parts of the architecture, or have direct access to the bearer services.

Wireless Application Protocol (WAP) in Mobile Computing:

Wireless Application Protocol or WAP is a programming model or an application environment and set of communication protocols based on the concept of the World Wide Web (WWW), and its hierarchical design is very much similar to TCP/IP protocol stack design. The most prominent features of Wireless Application Protocol or WAP in Mobile Computing:

WAP is a De-Facto standard or a protocol designed for micro-browsers, and it enables the mobile devices to interact, exchange and transmit information over the Internet.

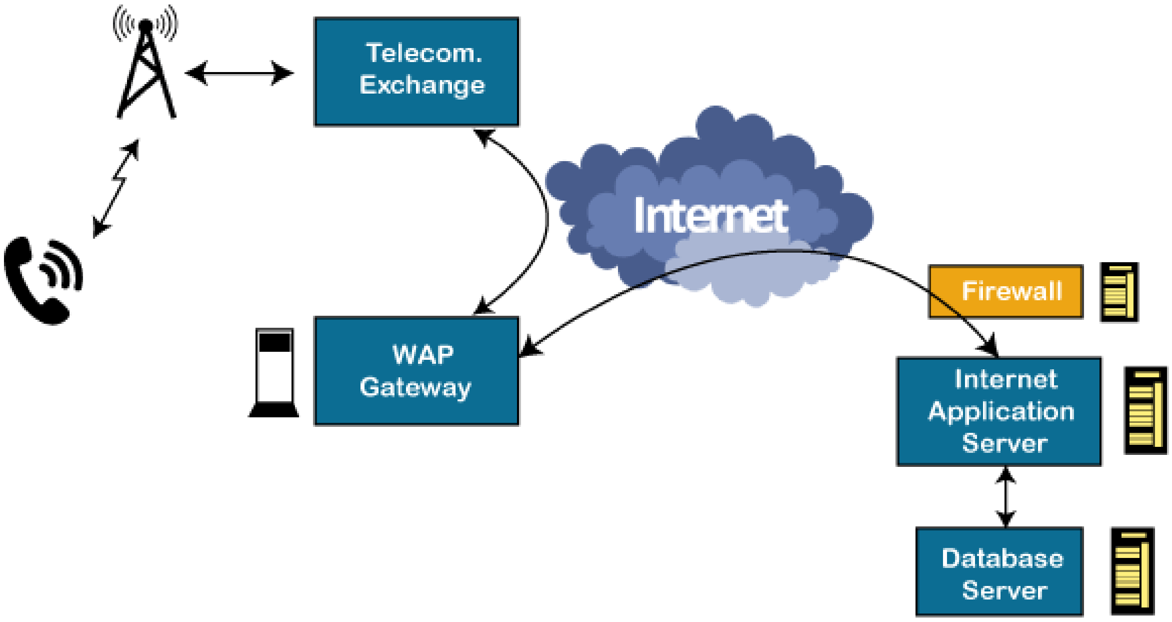
WAP is based upon the concept of the World Wide Web (WWW), and the backend functioning also remains similar to WWW, but it uses the markup language Wireless Markup Language (WML) to access the WAP services while WWW uses HTML as a markup language. WML is defined as XML 1.0 application.

In 1998, some giant IT companies such as Ericson, Motorola, Nokia and Unwired Planet founded the WAP Forum to standardize the various wireless technologies via protocols.

After developing the WAP model, it was accepted as a wireless protocol globally capable of working on multiple wireless technologies such as mobile, printers, pagers, etc.

In 2002, by the joint efforts of the various members of the WAP Forum, it was merged with various other forums of the industry and formed an alliance known as Open Mobile Alliance (OMA).

WAP was opted as a De-Facto standard because of its ability to create web applications for mobile devices.



Working of Wireless Application Protocol or WAP Model:

The following steps define the working of Wireless Application Protocol or WAP Model:

The WAP model consists of 3 levels known as Client, Gateway and Origin Server.

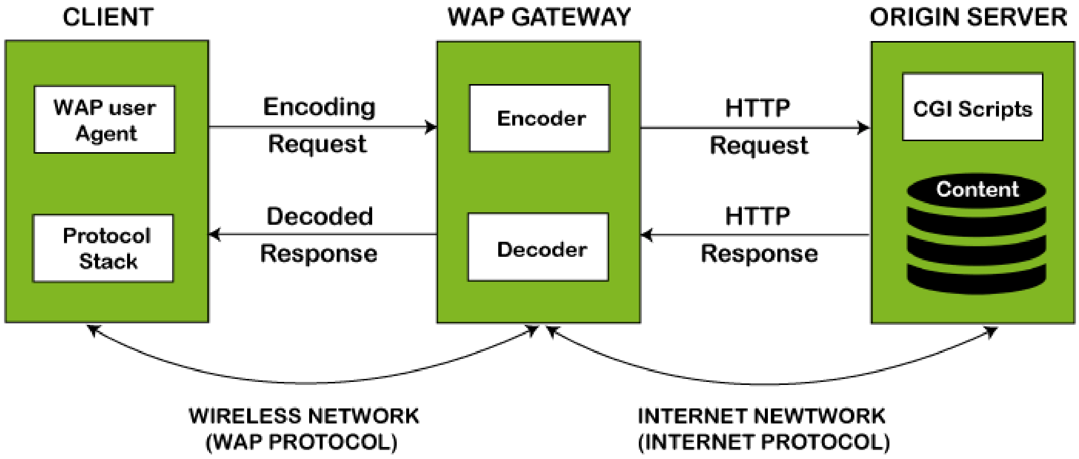
When a user opens the browser in his/her mobile device and selects a website that he/she wants to view, the mobile device sends the URL encoded request via a network to a WAP gateway using WAP protocol.

The request he/she sends via mobile to WAP gateway is called as encoding request.

The sent encoding request is translated through WAP gateway and then forwarded in the form of a conventional HTTP URL request over the Internet.

When the request reaches a specified Web server, the server processes the request just as it would handle any other requestand sends the response back to the mobile device through WAP gateway.

Now, the WML file's final response can be seen in the browser of the mobile users.



Benefits of Wireless Application Protocol (WAP):

Following is a list of some advantages of Wireless Application Protocol or WAP:

WAP is a very fast-paced technology.

It is an open-source technology and completely free of cost.It can be implemented on multiple platforms.

It is independent of network standards. It provides higher controlling options.

It is implemented near to Internet model.

By using WAP, you can send/receive real-time data.

Nowadays, most modern mobile phones and devices support WAP.Disadvantages of Wireless Application Protocol (WAP):

Following is a list of some disadvantages of Wireless Application Protocol or WAP:The connection speed in WAP is slow, and there is limited availability also.

In some areas, the ability to connect to the Internet is very sparse, and in some other areas, Internet access is entirely unavailable.

It is less secured.

WAP provides a small User interface (UI).

Applications of Wireless Application Protocol (WAP)

The following are some most used applications of Wireless Application Protocol or WAP:

WAP facilitates you to access the Internet from your mobile devices. You can play games on mobile devices over wireless devices.

It facilitates you to access E-mails over the mobile Internet.

Mobile hand-sets can be used to access timesheets and fill expenses claims.Online mobile banking is very popular nowadays.

It can also be used in multiple Internet-based services such as geographical location, Weather forecasting, Flight information, Movie & cinema information, Traffic updates etc. All are possible due to WAP technology.

WAP architecture:

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

Layers of WAP Protocol:

Application Layer:

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

Session Layer:

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

Transaction Layer:

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

Security Layer:

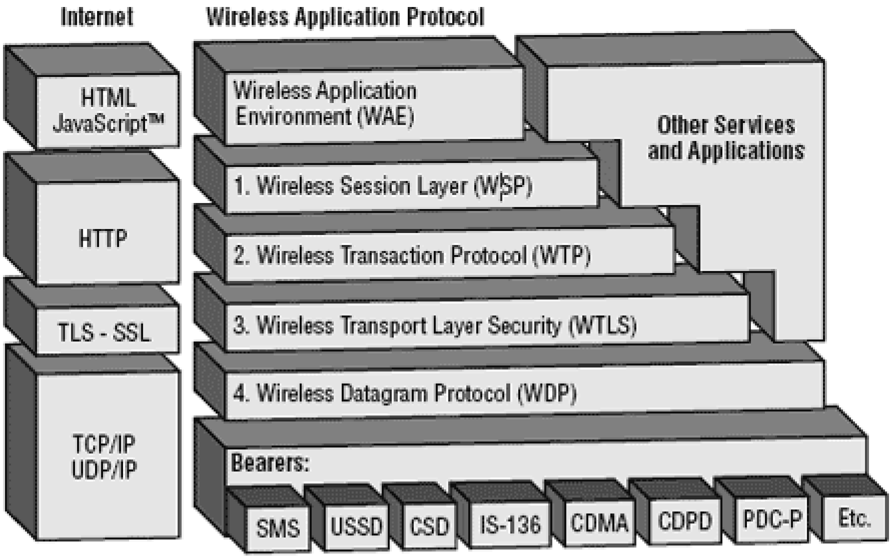
Wireless Transport Layer Security (WTLS). WTLS incorporates security features that are based upon the established Transport Layer Security (TLS) protocol standard. It includes data integrity checks, privacy, service denial, and authentication services.

Transport Layer:

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

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

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


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

Note that the mobile network bearers in the lower part of the figure above are not part of the WAP protocol stack.WAP Protocol:

It specifies the different communications and data transmission layers used in the WAP model:

Application Layer : This layer consists of the Wireless Application Environment (WAE), mobile device specifications, and content development programming languages, i.e., WML.

Session Layer : The session layer consists of the Wireless Session Protocol (WSP). It is responsible for fast connection suspension and reconnection.

Transaction Layer: The transaction layer consists of Wireless Transaction Protocol (WTP) and runs on top of UDP (User Datagram Protocol). This layer is a part of TCP/IP and offers transaction support.

Security Layer: It contains Wireless Transaction Layer Security (WTLS) and responsible for data integrity, privacy and authentication during data transmission.

Transport Layer: This layer consists of Wireless Datagram Protocol (WDP). It provides a consistent data format to higher layers of the WAP protocol stack.

WML

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

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

WML Versions:

WAP Forum has released a latest version WAP 2.0. The markup language defined in WAP 2.0 is XHTML Mobile Profile (MP). The WML MP is a subset of the XHTML. A style sheet called WCSS (WAP CSS) has been introduced alongwith XHTML MP. The WCSS is a subset of the CSS2.

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

WML 1.x is an earlier technology. However, that does not mean it is of no use, since a lot of wireless devices that only supports WML 1.x are still being used. Latest version of WML is 2.0 and it is created for backward compatibility purposes. So WAP site developers need not to worry about WML 2.0.

WML Decks and Cards:

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

When a WML page is accessed from a mobile phone, all the cards in the page are downloaded from the WAP server. So if the user goes to another card of the same deck, the mobile browser does not have to send any requests to the server since the filethat contains the deck is already stored in the wireless device.

You can put links, text, images, input fields, option boxes and many other elements in a card.WML Program Structure:

Following is the basic structure of a WML program:

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.2//EN"
"http://www.wapforum.org/DTD/wml12.dtd">
<wml>
<card id="one" title="First Card">
<p>
This is the first card in the deck
</p>


</card>
```

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

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

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

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

WAP Site Design Considerations:

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

While designing a WAP site you must ensure that you keep things simple and easy to use. You should always keep in mind that there are no standard microbrowser behaviors and that the data link may be relatively slow, at around 10Kbps. However, with GPRS, EDGE, and UMTS, this may not be the case for long, depending on where you are located.

The following are general design tips that you should keep in mind when designing a service:Keep the WML decks and images to less than 1.5KB.

Keep text brief and meaningful, and as far as possible try to precode options to minimize the rather painful experience of user data entry.

Keep URLs brief and easy to recall.

Minimize menu levels to prevent users from getting lost and the system from slowing down. Use standard layout tags such as <big> and <b>, and logically structure your information.

Don't go overboard with the use of graphics, as many target devices may not support them.

WML – Environment:

To develop WAP applications, you will need the following:

A WAP enabled Web Server: You can enable your Apache or Microsoft IIS to serve all the WAP client request.A WAP Gateway Simulator: This is required to interact to your WAP server.

A WAP Phone Simulator: This is required to test your WAP Pages and to show all the WAP pages.You can write your WAP pages using the following languages:

Wireless Markup Language(WML) to develop WAP application. WML Script to enhance the functionality of WAP application. **Configuring Web Server:**

In normal web applications, MIME type is set to text/html, designating normal HTML code. Images, on the other hand, could be specified as image/gif or image/jpeg, for instance. With this content type specification, the web browser knowsthe data type that the web server returns.

To make your Apache WAP compatible, you have nothing to do very much. You simply need to add support for the MIME types and extensions listed below.

File Extension	MIME type
WML (.wml)	text/vnd.wap.wml
WMLScript (.wmls)	text/vmd.wap.wmlscript
WMLScriptc (.wmlsx)	application/vnd.wap.wmlscriptc
WMLC (.wmlc)	application/vnd.wap.wmlc

WBMP (.wbmp)	image/vnd.wap.wbmp

Configure Apache Web Server for WAP:

Assuming you have Apache Web server installed on your machine. So now we will tell you how to enable WAP functionality in your Apache web server.So locate Apache's file httpd.conf which is usually in /etc/httpd/conf, and add the following lines to the file and restart the server:

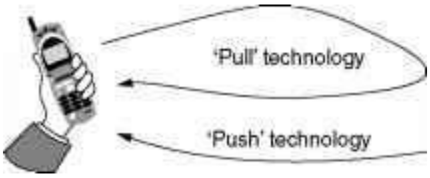
```
AddType     text/vnd.wap.wml     .wml
AddType       text/vnd.wap.wmlscript
.wmls                               AddType
application/vnd.wap.wmlc .wmlc
AddType      application/vnd.wap.wmlscriptc
.wmlsc     AddType      image/vnd.wap.wbmp
.wbmp
```

In dynamic applications, the MIME type must be set on the fly, whereas in static WAP applications the web server must beconfigured appropriately.

PUSH ARCHITECTURE

WAP Push Architecture:

The WAP Push framework introduces a means within the WAP effort to transmit information to a device without a previous user action. In the client/server model, a client requests a service or information from a server, which transmits information to the client. In this pull technology, the client pulls information from the server. An example of pull technology is WWW, in which a user enters a URL (the request), sent then to a server, which answers by sending a Web page (the response) to the user. In the push technology based on client/server model, there is no explicit request from the client before the server transmits its content.



Comparison of pull and push technology.Server

Pull and push technology:

Pull transactions are initiated by the client, whereas push transactions are initiated by the server.A push operation in WAP occurs when a Push Initiator transmits content to a client using either the Push OTA protocol or the Push Access Protocol (PAP). The Push Initiator does not share a protocol with the WAP client since the Push Initiator is on the Internet and the WAP client is on the WAP domain. The Push Initiator contacts the WAP Client through a translating Push Proxy Gateway (PPG) from the Internet side, delivering content for the destination client using Internet protocols. The PPG forwards the pushed content to the WAP domain, and the content is then transmitted over the air in the mobile network to the destination client. The PPG may be capable of notifying the Push Initiator about the final outcome of the push operation, and it may wait for the client to accept or reject the content in two-way mobile networks. It may also provide the Push Initiator with client capability lookup services by letting a Push Initiator select the optimal content for this client.

The Internet side PPG access protocol is called the PAP. The WAP side protocol is called OTAProtocol. The PAP uses XML messages that may be tunneled through various Internet protocols, for example, HTTP. The OTA protocol is based on WSP services. The PPG acts as an access point for content pushes from the Internet to the mobile network, and associated authentication, security, client control, and so on. The PPG owner decides the policies about who is able to gain access to the WAP network, who is able to push content, and so on. The PPG functionality may be built into the pull WAP gateway that givesthe benefit of shared resources and shared sessions over the air.

The PPG accepts pushed content from the Internet using the PAP. The PPG acknowledges successful parsing or reports unsuccessful parsing of the control information and may report debug information about the content. It may also perform a callback to the pushing server when the final status of the push submission has been reached, if the Push Initiator so requests.

When the content has been accepted for delivery, the PPG attempts to find the correct destination device and deliver the content to the client using the Push OTA protocol. The PPG attempts to deliver the content until a timeout expires, which can be set by the Push Initiator and/or the policies of the mobile operator.

The PPG may encode WAP content types into their binary counterparts. This transaction takes place before delivery over the air. Other content types may be forwarded as received. The Push Initiator may also precompile its content into binary form to take workload off the PPG, for example. When the PPG receives precompiled WML, WMLScript, or SIs, they are forwarded as received.

The PPG may implement addressing aliasing schemes to enable special multi- and broadcast cases, in which special addresses may translate to a broadcast operation.

A Push Initiator may query the PPG for client capabilities and preferences to create better formatted content for a particular WAP device. The PAP is used by an Internet-based Push Initiator to push content to a mobile network addressing its PPG. The PAP initially uses HTTP, but it can be tunneled through any other or future Internet protocol. The PAP carries an XML-style entity that may be used with other components in a multipart-related document. The PAP supports the following operations:

- Push Submission (Initiator to PPG)
- Result Notification (PPG to Initiator)
- Push Cancellation (Initiator to PPG)
- Status Query (Initiator to PPG)
- Client Capabilities Query (Initiator to PPG).

The push message contains three entities: a control entity, a content entity, and optionally a capability entity. They are used in a multipart-related message, which is sent from the Push Initiator to the PPG. The control entity is an XML document containing delivery instructions destined for the PPG, and the content entity is destined for the mobile device.

If the Push Initiator requested a confirmation of successful delivery, the message is transmitted from the PPG to the Push Initiator when the content is delivered to the mobile device over a two-way bearer, or transmitted to the device over a one- way bearer, and it contains an XML entity. The message is also transmitted in case of a detected delivery failure to inform the Initiator about it.

The Push Initiator relies on the response from the PPG; a confirmed push is then confirmed by the WAP device only when the target application has taken responsibility for the pushed content. Otherwise, the application must abort the operation and the Push Initiator knows that the content never reached its destination.

An XML entity can be transmitted from the Push Initiator to the PPG requesting cancellation of the previously submitted content. The PPG responds with an XML entity whether or not the cancellation was successful. An XML can also be transmitted from the Push Initiator to the PPG requesting status of the previously submitted content. The PPG responds with an XML entity. An XML entity transmitted from the Push Initiator to the PPG can request the capabilities of a device on the network. The PPG responds with a multipart related in two parts, in which the multipart root is the result of the request, and the second part is the capabilities of the device. The WAP is carried over HTTP/1.1 in this issue of WAP Push.

The SI content type provides the ability to send notifications to end users in an asynchronous manner. An SI contains a short message and a URI indicating a service. The message is presented to the end user upon reception, and the user is giventhe choice to either start the service indicated by the URI immediately or to postpone the SI for later handling. If the SI is postponed, the client stores it and the end user is given the possibility to act upon it at a later time.

The Push OTA protocol is a thin protocol layer on top of WSP, and it is responsible for transporting content from the PPG to the client and its user agents. The OTA protocol may use WSP sessions to deliver its content. Connection-oriented pushes require that an active WSP session is available, but a session cannot be created by the server. When there is no active WSP session, the Push framework introduces a Session Initiation Application (SIA) in the client that listens to session requests from the OTA servers and responds by setting up a WSP session for push purposes. The client may verify the identity information in this request against a list of recognized OTA servers before attempting to establish any push sessions. Push delivery may also be performed without the use of sessions in a connectionless manner, which is needed in one-way networks.

A connection-oriented push requires an active WSP session. Only the client can create sessions. If the server receives a requestfor a connection-oriented push to a client, and there are no active sessions to that client, the server cannot deliver the push content. A session request is sent to a special application in the client known as the SIA. This request contains information necessary for a client to create a push session. The SIA in the client after receiving a session request establishes a session with the PPG and indicates which applications accept content over the newly opened session. The SIA may also ignore the request if there is no suitable installed application as requested in the session request.When a client receives pushed content, a dispatcher looks at the push message header to determine its destination application. This dispatcher is responsible for rejecting content that does not have a suitable destination application installed, and for confirming push operations to the PPG when the appropriate application takes responsibility for pushed content.

****

CHAPTER 9

WIRELESS TELECOM NETWORK

9.1 GSM?

GSM stands for Global System for Mobile Communication. It is a digital cellular technology used for transmitting mobile voice and data services. Important facts about the GSM are given below –

The concept of GSM emerged from a cell-based mobile radio system at Bell Laboratories in the early 1970s.

GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard.GSM is the most widely accepted standard in telecommunications and it is implemented globally.

GSM is a circuit-switched system that divides each 200 kHz channel into eight 25 kHz time-slots. GSM operates on the mobile communication bands 900 MHz and 1800 MHz in most parts of the world. In the US, GSM operates in the bands 850 MHz and 1900 MHz.

GSM owns a market share of more than 70 percent of the world's digital cellular subscribers.

GSM makes use of narrowband Time Division Multiple Access (TDMA) technique for transmitting signals. GSM was developed using digital technology. It has an ability to carry 64 kbps to 120 Mbps of data rates.

Presently GSM supports more than one billion mobile subscribers in more than 210 countries throughout the world.

GSM provides basic to advanced voice and data services including roaming service. Roaming is the ability to use your GSM phone number in another GSM network.

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

Why GSM :

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

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

A GSM network comprises of many functional units. These functions and interfaces are explainedThe GSM network can be broadly divided into –

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

GSM - The Mobile Station

The MS consists of the physical equipment, such as the radio transceiver, display and digital signal processors, and the SIM card. It provides the air interface to the user in GSM networks. As such, other services are also provided, which include –

Voice
teleservices
Data bearer
services
The features' supplementary services

The MS Functions

The MS also provides the receptor for SMS messages, enabling the user to toggle between the voice and data use. Moreover, the mobile facilitates access to voice messaging systems. The MS also provides access to the various data services available in a GSM network. These data services include −

X.25 packet switching through a synchronous or asynchronous dial-up connection to the PAD at speeds typically at 9.6 Kbps.

General Packet Radio Services (GPRSs) using either an X.25 or IP based data transfer method at the speed up to 115 Kbps.

High speed, circuit switched data at speeds up to 64 Kbps.

We will discuss more about GMS services in GSM - User Services.

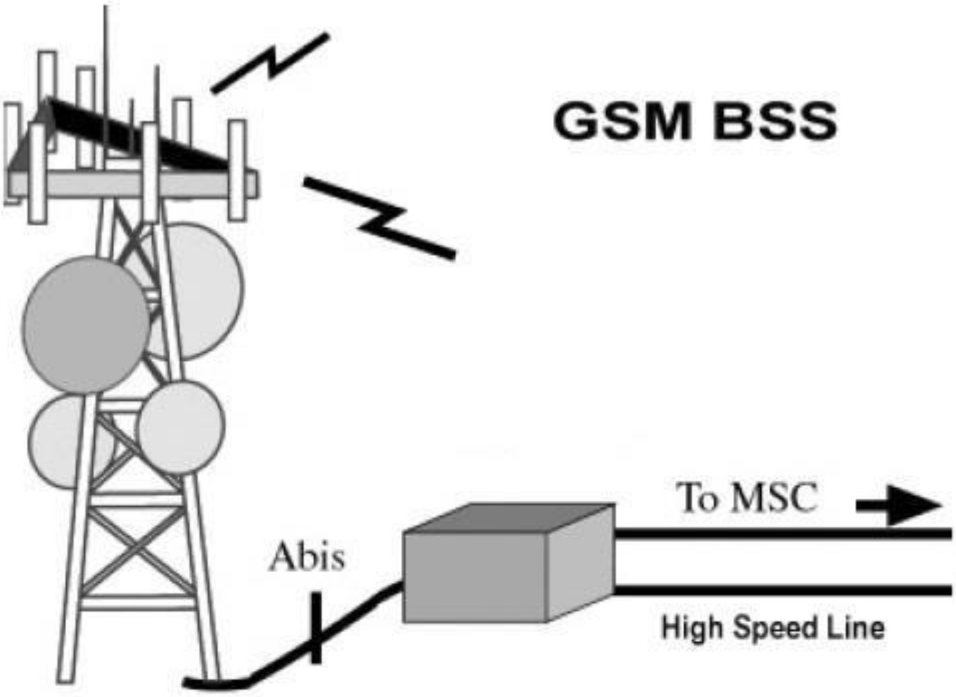
What is SIM:

The SIM provides personal mobility so that the user can have access to all subscribed services irrespective of both the location of the terminal and the use of a specific terminal. You need to insert the SIM card into another GSM cellular phone to receive calls at that phone, make calls from that phone, or receive other subscribed services.

GSM - The Base Station Subsystem (BSS)

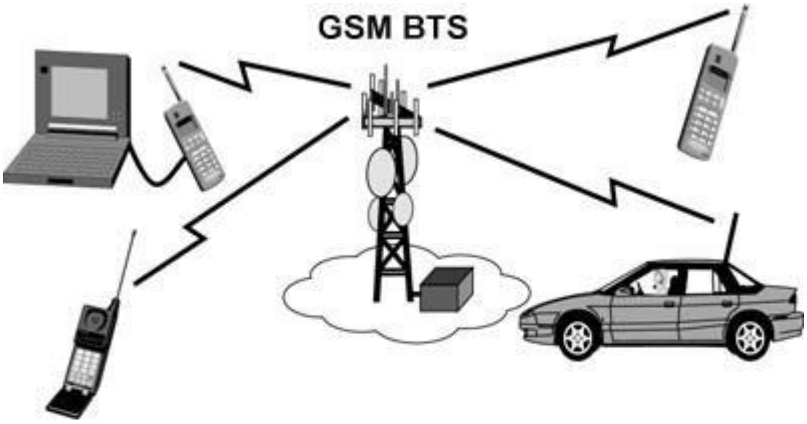
The BSS is composed of two parts −The Base Transceiver Station (BTS) The Base Station Controller (BSC)

The BTS and the BSC communicate across the specified Abis interface, enabling operations between components thatare made by different suppliers. The radio components of a BSS may consist of four to seven or nine cells. A BSS may have one or more base stations. The BSS uses the Abis interface between the BTS and the BSC. A separate high-speed line (T1 or E1) is then connected from the BSS to the Mobile MSC.



The Base Transceiver Station (BTS)

The BTS houses the radio transceivers that define a cell and handles the radio link protocols with the MS. In a large urban area,a large number of BTSs may be deployed.



The BTS corresponds to the transceivers and antennas used in each cell of the network. A BTS is usually placed in the center of a cell. Its transmitting power defines the size of a cell. Each BTS has between 1 and 16 transceivers, depending on thedensity of users in the cell. Each BTS serves as a single cell. It also includes the following functions −

Encoding, encrypting, multiplexing, modulating, and feeding the RF signals to the
antennaTranscoding and rate adaptation
Time and frequency synchronizing
Voice through full- or half-rate
services
Decoding, decrypting, and equalizing received
signalsRandom access detection
Timing advances
Uplink channel
measurements The Base
Station Controller (BSC)

The BSC manages the radio resources for one or more BTSs. It handles radio channel setup, frequency hopping, and handovers. The BSC is the connection between the mobile and the MSC. The BSC also translates the 13 Kbps voice channel used over the radio link to the standard 64 Kbps channel used by the Public Switched Telephone Network (PSDN) or ISDN.

It assigns and releases frequencies and time slots for the MS. The BSC also handles intercell handover. It controls the power transmission of the BSS and MS in its area. The function of the BSC is to allocate the necessary time slots between the BTS and the MSC. It is a switching device that handles the radio resources.

The additional functions include–

Control of frequency hopping

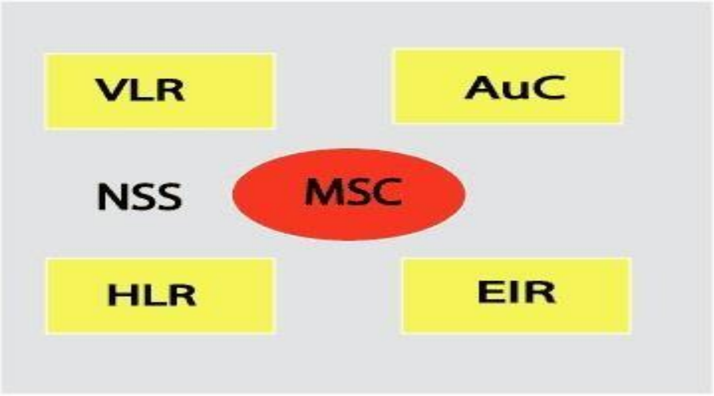
Performing traffic concentration to reduce the number of lines from the MSC Providing an interface to the Operations and Maintenance Center for the BSSReallocation of frequencies among BTSs

Time and frequency synchronization Power management

Time-delay measurements of received signals from the MS

GSM - The Network Switching Subsystem (NSS)

The Network switching system (NSS), the main part of which is the Mobile Switching Center (MSC), performs the switching of calls between the mobile and other fixed or mobile network users, as well as the management of mobile services such as authentication.



The switching system includes the following functional elements –Home Location Register (HLR):

The HLR is a database used for storage and management of subscriptions. The HLR is considered the most important database, as it stores permanent data about subscribers, including a subscriber's service profile, location information, and activity status. When an individual buys a subscription in the form of SIM, then all the information about this subscription is registered in the HLR of that operator.

Mobile Services Switching Center (MSC):

The central component of the Network Subsystem is the MSC. The MSC performs the switching of callsbetween the mobile and other fixed or mobile network users, as well as the management of mobile services such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber. It also performs such functions as toll ticketing, network interfacing, common channel signaling, and others. Every MSC is identified by a unique ID. Visitor Location Register (VLR):

The VLR is a database that contains temporary information about subscribers that is needed by the MSC in order to service visiting subscribers. The VLR is always integrated with the MSC. When a mobile station roams into a new MSC area, the VLR connected to that MSC will request data about the mobile station from the HLR. Later, if the mobile station makes a call, the VLR will have the information needed for call setup without having to interrogate the HLR each time.

Authentication Center (AUC):

The Authentication Center is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and ciphering of the radio channel. The AUC protects network operators from different types of fraud found in today's cellular world.

Equipment Identity Register (EIR):

The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where its International Mobile Equipment Identity (IMEI) identifies each MS. An IMEI is marked as invalid if it has been reported stolen or is not type approved.

GSM - The Operation Support Subsystem (OSS):

The operations and maintenance center (OMC) is connected to all equipment in the switching system and to the BSC. The implementation of OMC is called the operation and support system (OSS).

Here are some of the OMC functions−:

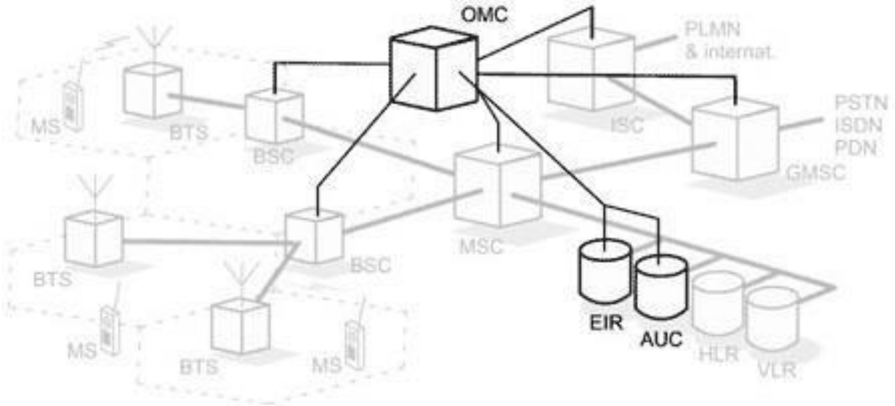
Administration and commercial operation (subscription, end terminals, charging, and statistics).Security Management.

Network configuration, Operation, and Performance Management.

Maintenance Tasks.

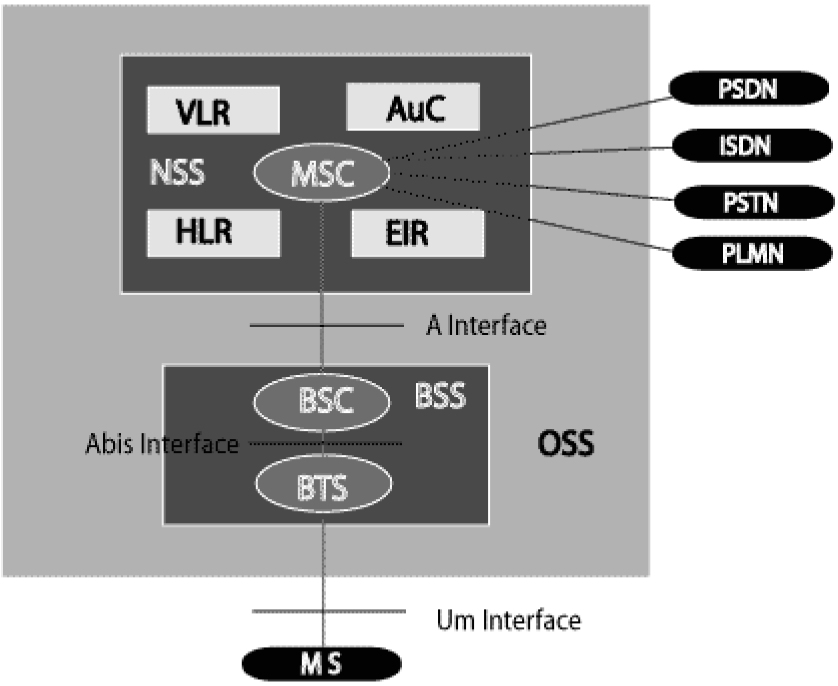
The operation and Maintenance functions are based on the concepts of the Telecommunication Management Network (TMN), which is standardized in the ITU-T series M.30.

Following is the figure, which shows how OMC system covers all the GSM elements.



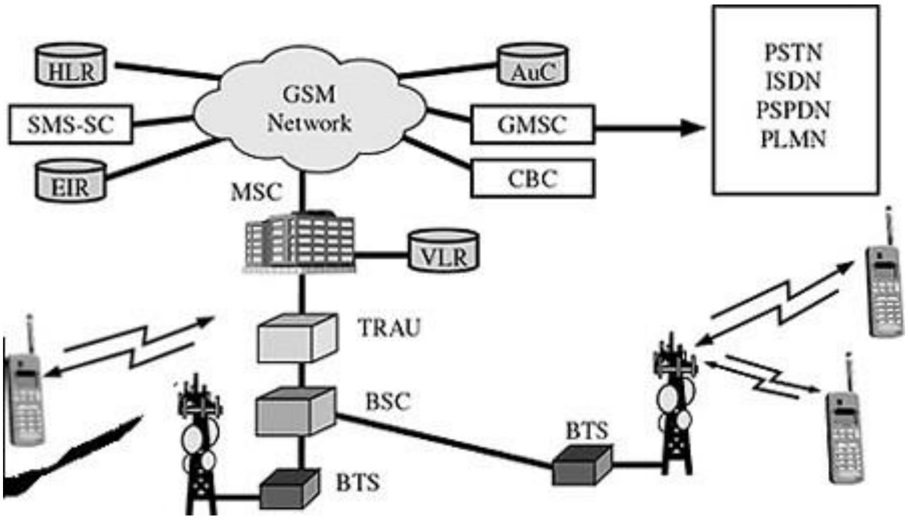
The OSS is the functional entity from which the network operator monitors and controls the system. The purpose of OSS is to offer the customer cost-effective support for centralized, regional, and local operational and maintenance activities that are required for a GSM network. An important function of OSS is to provide a network overview and support the maintenance activities of different operation and maintenance organizations.

A simple pictorial view of the GSM architecture is given below −



The additional components of the GSM architecture comprise of databases and messaging systems functions −Home Location Register (HLR)
Visitor Location Register (VLR) Equipment Identity Register (EIR) Authentication Center (AuC) SMS Serving Center (SMS SC) Gateway MSC (GMSC) Chargeback Center (CBC)
Transcoder and Adaptation Unit (TRAU)

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



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

GSM network areas

In a GSM network, the following areas are defined −

Cell − Cell is the basic service area; one BTS covers one cell. Each cell is given a Cell Global Identity (CGI), a number that uniquely identifies the cell.

Location Area − A group of cells form a Location Area (LA). This is the area that is paged when a subscriber gets an incoming call. Each LA is assigned a Location Area Identity (LAI). Each LA is served by one or more BSCs.

MSC/VLR Service Area − The area covered by one MSC is called the MSC/VLR service area.

PLMN − The area covered by one network operator is called the Public Land Mobile Network (PLMN). A PLMN can contain oneor more MSCs.

GPRS

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

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

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

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

Who owns GPRS ?

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

Key Features

Following three key features describe wireless packet data:

The always online feature - Removes the dial-up process, making applications only one click away.

An upgrade to existing systems - Operators do not have to replace their equipment; rather, GPRS is added on top of the existing infrastructure.

An integral part of future 3G systems - GPRS is the packet data core network for 3G systems EDGE and WCDMA.Goals of GPRS

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

Consistent IP services

Same infrastructure for different air interfaces Integrated telephony and Internet infrastructure Leverage industry investment in IP

Service innovation independent of infrastructure**Benefits of GPRS**

Higher Data Rate

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

Easy Billing:

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

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

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

Mobility - The ability to maintain constant voice and data communications while on the move.

Immediacy - Allows subscribers to obtain connectivity when needed, regardless of location and without a lengthy login session.

Localization - Allows subscribers to obtain information relevant to their current location.

Using the above three characteristics varied possible applications are being developed to offer to the mobile subscribers.

These applications, in general, can be divided into two high-level categories:

1. Corporation
2. Consumer

These two levels further include:

- Communications - E-mail, fax, unified messaging and intranet/internet access, etc.
- Value-added services - Information services and games, etc.
- E-commerce - Retail, ticket purchasing, banking and financial trading, etc.
- Location-based applications - Navigation, traffic conditions, airline/rail schedules and location finder, etc.
- Vertical applications - Freight delivery, fleet management and sales-force automation.

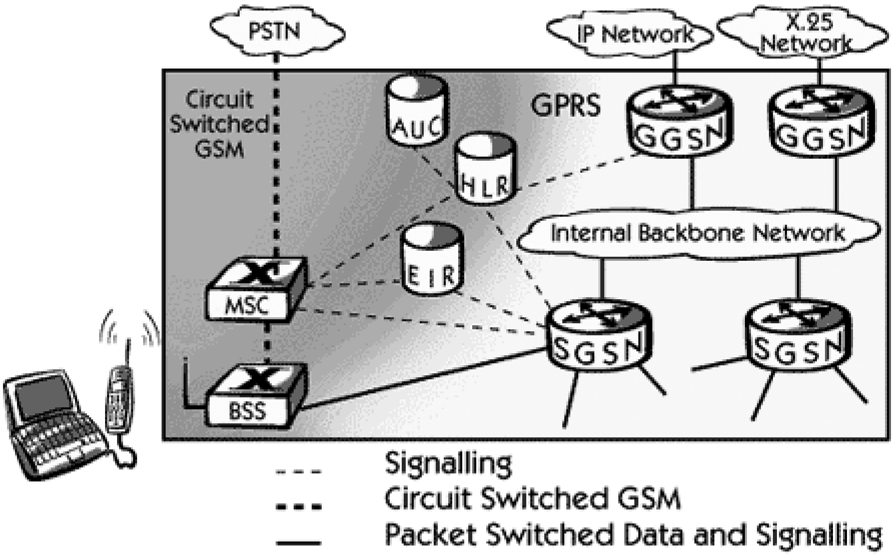
Advertising -: Advertising may be location sensitive. For example, a user entering a mall can receive advertisements specific to the stores in that mall.

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

GPRS architecture works on the same procedure like GSM network, but, has additional entities that allow packet data transmission. This data network overlaps a second-generation GSM network providing packet data transport at the rates from

9.6 to 171 kbps. Along with the packet data transport the GSM network accommodates multiple users to share the same air interface resources concurrently.

Following is the GPRS Architecture diagram:



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

GSM Network Element	Modification or Upgrade Required for GPRS.
Mobile Station (MS)	New Mobile Station is required to access GPRS services. These new terminals will be backward compatible with GSM for voice calls.
BTS	A software upgrade is required in the existing Base Transceiver Station(BTS).
BSC	The Base Station Controller (BSC) requires a software upgrade and the installation of new hardware called the packet control unit (PCU). The PCU directs the data traffic to the GPRS network and can be a separate hardware element associated with the BSC.
GPRS Support Nodes (GSNs)	The deployment of GPRS requires the installation of new core network elements called the serving GPRS support node (SGSN) and gateway GPRS support node (GGSN).
Databases (HLR, VLR, etc.)	All the databases involved in the network will require software upgrades to handle the new call models and functions introduced by GPRS.

GPRS Mobile Stations:

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

GPRS Base Station Subsystem:

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

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

GPRS Support Nodes

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

Gateway GPRS Support Node (GGSN):

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

Serving GPRS Support Node (SGSN):

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

Internal Backbone:

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

Routing Area:

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

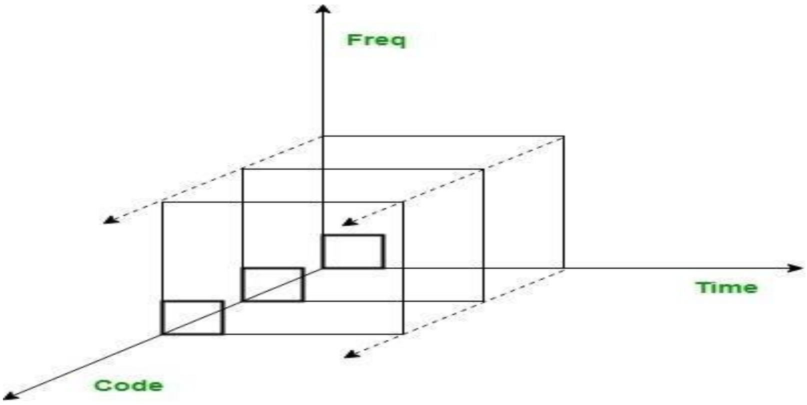
IS-95:

Interim Standard (IS)
95 Last Updated : 08
Aug, 2019

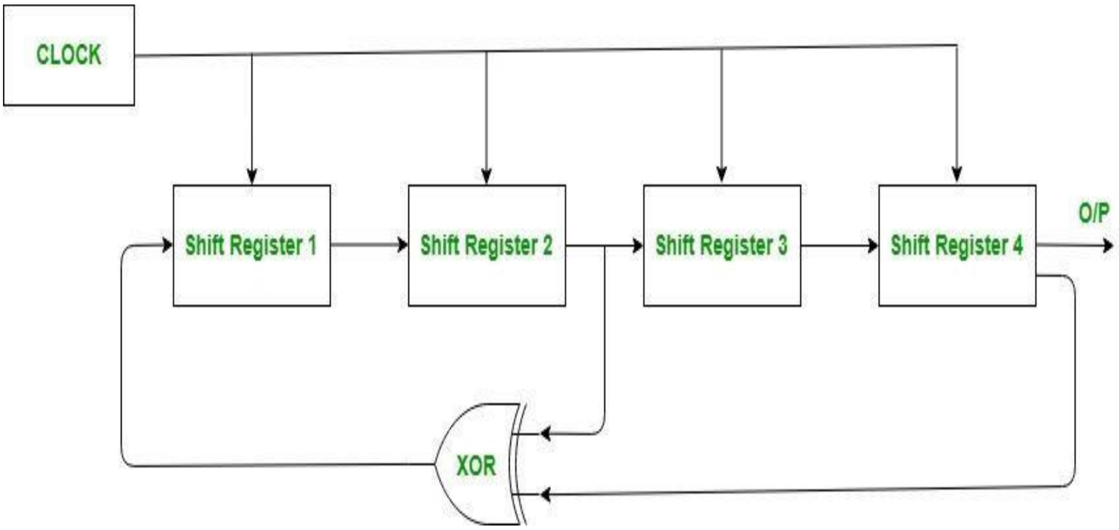
IS-95 stands for Interim Standard 95 and is also known as CDMAOne. It was the first ever CDMA-based digital cellular technology and was developed by Qualcomm. It is an 2G cellular system based on DS-CDMA. To understand IS-95 we need to understand DS and CDMA separately.

DSSS is Direct Sequence Spread Spectrum Technique which is a spread spectrum technique in which the data to be transmitted is encoded using spreading code and received and then decoded using the same code. It is used to avoid interference, spying and jamming. The spreading code used is known to transmitter and receiver only.

CDMA stands for Code Division Multiple Access. It uses the same bandwidth for all the users. However, each user is assigned a separate code which differentiates the from each other.



Narrow bandwidth signals are multiplied with a very large bandwidth signals called Pseudo Noise Code Sequence (PN code). Each user has its own PN code which is orthogonal to each other. Auto-correlation is maximum and cross-correlation is zero of these PN codes. They repeats itself after a very large time period and hence, appears to be random. PN Sequence is generated by Linear Feedback Shift Register.



Power Control in IS-95:

It solves the Near-far problem in which transmitters at different distances transmits signal of same powerthen the power of the signal of Transmitter (nearer to the base station) will be greater than that of Transmitter (farther to the base station). So in power control technique transmitter nearer to the base station transmits less power signal that of the transmitter farther.

It is of two types:

Open loop power control:

Transmitter senses the power of the received signal at the base station and then adjusts its transmitting power accordingly in subsequent transmissions.

Closed loop power control:

Base station sends the received signal power information to the transmitter and tells to incrementor decrement the transmission power accordingly in subsequent transmissions.

CDMA-2000

CDMA2000 is a code division multiple access (CDMA) version of IMT-2000 specifications developed byInternational Telecommunication Union (ITU).

It includes a group of standards for voice and data services – Voice – CDMA2000 1xRTT, 1X Advanced

Data – CDMA2000 1xEV-DO (Evolution-Data Optimized)

Features

CDMA2000 is a family of technology for 3G mobile cellular communications for transmission of voice, data and signals.

It supports mobile communications at speeds between 144Kbps and 2Mbps.

It has packet core network (PCN) for high speed secured delivery of data packets.

It applies multicarrier modulation techniques to 3G networks. This gives higher data rate, greaterbandwidth and better voice quality. It is also backward compatible with older CDMA versions.

It has multi-mode, multi-band roaming features

W-CDMA

Wideband Code Division Multiple Access (WCDMA) is a third-generation (3G) standard that employs the direct-sequence code division multiple access (DS-CDMA) channel access method and the frequency-division duplexing (FDD) method to provide high-speed and high-capacity service. WCDMA is the most commonly used variant of the Universal Mobile Telecommunications System (UMTS). It was developed by Japan's NTT DoCoMo and formed the basis of its Freedom of Multimedia Access (FOMA) 3G Network.

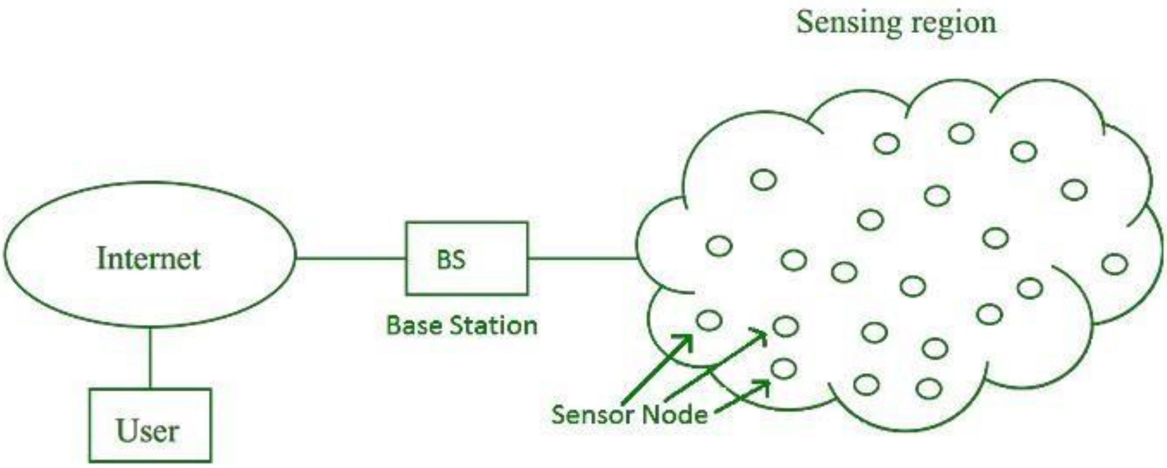
WIRELESS SENSOR NETWORK

Wireless Sensor Network (WSN)Difficulty Level : Basic

Last Updated : 03 Jun, 2021

Wireless Sensor Network (WSN) is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions.

Sensor nodes are used in WSN with the onboard processor that manages and monitors the environment in a particular area. They are connected to the Base Station which acts as a processing unit in the WSN System. Base Station in a WSN System is connected through the Internet to share data.



WSN can be used for processing, analysis, storage, and mining of the data.

Applications of WSN:Internet of Things (IOT)

Surveillance and Monitoring for security, threat detection Environmental temperature, humidity, and air pressure Noise Level of the surrounding

Medical applications like patient monitoringAgriculture

Landslide Detection

Challenges of WSN:

Quality of ServiceSecurity Issue Energy Efficiency

Network Throughput

Performance

Ability to cope with node failure Cross layer optimisation

Scalability to large scale of deployment

Components of WSN:

Sensors:

Sensors in WSN are used to capture the environmental variables and which is used for data acquisition. Sensor signalsare converted into electrical signals.

Radio Nodes:

It is used to receive the data produced by the Sensors and sends it to the WLAN access point. It consists ofa microcontroller, transceiver, external memory, and power source.

WLAN Access Point:

It receives the data which is sent by the Radio nodes wirelessly, generally through the internet.

Evaluation Software:

The data received by the WLAN Access Point is processed by a software called as Evaluation Software for presenting the report to the users for further processing of the data which can be used for processing, analysis, storage, and mining of the data.

****

CHAPTER-10

MESSAGING SERVICES

SHORT MESSAGE SERVICES

Stands for "Short Message Service." SMS is used to send text messages to mobile phones. The messages can typically be up to 160 characters in length, though some services use 5-bit mode, which supports 224 characters. SMS was originally created for phones that use GSM (Global System for Mobile) communication, but now all the major cell phone systems support it.

While SMS is most commonly used for text messaging between friends or co-workers, it has several other uses as well. For example, subscription SMS services can transmit weather, news, sports updates, and stock quotes to users' phones. SMS can also notify employees of sales inquiries, service stops, and other information pertinent to their business. Doctors can receive SMS messages regarding patient emergencies.

Fortunately, text messages sent via SMS do not require the recipient's phone to be on in order for the message to be successfully transmitted. The SMS service will hold the message until the recipient turns on his or her phone, at which point the message will be be sent to the recipient's phone. Most cell phone companies allow you to send a certain number of text messages every month for no charge. Though it would be a good idea to find out what that number is before you go text message crazy.

MULTIMEDIA MESSAGE SERVICES

- MMS stands for Multimedia Messaging Service. It is the standard way to send messages from one deviceto another through a network.

  As the name Multimedia, we can suggest from here that it is not only for sending text messages, we canalso send multimedia like images, audio clips and video clips, and many more things.
- It is the extension used for SMS(Short Message Service) where we send and receive text messages onlywith the limitation of only 160 characters in one SMS.

  Most of the smartphones support MMS messaging nowadays. Basically it is the advanced version of thetext messaging with the additional feature of multimedia.

Modes of sending MMS

There are basically six modes which are as follows:

- Sending messages to an MMS mobile phone via an MMS mobile phone.

  It can be sent in the same way as we send SMS messages, except that MMS messages include multimediacontents.
- Sending messages to a non-MMS mobile phone via an MMS mobile phone.

  Since the non-MMS mobile phones can’t receive a multimedia message, the MMS system automatically forwards the messages to the receiver’s corresponding email box and then sends a notification to his mobile phone.
- Sending messages to email boxes via an MMS mobile phone Multimedia messages can be sent via an MMS mobile phone to an email box, and the receiver logs on the email box to read the messages. However, mostemail boxes don’t support multimedia messages yet.
- Sending messages to an MMS mobile phone via an email box.

  A user logs on to his email box, selects multimedia messages to sent, inputs a receiver’s MMS mobile phone number, and send the messages as an attachment.
- Downloading multimedia messages from the internet to an MMS mobile phone.

  A user can customize and order multimedia messages on websites that provide MMSs and then send MMSto an MMS mobile phone.
- Sending messages from an MMS mobile phone to personal e-albums.

  A user can send MMS messages to his personal e-album via an MMS mobile phone. User writes MMS messages in mobile phones, inputs the album website number, and then sends the messages.

Advantages

- We can easily send and deliver MMS messages.
- The MMS messages which we received, we can store them (save them) and also we can forward messages.
- Users are using these services as they are user-friendly.

These services are interactive.

Image, video, and other media-rich content allows for better branding.Disadvantages

MMS service is not available on all mobile phones. So, we cannot use this service in all the phones.

Some multimedia content has some resolution issues due to the varied display sizes of different phones.

As it a service provided to us but there are also extra charges associated with it. If we have to use this service we have to pay extra charges for this service.

Users who have opted in to an MMS database don't necessarily have an MMS enabled phone. Sending bulk MMS messages is often only available through a dedicated messaging platform rather than a network.

MULTIMEDIA TRANSMISSION OVER NETWORK

Multimedia transmission over wireless networks highlighting general challenges driving the research on wireless technologies and networking techniques for mobile multimedia support. After an overview of wireless networks and multimedia transmission characteristics, a layered analysis is provided ranging from the application to physical protocol layers. This discussion is extended with a cross-layer perspective focusing on cross-layer design. The chapter also introduces a number of emerging wireless/mobile networking concepts including Cognitive Radio Networks (CRNs), ad hoc and multihop networks, and mobile content delivery with a discussion of key issues from multimedia networking perspective. These approaches are envisaged to increase wireless link rates while also improving system capacity, energy efficiency and spectral efficiency dramatically. Finally, we present and discuss major challenges for modeling and simulation of wireless multimedia networking in this diverse and dynamic environment.

****