INFORMATION TECHNOLOGY ESSENTIALS

SEMESTER II

Creating a Website – Working principle of a Website – Browser fundamentals – Authoring tools – Types of servers: Application Server – Web Server – Database Server

1.1 CREATING WEB SITE

Web site is a collection of web pages. Hence for a website design we need to design the webpages. Each webpage may contain texts, photos, videos, and social media buttons and so on. Technically, a webpage is a special type of document written in scripting languages such as HTML,CSS, JavaScript, PHP and so on. Web pages are written for web browsers. The web browsers are the programs like Internet Explorer, Google Chrome and Safari. These browsers have a simple but crucially important job: they read the web page document and display the perfectly formatted result.

Definition of website:

Website is a collection of webpages that are grouped together to achieve certain task under single domain name.

Why do people visit website?

The most important reason is to find the **required information.** This could be anything from a student looking for images for a school project, to finding the latest stock quotes, for getting the address of the nearest restaurant and so on. **To complete a task:** Visitors may want to buy the latest best-seller, download a software program, or participate in an online discussion about a favourite hobby.

Steps for creating the Website:

Step 1: Website creation:

Create a webpage using suitable scripting language. IF any image is associated with this web page then convert this image into appropriate format (JPEG or GIF is preferable). Embed this image appropriately in this webpage.

Step 2: Choosing the web hosting services

- Web hosting company hosts your webpages on web server. Thus your website will be available to anyone who knows your URL. Most web hosting companies offer hosting services for both personal and business use. The web host provides you with Internet access, email accounts and space for a personal or business website.
- If you are building a website for business use, your webhost can register a personalized domain name for your website. If you are building a website for business use, your web host can register a personalized domain name for your website.
- Small web sites (around 15-20 pages of contents) do not need much more than 1 or 2 MB of server space that hold all the HTML pages and graphics. Your web hosting package should provide at least MB of space so your web page has room to grow.

Step 3: Registering Domain Name

Domain name is an alias that points to actual location of your web site on web server. Domain names are managed by the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN has agreements with a number of vendors to provide domain name registration services.

Step 4: Planning your website

- **Type**: The type of site you need. Is this a news or informational site, a site for a company or service, a non-profit or cause driven site, an E-commerce shop etc. Each of these kinds of site has a slightly different focus that will influence its design.

- **Navigation**: Navigation means indication that how users will move around your site affects its information architecture as well as the overall usability of that site. Plan out the pages a site, create a sitemap, and develop a navigational structure from there.
- **Content**: The quality of your site's content will play an important role in it's success. Content is everything that your pages will contain, such as text, images, video and more. Before you start designing or building pages, you should have a clear strategy for the content that those pages will contain.

Step 5: Uploading Files

- To publish a website on the web, you must send the web pages created by you on the webserver using File Transfer Protocol (FTP). Using some software such as Microsoft Visual Studio or Adobe Dreamweaver one can upload the files on the webserver.

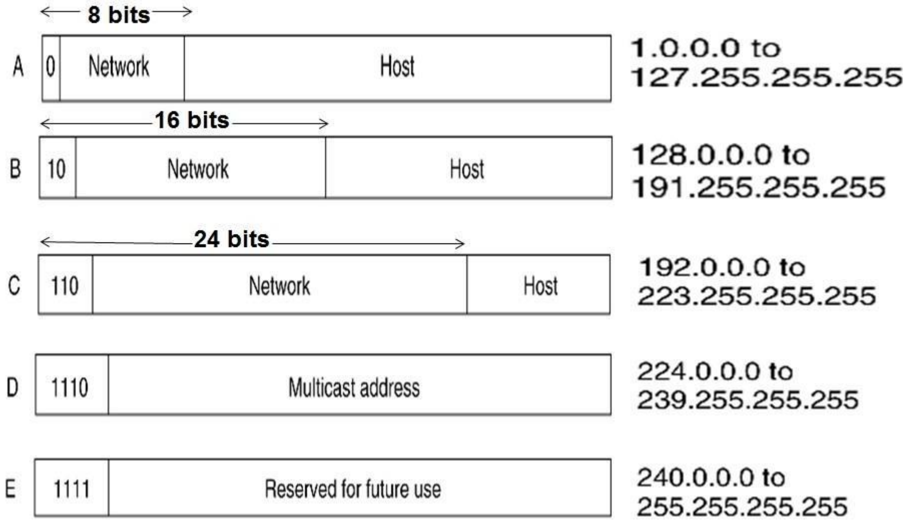
Testing the website:

Testing must be performed throughout the development of website

- **Multiple Browsers**: It is necessary to display the website on as many web browsers as possible to ensure that the contents of the website are consistently displayed and the work done is portable.
- **Multiple Operating Systems:** It is necessary to display the website on different operating systems.
- **Connection Speed:** Do not rely on the same connection speed when testing your website, especially if you work in a corporate environment where the connection to the Internet usually is faster than the average user's. Also test the download time for different connection speed.
- **Device Types**: Test the websites on the computer's having different screen size. It is necessary to ensure that pages are displayed consistently on all screen size.
- **Links:** Use a link validation tool to ensure that all of your links connect to a live page.
- **Security Testing:** This step is necessary to test the security vulnerabilities in application running on the website. Security is an important part of any web development plan.

1.2 IP ADDRESSING

- Each host on a TCP/IP network is assigned a unique 32-bit logical address that is divided into two main parts: the network number and the host number. This is called IP address. The IP address is grouped four into 8-bits separated by dots. Each bit in the octet has binary weight. There are five classes based on two categories, A, B, C, D and E.



- IP address is assigned to the devices participating in computer network. The IP protocol makes use of this address for communication between two computers. Using IP address particular node can be identified in the network.

1.3 DNS

- It is very difficult to remember numerical information but it is simple to remember the textual information. Consider that we want to access Priyanka's PC, then accessing it using the IP address www. 192.168.0.101 is definitely not comfortable, rather if we have the address www.priyanka@technical.com then accessing and remembering Priyanka's PC address is very simple. The names which are used to identify computer within a network are called domain names. Thus domain name is the name given to a network for human reference. Hence in DNS, instead of using the IP address name of the computer is used to access it. But two names can be the same. Hence to uniquely identify your computer the name must be referred using DNS hierarchy. Before understanding the hierarchy the commonly used domain names are:

Domain Names	Purpose
com	Commercial organization
gov	Government organization
edu	Educational institutions
int	International organization
net	Network group
org	Non-profit organization
mil	Military organization
in	Sub domain name used to refer India
uk	Sub domain name used to refer uk
jp	Sub domain name used to refer japan

- The domain name space is used to locate the computer uniquely. The internet logically arranges the domain names in a hierarchical form. There are some top level DNS such as com, org, edu. Etc. Then each domain is divided into sub-domains and then sub sub-domains and so on. For example the complete path for http://www.cse.tec.ac.in can be uniquely traced out the help of domain name space.

Working of DNS

There are two tasks that can be carried out by DNS servers:

- Accepting and then requesting the programs to convert domain names to IP address.
- Accepting and then requesting the other DNS servers to convert domain names to IP address.

Suppose PC A is interested in knowing the IP address of technicalpublications.org then it contacts nearest DNS server. This DNS server maintains huge database of domain names. The entry domain name technicalpublication.org is searched within this database and if the IP address for corresponding name is found then the IP address is returned to PC A. If it is not found, then the name of another DNS is suggested. If the request is made for some invalid domain name then the error message is returned.

1.4 URL

The Uniform Resource Locator (URL) is unique address for the file that has to be accessed over the internet. When we want to access some website we enter it's URL in the address bar of the web browser. For example if we want to access www.google.com then we must specify its URL in the address bar. However any other file such as some text file or image file or some HTML file can also be specified. The URL contains names of the protocol such as http://. The URL may contain the names of the protocol such as ftp. For example: ftp://ftp.funet.fi/pub/standards/RFC/rfc2166.txt the protocol identifier and the resource name are separated by a colon and two forward slashes. The syntax of writing URL is given below: protocol://username@hostname/path/filename. Sometimes instead of domain name servers IP addresses can also be used, for example http://192.168.0.1. But use of IP address as URL is not preferred because human cannot remember numbers very easily but they can remember names easily.

Absolute and Relative URL

- The absolute URL is a URL which directly point to a file. It exactly specifies exact location of a file or directory on the internet. Each absolute URL is unique.
  For example: http://www.vtubooks.com/home.aspx
- The relative URL points to the file or a directory in relation to the present directory.
  For example: http://www.webie.com/myphotos/mother.jpg

1.5 WORKING PRINCIPLE OF A WEBSITE

Features of Website Design

- **Quality of Web content** – people desire information in fast and reliable fashion. For business websites, content should include important information. These type of websites need to display high quality pictures of their products, and the highlight for clients testimonials.
- **Clear, User- friendly navigation** – A user friendly navigation scheme allows visitors to quickly find the information needed. Important links must be easy to find and given logical, simple and includes easy to understand labels.
- **Simple and professional design** - The website design must be simple and professional. Google is an excellent example of such a site. To keep websites simple a balances distribution of contents and graphics is required. The use of slightly contrasting colors and clear fonts is necessary. Also, one should break up sizeable blocks of texts with either spacing or images as appropriate.
- **Webpage speed** – People inherently lose patience quickly, when visiting a website. The website with heavy graphics, audio and video takes more time to load. A web design company must take care of all the controlling factors that will maintain the desirable speed of the website.
- **Search Engine optimization** – A well-designed website generally will receive many visitors, and one method to attract visitors is search engine optimization. This allows the insertion of search keywords in website content, an appropriate link profile, social media signals.
- **Web compatibility** – A website should easily render on various resolutions, screen sizes and browsers and with the increasing popularity of mobile devices, websites should function properly on these types of devices.

Web site Design Issues

- **Simplicity** – It is a general tendency of web designers to provide lot of animations, huge amount of information, extreme visuals and so on. This makes the web design enormous and it should be avoided. The web application must be moderate and simple.

- **Identity** – Web design must be based on the nature of the web application. It is driven by the objective of the web application, category of user using it. A web engineer must work to establish an identity for the web application through the design.
- **Consistency** – The contents of the web application should be constructed consistently. For example: text formatting, font style should be the same overall the text document of the web application. Similarly, the graphics design, color scheme and style must be identical over all the web pages of the web application. Navigation mechanism must be used consistently across web application elements.
- **Robustness** – The users always expects robust contents and functions of the web application. That means any required functionality should not be missing at all. If any function or content is missing or insufficient then that web application will fail.
- **Navigability** – The navigation should be simple and consistent. The design of navigations should intuitive and predictable in nature. That means any user should be in a position to make use of navigation links without any help.
- **Visual Appeal** – The web application are most visual and most dynamic and aesthetic in nature. There are various factors that contribute to visual appeal. The factors are – look and feel of the content, interface layout, color co-ordination, the balance of text, graphics and other media, navigation mechanism and so on.
- **Compatibility –** The web application can be used in variety of environment and configurations such as different browsers, internet connection types, operating systems and various browsers.

1.6 PHASES OF WEBSITE DEVELOPMENT

Web project can be designed in the four phases as given below -

Phase I: Strategy

In this phase, a strategic planner or project manager along with the client determines the objectives of the site. As an output of this phase **creative briefs** are prepared. The creative brief is a kind of document in which project objectives, requirements and key insights are clearly mentioned. Every team member makes use of creative brief as a guidelines fo the development.

Phase II: Design

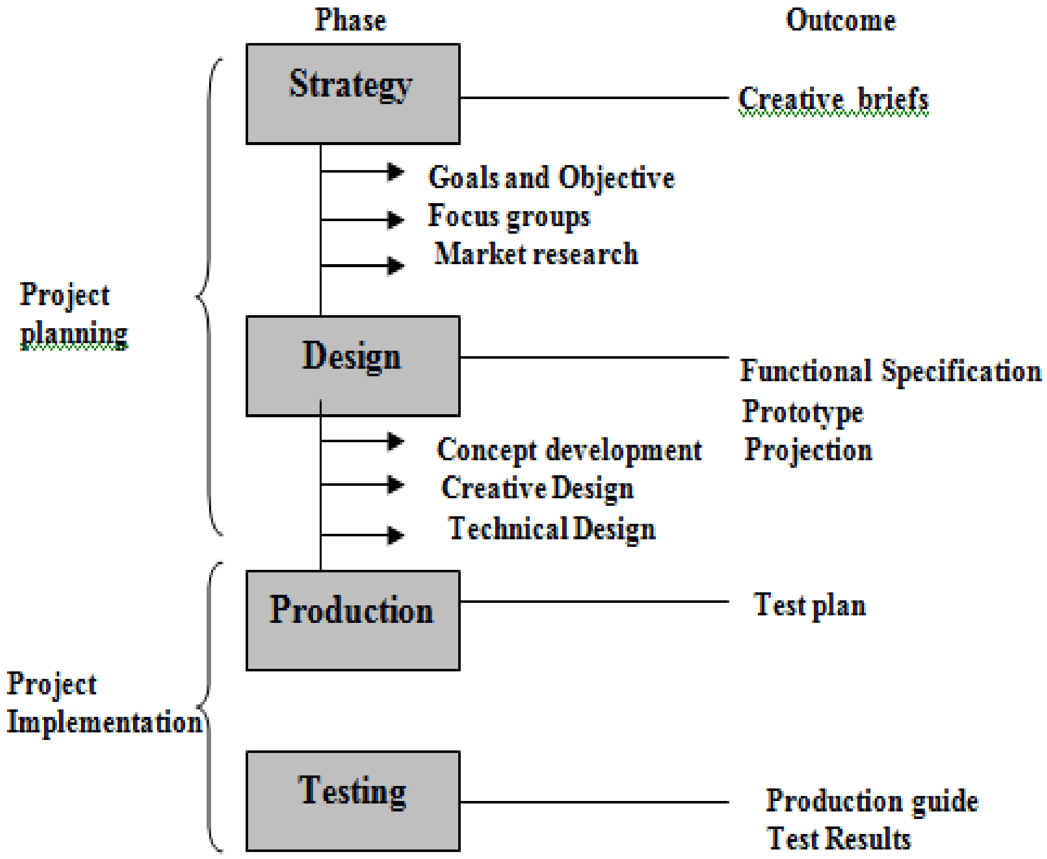
In this phase actual design of the website is done with the help of creative and technical team members. The front end is designed by the creative team in which user interface and interactions are designed. The back end is designed by the technical team which is responsible for designing the database architecture. As an outcome of this phase functional and technical specifications, site architecture are prepared.

Phase III: Production

During this phase actual site is built using the source code. Functionalities and features of the website are closely examined. If the client demands for a change in any functionality then a change order is issued. At the end of this phase a production guide is prepared.

Phase IV: Testing

At this phase all the functionalities and features of the website are tested, bugs are identified and resolved before launching the website. The QA manager develops the test plan. The test suit mentioned in it used to test the product thoroughly.



1.7 ENHANCING WEBSITE

There are varieties of ways by which one can enhance his website. The website can be enhanced using some key elements such as -

- **Contents -** This is the most important element of website. It helps to spread the business message in an appropriate manner. The content should be easy to understand. Those should be to the point and relevant. The information available on the website must be useful to the user.
- **Graphics -** Adding too much graphics in the webpage slows down its speed of loading. Hence Graphics is undesirable by any user. However the relevant and appealing graphics can be added to the website.
- **Color and Text -** The colors and text that is appearing on the website must be pleasant to the eyes. As a rule of thumb, the entire site must use at the most five to six colors. The text should not be too small or too large. The selection of the family of font for displaying the text must be appropriate so that the text can be readable.
- **Flash** – Use of flash animation makes the site attractive but at the same time there are many drawbacks that are associated with this key element. The first drawback is the flash files take a large amount time to load the data on the web page. Secondly if the flash animation is placed on the web page then the link for downloading the flash player must also be provided so that the animation can be viewed by the user.
- **Frames** – Frames must be avoided while designing the website. Instead of using frames the web designer must prefer the tables. The reason why the use of frames must be avoided in the web page is that – the search engine find it difficult to search the contents from the site containing the frames.
- **Organizing Files -** The files required by the website must be categorized and must be stored in sorted manner. This makes it easier to manage the information.

1.8 BROWSER FUNDAMENTALS

Definition:

Web browser is a kind of software which is basically used to use resources on the web.

- Over the networks, two computers communicate with each other. In this communication, when request is made by one computer then that computer is called **a client** and when the request gets served by another computer then that computer is called **server**. Thus exchange of information takes place via client-Server communication.
- When user wants some web document then he makes the request for it using the web browser. The browsers are the programs that are running on the client's machines. The request then gets served by the server and the requested page is then returned to the client. It is getting displayed to the client on the web browser. The web browser can browse the information on the server and hence is the name.
- Various web browsers that are commonly used are

Browser	Vendor
Internet Explorer	Microsoft
Google Chrome	Google
Mozilla Firefox	Mozilla
Netscape Navigator	Netscape Communications Corp
Opera	Opera Software
Safari	Apple

- Web browser supports variety of protocols but the most commonly used protocol on the web browser is **Hyper Text Transfer Protocol (HTTP).** This protocol is typically used when browser communicates with the server.

Functions Defined by Web Browser

Various functions of web browser are -

1. Reformat the URL and send a valid HTTP request.

2. When user gives the address of particular website it is in the form of domain name. The web browser converts the DNS to corresponding IP address.

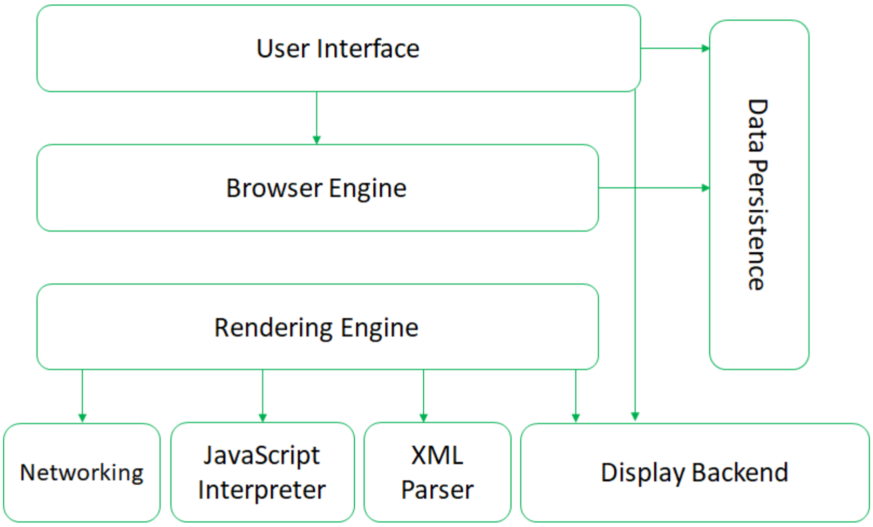
3. The web browser establishes a TCP connection with the Web browser while processing the user's request.

4. The web browser sends the HTTP request to the web server.

5. The web server processes the HTTP request sent by the web browser and returns the desired web page to the client machine. The web browser on the client's machine displays this webpage in appropriate format.

Web Browser Architecture

The web browser architecture is represented by following figure –



The main components of web browser architecture are as follows -

User Interface:

Using the user interface user interacts with the browser engine. The user interface contains, Address bar, back/forward button, book mark menu and so on. The page requested by the user is displayed in this user interface.

Browser Engine:

It contains the mechanism by which the input of user interface is communicated to the Rendering Engine. The browser engine is responsible for querying the rendering engine according to various user interfaces.

Rendering Engine:

It is responsible for displaying the requested contents on the screen. The rendering engine interprets the HTML, XML and JavaScript that comprises the given URL and generates the layout that is displayed in the user interface. The main components of rendering engine are HTML parser. The job of the HTML parser is to parse the HTML mark-up into a parse tree. It is important to note that Chrome, unlike most browsers, holds multiple instances of the rendering engine – one for each tab, each tab is a separate process. Different browsers use different rendering engines – Internet Explorer uses Trident, Firefox uses Gecko, Safari uses Webkit, Chrome and Opera uses WebKit.

Networking:

The functionality of networking is to retrieve the URL using common internet protocols such as HTTP and FTP. The networking is responsible to handle the internet communication and security issues. The network component may use the cache for retrieved documents. This feature is useful for increasing the response time.

JavaScript Interpreter:

The interpreter executes the JavaScript code which is embedded in a web page.

User Interface Backend:

It is basically used to draw the widgets like combo boxes and windows.

Data Persistence:

This is a small database created on local drives of the computer where the browser is installed. The data storage manages user data such as book marks, cookies and preferences.

Working of Web Browser

We often browse the internet for several reasons. It is more interesting to know about how a web page demanded by us gets displayed on our browser. Following is the stepwise explanation of this process -

Step 1:

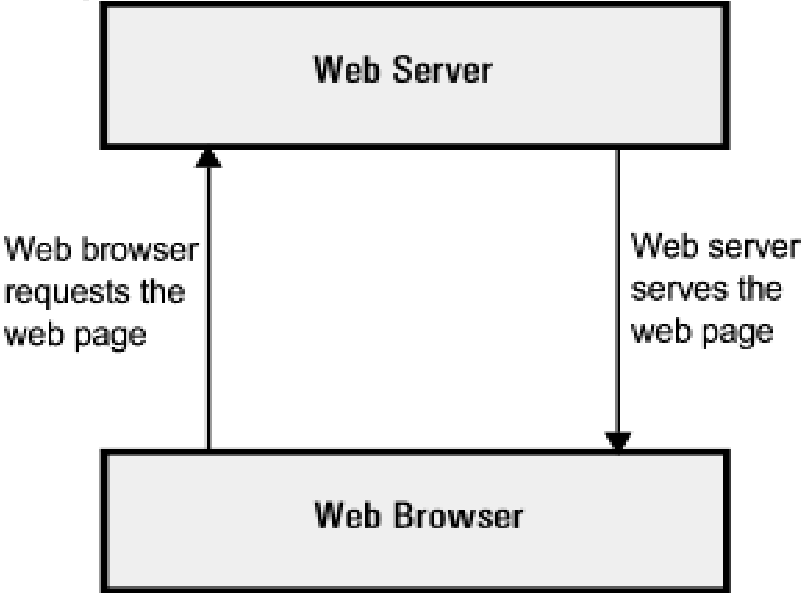
- First user types the website address for demanding the desired web page for example - **http://www.vtubooks.com/home.aspx** and then the home page of this website appears on the screen.
- The web address is divided into three parts:
  (i) The first part is the protocol. The **http** is a hypertext transfer protocol which tells the web browser that user wishes to communicate with web server on **port 80**. Port 80 is reserved for the communication between web server and web browser.
- The second part is the server address. This tells the web browser which server it needs to contact in order to retrieve the information you are looking for. The web browser communicates with a **Domain Name Server (DNS)** to find out the IP Address for the website. All communications on the internet use IP Addresses for communications. Use of the numeric address for accessing the web server is avoided because it is easier to remember textual information than that of numeric one. Hence normally the web server's addresses are textual.
- The third part of this address donates the resource user wants to see.

Step 2:

The web browser, on locating the IP Address which it requires (by communicating with the name server), send a request directly to the web server, using port 80, asking for the file **home.aspx**.

Step 3:

The web server sends the html for this page back to user's web browser. If there are additional files needed in order to show the web page (like some images for example) the web browser makes additional requests for each of these.


Web Server
Web browser requests the web page
Web server serves the web page
Web Browser

Basic features of Web Browsers

1. Web browsers should be able to look at the web pages throughout internet or connect to various sites to access information.
2. The Web browser must enable you to follow the hyperlinks on a Web and type in a URL for it to follow. One of the main features of a browser is to search the information on the current page as well as search the WWW itself.
3. Browser give you the facility to save a web page in a file on your computer, print a Web page and send the contents of a Web page e-Mail to others on the internet.
4. Web browser should be able to handle text, images of the World Wide Web, as well as the hyperlinks to digital video, or other types of information.
5. Web browsers interact not just with the Web, but also with your computer's operating system and with other programs, called plug-ins that gives the browser enhanced features.

6. Another important feature to insist on in your browser is **caching**. A browser that caches keeps of the pages you visit so that it does not have to download them again if you want to return to them. Reloading a page from the cache is much quicker that downloading it again from the original source.

7. The most important feature of any browser is ease of use. While all Web browsers are fundamentally simple to use, it makes user comfortable.

Comparisons among popular Web Browsers:

S.No	Features	Firefox	Chrome	Internet Explorer
1.	Fast JavaScript engine for better performance	Yes	Yes	Yes
2.	Notifications when add-ons slow browser performance	No	No	Yes
3.	Simple browsing controls for better browsing experience	Yes	Yes	Yes
4.	Combined search and address bar	No	Yes	Yes
5.	Protection from malicious cross-site scripting attacks	Yes	Yes	Yes
6.	Automatic recovery of crashed tabs	Yes	Yes	Yes
7.	Compatibility mode to view websites designed for web browsers	No	No	Yes
8.	Developer tools built-in to the browser	No	Yes	Yes
9.	Reopen accidently crashed tab	No	Yes	Yes
10.	Best protection against the phishing attacks	Yes	No	Yes
11.	Different operating system	Windows, Linux, MAC	Windows, Linux, MAC	Windows, MAC

1.9 HTTP PROTOCOL

- **Hyper Text Transfer Protocol (HTTP)** takes part in web browser and web server communication. Hence it is called a **Communication protocol.** The basic features of HTTP protocol are that it follows the **request response model.** The client makes a request for desired web page by giving the URL in the address bar. This request is submitted to the web server and then web server gives response to the web browser by returning the required web page.

HTTP Request Message Structure

The basic structure of request message is given by following general form -

<start line>
<Header fields>
<Blank Line>
<Message Body>

Let us discuss this structure in detail:

Start line

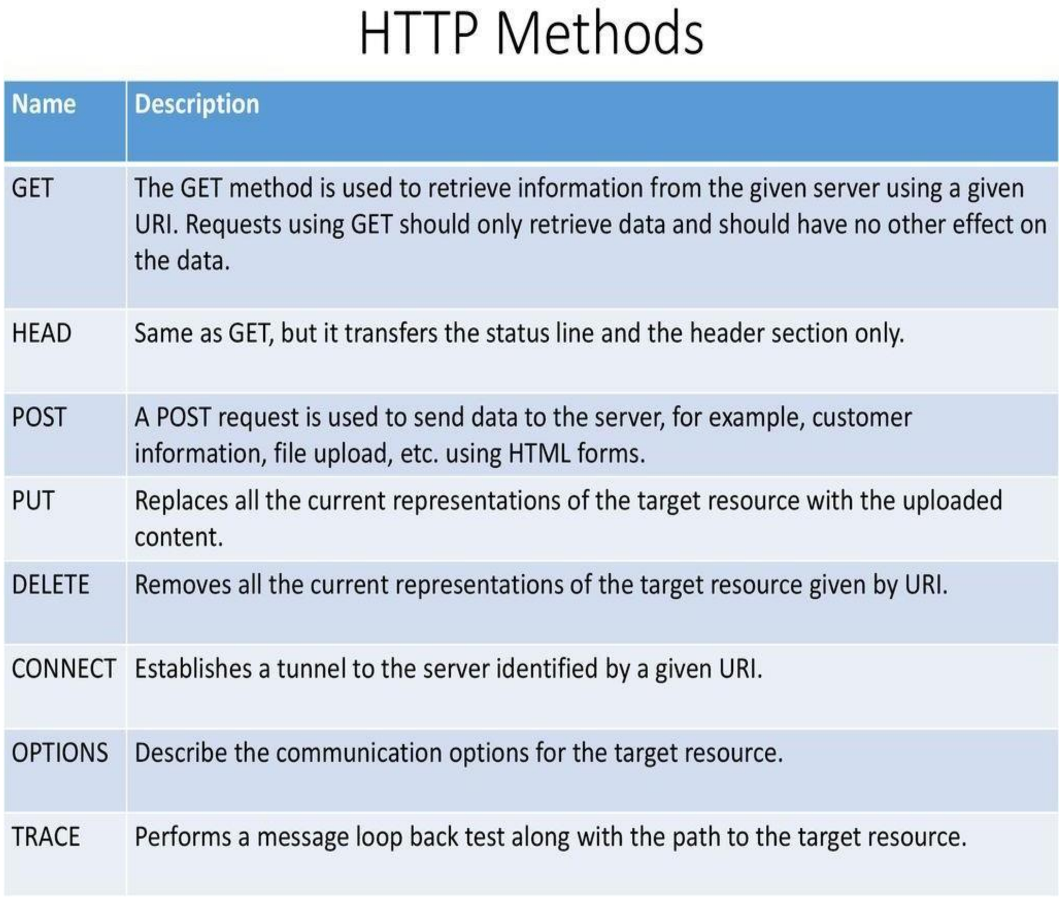
The **start line** consists of three parts which are separated by a single space. These parts are - 1) Request method 2) Request-URI 3) HTTP version

Request method:

The method defines the CONNECT method which is used during the web browser and server communication. It is always written in Upper Case letters. The primary method in HTTP is **GET.** The GET method is used when -

1. You type a URL in address bar.
2. When you click on some hyperlink which is present in the document.
3. When browser downloads images for display within a HTML document.

There is another commonly used method and i.e POST. The POST method is typically used to send information collected from a user form. Various methods used by HTTP are as given below-



HTTP Methods

Name	Description
GET	The GET method is used to retrieve information from the given server using a given URI. Requests using GET should only retrieve data and should have no other effect on the data.
HEAD	Same as GET, but it transfers the status line and the header section only.
POST	A POST request is used to send data to the server, for example, customer information, file upload, etc. using HTML forms.
PUT	Replaces all the current representations of the target resource with the uploaded content.
DELETE	Removes all the current representations of the target resource given by URI.
CONNECT	Establishes a tunnel to the server identified by a given URI.
OPTIONS	Describe the communication options for the target resource.
TRACE	Performs a message loop back test along with the path to the target resource.

Request URI

The **U**niform **R**esource **I**dentifier (URI) is a string used to identify the names or resources on the Internet. The URI is a combination of URL and URN. The URL stands for **U**niform **R**esource **L**ocator and URN stands for **U**niform **R**esource **N**ame. The web address denotes the URL and specific name of the place or a person or item denotes the URN. For examples

Urn: ISBN 978-81-8431-123-2 specifies the address of some book.

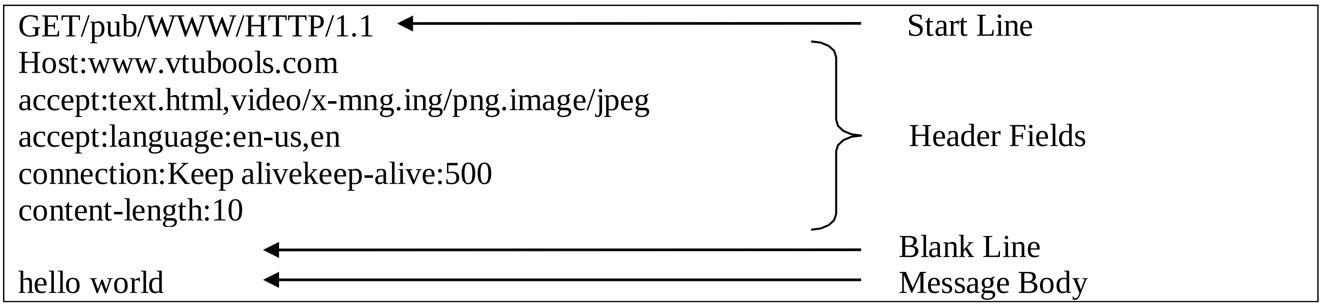
Every URI consist of two parts, the part before the colon: denotes the scheme and the part after colon depend upon the **scheme**. The URIs is case insensitive but generally written in lower case. If the URI is written in the form of http: then it is both an URI and URL but there are some other URI which can also be used as URL. For example

URL	Intended Server
ftp://ftp.mywebsite.com/index.txt	File can be located on FTP server
telnet://mywebsite.org	Telnet Server
mailtomyself@ mywebsite.org	Mail Box
http://www.mywebsite.org	Web Server

HTTP Version:
The first HTTP version was HTTP/0.9 but the official version of HTTP was HTTP/1.1.

Header Fields and Message body
The host header filed is associated with the HTTP request. The header files are in the form of field name and field value. Thus typical structure of http request is given in the diagram.

HTTP Request Message Structure:



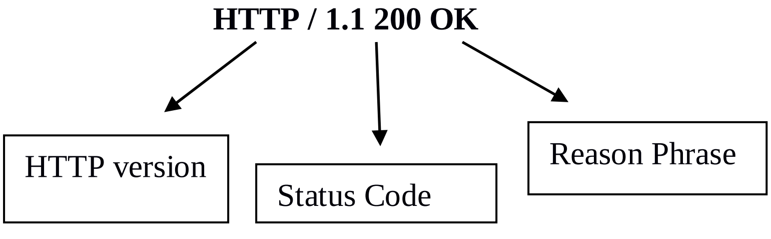
```
GET/pub/WWW/HTTP/1.1
Host:www.vtubools.com
accept:text.html,video/x-mng.ing/png.image/jpeg
accept:language:en-us,en
connection:Keep alivekeep-alive:500
content-length:10

hello world
```

HTTP Response Message Structure:
The structure of response message is similar to the request message structure. It is as follows
<status line>
<Header fields>
<Blank Line>
<Message Body>

Status Line:
Status line is similar to the start line in the request message. It consists of three fields.

HTTP Version	Status code	Reason phrase

The HTTP version denotes the HTTP version such as HTTP/1.1. The status code is a numeric code indicating the type of response. The reason phrase is in the text string form and presents the information about the status code.
For example –



Following table explains some commonly used status codes:

Status Code	**Reason Phrase**	**Description**
200	OK	This is a Standard response for request
201	Created	It shows that the request is fulfilled and a new resource is being created
202	Accepted	When the request is accepted for processing but is not processed yet is denoted by this status code.
301	Moved Permanently	The URI for requested resource is moved at some another location.
401	Unauthorized	The requested resource is protected by some passwords and the usedr has not provided any password.
403	Forbidden	The requested resource is present on the server but the server is not able to respond it.

The header field in the response message is similar to that of the request message. The message body consists of response message.

For example

```
HTTP/1.1 200 OK
Date: Fri, 1 Jan 2010 07:59:01 GMT
Server:Apache/2.0.50 (Unix) mod_perl/1.99_10 perl/v5.8.4
Mod_ssl/2.0.50 OpenSSL/0.9.7d DAV/2 PHP/4.3.8
Last-Modified: Mon, 23 Feb 2009 08:32:41 GMT
Accept-Ranges: bytes
Conten-Length:2010
Content-Type: text/html
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01
Transitional//EN">
<html>…</html>
```

The response header fields are enlisted in the following table:

Header field	**Description**
Date	It represents the date and thme at which the response is generated
Server	The name of the server which is responding.
Last-Modified	The date and time at which the response is last modified.
Accept-ranges	It specifies the unit which is used by the client to accept the range request.For example if there is a large document and only a single web page is currently needed then this specifies the Accept-range

Cache Control:

Many times the response header files are used in conjunction with cache control. Cache is used as a repository. Use of cache improves the system performance. Many browsers stores web pages viewed by the client in the cache memory. This brings efficiency in browsing web pages. For instance, client reads a daily Newspaper on his PC then caching the corresponding web address or web pages will quickly display the web page.

HTTP Tunnelling:

HTTP Tunnelling is a mechanism by which the communication performed by various network protocol is encapsulated by the HTTP Protocol. HTTP tunnelling can be used in the chat like applications for communications from network locations with restricted connectivity.

The application that wishes to communicate with a remote host opens an HTTP connection to a mediator server. Using HTTP request the host communicates with the mediator server by encapsulating the actual communications within those requests. The mediator server then unwraps the data and sends to the remote destined hosts. The remote host when sends the response to the requesting hosts, wraps the response in the HTTP protocol and then the response is given. In this case the application becomes the tunnelling point.

Features of HTTP Protocol:

1. It is a communication protocol used between the web browser and web server.
2. This protocol is based on request-response messaging. That means client makes the request of desired web pages and then the server responds it by sending the requested resource.
3. It is a stateless protocol. That means HTTP protocol cannot remember the previous user's information not it remembers the number of times the user has visited particular website.
4. The request-response message consists of plain text fairly in readable form.
5. The HTTP protocol has a cache control. This is an advanced feature of HTTP. Most of the web browsers automatically store the recently visited pages. This is very useful feature because if the user requests the same web pages that have been visited already then it can be displayed from the cache memory instead of requesting the web server and bringing it from there.

1.10 AUTHORING TOOLS

Definition:

A web authoring tool is a software package which developers use to create and package e-learning content deliverable to end users. The multimedia authoring tools provide the capability for creating a complete multimedia presentation, including interactive user control.

Some examples of the authoring tools are:

1. Macromedia Flash
2. Macromedia Director
3. Author ware
4. Quest

Authoring software provides an integrated environment for combining the content and functions of a project. It enables the developer to create, edit, and import data. In multimedia authoring tools, multimedia elements and events are considered as object. Each object is assigned properties and modifiers. On receiving messages, the objects perform tasks depending upon properties and modifiers.

Features of Authoring tools:

1. Programming Features:

Authoring tools offer the programming using high level languages or support for scripting environment. The tools that offer the programming features are Macromedia Flash, HyperCard, Metacard and Tool Book. Some authoring tools offer direct importing of preformatted text, including facilities, complex text search mechanisms and hyper linkage tools. Visual authoring tools such as Author ware and Icon Author are suitable for slideshows and presentations.

2. Interactivity features:

The interactivity feature allows the user to have control flow of information. Using the interactivity features the contents are well organized by the user. The conditional branching support the complex programming logic, subroutines, event tracking and message passing among objects and elements.

3. Editing and organizing features:

The elements of multimedia – image, animation, text, digital audio and MIDI music and video clips need to be created, edited and converted to standard file formats and the specialized applications provide these capabilities. Editing tools for these elements, particularly text and still images are often included in as authoring tools. Some authoring tools provide a visual flowcharts system or overview facility for illustrating your project's structure at a macro level. Storyboards navigation diagrams too can help organize a project.

4. Delivery Features:

Delivering your project may require building run time version of the project using the multimedia authoring software. A run time version allows your project to play back without requiring the full authoring Multimedia Systems software and all its tools and editors. Many times the run time version does not allow user to access or change the content, structure and programming of the project.

5. Cross Platform feature:

By this feature, it is possible to transfer the content across the platform easily. The run time players are available for providing the compatibility to the authoring tool sto work in other platforms.

Examples of Authoring Tools:

1. Macromedia Flash:

Adobe Flash Player is a multimedia platform which has become the standard for implementing animation and interactivity into web pages to create ads, integrate video into websites.

2. HyperCard:

It is a hypermedia program created for Macintosh Computer. It combines database abilities with a graphical, flexible, user-modifiable interface. HyperCard also features Hyper talk, a programming language for manipulating data and the user interface.

3. Front Page:

It is a website administration tool from Microsoft for the Microsoft windows. FrontPage consists of a Split View option to allow the user to code in code view and preview in design view without the hassle of switching from the design view and code view tabs for each review. Interactive Buttons gives users a new way to create web graphics for navigation and links eliminating the need for a complicated package.

4. Dreamweaver:

Dreamweaver is a web authoring tool rather than a multimedia tool. It does however support a wide range of multimedia file types. These include graphics formats such a s JPEG, GIF, PNS as well as Short wave files. Support exists for embedding other media such as audio and video within HTML or a script. A range of interactive elements are pre-scripted as behaviours, including some that can be used for multimedia and interactivity. An extensive range of languages including HTML, XML, ASP, PHP, JSP, JavaScript and VBScript are supported by Dreamweaver.

5. Netobjects Fusion:
It is a tool that is a solution for small business websites, from planning, building and managing your site to promoting and growing online business quickly and effectively. One can drag images, text and other objects anywhere on the page and simply drop them in. The Netobjects fusion is the first program to remove the tedious hand coding from creating pixel-precise page layouts in HTML.

1.11 TYPES OF SERVER

Application Server - Web Server - Database Server

Web Server:

Web servers are computers that deliver (*serves up*) Web pages. Every Web server has an IP address and possibly a domain name. For example, if you enter the URL *http://www.webopedia.com/index.html* in your browser, this sends a request to the Web server whose domain name is *webopedia.com*. The server then fetches the page named *index.html* and sends it to your browser.

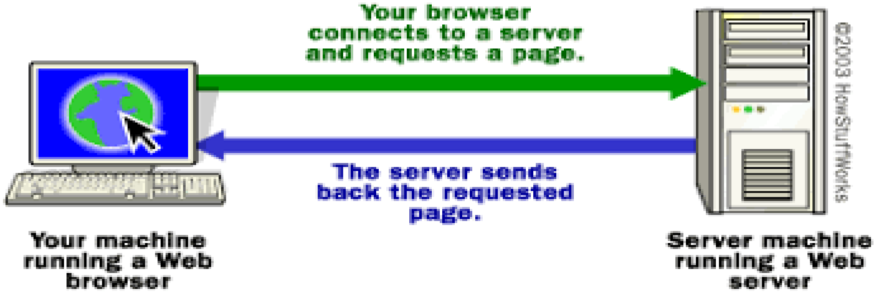
Any computer can be turned into a Web server by installing server software and connecting the machine to the Internet. There are many Web server software applications, including public domain software and commercial packages.

Functions of web server:

- The web server accepts the requests from the web browser.
- The user request is processed by the web server
- The web server responds to the users by providing the services which they demand for over the web browsers.
- The web servers serve the web based applications
- The DNS translate the domain names into the IP addresses
- The server verifies for the given address, finds the necessary files, runs appropriate scripts, exchange cookies if necessary and returns back to the browser
- Some servers actively participate in session handling techniques.

Examples of web servers: Apache web server, IIS web server

Apache web server	IIS web server
Apache web server is useful on both Unix based systems and on Windows platform	IIS web server is used on Windows Platform
It is an open source product that provides reliability and efficiency	It is vendor specific product and can be used on windows product only
The Apache web server can be controlled by editing the configuration file httpd.conf	For IIS web server, the behaviour is controlled by modifying the window based management programs called IIS snap-in. We can access IIS snap-in through the Control -Panel ->Administrative Tools
It is also called a free web server named as LAMP : (Linux/Apache/MySQL/PHP)	It is currently owned by Microsoft, and was designed with .NET frameworks.


Your browser connects to a server and requests a page.
The server sends back the requested page.
Your machine running a Web browser
Server machine running a Web server
©2003 HowStuffWorks

Database Server:

Database is a collection of information that is organized so that it can be easily accessed, managed and updated. Data is organized into rows, columns and tables and it is indexed to make it easier to find relevant information. Data gets updated, expanded and deleted as new information is added.

Database Management is a piece of software that manages databases and lets you create, edit and delete databases.

DBMS examples include MySQL, PostgreSQL, Microsoft Access, SQL Server, FileMaker, Oracle, RDBMS, dBase, Clipper, and FoxPro.

What is a database server?

It is similar to data warehouse where the website store or maintain their data and information. A Database Server is a computer in a LAN that is dedicated to database storage and retrieval. The database server holds the Database Management System (DBMS) and the databases. Upon requests from the client machines, it searches the database for selected records and passes them back over the network**.**

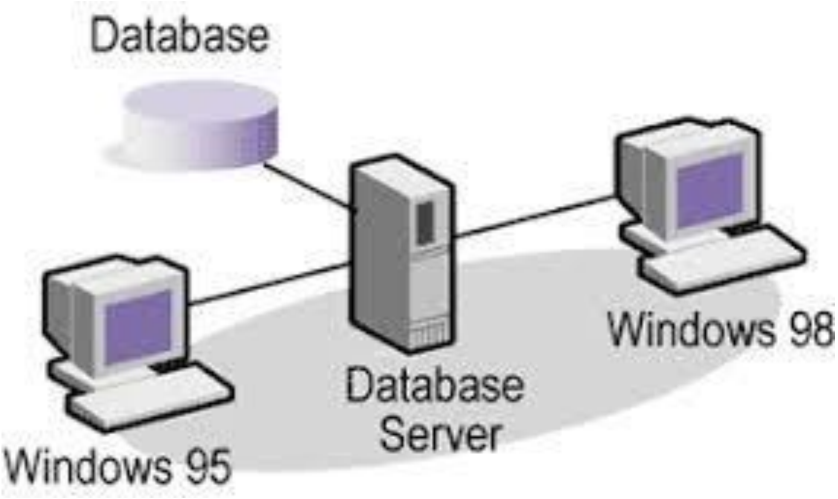
A database server can be defined as a server dedicated to providing database services. Such a server runs the database software. A database server can typically be seen in a client-server environment where it provides information sought by the client systems.

A database server is useful for organizations that have a lot of data to deal with on a regular basis. If you have client-server architecture where the clients need process data too frequently, it is better to work with a database server. Some organizations use the file server to store and process data. A database server is much more efficient than a file server.

In Database Network the client execute SQL requests to the database server. The Network Database Server Process the client database request and the executed answers of SQL command are come back over the network computer. In the whole concept Database server serves its own power to process the request or search the requested result. The Database server some time also known as SQL engine.

All database functions are controlled by the database server. Any type of computer can be used as database server. It may be microcomputer, minicomputer or mainframe computer. In large organization networks, the mainframe computers are used as server. Some people refer to the central DBMS functions as the back-end functions, whereas the application programs on the client computer as front-end programs. You can say that client is the application, which is used to interface with the DBMS, while database server is a DBMS.

The Database server manages the recovery security services of the DBMS. It enforces the constraints that are specified inside the DBMS. It controls and manages all the clients that are connected to it. It handles all database access and control functions. It provides concurrent access control. It provides better security and server hides the DBMS from clients. It provides the multi-user environment. Several users can access the database simultaneously. All the data is stored on the data server therefore, the DBA can easily create the backup of the database.



Application Server:

An application server is a server program in a computer in a distributed network that provides the business logic for an application program. The application server is frequently viewed as part of a three-tier application, consisting of a graphical user interface (GUI) server, an application (business logic) server, and a database and transaction server. More descriptively, it can be viewed as dividing an application into:

- A first-tier, front-end, Web browser-based graphical user interface, usually at a personal computer or workstation
- A middle-tier business logic application or set of applications, possibly on a local area network or intranet server
- A third-tier, back-end, database and transaction server, sometimes on a mainframe or large server

The examples of application servers:

Jboss : open-source server from Jboss community
Glassfish: provided by Sun Microsystem, now acquired by Oracle
Weblogic : provided by Oracle
Websphere : provided by IBM

Comparison among Various Types Of Servers

Application Server	Web Server
A server that exposes business logic to client applications through various protocols including HTTP	A server that handles HTTP protocol
Application server is used to serve web based applications and enterprise based application (i.e servlets and JSP). Application server may contain a web server internally	Web server is used to serve web based applications (i.e servlets and JSP)
Resource utilization is high	Resource utilization is low

Web Server	Database Server
Web server makes use of the languages like PHP , ASP, JSP. It makes use of the protocols such as FTP and HTTP	The database server has its own specific program language or query language.
Web server is used to save the static and dynamic contents and pages of website	Database server deals with the storing and managing the data of a computer or computer programs
Web server only performs web based services	Database server can manage the web based, enterprise based services at the same time
Apache HTTP server, Microsoft Internet Information Services (IIS), Google Web Server(GWS) and Sun Java Systems web server are examples of web server	Oracle , SAP, MySQL and DB2 are some common examples of database server.

UNIT II
NETWORKING ESSENTIALS

Fundamentals of computer network – Types of computer networks – Network layer – TCP / IP model – Wireless Local Area Network – Ethernet – Wifi – Network Routing – Switching – Network Components

1. FUNDAMENTALS COMPUTER NETWORKS

Communication means to convey a message, a picture, speech or an idea that is received and understood clearly and correctly by the person for whom it is conveyed. Network is a set of devices connected by media links. The link connecting the devices is often called communication channels. Computer networking consists of two or more computers that are linked in order to share resources, exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams. Data communication consists of five elements. They are sender, receiver, message, transmission medium and protocol.

- **Sender:** Sender machine creates data and send it to the receiver machine.
- **Receiver:** Receive data and information from sender
- **Message:** The message is the information or data, that is to be communicated. It may consist of text, numbers, pictures, sounds, videos or any combination devices.
- **Protocol:** A set of rules that defines how data is formatted and processed on a network.
- **Transmission media**: It is a path between sender and receiver .Message is transmitted through this medium.

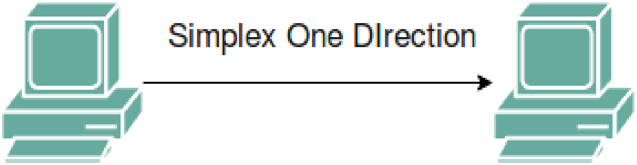
Point – to – Point link: In data communication, the point to point is commonly used to establish a direct connection between two networking devices. Point – to – point networks provide a dedicated link between any two stations. The data packets are sent from source station to the destination.

Multi-point link: Multi-point communication means one to many i.e. one source machine communicate with multiple receiver machine.

Transmission Modes in Computer Networks (Simplex, Half-Duplex and Full-Duplex)

a. Simplex Mode

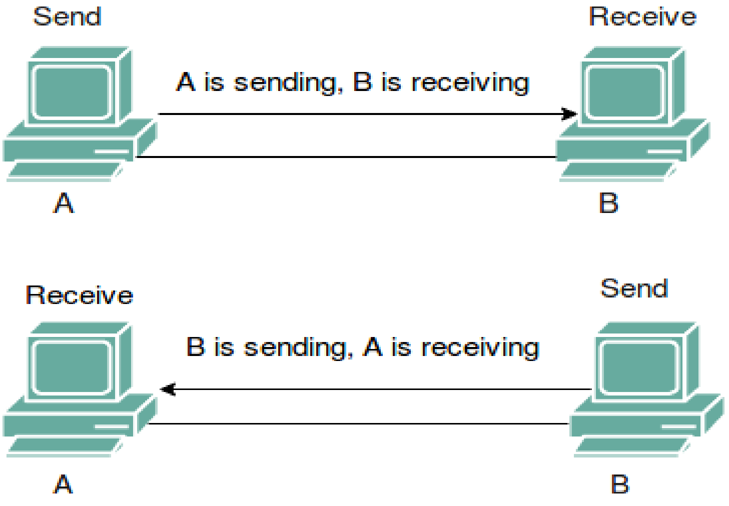
In Simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit, the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction. Example: Keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.



b.Half-Duplex Mode

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time. The entire capacity of the channel can be utilized for each direction.

Example: Walkie- Talkie in which message is sent one at a time and messages are sent in both the directions.

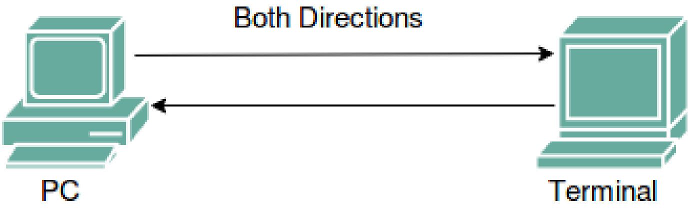


c. Full-Duplex

In full-duplex mode, both stations can transmit and receive simultaneously. In full_duplex mode, signals going in one direction share the capacity of the link with signals going in other direction, this sharing can occur in two ways:

- Either the link must contain two physically separate transmission paths, one for sending and other for receiving.
- Or the capacity is divided between signals travelling in both directions.

Full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however must be divided between the two directions. Example: Telephone Network in which there is communication between two persons by a telephone line, through which both can talk and listen at the same time.



Topologies

The physical topology of a network refers to the configuration of cables, computers, and other peripherals:

- Mesh
- Star
- Ring
- Bus
- Hybrid

a) Mesh Topology

Key Characteristics:

- Fully connected
- Robust – Highly reliable
- Not flexible
- Poor expandability

Media used for the connection (links) can be twisted pair, co-axial cable or optical fiber.. Mesh Topology is not flexible and has a poor expandability as to add a new node **‘ n’**links have to be laid because that new node has to be connected to each of the existing nodes via dedicated link, for the same reason the cost of cabling will be very high for a larger area.

b) Star Topology

- Each machine is connected to a central hub or switch.
- It allows each machine on the network to have a point to point connection to the central hub.
- All of the traffic which transverses the network passes through the central hub.
- The hub acts as a signal booster or repeater which in turn allows the signal to travel greater distances.
- Most widely implemented, Hub is the single point of failure.

Advantages	Disadvantages
Easily expanded without disruption to the network	Requires more cable
Cable failure affects only a single user	A central connecting device allows for a single point of failure
Easy to troubleshoot and isolate problems.	More expensive than bus topologies because of the cost of the hubs

c) Ring Topology

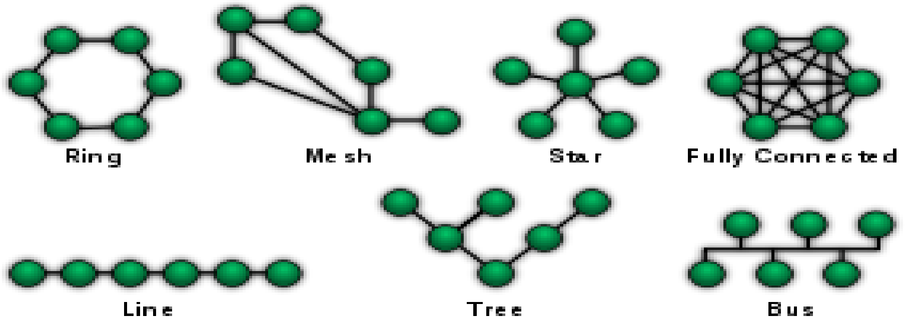
- Each computer is connected to the network in a closed loop or ring.
- Each machine or computer has a unique address that is used for identification purposes.
- The signal passes through each machine or computer connected to the ring in one direction.
- Ring topologies typically utilize a token passing scheme, used to control access to the network. Ring technique is based on the use of a small frame called a token that circulates when all the stations are idle. Whenever a station wishes to send a frame it waits until it receives a token. Since ring topologies use token passing to control access to the network, the token is returned to sender with the acknowledgement.
- Ring speeds are 4Mbps, 16 Mbps and 100 Mbps and uses twisted pair and fibre optic cable.
- By utilizing this scheme, only one machine can transmit on the network at a time.

Advantages	Disadvantages
Cable faults are easily located, making troubleshooting easier	Expansion to the network can cause network disruption
Ring networks are moderately easy to install	A single break in the cable can disrupt the entire network.

d) Bus Topology

- Each machine is connected to a single cable.
- Each computer or server is connected to the single bus cable through some kind of connector.
- A signal from the source travels in both directions to all machines connected on the bus cable until it finds the address on the network that is the intended recipient.
- If the machine address does not match the intended address for the data, the machine ignores the data.
- Alternatively, if the data does match the machine address, the data is accepted.

Advantages	Disadvantages
Cheap and easy to implement	Network disruption when computers are added or removed
Require less cable	High cost of managing the network Single point of failure.
Does not use any specialized network equipment	A break in the cable will prevent all systems from accessing the network. Difficult to troubleshoot.



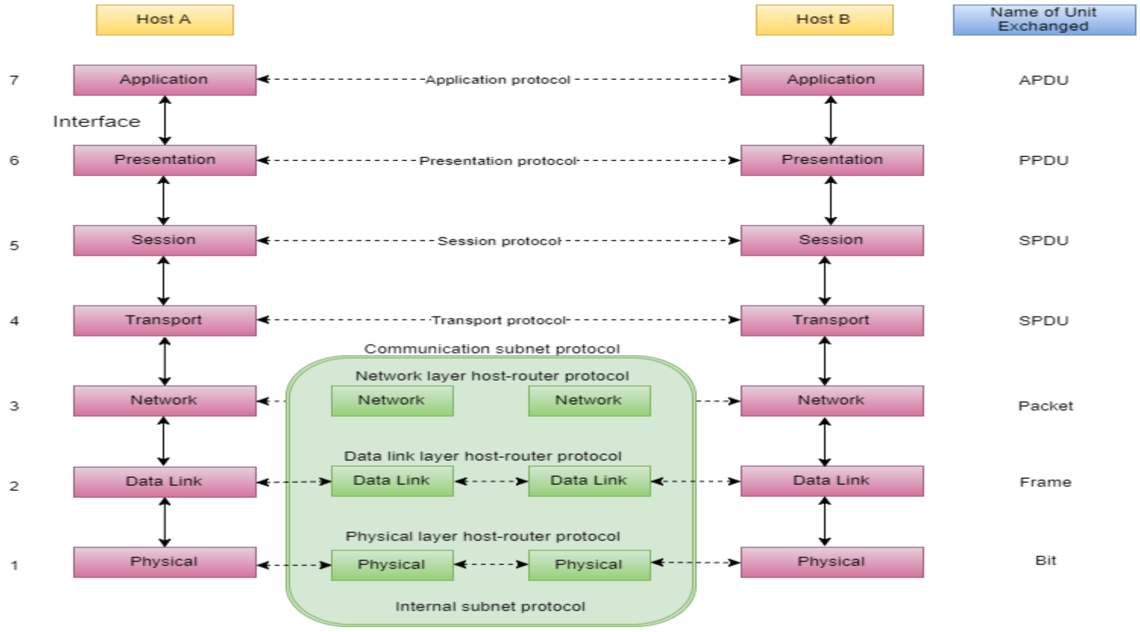
1.1 THE OSI MODEL

There are n numbers of users who use computer network and are located over the world. So to ensure, national and worldwide data communication, systems must be developed which are compatible to communicate with each other ISO has developed a standard. ISO stands for **International organization of Standardization**. This is called a model for **Open System Interconnection** (OSI) and is commonly known as OSI model.

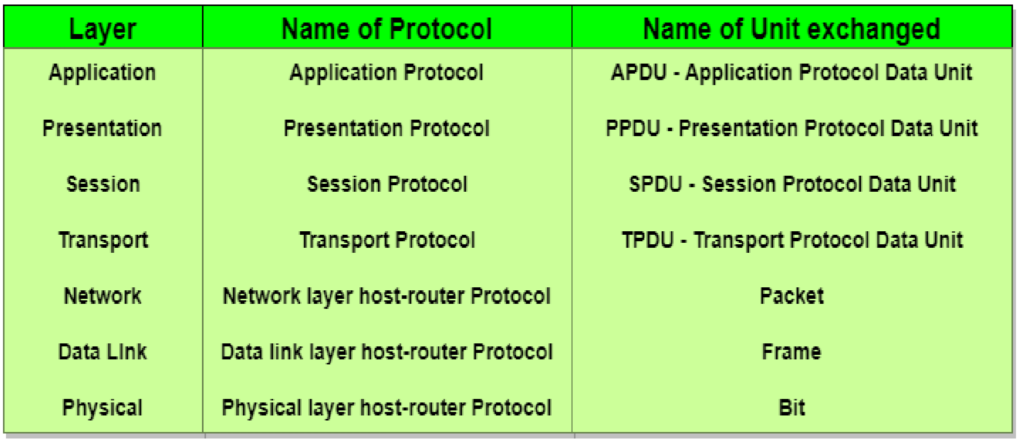
The ISO-OSI model is a seven layer architecture. It defines seven layers or levels in a complete communication system. They are:

1. Application Layer
2. Presentation Layer
3. Session Layer
4. Transport Layer
5. Network Layer
6. Datalink Layer
7. Physical Layer

Below we have the complete representation of the OSI model, showcasing all the layers and how they communicate with each other.



In the table below, we have specified the **protocols** used and the **data unit** exchanged by each layer of the OSI Model.



Layer	Name of Protocol	Name of Unit exchanged
Application	Application Protocol	APDU - Application Protocol Data Unit
Presentation	Presentation Protocol	PPDU - Presentation Protocol Data Unit
Session	Session Protocol	SPDU - Session Protocol Data Unit
Transport	Transport Protocol	TPDU - Transport Protocol Data Unit
Network	Network layer host-router Protocol	Packet
Data Link	Data link layer host-router Protocol	Frame
Physical	Physical layer host-router Protocol	Bit

Feature of OSI Model

1. Big picture of communication over network is understandable through this OSI model.
2. We see how hardware and software work together.
3. We can understand new technologies as they are developed.
4. Troubleshooting is easier by separate networks.
5. Can be used to compare basic functional relationships on different networks.

Principles of OSI Reference Model

The OSI reference model has 7 layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

1. A layer should be created where a different abstraction is needed.
2. Each layer should perform a well-defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that architecture does not become unwieldly.

Functions of Different Layers

Following are the functions performed by each layer of the OSI model. This is just an introduction, we will cover each layer in details in the coming tutorials.

Layer 1: The Physical Layer

1. Physical Layer is the lowest layer of the OSI Model.
2. It activates, maintains and deactivates the physical connection.
3. It is responsible for transmission and reception of the unstructured raw data over network.
4. Voltages and data rates needed for transmission is defined in the physical layer.
5. It converts the digital/analog bits into electrical signal or optical signals.
6. Data encoding is also done in this layer.

Layer 2: Data Link Layer

1. Data link layer synchronizes the information which is to be transmitted over the physical layer.
2. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
3. Transmitting and receiving data frames sequentially is managed by this layer.
4. This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.
5. This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.

Layer 3: The Network Layer

1. Network Layer routes the signal through different channels from one node to other.
2. It acts as a network controller. It manages the Subnet traffic.
3. It decides by which route data should take.
4. It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.

Layer 4: Transport Layer

1. Transport Layer decides if data transmission should be on parallel path or single path.
2. Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer
3. It receives messages from the Session layer above it, convert the message into smaller units and passes it on to the Network layer.
4. Transport layer can be very complex, depending upon the network requirements.

Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

Layer 5: The Session Layer

1. Session Layer manages and synchronize the conversation between two different applications.
2. Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

Layer 6: The Presentation Layer

1. Presentation Layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data.
2. While receiving the data, presentation layer transforms the data to be ready for the application layer.
3. Languages(syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.
4. It perfroms Data compression, Data encryption, Data conversion etc.

Layer 7: Application Layer

1. Application Layer is the topmost layer.
2. Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc are services provided by application layer.
3. This layer mainly holds application programs to act upon the received and to be sent data.

Merits of OSI reference model

1. OSI model distinguishes well between the services, interfaces and protocols.
2. Protocols of OSI model are very well hidden.
3. Protocols can be replaced by new protocols as technology changes.
4. Supports connection oriented services as well as connectionless service.

Demerits of OSI reference model

1. Model was devised before the invention of protocols.
2. Fitting of protocols is tedious task.
3. It is just used as a reference model.

2. TYPES OF COMPUTER NETWORKS

Computer Networks can be categorized depending on their size, distance and the structure namely: LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network).

LAN (Local Area Network)

A **Local Area Network** is a privately owned computer **network** covering a **small Networks geographical area,** like a home, office, or groups of buildings e.g. a school Network. It is used to connect the computers and other network devices so that the devices can communicate with each other to share the resources. The resources to be shared can be a hardware device like printer, software like an application program or data. The size of LAN is usually small.

Characteristics of LAN:	**Advantages of LAN:**
• Easy resource sharing • Data transfer rate are high • Small area covered by LAN • Cost of setting up the network is usually low • Flexibility, low error rate, reliability of operation and simple maintenance	• Availability to share hardware andsoftware resources • Support for heterogeneous forms ofhardware and software • Access to other LANs and WANs • Private ownership • Secure transfers at high speed with low error rates

MAN (Metropolitan Area Networks)

MAN stands for Metropolitan Area Networks is one of a number of types of networks. A MAN is a relatively new class of network. MAN is larger than a local area network and as its name implies, covers the area of a single city. MANs rarely extend beyond 100 KM and frequently comprise a combination of different hardware and transmission media. A MAN can be created as a single network such as Cable TV Network, covering the entire city or a group of several Local Area Networks (LANs). It this way resource can be shared from LAN to LAN and from computer to computer also. MANs are usually owned by large organizations to interconnect its various branches across a city.

The two most important components of MANs are security and standardization. Security is important because information is being shared between dissimilar systems. Standardization is necessary to ensure reliable data communication.

A MAN often acts as a high speed network to allow sharing of regional resources (similar to a large LAN). It is also frequently used to provide a shared connection to other networks using a link to a WAN. MAN provides the transfer rates from 34 to 150 Mbps.

WAN (Wide Area Networks)

A wide area network (WAN) is a telecommunication network. A wide area network is simply a LAN of LANs or Network of Networks. WANs connect LANs that may be on opposite sides of a building, across the country or around the world. WANS are characterized by the slowest data communication rates and the largest distances. WANs can be of two types: an enterprise WAN and Global WAN.

WANs (wide area networks) generally utilize different and much more expensive networking equipment than do LANs (Local Area Networks). Key technologies often found in WANs (wide area networks) include SONET, Frame Relay, and ATM. Each node in a WAN is a router that accepts an input packet, examines the destination address, and forwards the packet on to a particular telecommunication line. A router must select the one transmission line that will provide a path to the destination and in an optimal manner.

In a WAN, when the packet is sent from one router to another via one or more intermediate routers, the packets is received at each intermediate router in its entirety. This packet is stored in that router until the required output line is free. WAN uses hierarchical addressing because they facilitate routing. Addressing is required to identify which network input is to be connected to which network output.

3. TCP/IP MODEL:

TCP/IP stands for Transmission Control Protocol/ Internet Protocol. This model is based on a five layer model for networking: Physical layer, Datalink layer, network layer, transport layer and application layer. The TCP/IP protocol stack is open. The TCP/IP protocol stack models a series of protocol layers for networks and systems that allows communication between any types of devices.

TCP breaks messages into packets, hands them off to IP software for delivery, and then orders and reassembles the packets at their destinations. IP stands for the Internet Protocol. It deals with the routing of packets through the maze of interconnected networks to their final destination. At the physical and Datalink layers, the TCP/IP protocols do not define any standards.

Application Layer
Transport Layer
Internet Layer
Datalink layer
Physical Layer

Fig: TCP/IP Protocol suite

Functions of TCP/IP Layers:

1. Application Layers: Application layer includes all process and services that uses the transport layer to deliver the data. The original TCP/IP Specification described a number of different applications that fit into the top layer of the protocol stack. These applications include Telnet, FTP, SMTP and DNS. TELNET is the Network Terminal Protocol, which provides remote login over the network. FTP is used for interactive file transfer. SMTP delivers electronic mail.

2. Transport Layer: This layer provides communication session management between host computers. It also defines the level of services and status of the connection used when transporting data. It also manages connection oriented steams, flow control, reliable transport and multiple transmissions. Application programs send the data to the transport layer protocols TCP and UDP. An application is designed to choose either TCP/UDP based on the services it needs. The transport layer provides peer entities on the source and destination hosts to carry on a conversation. Data may be user data or control data. Two modes are available- full duplex and half duplex. In full-duplex operation, both sides can transmit and receive data simultaneously, whereas in half-duplex, a side can only send or receive at one time.

3. Network or Internet Layers: Packages data into IP datagrams, which contain source and destination address information that is used to forward the datagrams between hosts and across networks. It performs routing of IP datagrams.

The internet/network level protocol (IP, ARP, ICMP) handles machine to machine communication. The primary protocol used to move data is the IP which provides fragmentation and addressing services. IP provides a connectionless method of delivering data from one host to another. It does not guarantee delivery and does not provide sequencing of datagrams. It attaches a header to datagram that includes source address and destination address, both of which are unique Internet Addresses.

4.Network Interface Layer: It contains two sub layers: DataLink Layer and Physical Layer. This layer is also called as host to network layer. This layer cannot define any protocol. It is responsible for accepting and transmitting IP datagrams. This layer may consist of a device driver in the operating systems and the corresponding network interface card in the machine. It specifies details of how data is sent physically sent through the network including how the bits are electrically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber or twisted pair copper wire.

Addressing:
An Internet employing TCP/IP protocols uses four level of addresses:

Physical Address: It is the lowest address and is also referred to as link address. The physical address of the node is defined by its LAN or WAN. The physical address is included in the frame by the data link layer.

Logical Address: Logical addresses are necessary for universal communications. It is a 32-bit address which uniquely defines host connected to Internet.

Port Address: In TCP/IP architecture, the label assigned to a process is called Port address. In TCP/IP the port address is of 16 bit.

Specific Address: They get changed to corresponding port and logical addresses by the station or the host who sends it.

Difference between TCP and IP

TCP	IP
TCP is used to transfer packet data	IP is responsible for logical addressing
TCP guarantees transfer of packet on a particular address	IP obtains that particular address
TCP breaks messages to packets and hands them off to the IP for software delivery, orders and then reassemble the packets at their destinations	IP deals with the routing of packets through the maze of interconnected networks to their final destination.
TCP is connection oriented protocol	Connectionless protocol
Reliable	Not Reliable

4. NETWORK LAYER

The main objective of the network layer is to allow end systems, connected to different networks, to exchange information through intermediate systems called router. The unit of information in the network layer is called a packet. It is responsible for addressing messages and data so that they are sent to the correct destination, and for translating logical addresses and names into physical addresses. This layer is also responsible for finding the path through the network to the destination computer. Lowest layer that deals with host-to-host communication, call this end-to-end communication.

Functions of Network Layer:

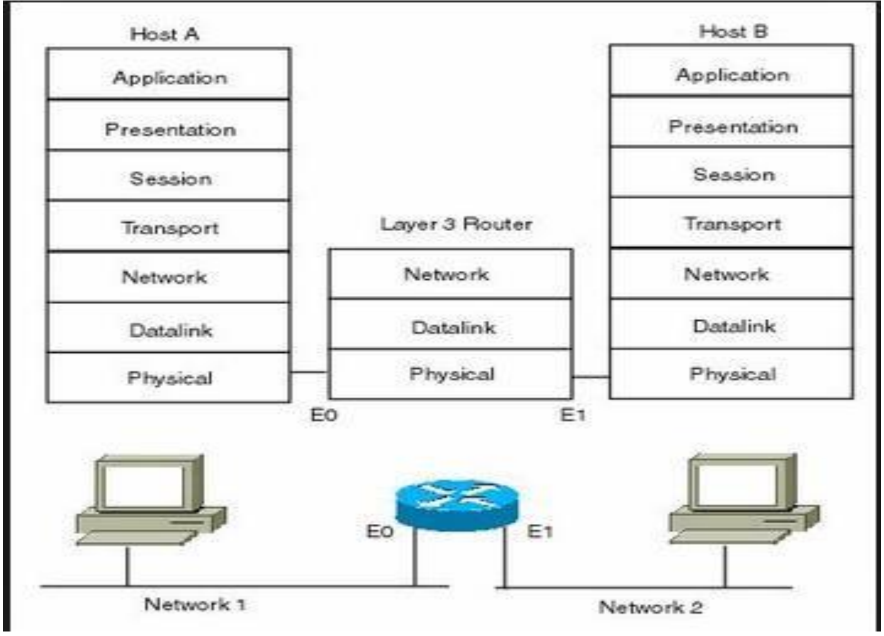
a) Logical Addressing- Data link layer implements physical addressing. When a packet passes network boundary, an addressing system is needed to distinguish source and destination, network layer performs these functions.

b)Routing- Network layer route or switch the packets to its final destinations in an internetwork.

c)Frame Fragmentation- If it determines that a downstream router's Maximum Transmission Unit(MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assemble at the destination station.

Principle of network Layer:

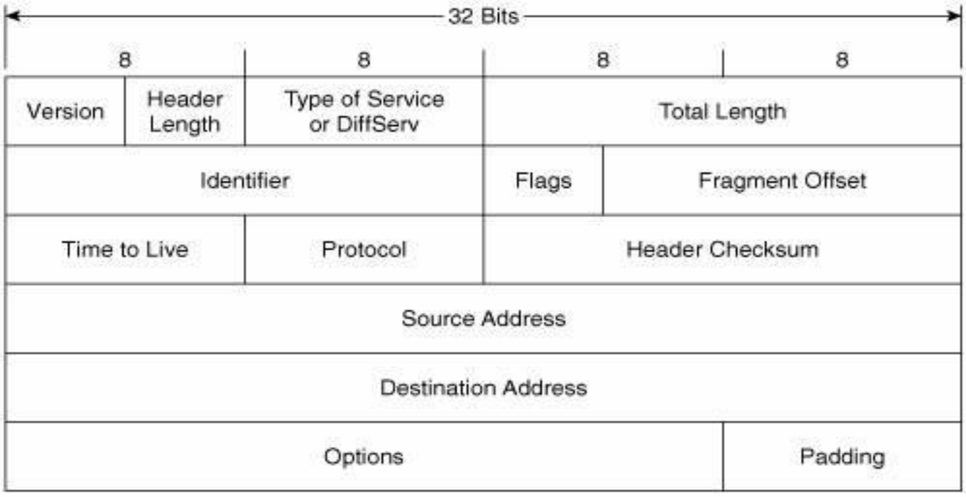
Each network layer entity is identified by a network layer address. This address is independent of the data link layer addresses that it may use. The network layer is conceptually divided into data plane and the control Plane. The data plane consists of protocols and mechanisms that allow hosts and routers to exchange packets carrying user data. The control plane contains the protocols and mechanisms that enable routers to efficiently learn how to forward packets towards their final destination. Datagram is used to provide a connectionless service while a virtual circuit is used in networks that provide a connection oriented service. Datagram is a type of packet that happens to be sent in a connectionless manner over the network. Every datagram carries enough information to let the network forward the packet to its correct destination. The network layer limits the maximum packet size.



5. IP Address:

Each computer in a TCP/IP network must be given a unique identifier, or IP address. This address, which operates at Layer 3, allows one computer to locate another computer on a network. All computers also have a unique physical address, which is known as a MAC address. These are assigned by the manufacturer of the NIC. MAC addresses operate at Layer 2 of the OSI model. An IP address (IPv4) is a 32-bit sequence of ones and zeros. To make the IP address easier to work with, it is usually written as four decimal numbers separated by periods. For example, an IP address of one computer is 192.168.1.2.. This dotted decimal notation also prevents a large number of transposition errors that would result if only the binary numbers were used.

IPV4 Format:



Version:(4 bits): Indicates the version number, to allow evolution of the protocol.
Internet Header Length(IHL 4 bits): Length of header in 32 bit words. The minimum value is five for a minimum header length of 20octets.
Type-of-Service: The Type-of-Service field contains an 8-bit binary value that is used to determine the priority of each packet. This value enables a Quality-of-Service (QoS) mechanism to be applied to high priority packets, such as those carrying telephony voice data. The router processing the packets can be configured to decide which packet it is to forward first based on the Type-of-Service value.

Total length: total datagram length, in octets.
Identifier (16 bits): A sequence number that, together with the source address, destination address, and user protocol, is intended to uniquely identify a datagram.
Fragment Offset: A router may have to fragment a packet when forwarding it from one medium to another medium that has a smaller MTU. When fragmentation occurs, the IPv4 packet uses the Fragment Offset field and the MF flag in the IP header to reconstruct the packet when it arrives at the destination host. The fragment offset field identifies the order in which to place the packet fragment in the reconstruction.
Flags(3 bits): Only two of the bits are currently defined: MF(More Fragments) and DF(Don't Fragment):
More Fragments flag (MF): The More Fragments (MF) flag is a single bit in the Flag field used with the Fragment Offset for the fragmentation and reconstruction of packets When a receiving host sees a packet arrive with the MF = 1, it examines the Fragment Offset to see where this fragment is to be placed in the reconstructed packet. When a receiving host receives a frame with the MF = 0 and a non-zero value in the Fragment offset, it places that fragment as the last part of the reconstructed packet. An unfragmented packet has all zero fragmentation information (MF = 0, fragment offset =0).
Don't Fragment flag (DF): The Don't Fragment (DF) flag is a single bit in the Flag field that indicates that fragmentation of the packet is not allowed. If they Don't Fragment flag bit is set, then fragmentation of this packet is NOT permitted. If a router needs to fragment a packet to allow it to be passed downward to the Data Link layer but the DF bit is set to 1, then the router will discard this packet.
IP Destination Address: The IP Destination Address field contains a 32-bit binary value that represents the packet destination Network layer host address.
IP Source Address: The IP Source Address field contains a 32-bit binary value that represents the packet source Network layer host address.

Time to Live: The Time-to-Live (TTL) is an 8-bit binary value that indicates the remaining "life" of the packet. The TTL value is decreased by at least one each time the packet is processed by a router (that is, each hop). When the value becomes zero, the router discards or drops the packet and it is removed from the network data flow. Decrementing the TTL value at each hop ensures that it eventually becomes zero and that the packet with the expired TTL field will be dropped.
Protocol: This 8-bit binary value indicates the data payload type that the packet is carrying. The Protocol field enables the Network layer to pass the data to the appropriate upper-layer protocol. Example values are: 01 ICMP, 06 TCP, 17 UDP.
Header checksum (16 bits): An error-detecting code applied to the header only. Because some header fields may change during transit (e.g., time to live, segmentation-related fields), this is re-verified and recomputed at each router. For purposes of computation, the checksum field is itself initialized to a value of zero.
Options (variable): Encodes the options requested by the sending user.
Padding (variable): Used to ensure that the datagram header is a multiple of 32 bits.

5. WLANS - WIRELESS LOCAL AREA NETWORKS

A WLAN, or wireless LAN, is a network that allows devices to connect and communicate wirelessly. Unlike a traditional wired LAN, in which devices communicate over Ethernet cables, devices on a WLAN communicate via Wi-Fi.

The primary difference is how the data is transmitted. In a LAN, data is transmitted over physical cables in a series of Ethernet packets containing. In a WLAN, data is transmitted over the air using one of Wi-Fi 802.11 protocols.

Advantages of WLAN

- Devices are connected wirelessly, eliminatingthe need for cables.
- It also provides a way for small devices, such as smartphones and tablets, to connect to the network.
- WLANs are not limited by the number of physical ports on the router and therefore can support dozens or even hundreds of devices.
- The range of a WLAN can easily be extended by adding one or more repeaters.

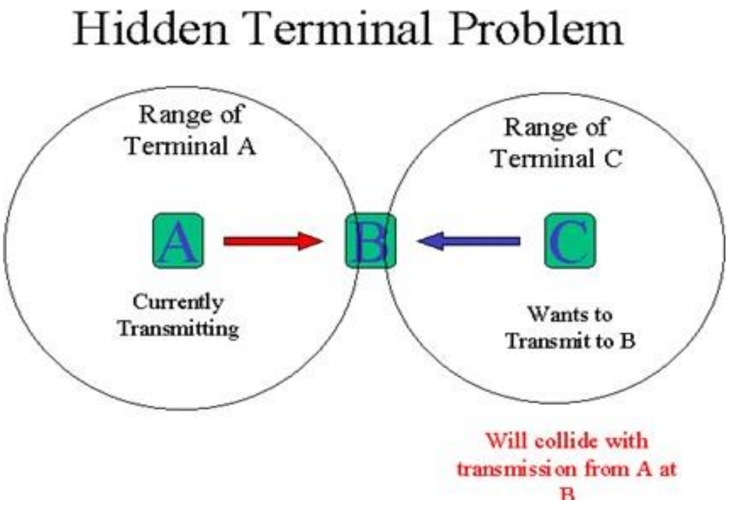
Disadvantages of WLAN

- Wireless networks are naturally less secure than wired networks.
- Any wireless device can attempt to connect to a WLAN, so it is important to limit access to the network if security is a concern. wireless networks are more susceptible to interference from other signals or physical barriers.

Hidden Terminal:

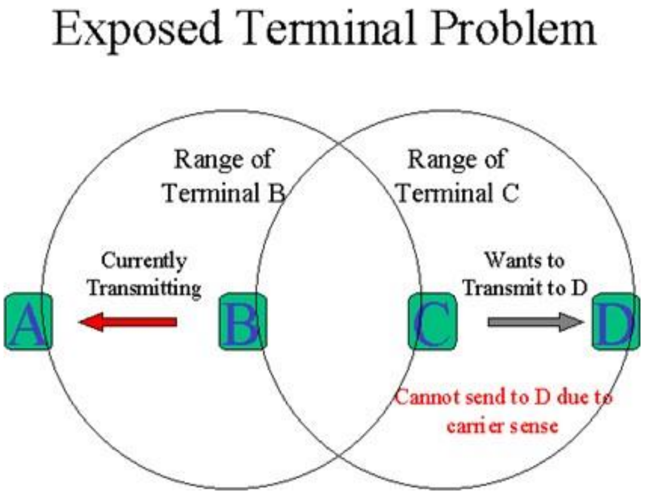
- As seen in the above problem, the transmission range of A reaches B but not C. Similarly, the range of C reaches B but not A. Also the range of B reaches both A and C.
- Now, the node A starts to send something to B and C doesn't receive this transmission.
- Now C also wants to send data to B and senses the carrier. As it senses it to be free, it also starts sending to B.
- Hidden terminal problem occurs when two nodes that is outside each other's range performs simultaneous transmission to a node that is within the range of each of them resulting in a collision.

- That means the data from both parties A and C will be lost during the collision.
- Hidden nodes mean increased probability of collision at receiver end.
- One solution to avoid this is to have the channel sensing range much greater than the receiving range. Another solution is to use the Multiple Access with Collision Avoidance
  (MACA).



Exposed Terminal:

- Consider the same above diagram. Here imagine a situation wherein the B node is currently sending some data to node A.
- Now the other node C which is right now free want to send data to some node D(not in diagram) which is outside the range of A and B.
- Now before starting transmission it senses the carrier and realizes that the carrier is busy (due to interference of B’s signal).
- Hence, the C node postpones the transmission to D until it detects the medium to be idle.
- However such a wait was un-necessary as A was outside the interference range of C.
- Also a collision at B will be a weak enough to be unable to penetrate into C
- Exposed terminal problem occurs when the node is within the range of a node that is transmitting and it cannot be transmitted to any node. Exposed node means denied channel access unnecessarily which ultimately results in under-utilization of bandwidth resources. It also results in wastage of time-resource



WLAN Protocols:

Multiple Accesses with Collision Avoidance (MACA) is a slotted media access control protocol used in wireless LAN data transmission to avoid collisions caused by the hidden station problem and to simplify exposed station problem. The basic idea of MACA is a wireless network node makes an announcement before it sends the data frame to inform other nodes to keep silent. When a node wants to transmit, it sends a signal called *Request-To-Send* (RTS) with the length of the data frame to send. If the receiver allows the transmission, it replies the sender a signal called *Clear-To-Send* (CTS) with the length of the frame that is about to receive. Meanwhile, a node that hears RTS should remain silent to avoid conflict with CTS; a node that hears CTS should keep silent until the data transmission is complete.

Multiple Access with Collision Avoidance (MACA) for Wireless LAN's

WLAN data transmission collisions may still occur, and the MACA for Wireless (MACAW) is introduced to extend the function of MACA. It requires nodes sending acknowledgements after each successful frame transmission, as well as the additional function of Carrier sense

Carrier Sense Multiple Access/Collision Avoidance

In CSMA/CA, as soon as a node receives a packet that is to be sent, it checks to be sure the channel is clear (no other node is transmitting at the time). If the channel is clear, then the packet is sent. If the channel is not clear, the node waits for a randomly chosen period of time, and then checks again to see if the channel is clear. This period of time is called the backoff factor, and is counted down by a backoff counter. If the channel is clear when the backoff counter reaches zero, the node transmits the packet. If the channel is not clear when the backoff counter reaches zero, the backoff factor is set again, and the process is repeated.

6. ETHERNET

Ethernet refers to the family of Local-Area Network (LAN) covered by the IEEE 802.3 standard that defines what is commonly known as the CSMA/CD protocol. Four data rates are currently defined for operation over optical fiber and twisted-pair cables : 10 Mbps-10 Base-T Ethernet, 100Mpbs-Fast Ethernet, 1000 Mbps-Gigabit Ethernet and 10,000 Mbps-10 Gigabit Ethernet. Ethernet uses a communication concept called datagrams to get message across the network. Ethernet uses a CSMA/CD multiple access algorithm.

Carrier Sense Multiple Access with Collision Detection (CSMA/ CD)

When node has data to transmit, the node first listens to the cable to see if a carrier(signal) is being transmitted by another node. This may be achieved by monitoring whether a current is flowing in the cable. The individual bits are sent by encoding them with a 10 clock using Manchester encoding. Data is only sent when no carrier is observed (i.e no current present) and the physical medium is therefore idle.

Any node which does not need to transmit, listens to see if other nodes have started to transmit information to it. The collision will result in the corruption of the frame being sent, which will subsequently be discarded by the receiver since a corrupted Ethernet frame will not have a valid 32- bit MAC CRC at the end.

If two or more stations have messages to send at the same time and they are separated by significant distances on the bus/channel, each may begin transmitting at roughly the same time without being aware of the other station. The signals from each node will superimpose on the channel and is garbled beyond the decoding ability of the receiving station. This is termed as "collision".

When there is data waiting to be sent, each transmitting node also monitors its own transmission. If it observes a collision, it stops transmission immediately and instead transmits a 32-bit jam sequence. The purpose of this sequence is to ensure that any other node which may currently be receiving this frame will receive the jam signal in place of the correct 32-bit MAC CRC, this causes the other receivers to discard the frame due to a CRC error. When two or more transmitting nodes each detect a corruption of their own data (i.e a collision), each responds in the same way by transmitting the jam sequence.

MAC addresses

- Every device connected to an Ethernet network has a unique MAC address, assigned by the manufacturer of the network card. Its function is like that of an IP address, since it serves as a unique identifier that enables devices to talk to each other.

Preamble (7 bytes)	**Start Frame Delimiter (1 byte)**	**Destination Address (6 bytes)**	**Source Address (2 bytes)**	**Length or Type (2 bytes)**	**Data and Padding**	**CRC (4 bytes)**

- **Preamble** allows the receiver to synchronize with the signal. It is a sequence of alternating 0 and 1.
- **Start Frame Delimiter (SFD):** The sequence 10101011, which indicates the actual start of the frame and enables the receiver to locate the first bit of the rest of the frame.
- Both the source and destination host address are identified with a 48 bits address.
- **Type** field serves as the de-multiplexing key, i.e. it identifies to which of possibly many higher level protocols this frame should be delivered.
- **Data**: It is a minimum of 46 bytes and a maximum of 1500 bytes. The reason for minimum frame size is that the frame must be long enough to detect a collision.

- **CRC**: This field contains error detection information.
- Ethernet is a bit oriented protocol. Each frame transmitted on an Ethernet is received by every adaptor connected to that Ethernet.

7. WiFi

- WiFi means “Wireless Fidelity”. It is a wireless technology that uses radio frequency to transmit data through the air. The standard for Wireless Local Area Networks (WLANs). It’s actually IEEE 802.11, a family of standards. WiFi is based on the 802.11 standard: 802.11a and 802.11g.WiFi systems are the half duplex shared media configuration, where all stations transmit and receive on the same radio channel.

- WiFi combines concepts found in CSMA/CD and MACAW, but also offers features to preserve energy. The developers of the 802.11 specifications develop a collision avoidance mechanism called the Distributed Control Functions(DCF). According to DCF, a WiFi station will transmit only when the channel is clear. All transmissions are acknowledged, so if a station does not receive an acknowledgement, it assumes a collision occurred and retires.

ISM Band

- ISM stands for industrial, scientific and medical. ISM bands are set aside for equipment that is related to industrial or scientific processes or is used by medical equipment. Perhaps the most familiar ISM-band device is the microwave oven, which operates in the 2.4-Ghz ISM band. The ISM bands are license-free, provided that devices are low-power. You don’t need a license to set up and operate a wireless network.

- WLAN Architecture: **Ad-Hoc mode**: Peer-to-peer setup where clients can connect to each other directly. Generally not used for business networks. Mobile stations communicate to each other directly. It’s set up for a special purpose and for a short period of time. For example, the participants of a meeting in a conference room may create an ad hoc network at the beginning of the meeting and dissolve it when the meeting ends.

WiFi networks services are as follows:

Distribution: This service is used by mobile stations in an infrastructure network every time they send data. Once a frame has been accepted by an access point, it uses the distribution service to deliver the frame to its destination. Any communication that uses an access point travels through the distribution service, including communications between two mobile stations associated with the same access point.

Integration: is a service provided by the distribution system, it allows the connection of the distribution system to a non-IEEE 802.11 network. The integration function is specific to the distribution system used and therefore is not specified by 802.11, except in terms of the services it must offers.

Authentication/Deauthentication: Physical security is a major component of a wired LAN security solution. Wired network's equipment can be locked inside offices. Wireless network cannot offer the same level of physical security, however, and therefore must depend on additional authentication routines to ensure that users accessing the network are authorized to do so.

Deauthentication: terminates an authenticated relationship. Because authentication is needed before network use is authorized, a side effect of deauthentication is termination of any current association.

Association: Delivery of frames to mobile stations is made possible because mobile stations register, or associate, with access points. The distribution system can then use the registration information to determine which access point to use for any mobile stations.

Reassociations: When a mobile station moves between basic services areas within a single extended service area, it must evaluate signal strength and perhaps switch the access point with which it is associated.

8. ROUTING

Routing is the process of transferring the packets from one network to another network and delivering the packets to the hosts. The traffic is routed to all the networks in the internetwork by the routers. In the routing process a router must know following things:

- Destination device address.
- Neighbor routers for learning about remote networks.
- Possible routes to all remote networks.
- The best route with the shortest path to each remote network.
- How the routing information can be verified and maintained.

Definition of Static Routing

Static routing does not involve any change in routing table unless the network administrator alters or modify them manually. Static routing algorithms function well where the network traffic is predictable. This is simple to design and easy to implement. There is no requirement of complex routing protocols.

Static routing is also known as **non-adaptive** routing which enables a pre-computed route to be fed into the routers offline. The administrative distance is a metric to measure the trustworthiness of the information received from a router. The default administrative distance for static route is 1, consequently the static routes will only be included in the routing table when there is a direct connection to that network. Static routes can be considered as an efficient method for a small and simple network that does not change frequently.

Definition of Dynamic Routing

Dynamic routing is a superior routing technique which alters the routing information according to the changing network circumstances by examining the incoming routing update messages. When the network change occurs, it sends out a message to the router to indicate that change, the routing software recalculates routes and sends the new routing update message. These messages pervade the network, enabling the router to change their routing tables accordingly.

The technique uses routing protocols to disseminate knowledge such as RIP, OSPF, BGP, etc. Unlike static routing, it does not require manual updation instead its automatic in manner and updates the routing table information periodically relying upon network conditions. For doing so, it requires extra resources for storing the information.

Dynamic routing is also referred to as **adaptive routing**. These algorithms change their routing decisions to reflect the changes in the topology or traffic.

Basis for comparison	Static Routing	Dynamic Routing
Configuration	Manual	Automatic
Routing table building	Routing locations are hand-typed	Locations are dynamically filled in the table.
Routes	User defined	Routes are updated according to change in topology.
Routing algorithms	Doesn't employ complex routing algorithms.	Uses complex routing algorithms to perform routing operations.
Implemented in	Small networks	Large networks
Link failure	Link failure obstructs the rerouting.	Link failure doesn't affect the rerouting.
Security	Provides high security.	Less secure due to sending broadcasts and multicasts.
Routing protocols	No routing protocols are indulged in the process.	Routing protocols such as RIP, EIGRP, OSPF, BGP etc are involved in the routing process.
Additional resources	Not required	Needs additional resources to store the information.

Advantages and Disadvantages Static Routing

Advantages	Disadvantages
• Easily implemented in a small network. • No overheads are produced on router CPU. • Secure because the routes are managed statically. • It is predictable as the route to the destination is fixed. • Extra resources (such as CPU and memory) are not required as update mechanisms are not needed. • Bandwidth usage is not required between routers.	• Unsuitable for complex topologies and largenetworks. • Large networks increase configuration complexity and time consumption. • Link failure can hinder traffic rerouting. • The administrator must be extra careful while configuring the routes.

Advantages and Disadvantages of Dynamic Routing

Advantages	Disadvantages
• Suitable for all the topologies. • Network size doesn't affect the router operations. • Topologies are adapted automatically to reroute the traffic.	• Initially, it could be complicated toimplement. • The broadcasting and multicasting ofrouting updates make it less secure. • Routes rely on current topologies. • Additional resources are required such as CPU, memory and link bandwidth.

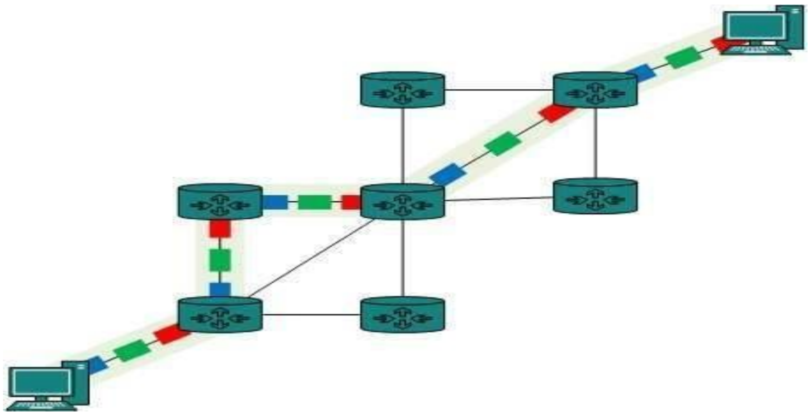
9. SWITCHING

Switching is process to forward packets coming in from one port to a port leading towards the destination.

Circuit Switching

When two nodes communicate with each other over a dedicated communication path, it is called circuit switching.There 'is a need of pre-specified route from which data will travel and no other data is permitted. In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place.Circuits can be permanent or temporary. Applications which use circuit switching may have to go through three phases:

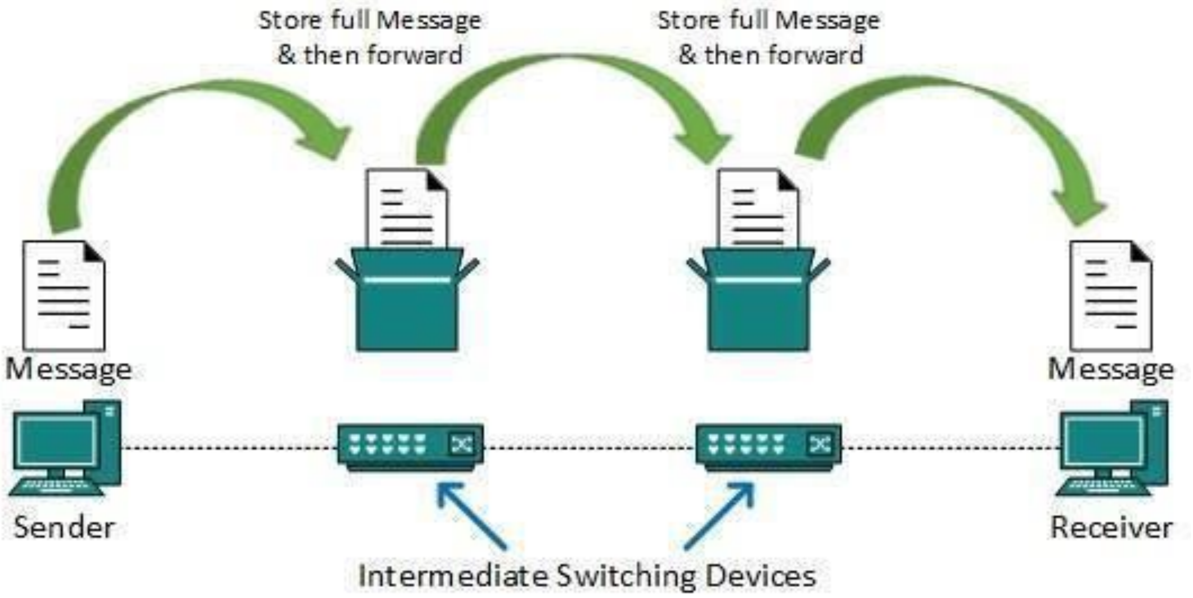
- Establish a circuit
- Transfer the data
- Disconnect the circuit



Circuit switching was designed for voice applications. Telephone is the best suitable example of circuit switching. Before a user can make a call, a virtual path between caller and callee is established over the network.

Message Switching

This technique was somewhere in middle of circuit switching and packet switching. In message switching, the whole message is treated as a data unit and is switching / transferred in its entirety. A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop. If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits.

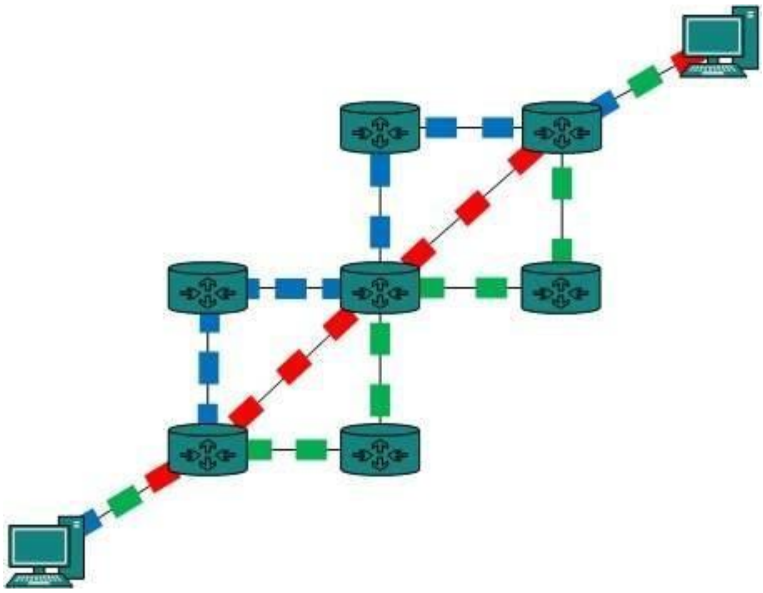


This technique was considered substitute to circuit switching. As in circuit switching the whole path is blocked for two entities only. Message switching is replaced by packet switching. Message switching has the following drawbacks:

- Every switch in transit path needs enough storage to accommodate entire message.
- Because of store-and-forward technique and waits included until resources are available, message switching is very slow.
- Message switching was not a solution for streaming media and real-time applications.

Packet Switching

Shortcomings of message switching gave birth to an idea of packet switching. The entire message is broken down into smaller chunks called packets. The switching information is added in the header of each packet and transmitted independently. It is easier for intermediate networking devices to store small size packets and they do not take many resources either on carrier path or in the internal memory of switches.



Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities. Packets are stored and forwarded according to their priority to provide quality of service.

10. NETWORK COMPONENTS

Computer network is a group of two or more computers that connect with each other to share a resource. **Sharing of devices and resources is the purpose of computer network.** You can share printers, fax machines, scanners, network connection, local drives, copiers and other resources.

Major computer network components include:

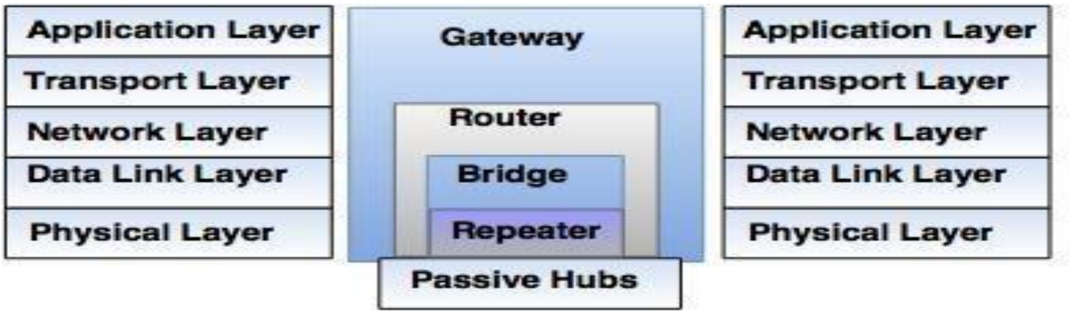
- **Repeater –**Repeater operate at the physical layer. It forwards bits from one LAN segment to another. The basic purpose of a repeater is to extend the distance of LAN. A repeater is a network device that is used to regenerate or replicate signals that are weakend or disorted by transmission over long distance and through areas with high levels of electromagnetic interference. Repeaters do not have physical addresses on the network and do not translate anything.
- **Bridge** – Bridge operates at the Data link layer. It has a single input and single output port. A bridge extends the maximum distance of network by connecting separate network segments. A bridge simply passes on all the signals it receives. It uses MAC addresses to handle traffic flow. Bridge performs data link functions such as error detection, frame formatting and frame routing.

  Advantages: Simple to use and install, transparent to users, additional software is not required, it forms single logical networks.

  Limitations: It suffers from broadcast storms, fault isolation is not provided.
- **Router –**When we talk about computer network components, the other device that used to **connect a LAN with an internet connection is called Router**. When you have **two distinct networks** (LANs) or want to share a single internet connection to multiple computers, we use a Router**.**
- **Gateway** – Gateway is combination of networking hardware and software that connects two dissimilar kinds of networks. A gateway is a protocol converter and operates on all seven layers of the OSI model. A gateway can accept a packet formatted for one protocol (TCP /IP) and convert it to a packet formatted for another protocol (Apple Talk) before forwarding it.
- **Network Interface Card (NIC) – Network adapter** is a device that enables a computer to talk with other computer/network. Using unique **hardware addresses (MAC address)** encoded on the card chip, the data-link protocol employs these addresses to discover other systems on the network so that it can transfer data to the right destination.

  There are **two types of network cards**: **wired and wireless**. The wired NIC uses cables and connectors as a medium to transfer data, whereas in the wireless card, the connection is made using antenna that employs radio wave technology.
- **Hub** –Hub is a device that splits a network connection into multiple computers. It is like a distribution center. When a computer request information from a network or a specific computer, it sends the request to the hub through a cable. The hub will receive the request and transmit it to the entire network. Each computer in the network should then figure out whether the broadcast data is for them or not.

- **Advantages**: most economical way of expanding network, simple, inexpensive network.
- **Limitations**: cannot connect different Ethernet types, hubs do not isolate collision domains
- **Switches** –Switch is a telecommunication device grouped as one of computer network components. Switch is like a Hub but built in with advanced features. It uses **physical device addresses** in each incoming messages so that it can deliver the message to the right destination or port. Like Hub, switch don't broadcast the received message to entire network, rather before sending it checks to which system or port should the message be sent.



Types of Connecting Devices

UNIT III- MOBILE ESSENTIALS

Cell phone working fundamentals – Cell phone frequencies & channels – Digital cell phone components – Generations of cellular networks – Cell phone network technologies / architecture – Voice calls & SMS

1. TERMS OF COMMUNICATIONS:

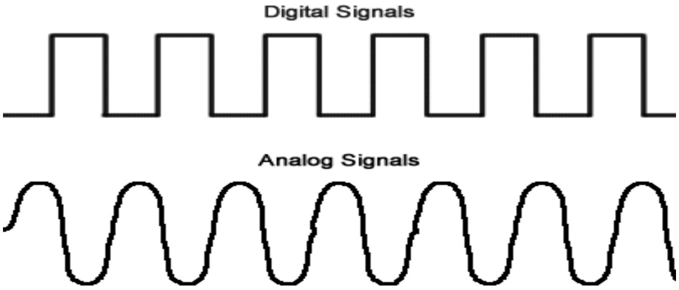
i) **Data and Information:** Data is defined as a raw-fact whereas the information is derived from the data.

ii) **Signals:** Signals are electromagnetic or electrical representations of data

iii) **Transmission:** Transmission is the communication of data by the propagation and processing of signals

iv) **Analog Data:** This takes continuous values in some intervals. For example: (i)voice and video are continuously varying patterns. (ii)Temperature and Pressure are continuous

v) **Digital Data:** This takes on discrete values. For example: Text and Integers.



vi) **Analog Transmission:** It is a way of transmitting analog signals without considering the content of the signals. The signal can either be analog data or digital data.

vii) **Digital Transmission:** Digital Transmission is concerned with the content of the signals.

2. FUNDAMENTALS OF CELLULAR NETWORKS:

In terrestrial communication high power transmitters are used so that the area covered is large. For example Radio communication. In mobile or cellular communication, low power transmitters are used. So the area covered is less when compared with terrestrial Communication. So, even for a small location, more number of transmitters are required. The coverage area of a cellular transmitter is called as cell and it is hexagonal in shape.

Cells:

In a cellular network, total area is subdivided into smaller areas called "cells". Each cell can cover a limited number of mobile subscribers within its boundaries. Each cell can have a base station with a number of RF channels. Frequencies used in a given cell area will be simultaneously reused at a different cell which is geographically separated. In wireless telephony, a cell is the geographical area covered by a cellular telephone transmitter. The transmitter facility itself is called the cell site. The essence of a cellular network is the use of multiple low power transmitters. Because the range of such a transmitter is small, an area can be divided into cells, each one served by its own antenna. Each cell is allocated a band of frequencies and is served by a base station. Each base station consists of a transmitter, receiver and a control unit.

Frequency: Frequency is the rate at which the signal repeats [in cycles per second].

Spectrum: The spectrum of a signal is the range of the frequency / frequencies that it contains.

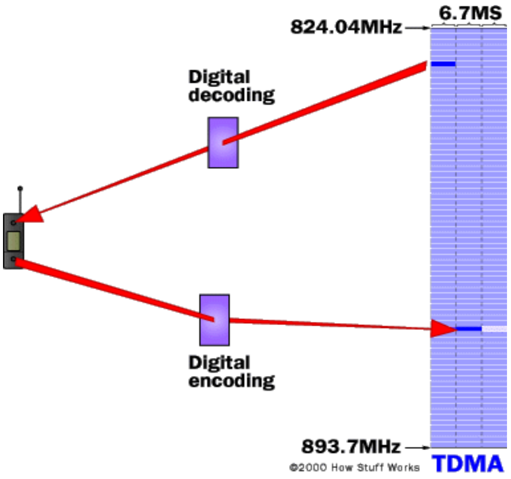
Frequency Reuse: In a cellular system, each cell has a base transceiver. The transmission power is carefully controlled to allowed communication within the cell using a given frequency band by limiting the power at that frequency that escapes the cell into adjacent cells. But, it is not possible to implement in practical usage to use the same frequency band in two adjacent cells. But it is possible to use them at some distance from one another. Key design issue is to determine the minimum separation between two cells using the same frequency band so that cells do not interfere with each other.

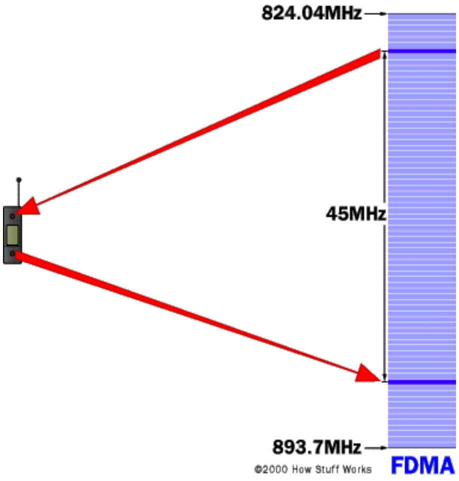
Reason for Hexagonal cell concept and not circular structure:

By using hexagonal concept, we can divide the geographical area into less number of transmitters used is less. In reality, the shape is irregular polygon. If we use circular concept, the hidden areas are not covered properly.

3. TECHNOLOGIES BASED ON SHARING:

TDMA: Narrow band means "channels" in the traditional sense. Each conversation gets the radio for one-third of the time. This is possible because voice data that has been converted to digital information is compressed so that it takes up significantly less transmission space. Therefore, TDMA has three times the capacity of an analog system using the same number of channels. TDMA systems operate in either the 800-MHz (IS-54) or 1900-MHz (IS-136) frequency bands. Time division multiple access (TDMA) is a channel access method (CAM) used to facilitate channel sharing without interference. TDMA allows multiple stations to share and use the same transmission channel by dividing signals into different time slots. Users transmit in rapid succession, and each one uses its own time slot. Thus, multiple stations (like mobiles) may share the same frequency channel but only use part of its capacity. TDMA is used in most 2G cellular systems, while 3G systems are based on CDMA



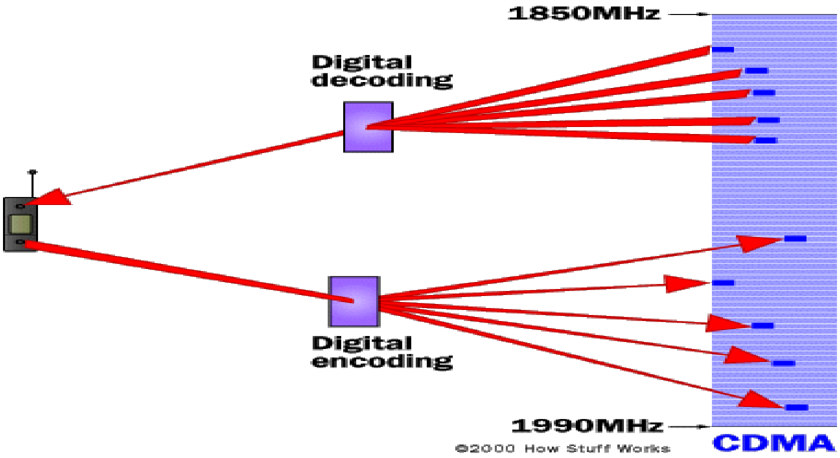


FDMA:

FDMA separates the spectrum into distinct voice channels by splitting it into uniform chunks of bandwidth. To better understand FDMA, think of radio stations: Each station sends its signal at a different frequency within the available band. FDMA is used mainly for analog transmission. While it is certainly capable of carrying digital information, FDMA is not considered to be an efficient method for digital transmission

CDMA:

CDMA takes an entirely different approach from TDMA. CDMA, after digitizing data, spreads it out over the entire available bandwidth. Multiple calls are overlaid on each other on the channel, with each assigned a unique sequence code. CDMA is a form of spread spectrum, which simply means that data is sent in small pieces over a number of the discrete frequencies available for use at any time in the specified range.



4. CELL PHONE FREQUENCIES AND CHANNELS:

- A cell phone carrier typically gets 832 radio frequencies to use in a city. Each cell phone uses two frequencies per call, a duplex channel. So there are typically 395 voice channels per carrier. (The other 42 frequencies are used for control channels).
- Therefore, each cell has about 56 voice channels available. In other words, in any cell, 56 people can be talking on their cell phone at one time. With digital transmission methods (2G), the number of available channels increases. For example, a TDMA-based digital system can carry three times as many calls as an analog system, so each cell has about 168 channels available.
- Frequency bands: Uplink: 890-915 MHz, Downlink:935-960 MHz
- Frequency range: 50 MHz (25 MHz Up, 25 MHz Down)
- Carrier spacing: 200 kHz (but time shared between 8 subscribers)
- Duplex distance: 45 MHz(FDD)
- Communication between the base station and mobiles is defined by the standard common air interface(CAI)
  1. **Forward voice channel (FVC) :** Voice transmission from base station to mobile.
  2. **Reverse voice channel (RVC) :** Voice transmission from mobile to base station.
  3. **Forward control channels (FCC):** Initiating mobile call from base station to mobile.
  4. **Reverse control channels (RCC):** Initiating mobile call from mobile to base station.
- Channels (frequencies) used in one cell can be reused in another cell some distance away, which allows communication by a large number stations using a limited number of radio frequencies.

Channel Assignment

- **Fixed channel assignment (FCA) :** Channels are pre-allocated to the cells during planning phase.
- **Dynamic channel assignment (DCA):** No pre-allocation. When a call comes/arrives at a cell then a channel not in use is selected.
- It requires the MSC to collect real time data, channel occupancy data, traffic distribution, radio signal strength, etc.,
- DCA schemes perform better under non-uniform and low traffic density. FCA performs well under high and uniform traffic.
- In FCA, the area is partitioned into a number of cells, and a number of channels are assigned to each cell according to some reuse pattern, depending on the desired signal

quality. Channel assignment schemes can be implemented in centralized or distributed fashion.

- In a centralized methods, the channels is assigned by a central controller, whereas in distributed methods a channel is selected either by the local base station of the call is initiated by the mobile. Channel assignment based on local assignment can be done for both FCA and DCA method.
- FCA method behave like a number of small groups of servers, while DCA provides a way of making these small group of servers behave like large servers.
- DCA method performs better under low traffic intensity. FCA method becomes superior at high offered traffic, especially in the case of uniform traffic.

Channel Borrowing:

- It is a combination of fixed and dynamic channel assignment. A channel set is nominally assigned to each cell.
- When all the channels in a cell are occupied, the cell borrows channels from other cells to accommodate the incoming new/handoff calls, as long as the borrowed channels do not interfere with the ones used by existing calls. Otherwise the call is blocked.
- The channel borrowing schemes are more flexible in the sense that by “moving” (borrowing) channels from less busy cells to more busy cells, a balanced performance throughout in the system can be achieved.
- Borrowing a channel x carries a penalty: cells that were originally allocated this channel x, may not be able to use this channel, since they may be within the co-channel interference range of the cell that borrowed the channel.
- Thus the decreased blocking probability at the cell that borrowed a channel is obtained at the cost of decreasing the capacity of other cells, which in turn causes QoS degradation in these cells.

5. CELL PHONE NETWORK TECHNOLOGIES/ ARCHITECTURE:

- In a cellular mobile communication system, the service area is divided into many small areas called cells. A cell station is installed in each, and tracking connections are carried out in accordance with the movements of the user.
- As users move across multiple cells in this system, it is always necessary to identify the cell in which the mobile stations are located. The essential control technologies to smoothly continue communications as users move among cells are “location registration” and “hand-over”.
- The cell configuration in mobile communication includes both large zone systems in which a single base station covers the entire service area, and cellular systems in which the service area is divided into several smaller areas, each of which has a base station.
- Although the large zone system can cover a larger service area as the radio waves can reach greater distances, the repeated use of frequencies is not possible except in more distant locations. Because the cellular system can repeatedly use limited frequency resources, it can cover global-scale service area with only a small number of frequency bandwidths.
- The basic consideration in cell configuration relates to the cell-shape repetition pattern. A method in which cells are combined in a pattern of hexagons has proved effective in both systems.
- Cells are amorphous (no uniform shape among cells), not a constant size and have overlap in areas of coverage. Cells area of coverage is determined by the distance limits for which a user can place a call with acceptable QoS.
- A useful modeling tool for cellular planning is the hexagonal cell layout. It minimizes cell overlap.

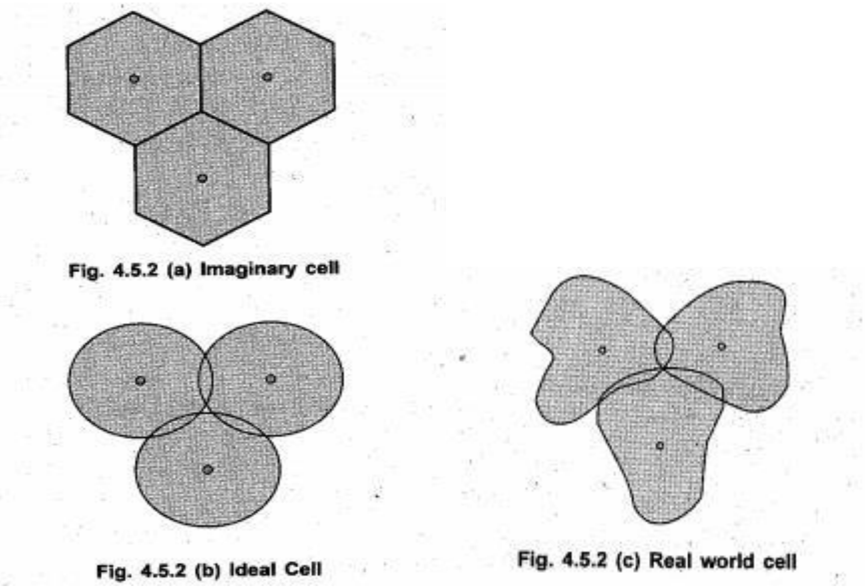


Fig. 4.5.2 (a) Imaginary cell

Fig. 4.5.2 (b) Ideal Cell

Fig. 4.5.2 (c) Real world cell

Location Registration:

- Under a cellular mobile communication system, connections cannot be automatically made unless the network side always identifies where the mobile unit is located as the unit itself is continuously moving in space, unlike the situation with a fixed telephone. The process that carries out this essential function is known as **location registration.**
- Location information is registered in the network via signals from the cell station to the mobile unit. When a location change is subsequently detected, the mobile unit updates its internal location registration and notifies the network.
- When the mobile unit is turned on, the mobile unit uses signal from the cell station to compare the location information stored within its internal memory, and notifies the network of the new registration location if it detects any difference.
- While location registration in cellular mobile communication systems is generally carried out by multiple-cell registration area units, frequent location registration switchovers can occur around cell boundaries due to fluctuation in reception levels.
- Overlay location registration is a method to establish an individual area for each mobile unit using the mobile unit's initial location registration point as the center. This can substantially reduce location registration traffic as re-establishing an overlay area with a new location registration point as the center is needed only if the mobile unit goes out of the initial overlay area.

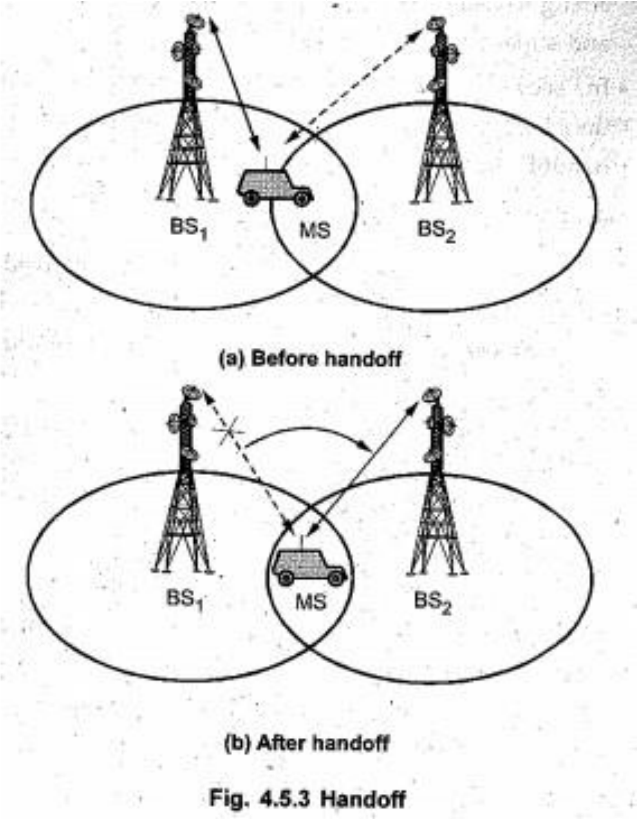
Handoff

- There are cases in which a mobile unit traverses multiple cells of a cellular mobile communication system during a call. This demands the use of "hand-over", the radio channel is switched over automatically to the appropriate cell during the call. Excessive signal interference can trigger "interference channel switchover" will select and switch the signal over to a radio channel within the same cell with less interference.
- When a registered phone moves closer to a stronger tower, the call is 'handed off'. The call is then routed through the new tower. This handoff is fully automatic and is generally transparent to the user. Sometimes, for technical reasons, a call may be routed to a weaker tower.
- Handover may take place in several condition:
  1. within the cell: Intracell handover
  2. between cells in the same cell layer: Intercell handover
  3. between cells of different layers: Interlayer handover
  4. between cells of different networks: Internetwork handover

- Handoff operation identifying a new base station and reallocating the voice and Control channels with the new base station.
- Handoff must ensure that the drop in the measured signal is not due to momentary fading and that the mobile is actually moving away from the serving base station.
- Dwell time: The time over which a call may be maintained within a cell without handoff .
- Dwell time depends on propagation, interference, distance and speed.
- Handoff measurement are as follows:

1. In first generation analog circular systems, signal strength measurements are made by the base station and supervised by the MSC.

2. In second generation systems (TDMA), handoff decisions are mobile assisted, called mobile assisted, called mobile assisted handoff (MAHO).



(a) Before handoff

(b) After handoff

Fig. 4.5.3 Handoff

Handoff Mechanism

- Base station continuously measure received signal strength indication.
- Based on this measurements decide the Handoff request.
- Once Handoff request is identified, asks adjacent cells to measure the RSSI on that mobile and send the measurements.
- Identifies the candidate cell for Handoff
- Start Handoff
- Handoffs are of two types: Hard and soft handoffs
- The hard handoff can be further divided into two different types: Intra and intercell handoffs
- The soft handoff can also be divided into two different types : multiway soft handoffs and softer handoffs.
- **Hard Handoff:** Early systems used a hard handoff. In a hard handoff, a mobile station only communicates with one base station. When the MS moves from one cell to another, communication must first be broken with the previous base station before communication

can be established with the new one. This may create a rough transition. The mobile ends communication with old base station BEFORE beginning communication with the new one.

- **Soft Handoff:** New systems use a soft handoff. In this case, a mobile station can communicate with two base stations at the same time. This means that, during handoff, a mobile station may continue with the new base station before breaking off from the old one. The mobile begins communication with the new base station BEFORE ENDING communications with the old.
- Soft handoff can only be used between CDMA channels having identical frequency assignments. Soft handoff provides diversity of Forward and Reverse Traffic channel paths on the boundaries between base stations.
- **Roaming**: Roaming means a user can have access to communication or can be reached where there is coverage. A service provider usually has limited coverage. Neighboring service provider can provide extended coverage through a roaming contract. The situation is similar to snail mail between countries. The charge for delivery of a letter between two countries can be divided upon agreement by the two countries.
- **Intersystem handoff:** If a mobile moves from one cellular system to a different cellular system controlled by a different MSC. Handoff requests is much important than handling a new call. The reason of handoff failures

a) No channel is available on selected BS

b) Handoff is denied by the network for reasons such as lack of resources. For example, no bridge or no suitable channel card, the MS has exceeded some limit on the number of handoffs that may be attempted in some period of time.

c) It takes the network too long to set up the handoff after it has been initiated.

d) The target link fails in some way during the execution of handoff.

Frequency Reuse:

- Cellular technology enables mobile communication because they use of a complex two-way radio system between the mobile unit and the wireless network.
- It uses radio frequencies (radio channels) over and over again throughout a market with minimal interference, to serve a large number of simultaneous conversations. This concept is the central tenet to cellular design and is called frequency reuse.
- Most frequency reuse plans are produced in groups of seven cells. Same frequency is reused by each sector.
- The number of cells per cluster defines the reuse pattern and this is a function of the cellular geometry. Cell sizes vary from some 100m upto 35 km depending on user density, geography, transceiver power etc. The hexagonal shape of cells is idealized.
- By limiting the coverage area to within the boundary of the cell, the channel groups may be reused to cover different cells.
- Consider a cellular system which has a total of S duplex channels. Each cell is allocated a group of k channels, k<S. The S channels are divided among N cells.
- The total number of available radio channels S=kN
- The N cells which use the complete set of channels is called cluster. The cluster can be repeated M times within the system. The total number of channels, C is used as a measure of capacity C=MkN = MS.
- The capacity is directly proportional to the number of replication M. The cluster size, N, is typically equal to 4, 7 or 12. Small N is desirable to maximize capacity.
- The frequency reuse factor is given by 1/N.

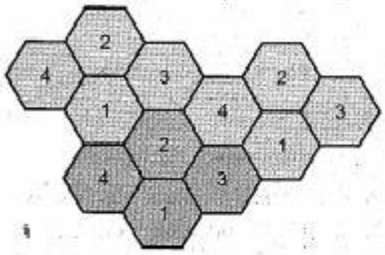


Fig. 4.5.6 (a) Frequency reuse factor =4

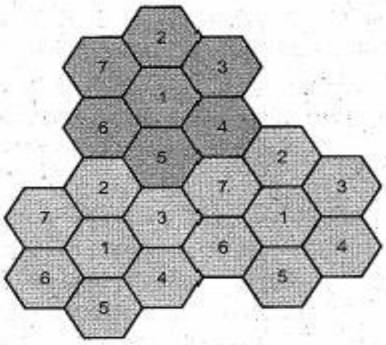


Fig. 4.5.6 (b) Frequency reuse factor =7

Cell Splitting

- Cell splitting increases the capacity of cellular system since it increases the number of times the channel are reused.
- Cell splitting – defining new cells which have smaller radius than original cells by installing these smaller cells. Capacity increases due to additional number of channels per unit area.
- Cell splitting is process of subdividing a congested cell into smaller cells each with its own base station.
- When traffic density starts to build up and frequency channels in each cell cannot provide enough mobile cells the original cell can be split into smaller cells.
- The original congested bigger cell is called macrocell and the smaller cells are called microcells.
- Capacity of cellular network can be increased by creating micro cells within the original cells which are having smaller radius than macro-cells, therefore the capacity of a system increases because more channels per unit area are now available in a network.
- Splitting of cells causes an unbalanced situation in power and frequency reuse distance. Hence it becomes necessary to split small cells in the neighboring cells. Thus cell splitting affects the neighboring cells.

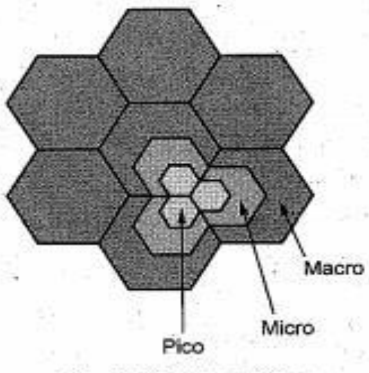


Fig. 4.5.7 Cell splitting

6. GENERATION OF CELLULAR NETWORKS

First generation:

- The first generation (1G) mobile phone networks uses analog signal to transmit the voice calls only between the two transmitters. The main technology of this first generation mobile system was FMDA / FDD and analog FM.
- One example is advanced mobile phone system (AMPS) used in North America . AMPS is an analog cellular phone system.
- It uses 800 MHz ISM band and two separate analog channels; forward and reverse analog channel s. The band between 82 4 to 849 MHz is used for reverse communication from MS

To BS. The band between 869 to 894 MHz is used for forward communication from BS to MS. Each band is divided into 83230 khz channels.

Second generation:

- Second generation (2G) mobile network is the next stage in the development of wireless technology to overcome the limitation 1G by primarily focusing on transmission of voice and data with digital signal.
- Many digital cellular systems rely on Frequency shift keying (FSK) to send data back and forth over AMPS. FSK uses two frequency, one for 1s and other for 0s.Digital cell phones have contain a lot of processing power.
- 2.5 G network's also bought into the market some popular application your few of which are : Wireless Application Protocol (WAP), General Packet Radio Service (GPRS),High Speed Circuit Switched Data(HSCSD) ,Enhanced Data Rates for GSM Evolution (EDGE) .

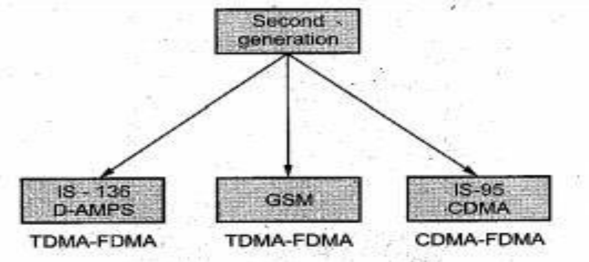
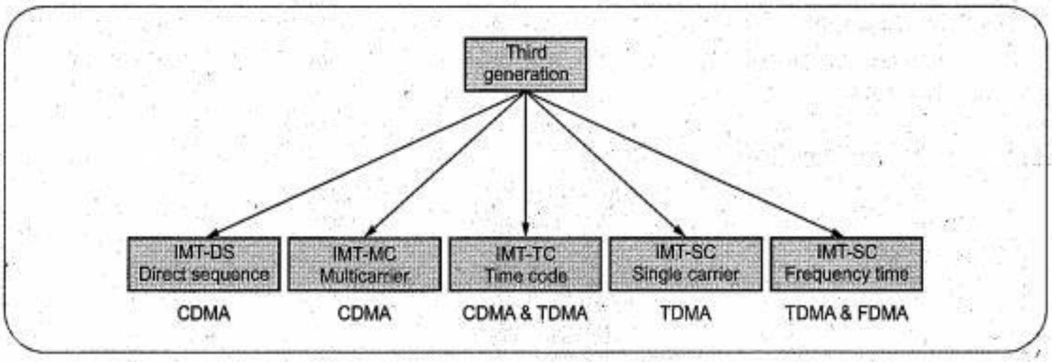


Fig. 4.4.1

Third Generation:

- Third Generation (3G) was arrived because of low speed and incompatible technologies used on previous generations.
- It is based on the International Telecommunication Union (ITU) family of standards under the International Mobile Telecommunication -2000 (IMT2000).
- The main features of (3G) is that it allows Higher data transmission rates and increased capacity for the traditional voice call and high speed data application such as Global roaming, Internet mobile, video conferencing , video calls and 3D gaming.
- 3G networks are wide area cellular Telephone Network which evolved to incorporate high-speed internet access and video telephony. Goal of the 3G technologies are mentioned below:
  - Allow both digital data and voice communication.
  - To facilitate Universal personal communication
  - Listen music, watch movie ,access internet video conferencing, etc.



IMT -2000 defines a set of Technical requirements:

- Requires high data rates: 144 KBPS in all environment and 2Mbps in low- mobility and indoor environments.
- Support symmetrical and asymmetrical data transmission.
- It also supports circuit -switched and packet switched based service.

- Required speech quality comparable to wire line quality.
- Improved spectral efficiency.
- Several simultaneous service to end user for multimedia service.
- Support Global roaming.
- Open architecture for the Rapid introduction of new service and Technology.

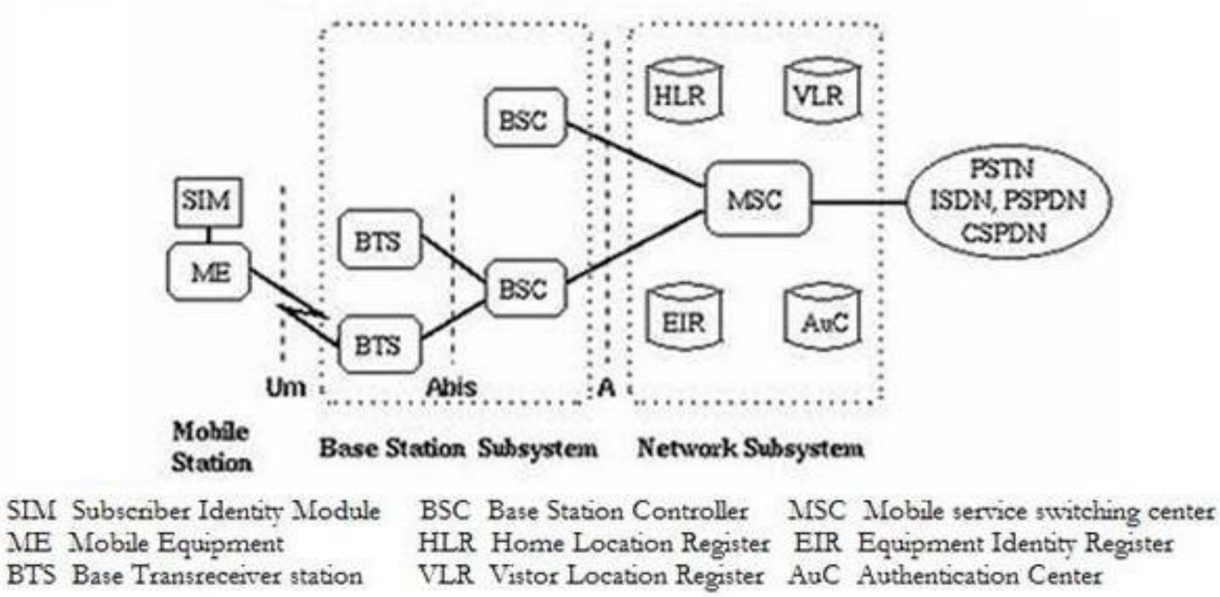
Fourth Generation:

- 4G is called as MAGIC because the user can use the mobile multimedia at any time anywhere with Global mobility support on integrated wireless solution and customized personal service at high speed data rates than previous generations.
- 4G will be a fully IP -based integrated system .4G will be capable of providing between 100 Mbps and 1 Gbit/s speed both indoor and outdoor with premium quality and high security.

Fifth Generation:

Fifth generation (5G) is a packet switched wireless mobile communication system with extensive area coverage and high throughput. Hence, it is called as real world wireless or wireless world-wide web (WWWW).

7. GSM ARCHITECTURE


SIM
ME
BTS
BTS
BSC
BSC
HLR
VLR
MSC
EIR
AuC
PSTN
ISDN, PSPDN
CSPDN
Um
Abis
A
Mobile Station
Base Station Subsystem
Network Subsystem
SIM Subscriber Identity Module
ME Mobile Equipment
BTS Base Transreceiver station
BSC Base Station Controller
HLR Home Location Register
VLR Vistor Location Register
MSC Mobile service switching center
EIR Equipment Identity Register
AuC Authentication Center

- GSM stands for Global System for Mobile Communication. It is widely for digital cellular radio. It is the second generation cellular standard developed to cater voice services and data delivery using digital modulation. GSM supports 200 full duplex channels per cell each channel uses different uplink and downlink frequency.
- GSM handles channel access using a combination of FDMA, TDMA. GSM is an open source system and it allows access to code. GSM comes in three frequency bands 900MHz, 1800MHz, 1900MHz. The maximum distance covered by the GSM is 35km.

Performance Characteristics of GSM:

- Communication: Mobile, wireless digital, communication support for voice and data services.
- Total Mobility: International access, chip card enables use of access points of different providers
- World Wide Connectivity
- High Capacity: Better frequency efficiency, smaller cells, more customers per cell

- High Transmission quality: High audio quality and uninterrupted phone calls at higher speeds.

Security functions: access control, authentication via chip card and PIN.

The GSM network architecture consists of three major subsystems:

- Mobile Station (MS)
- Base Station Subsystem (BSS)
- Network and Switching Subsystem (NSS)

Base Station Subsystem

- Base station subsystem (BSS) consists of base Transceiver system (BTS) and base station controller (BSC). The base station controller (BSC) is in control of and supervises a number of Base Transceiver Stations (BTS). The BSc is responsible for the allocation of radio resources to a mobile call and for the handovers that are made between base stations under his control .Other handovers are under control of the MSC.
- Each BSC connects to a number of base transceiver station (BTS) which, in turn, provide radio interfaces for mobile devices. BSC manages the radio resources for one or more BTSs. It handles radio channel setup, frequency hopping and and handovers. The BSc also translates the 13 kbps voice channel used over the radio link to the standard 64kbps channel used by the public Switched Telephone Network or ISDN.

Functions performed by the BSC :

- Processing of signals.
- Controlling signals to the connected BTSs and control of handover of signals from one BTS to another within a BSS.
- Control and handover of the signals from BSC to MSC.
- Traffic control by continuous measurement of the frequency channel spectrum being used at any given instant.
- Authentication, encryption and decryption of data.
- Updating location registry of the MSs.

Base transceiver station houses the radio transceiver that define a cell and handles the radio link protocols with the mobile stations. BST serves one or more cells in cellular Network and contains more than one transceiver. This transceiver provides full duplex communication to the mobile stations. Usually a BTS is used to manage one cell in the GSM cellular network, but using a sectorized Antenna, a single BTS can be used to manage many cells.

Main functions performed by the BTS:

- Formation of cells using appropriately.
- Directed antennae.
- Processing of signals.
- Amplification of signals to acceptable strength so that they can be transmitted without loss of data.
- Channel coding and decoding.
- Frequency hopping so that multiple channels for various mobile stations can operate simultaneously using different channels band frequency data.
- Encryption and decryption of data

Network Switching Subsystem

- Its acts as an interface between wireless and fixed networks. It mainly consists of switches and databases and manages functions such as handovers between BSSs, worldwide user localization, maintenance of user accounts and call charges, and management of roaming.

- Mobile service switching Centre (MSC) is a main component of network switching subsystem. It acts as switching node of PSTN. Network subsystem includes four different type of database:
  - Home location register.
  - Visitor location registers.
  - Equipment identity registers.
  - Authentication center

Mobile Services Switching Centre (MSC)

- MSC consists mainly of high-performance digital ISDN switches. It connects to a number of BSCs over the 'A' interface. It also connects to other MSCs and to fixed-line networks through GMSCs. It is used to manage BSCs in a geographical area. MSC performs all necessary functions in order to handle the calls to and from the mobile station.
- MSC performs following functions :
  - Call routing.
  - Collection of billing information.
  - Call setup, monitoring and release.
  - Mobility management like registration, location updating and call Handoff between BSC and MSC.
  - Management of signaling protocol.
- The Home Location Register (HLR) and the Visitor Location Register (VLR) are located within the MSC.

Home Location Register HLR

- It includes all permanent users information .HLR is a database used for storage and management of subscription. HLR stores following information :
  - Subscriptions information.
  - International Mobile Station Identify (IMSI)
  - One or more Mobile Station International ISBN numbers (MSISDN)
  - Location information which required for billing and routing of calls towards the MSC where the MS is registered.
- Each mobile user has only one HLR record worldwide, which is updated constantly on a real-time basis. Each MS must register at a specific HLR of a specific MSC. The HLR contacts AuC in the network subsystem for authentication.
- Each HLR is associated to an MSC so that when an MS registered at a certain HLR moves to another location area (LA). Serviced by another MSC, the user's home MSC update the user's current VLR. The database contains other useful information like tele-services and bearer services subscription Information, Service restrictions etc.
- Location Area Identity (LAI) is broadcasted by the BTS so a mobile station can determine if it has entered a new location area. If a new location area is entered the MSC is in formed and the VLR and HLR is updated. Each cell in a location area is allocated a Cell Identity (CI) consisting of 16 bits. The CI and LAI form a globally unique identifier of a cell. If the HLR fails the system fails. The HLR manages the location updates as mobile phones roam. HLR connects and interacts with a number of other components on the system
  - The Gateway MSC for handling incoming calls.
  - The VLR for handling request from mobile phones to attach to the network.
  - The SMSC for handling incoming SMS.
  - The voice system for delivering notification to the mobile phone that a message is waiting.

Visitor Location Register

A VLR is a database similar to the HLR, which is used by the mobile network to a temporarily hold profiles of roaming users. This VLR data is based on the user information retrieved from a HLR.

MSCs use a VLR to handle roaming users. Dynamic real time database that stores both permanent and temporary subscriber data which is required for communication between the MS's in the coverage area of the MSC associated with that VLR.
VLR controls those mobiles roaming in its area and reduces number of queries to HLR. Its database contains IMSI, TMSI, Location Area and authentication key. If a roamer makes a call the VLR will have the information it needs for the call setup.

The VLR primary functions are:

a) To inform the HLR that a MS has arrived in the particular area covered by the VLR.
b) To track where the subscriber is within a VLR area when it is not active.
c) To allocate roaming numbers during the process of incoming calls.
d) The VLR is reset daily.

Equipment Identity Register (EIR):
The EIR keeps a black list of stolen phones that should be barred from access. Stolen phones can be re-flashed with a new IMEI and thus avoid the EIR check. EIR can also block phones that are malfunctioning and disturb the network. The EIR feature is used to reduce the number of GSM mobile handset thefts by providing a mechanism to assist network operators is preventing stolen or disallowed handsets from accessing the network. This control is done by comparing the International Mobile Equipment Identity that is provided during handset registration to a set of three lists provided by the network operator.

a) Black list – Mobile Stations (MS) on the Black list will be denied access to the network.
b) White List – MS's on the White List will be allowed access to the network.
c) Gray List – MS's on the Gray List will be allowed on the network, but may be tracked.

Authentication Centre (AUC):
The AUC verifies the identity of the user and ensures the confidentiality of each call. The AUC holds the secret key that is shared between the SIM and the network. The key never leaves the SIM nor the AUC. Network nodes can request the encryption of a set of challenges from the AUC. A challenge is then sent to the mobile station and if the respond matches the subscriber is authenticated. The authentication process also controls encryption for privacy. It is generally associated with HLR. The AUC and the EIR can be implemented as standalone nodes or as combined AUC/EIR node.

How are the HLR and VLR used?
Each mobile network has its own HLR's and VLR's. When a MSC detects a mobile user's presence in the area covered by its network, it first checks a database to determine if the user is in his/her home area or is roaming.
a) User in Home area: HLR has necessary information for initiating, terminating or receiving a call.
b) User in Roaming: VLR contacts the user's HLR to get the necessary information to set up a temporary user profile. The user's location is recorded in the HLR, and in case the sure roaming, it is also recorded in the VLR.

Suppose that the user wants to make a call:
a) User in Home area: MSC contacts the HLR prior to setting up the call.
b) User in Roaming: MSC contacts the VLR prior to setting up the call.

Suppose that there is a call for the user (call goes to the home MSC) :
a) User in Home area: Home MSC delivers the call immediately.
b) User in Roaming: Home MSC contacts the VLR to determine the appropriate switch in the roaming area to handle the arriving call and then transfers the call to the roaming area MSC.

Operation and Maintenance Center (OMC) supervises operation of particular GSM system blocks. OMC is connected to all switching blocks and performs management functions:

a) Traffic Accounting

b) Traffic Monitoring

c) Management in case of failure

d) HLR Management

Mobile Station

- A mobile station (MS) is equipment within the network that is used in applications involving motion. It can be a hand-held device or any kind of device installed in a mobile vehicle like a car, bus, boat or airplane.
- Each MS has a unique international mobile station equipment identity (IMEI) number. The IMEI is often used for preventing a stolen cell phone from accessing the GSM network. IT isn’t used, however, for identifying the subscriber.
- Each MS requires a Subscriber Identification Module (SIM), which stores a unique international mobile subscriber identity (IMSI). The MS can be locked or unlocked to a SIM provided by the operator.
- Equipment Identity Register (EIR) contains a list of all valid mobiles. Authentication Center (AuC) stores the secret keys of all SIM cards. Each handset has a International Mobile Equipment Identity (IMEI) number.
- Each IMSI contains a unique mobile country code (MCC), a mobile network code(MNC), and a ciphering key (Kc) for authentication center (AuC) in the GSM network subsystem.

SIM card

- Identity modules are synonymous with mobile devices that interoperate with GSM cellular networks. Under the GSM framework, a mobile device is referred to as a Mobile Station and is partitioned into two distinct components: the Universal Integrated Circuit Card (UICC) and the Mobile Equipment (ME).
- A UICC, commonly referred to as a an identity module (e.g., Subscriber Identity Module [SIM], Universal Subscriber Identity Module [USIM], CDMA Subscriber Identity Module [CSIM], is a removable component that contains essential information about the subscriber.
- The ME and the radio handset portion cannot fully function without a UICC. The UICC’s main purpose entails authenticating the user of the mobile device to the network providing access to subscribed services. The UICC also offers storage for personal information, such as phonebook entries, text messages; last numbers dialed (LND) and service-related information.
- SIM stores following types of information:
    1. SIM stores the International Mobile Subscriber Identity (IMSI), which is a unique identifier for each subscriber in the system.
    2. Subscriber can maintain a list of the numbers they call or they are called from more frequently.
    3. Information about SMS traffic.
    4. Information about subscriber’s location: The SIM stores the last area where the subscriber has been registered by the system.
    5. Information about calls: The last numbers dialed are stored in a file in the SIM file system.
    6. Information about the provider: It is possible to extract the provider name and the mobile network commonly used for communications, along with mobile networks that are forbidden to the subscriber.
    7. Information about the system: Every SIM card has a unique ID stored in it.
- SIM card (Subscriber Identification Module (SIM)) is a type of smart card used in mobile phone. The SIM is a detachable smart card containing the user’s subscription information and phone book. This allows user to retain his or her information even after switching off the handset. Alternatively, the user can also change service providers while retaining the

handset simply by changing the SIM. SIM card securely stores the service subscriber key having 15 digit.

- The digits of the key are:

  a) First 3 digits – Mobile country code
  b) Second 2 digits – Mobile network code
  c) Third 10 digits – Mobile station identification number

BSS interface

- **Um interface:** Mobile station and base station subsystem communicates across Um interface, also known as air interface or radio link.
- **Abis interface:** Base transceiver station (BTS) and base station controller (BSC) communicates across Abis interface.
- **A interface:** Base station subsystem communicates with mobile service switching center across A interface.

GSM Channels

- Physical channel corresponds to a time slot on a frequency carrier. There are 8 physical channels per carrier in GSM. Physical channel can be used to transmit speech, data or signaling information.
- The channel from the base station to the mobile unit is known as the downlink or forward channel. The channel from the mobile unit to the base station is known as the uplink or reverse channel.

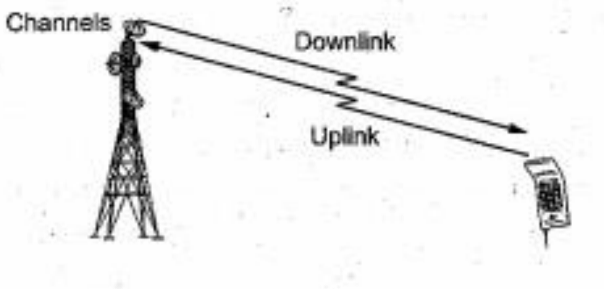


Fig. 4.4.6 GSM channel

- **Physical channel:** Each timeslot on a carrier is referred to as a physical channel.
- **Logical channel:** Variety of information is transmitted between the MS and BTS. GSM logical channels consist of two types: Control channels and traffic channels.
- **Control channels:** Control channels are subdivided into three types: Broadcast Control Channel, Common Control Channel and Dedicated Control Channel.
- Channels used for communication between the MS and BSS when a call is in progress.
- Control channels used by idle mode mobiles to exchange signaling information, required changing to dedicated mode.
- Mobiles in dedicated mode monitor the surrounding Base Stations for handover and other information. Control Channels include:

  1) Broadcast Control Channel (BCCH) serves for BS identification, broadcasts and frequency allocations.
  2) Frequency Control Channel (FCCH) and Synchronization Channel (SCH)-used for synchronization, and physical layer definition (time slots, burst time)
  3) Random Access Channel (RACH) used by mobile to request access to the network.
  4) Paging Channel (PCH) used for locating the mobile user.
  5) Access Grant Channel (AGCH) used to obtain a dedicated channel. (Following the request of RACH)

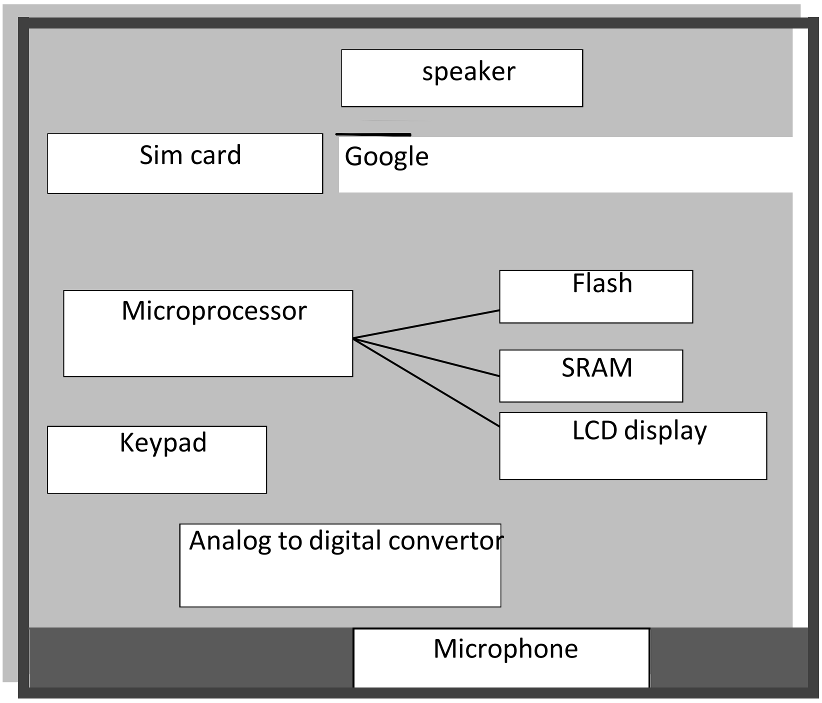
Channel Assignment:

- Channel Assignment are of two types: Fixed and Dynamic.

- **Fixed channel assignment:** Each cell is given a fixed number of channels. Any new call within a cell can only be serviced by unused channels in that cell. Otherwise the call is blocked. A cell which has ran out of channels may "borrow" channels from a neighboring cell.
- **Dynamic channel assignment:** Channels are allocated to cells based on incoming call requests. It controlled by a centralized entry, usually a MSC Mobile Switching Center. Dynamic Channel allocation requires collection of real time data on channel use, traffic distribution across the network and received signal strength indication (RSSI) for each channel on a continuous basis
- There are five different cell sizes in a GSM network. These are macro, micro, pico, femto and umbrella cells.
- Macro cells are cells where the base station antenna is installed on a mast above average roof top level. Micro cells are cells whose antenna height is under average roof top level. Pico cells are small cells whose coverage diameter is a few dozen meters. These are mainly used in indoors applications.
- Femto cells are cells designed for use in residential or small business environments and connect to the service provider's network via a broadband internet connection.
- Umbrella cells are used to cover shadowed regions of smaller cells and fill in gaps in coverage between those cells. Horizontal radius of the cells varies depending on the antenna height, antenna gain and propagation conditions. Maximum distance the GSM supports is 35 kilometers. Most 2G GSM networks operate in the 900 MHz or 1800 MHz bands while 3G GSM in the 2100 MHz frequency band.

8. DIGITAL CELL PHONE COMPONENTS

- Cell phone and said is composed of two components: **Radio Frequency (RF) and baseband.** RF is the mode of communication for wireless Technologies of all kinds including cordless phones, Radar, ham radio, GPS and radio and television broadcast. RF waves are electromagnetic waves which propagate at the speed of light.
- **Base band**: In telecommunications, it is the frequency range occupied by a message signal prior to modulation it can be considered as a synonym to low -pass.
- Mobile phone contains SMD components ,microprocessor ,Flash Memory etc., In addition to the circuit board, mobile phone also as Antenna ,Liquid crystal display(LCD), keyboard , microphone , speaker and battery.



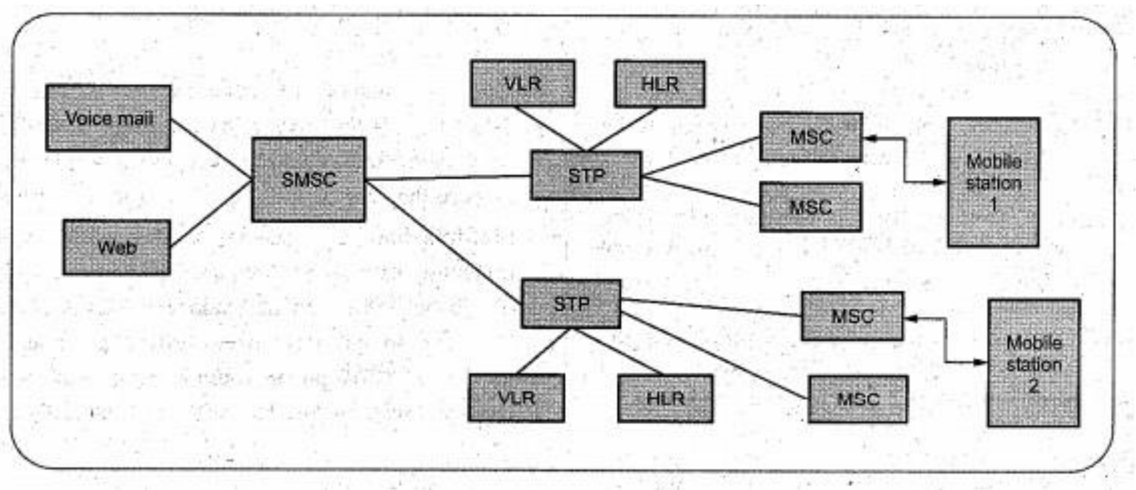
- Mobile devices contain nonvolatile and volatile memory volatile memory (i.e,RAM) is used for dynamic storage and its content or lost when power is drained from the mobile device. Nonvolatile memory is persistent as its contents are not affected by laws of power or overwriting data upon reboot. Mobile devices typically contain one or two different type of non-volatile Flash Memory. These types are NAND and NOR. NOR flash as faster read times, slower write times than NAND and is nearly immune to corruption and bad blocks while allowing random access to any memory location.
- NAND Flash Memory contains PIM data, graphics, and audio, video and other user files. NAND flash memory may leave multiple copies of transaction based files due to wear leveling algorithms and garbage collection routines. Since NAND Flash Memory cells can be re-used for only a limited amount of time before they become unreliable, wear leveling algorithms are used to increase the lifespan of flash memory storage ,by arranging data so that erasures and rewrite are distributed evenly across the SSD.
- When your mobile phone transmits audio it applies an oscillating electric current to the mobile phone antenna. The mobile phone antenna then emits corresponding electromagnetic waves, which are also known as radio waves. To receive calls the mobile phone antenna intercepts an electromagnetic wave of a particular frequency.
- Mobile phone antennas transmit signals to radio Towers and receive signals back simultaneously. In a cellular network the towers are distributed over portion of land called cells .Each cell of land contains at least one Radio tower. Each cell is also assigned a number of frequencies which correspond to Radio base stations. Other cells can use the same frequencies as long as they are not adjacent. Mobile phones uses following components:
- **Digital signal processor:** It is generally rated as having 40 MIPS (millions of instructions per second) to conduct for calculation of signal manipulation at high speed. This chip deals with the both compression and decompression of the signal.
- **Microprocessor**: It performs command and control signaling with the base station, and coordinates the rest of functions on the board.
- **Flash memory and ROM chips** of the mobile phone acts as a storage location for the phone .The power and radio frequency section of the phone, phone recharging and power management act are controlled by this chip.
- **SIM card** (Subscriber Identification module (SIM)) is a type of Smart Card used in mobile phone. The SIM is a detachable Smart Card containing the user's subscription information and phone book.
- Mobile phones have special code associated with them. these include:
- **Electronic serial number (ESN)**: It is a unique 32 bit number programmed in the phone.
- **Mobile identification number (MIN):** I. t is 10 digit number derived from the phone's number.
- **System Identification Code (SID)** : It is unique 5 digit number that is assigned to each carrier by the FCC.
- ESN is a permanent part of the phone while MIN and SID codes are programmed in the phone when your service plan is selected and activated.

9. SHORT MESSAGE SERVICE:

- Short Message Service is a globally accepted wireless service that enables the transmission of alphanumeric messages between mobile subscribers and external systems such as electronic mail, paging and voice mail systems. Not requiring the end to end establishment of a traffic path.
- The service makes use of a short message service center (SMSC) which acts as a store and forward system, for short messages. The wireless network provides for the transport of short messages between the SMSCs and wireless handsets. SMS also guarantees delivery of

the short message by the network. Temporary failures are identified, and the short message is stored in the network until the destination becomes available.

- SMS messages are transported in the core network. The SMSC cans end SMS messages to the end device using a maximum payload of 140 octets. This defines the upper bound of an SMS message to be 160 characters using 7 bit encoding. It is possible to specify other schemes such as 8 bit or 16 bit encoding which decreases the maximum message length to 140 and 70 characters respectively.
- Send or receive during voice or data calls: SMS messaging makes use of a separate channel, normally used for transfer of control messaging to transfer its packets. Being out of band, this means voice and data calls will not be interrupted by SMS transfer. Furthermore, the low bandwidth requirements of transmitting short alphanumeric strings allow messaging worldwide with very low latency. This of course depends upon network operator agreements.
- The SMSC relays SMS messages from a Mobile Equipment (ME) to another ME. The SMS is sent to the nearest call master, forwarded to the SMSC. The SMSC stores the SMS and then attempts to deliver it to the destination ME.
- After a preset period of time, known as validity period, the message is deleted from the SMSC if it cannot be delivered. The SMS can also be forwarded on to a computer or logical ME is the mobile Network's LAN.
- External messaging entities such as web and email are inputs to the networks. These feed directly into the SMSC. This example has the SMSC connected to two separate base stations. Two signal transfer points link the SMSC to the mobile switching center. The HLR is accessed through the signal transfer point and the VLR feeds directly into the MSC. Finally the MSC transmits to the base station. The base station then provides the wireless link to all mobile stations, mobile phones.



Step 1: The mobile station is powered on and registered with the network.
Step 2: The MS transfers the SMS to the MSC.
Step 3: The MSC interrogates the VLR to verify that the message transfer does not violate the supplementary services invoked or the restrictions imposed.
Step 4: The MSC send the short message to the SMSC using the forward short message operation.
Step 5: The SMSC delivers the short message to SME (acknowledgement is optional).
Step 6: The short message is submitted from the ESME (External Short Message Entity) to the SMSC.
Step 7: After completing its internal processing, the SMSC interrogates the HLR.
Step 8: The SMSC send the short message to the MSC using forward short message operation.
Step 9: The MSC retrieves the subscriber information from the VLR. This operation may include an authentication procedure.
Step 10: The MSC transfers the short message to the mobile station.

Step 11: The MSC returns to the SMSC the outcome of the forward short message operation.
Step 12: If requested by the ESME, the SMSC returns a status report indicating delivery of the short message.
Step 13: The SMSC acknowledges to the MSC the successful outcome of the forward short message operation.

10. VOICE CALLS

Cell Phones are used to

- Store contact information
- Make task or to-do lists
- Send or receive e-mail
- Get information (news, entertainment, stock quotes) from the Internet
- Play games
- Watch TV
- Send text messages
- Take photos and videos

A single cell in an analog mobile phone system uses one-seventh of the available duplex voice channels. That is, each cell (of the seven on a hexagonal grid) is using one-seventh of the available channels so it has a unique set of frequencies and there are no collisions:

- A cell phone carrier typically gets 832 radio frequencies to use in a city.
- Each cell phone uses two frequencies per call -- a duplex channel -- so there are typically 395 voice channels per carrier. (The other 42 frequencies are used for control channels -- more on this later.)

Therefore, each cell has about 56 voice channels available. In other words, in any cell, 56 people can be talking on their cell phone at one time. Analog cellular systems are considered first-generation mobile technology, or 1G. With digital transmission methods (2G), the number of available channels increases. For example, a TDMA-based digital system (more on TDMA later) can carry three times as many calls as an analog system, so each cell has about 168 channels available.

Cell phones have low-power transmitters in them. Many cell phones have two signal strengths: 0.6 watts and 3 watts (for comparison, most CB radios transmit at 4 watts). The base station is also transmitting at low power. Low-power transmitters have two advantages:

The cellular approach requires a large number of base stations in a city of any size. A typical large city can have hundreds of towers. But because so many people are using cell phones, costs remain low per user. Each carrier in each city also runs one central office called the **Mobile Telephone Switching Office** (**MTSO**). This office handles all of the phone connections to the normal land-based phone system and controls all of the base stations in the region.

Cell-phone Codes

All cell phones have special **codes** associated with them. These codes are used to identify the phone, the phone's owner and the service provider. Here's what happens to the call:

- When you first power up the phone, it listens for an **SID** (see sidebar) on the control channel. The control channel is a special frequency that the phone and base station use to talk to one another about things like call set-up and channel changing. If the phone cannot find any control channels to listen to, it knows it is out of range and displays a "no service" message.
- When it receives the SID, the phone compares it to the SID programmed into the phone. If the SIDs match, the phone knows that the cell it is communicating with is part of its home system.
- Along with the SID, the phone also transmits a registration request, and the MTSO keeps track of the phone's location in a database -- this way, the MTSO knows which cell you are in when it wants to ring your phone.

- The MTSO gets the call, and tries to find you. It looks in its database to see which cell you are in.
- The MTSO picks a frequency pair that your phone will use in that cell to take the call.
- The MTSO communicates with your phone over the control channel to tell it which frequencies to use, and once your phone and the tower switch on those frequencies, the call is connected. Now, you are talking by two-way radio to a friend.
- As you move toward the edge of your cell, your cell's base station notes that your signal strength is diminishing. Meanwhile, the base station in the cell you are moving toward (which is listening and measuring signal strength on all frequencies, not just its own one-seventh) sees your phone's signal strength increasing. The two base stations coordinate with each other through the MTSO, and at some point, your phone gets a signal on a control channel telling it to change frequencies. This handoff switches your phone to the new cell.

Let's say you're on the phone and you move from one cell to another -- but the cell you move into is covered by another service provider, not yours. Instead of dropping the call, it'll actually be handed off to the other service provider. If the SID on the control channel does not match the SID programmed into your phone, then the phone knows it is **roaming**. The MTSO of the cell that you are roaming in contacts the MTSO of your home system, which then checks its database to confirm that the SID of the phone you are using, is valid. Your home system verifies your phone to the local MTSO, which then tracks your phone as you move through its cells.

Cell-phone Codes:

Electronic Serial Number (ESN): a unique 32-bit number programmed into the phone when it is manufactured.

Mobile Identification Number (MIN): a 10-digit number derived from your phone's number

System Identification Code (SID): a unique 15-bit number that is assigned to each carrier by the Federal Communications Commission (FCC).

11. MULTI -BAND AND MULTI-MODE PHONES

- A band is a portion of the RF spectrum with the distinct propagation characteristics and /or requiring radios with distinct technological characteristic.
- A portion of the RF spectrum allocated for a specific purpose. For example: ISM (multiple), cellular, PCS, Television (multiple). A radio which is a ‘multiband’ works in multiple bands with or no modification.
- Mode is method of communication. The PCS defines bands and constrains the allowed mode in each band. Radios traditionally use a single mode because they are typically used for just one thing.
- Multiple bands: A phone that has multiple band capability can switch frequencies. For example, a dual band TDMA phone could use TDMA services in either an 800-MHz or a 1900MHz system. A quad band GSM phone could use GSM service in the 850-MHz, 900-MHz, 1800-MHz or 1900-MHz band.

Why Multiband /Multimode Radio (MMR)?

- **Military:** Interoperability a perpetual problem, becoming particularly acute with the advent of rapid joint service ops in the 1980s. Primary instigators for the software –defined radio (SDR), but the underlying motivation is to have multiband/multimode capabilities.
- **Public safety:** Analogous to military application, except interest in interoperable radio is much more recent and cost is much bigger issue.
- “All-in-ones “and personal digital assistants (PDAs).
- Dynamic spectrum and new paradigms for spectrum management. Multiband/multimode radio is enabling technology for these things, however, white space seek/detect is a new application.

Commercial mobile telecommunications

- Low–cost 3-band 4-band transceivers widely available, primarily to accommodate regional and international roaming.
- Low cost possible because each band individually has small tuning range and is limited to one mode or a family of very similar modes, modest performance requirement and extremely large production volumes.
- Multiple modes: In cell phones, 'mode' refers to the type of transmission technology used.so, a phone that supported AMPS and TDMA could switch back and forth as needed. It's important that one of the modes is AMPS – this gives you analog services if you are in an area that does not have digital support.
- **Multiple bands /multiple modes**: This best of both worlds allows you to switch between frequency bands and transmission modes as needed.
- Changing bands or modes is done automatically by phones that support these options .usually the phone will have a default option set , such as 1900-MHz TDMA and will try to connect at that frequency with that technology first. If it supports dual bands, it will switch to 800MHz if it cannot connect at 1900 MHz and if the phone supports more than one mode it will try the digital mode(s) first, and then switch to analog.

Difference between CDMA and GSM:

CDMA	**GSM**
Carrier spacing is 1230kHz	Carrier spacing is 200kHz
It uses CDMA technology	It uses FDMA / TDMA
It uses QPSK /BPSK modulation techniques	It uses GMSK modulation techniques
Frequency separation is 45MHz	Frequency separation is 45/95MHz
Downlink frequency is 869 to 894 MHz	Downlink frequency is 925 to 960 MHz and 1805 to 1800 MHz
Uplink frequency is 824 to 849MHz	Uplink frequency is 880 to 915 MHz and 1710 to 1785 MHz