Department of Electronics and Communication Engineering

NSS College of Engineering, Palakkad

INDUSTRIAL TRAINING ON TELECOM TECHNOLOGIES

conducted by Bharat Sanchar Nigam Limited, Cochin, Kerala, India

(April 2013 - May 2013)

REPORT

Submitted By

Vidya Viswanathan

NSALEEC092

CONTENTS

4. Transmission units

5. Data communication

6. Internet

CHAPTER 1

Bharat Sanchar Nigam Limited

1.1 INTRODUCTION

Bharat Sanchar Nigam Limited (abbreviated **BSNL**) is an Indian state-owned telecommunications company headquartered in New Delhi, India. It was incorporated on 15 September 2000. It took over the business of providing of telecom services and network management from the erstwhile Central Government Departments of Telecom Services (DTS) and Telecom Operations (DTO), with effect from 1 October 2000 on going concern basis. It is the largest provider of fixed telephony and fourth largest mobile telephony provider in India, and is also a provider of broadband services. However, in recent years the company's revenue and market share plunged into heavy losses due to intense competition in the Indian telecommunications sector.

BSNL is India's oldest and largest communication service provider (CSP). It had a customer base of 95 million as of June 2011. It has footprints throughout India except for the metropolitan cities of Mumbai and New Delhi, which are managed by Mahanagar Telephone Nigam (MTNL).

BSNL, then known as the Department of Telecommunications, had been a near monopoly during the socialist period of the Indian economy. During this period, BSNL was the only telecom service provider in the country. MTNL was present only in Mumbai and New Delhi. During this period BSNL operated as a typical state-run organization, inefficient, slow, bureaucratic, and heavily unionized. As a result subscribers had to wait for as long as five years to get a telephone connection. The corporation tasted competition for the first time after the liberalization of Indian economy in 1991. Faced with stiff competition from the private telecom service providers, BSNL has subsequently tried to increase efficiencies itself. DoT veterans, however, put the onus for the sorry state of affairs on the Government policies, where in all state-owned service providers were required to function as mediums for achieving egalitarian growth across all segments of the society. The corporation (then DoT), however, failed to achieve this and India languished among the most poorly connected countries in the world. BSNL was born in 2000 after the corporatization of DoT. The corporatisation of BSNL was undertaken by an external international consulting team consisting of a consortium of A.F.Ferguson& Co, JB Dadachanji and NM Rothschild - and was probably the most complex corporatisation exercise of its kind ever attempted anywhere because of the quantum of assets (said to be worth USD 50 Billion in terms of breakup value) and over half a million directly and indirectly employed staff. Satish Mehta, who led the team later confessed that one big mistake made by the consortium was to recommend the continuation of the state and circle based geographical units which may have killed the synergies across regions and may have actually made the organisation less efficient than had it been a seamless national organisation. VinodVaish, then Chairman of the Telecom Commission made a very bold decision to promote younger talent from within the organisation to take up a leadership role and promoted the older leaders to a role in licensing rather than in managing the operations of BSNL. The efficiency of the company has since improved, however, the performance level is nowhere near the private players.

The corporation remains heavily unionised and is comparatively slow in decision making and its implementation, which largely acts at the instances of unions without bothering about outcome. Management has been reactive to the schemes of private telecom players. Though it offers services at lowest tariffs, the private players continue to notch up better numbers in all areas, years after year. BSNL has been providing connections in both urban and rural areas. Pre-activated Mobile connections are available at many places across India. BSNL has also unveiled cost-effective broadband internet access plans (DataOne) targeted at homes and small businesses. At present BSNL enjoy's around 60% of market share of ISP services.

2007 was declared as "Year of Broadband" in India and BSNL announced plans for providing 5 million broadband connectivity by the end of 2007. BSNL upgraded Dataone connections for a speed of up to 2 Mbit/s without any extra cost. This 2 Mbit/s broadband service was provided by BSNL at a cost of just US$ 11.7 per month (as of 21 July 2008 and at a limit of 2.5GB monthly limit with 0200-0800 hrs as no charge period). Further, BSNL is rolling out new broadband services such as triple play BSNL planned to increase its customer base to 108 million customers by 2010. With the frantic activity in the communication sector in India, the target appear achievable.
BSNL is a pioneer of rural telephony in India. BSNL has recently bagged 80% of US$ 580 m (INR 25 billion) Rural Telephony project of Government of India.

On 20 March 2009 BSNL advertised the launch of BlackBerry services across its Telecom circles in India. The corporation has also launched 3G services in select cities across the country. Presently, BSNL and MTNL are the only players to provide 3G services, as the Government of India has completed auction of 3G services for private players. BSNL shall get 3G bandwidth at lowest bidder prices of Rs 185 billion, which includes Rs 101.86 billion for 3G and Rs 83.13 billion for BWA.

As of December 2011, many other private operators have started rolling out their 3rd Generation (aka 3G) services alongside and are enjoying some success in their campaigns to get market share. While BSNL still maintains its connectivity standard and expands to many more areas including rural areas with their 3G services. Also the network infrastructure has been upgraded from to provide 3.6 Mbit/s to 7.2 MBits/sec. It is enjoying a slow but somewhat steady success in gaining market share in this regard.

The introduction of MNP(Mobile Number Portability) which is an service that lets the consumer change wireless service providers while retaining their actual mobile number, BSNL has seen many customers opting for this service to move away from the services to other operators. Despite this as the Indian Wireless market grows BSNL still has a loyal base of subscribers and many more subscribers being added to it every day. This provides customer services for 95 million as of June 2011.

BSNL announced the discontinuation of its telegram services from 15 July 2013, after 160 years in service. It was opened to the public in February 1855; in 2010 it was upgraded to a web-based messaging system in 2010, through 182 telegraph offices across India.

1.2 Services

BSNL provides almost every telecom service in India. Following are the main telecom services provided by BSNL:

- **Universal Telecom Services** : Fixed wireline services and landline in local loop (WLL) using CDMA Technology called **bfone** and **Tarang**respectively. As of 30 June 2010, BSNL had 75% marketshare of fixed lines.
- **Cellular Mobile Telephone Services**: BSNL is major provider of Cellular Mobile Telephone services using GSM platform under the brand name Cellone& Excel (BSNL Mobile). As of 30 June 2010 BSNL has 13.50% share of mobile telephony in the country.
- **WLL-CDMA Telephone Services**: BSNL's WLL (Wireless in Local Loop)service is a service giving both fixed line telephony & Mobile telephony.
- **Internet**: BSNL provides Internet access services through dial-up connection (as Sancharnet through 2009) as Prepaid, NetOne as Postpaid and ADSL broadband as BSNL Broadband BSNL held 55.76% of the market share with reported subscriber base of 9.19 million Internet subscribers with 7.79% of growth at the end of March 2010. Top 12 Dial-up Service providers, based on the subscriber base, It Also Provides Online Games via its Games on Demand (GOD)
- **Intelligent Network (IN)**: BSNL offers value-added services, such as Free Phone Service (FPH), India Telephone Card (Prepaid card), Account Card Calling (ACC), Virtual Private Network (VPN), Tele-voting, Premium Rae Service (PRM), Universal Access Number (UAN).
- **3G**:BSNL offers the '3G' or the'3rd Generation' services which includes facilities like video calling, mobile broadband, live TV, 3G Video portal, streaming services like online full length movies and video on demand etc.
- **IPTV**:BSNL also offers the 'Internet Protocol Television' facility which enables customers to watch television through internet.
- **FTTH**:Fibre To The Home facility that offers a higher bandwidth for data transfer. This idea was proposed on post-December 2009
- **Helpdesk**: BSNL's Helpdesk (Helpdesk) provide help desk support to their customers for their services.
- **VVoIP**: BSNL, along with SaiInfosystem - an Information and Communication Technologies (ICTs) provider - has launched Voice and Video Over Internet Protocol (VVoIP). This will

allow to make audio as well as video calls to any landline, mobile, or IP phone anywhere in the world, provided that the requisite video phone equipment is available at both ends.

- **WiMax**: BSNL has introduced India's first 4th Generation High-Speed Wireless Broadband Access Technology with the minimum speed of 256kbit/s. The focus of this service is mainly rural customer where the wired broadband facility is not available.

BSNL is divided into a number of administrative units termed as telecom circles, metro districts, project circles and specialized units. It has 24 telecom circles, 2 metro districts, 6 project circles, 4 maintenance regions, 5 telecom factories, 3 training institutions and 4 specialized telecom units.

While it did not participate in the 3G auction, BSNL paid the Indian government Rs. 101.87 billion for 3G spectrum in all 20 circles it operates in. State-owned MTNL provides 3G services in the other 2 circles - Delhi and Mumbai. Both these state-owned operators were given a head start by the government in the 3G space by allotting the required 3G spectrum, on the condition that each will have to pay an amount which will be equivalent to the highest bid in the respective service areas as and when the 3G auctions take place. BSNL recently launched a 3G wireless pocket router named Winknet Mf50 for 5800/- Indian rupees. It was released in collaboration with another telecom service provider Shyam networks. Winknet Mf50 enables you to connect multiple devices to the internet using a single sim card.

BSNL has the largest 3G network in India. Additionally, BSNL 3G services usually cover not only the main town/city but also the adjoining suburbs and rural areas as well. As of now BSNL has 3G services in 826 cities across India. The following is a list of BSNL 3G enabled towns/cities. This list covers only BSNL 3G services provided through HSDPA/HSUPA and HSPA+ for GSMsubscribers and not EVDO for CDMA subscribers.

The Brand Trust Report published by Trust Research Advisory ranked BSNL in the 65th position of the list of Most Trusted brands.BSNL competes with 14 other mobile operators throughout India. They are Aircel, Airtel, Idea, Loop Mobile, MTNL, MTS, Reliance Communications, Tata DoCoMo, Uninor, Videocon, Virgin Mobile and Vodafone.

BSNL goes by the motto "Connecting India, faster"[27] and displays the same at their homepage. BSNL offers seamless coverage in almost all forests of India in collaboration with state forest department.BSNL enforces censorship of online content as per orders of Indian Department of Telecom.

CHAPTER 2

2. BROADBAND

2.1 Overview of Broad Band Services

2.1.1 Introduction:

The confluence of two forces—the globalization of business and the networking of information technology—has created the Internet economy. Advances in telecommunications and data technology are creating new opportunities for countries, businesses and individuals—just as the Industrial Revolution changed fortunes around the globe. The new economy is defining how people do business, communicate , shop, have fun, learn, and live on a global basis—connecting anyone to anything. The evolution of Internet has come into existence & Internet service is expanding rapidly. The demands it has placed upon the public network, especially the access network, are great. However, technological advances promise big increases in access speeds, enabling public networks to play a major role in delivering new and improved telecommunications services and applications to consumers .The Internet and the network congestion that followed, has led people to focus both on the first and last mile as well as on creating a different network infrastructure to avoid the network congestion and access problems. The solution to this is Broadband. Broadband indicates a means of connectivity at a high or 'broad' bandwidth, which is capable of delivering multiple services simultaneously. It generally refers to transmission of data over numerous frequencies. There were no uniform standards for Broadband connectivity and various countries followed various standards. Recently ITU had stepped in and has defined Broadband. According to International Telecommunication Union Broadband is defined as "Transmission capacity that is faster than primary rate ISDN, at 1.5 to 2 Mb/s" But in developing countries, as the average financial capability as well as usage, is low, broadband is redefined**.** Recognizing the potential of ubiquitous Broadband service in growth of GDP and enhancement in quality of life through societal applications including tele-education, tele-medicine, e-governance, entertainment as well as employment generation by way of high speed access to information and web-based communication, Government of India have finalised a policy to accelerate the growth of Broadband services.

Broadband Policy 2004 defines Broadband as "An 'always-on' data connection supporting interactive services including, – Internet access and has the capability of the minimum download speed of 256 kilo bits per second (kbps) to an individual subscriber from the Point Of Presence (POP) of the service provider".

–The interactive services will exclude any services for which a separate licence is specifically required, for example, real-time voice transmission, except to the extent that it is presently permitted under ISP licence with Internet Telephony.

2.1.2 Features of Broadband

- **Fast connection to the Internet**

  Access to the services which would otherwise be impossible on a slower dial up connection.These include facilities such as downloading music or video footage ,listening to your favourite radio station or downloading (or sending) large attached files with emails.

- **"Always-on" connection**

  Means that you are permanently connected to the internet; hence no need to dialup a connection everytime you want to surf the web, send email, etc.

- **Flat-rate billing**

  If you choose an uncapped rate there will be no additional charges for the time you are online.You can use it as much or as little as you would like, for a fixed fee.Some connections are available at a lowercost, but limit you to the amount of data being downloaded (known as 'capped rate').

- **Dedicated connection**

  Simultaneous use of both telephone & dataline.

2.1.3 Broadband Services

- **High speed Internet**

  Means that you are permanently connected to the internet, and don't need to dialup a connection every time you want to surf the web, send email, etc.

- **Video on Demand**

  Enables the user to select from an online library of content and select any of the available choices for viewing at a convenient time with full DVD like controls. This is similar to borrowing a Video for viewing.

- **Video Multicasting**

  Similar to cable or terrestrial broadcast–the user can join at any time but the stream begins and ends at the reappointed times.

- **Interactive Gaming**

  Enables multiple players to play online game spitted against eachother or against computers, through gaming servers employed by gaming content providers.

- **Audio and Video Conferencing**

  Share ideas, information, and applications using video or audio.

- **Distant Learning**

  Consists of electronic classrooms with2-wayandmulti-way communication among teachers and students.

All these services require the service provider to have tie-ups with the various content providers.

2.1.4 Network Architecture of Broadband

Network architecture can be broadly classified into three categories:

1. Last mile connecting the subscriber– Access Network
2. Metro Area Network comprising of Core Network .NIBII Backbone supporting Multi Service Platform
3. Service Provisioning Equipment at the Provider's Premises.

2.1.4(a) Broadband Access Technology

Broadband access technology is broadly classified into two categories.They are Wired Line &Wireless which is further classified as given below. Wireline technologies include traditional telephone lines, coaxial cable lines, and fiberoptic lines. Wireless communications involve cellular and fixed wireless technology, high speed shortrange communications and satellite transmission.

Wireless	**Wireline**
3GMobile	DSL(Digital Sub's Line)
Wi-Fi(Wireless Fidelity)	Cable Modem
WiMAX	Optical Fibre Technologies
LMDS& MMDS	PLC(Power Line Communication)

FSO(Free Space Optics)	
Satellite	

For utilizing the existing copper cable, we have adopted DSL Technology. Because physical infrastructure and geography are vastly different from country to country, technology that works well in one geographic area may not work as well in another. Therefore, it is up to each individual locality to determine the technologies that best meet its needs. To handle the increasing bandwidth demand, localities are considering upgrading their current telecommunications infrastructure or installing new infrastructure. It is essential that communities and operators consider the present and future needs of their citizens when examining the most appropriate systems. Broadband should be considered an *accelerator* of economic development .

2.1.4(b) Factors affecting Broadband Access Choices

o Population density
o Existing infrastructure (e.g., twisted pair, cable, fiber)
o Government policies
o Competitive and regulatory dynamics
o Technology evolution

2.1.4(c) Applications of Broadband

· Basic WWW browsing and Email access
· Run Servers (Web / FTP)
· Business tariff, can depend on company
· Some technologies are asymmetric (cable, ADSL)
· Video On Demand (VOD)
· Audio Streams (Internet Radio)
· Fast File Transfers (Possibility of downloading large files in short period of time)

2.2 BROADBAND WIRELINE ACCESS TECHNIQUES

2.2.1 Digital Subscriber Line Technology

DSL is the family of technology, which transforms the narrowband Copper access network into broadband. DSL does not refer to a physical line but the equipment, which transforms the already existing media into a digital line. DSL has various family members, which can be broadly classified as

· Symmetric DSL

Provide identical data rates upstream & downstream

· Asymmetric DSL

Provide relatively lower rates upstream but higher rates downstream.

DSL exploits the copper wires which have a much greater bandwidth or range of frequencies than that demanded for voice without disturbing the line's ability to carry phone conversations. The wires themselves can carry frequencies up to several million Hertz. There are several forms of digital subscriber lines, or xDSL with the x depending on the particular variety of DSL. All xDSL connections use the same ordinary pair of twisted copper wires that already carry phones calls among homes and businesses. Unlike cable modem connections, which broadcast everyone’s cable signals to everyone on a cable hub, xDSL is a point-to-point connection, unshared with others using the service. The most common form of xDSL is ADSL. The A stands for asymmetric, meaning that data transmission rate is not the same in both directions ie.,more bandwidth, or data-carrying capacity, is devoted to data traveling downstream-from the Internet to your PC-than to upstream data traveling from your PC to the Internet. The reason for the imbalance is that, generally upstream traffic is very limited to a few words at a time, like for example –an URL request and downstream traffic, carrying graphics, multimedia, and shareware program downloads needs the extra capacity. Downstream data moves at about 8Mbps for the most common forms of DSL.

Transmission rates depend on the quality of the phone line, the type of equipment it uses, the distance from the PC to a phone company switching office, and the type of xDSL being used.

Common types of DSL:

2.2.2 HDSL(High Data-rate Digital Subscriber Line)

HDSL is a better way of transmitting T1/E1(Primary rate as per American standard(1.544Mb/s) &European standard(2.048Mb/s))over copperwires usingless bandwidth without repeaters.Can be viewed as equivalent of PCM stream.It offers the same bandwidth, both upstream and downstream. It can work up to a distance of 3.66 to 4.57 kms depending upon the speed required. When delivering 2048kbps– On 2 phonelines, each line carries 1168kbps and On 3 phonelines, each line carries 784kbps.No provision exists for voice because it uses the voice band. HDSL over single phone line requires more aggressive modulation, works only shorter distance and requires better phone line.

2.2.3 SDSL(Single-Line Digital Subscriber Line)

SDSL is a single line version of HDSL that transmits T1/E1 signals over a single twisted pair line. It can work upto 3.7kms on 0.5mm diacable. However, SDSL will not reach much beyond 10,000 feet while ADSL reaches rates above 6Mbps at the same distance. SDSL is mainly used by small businesses. It does not allow to use the phone at the same time but the speed of downloading and uploading is the same.

2.2.4 RADSL(Rate-Adaptive Digital Subscriber Line)

RADSL is a variation of ADSL where the modem adjusts the speed of connection depending on the length and quality of the line.

2.2.5 VDSL(Very-high Data-rate DSL)

Originally named VADSL (A–Asymmetric) but was later extended to support both symmetric & asymmetric. Requires one phone line and supports both voice & data. It works between 0.3-1.37kms depending on speed. Upstream data rate can be 1.6-2.3 Mbps. Downstream data rate is 13-52 Mbps.

2.2.6 ADSL (Asymmetric Digital Subscriber Line)

ADSL is one of the number of access technologies that can be used to convert the access line into a high speed digital link and to avoid overloading the circuit switched PSTN. You can use the same phone line for Internet service at the same time it’s carrying a voice call because the two signals use widely separated areas of the frequency spectrum. A splitter next to your xDSL modem combines the low-frequency voice signals and the higher- frequency data signals. A splitter on the other end of the line breaks the voice and data signals apart again, sending voicecalls into the plain old telephone system (POTS) and computer data through high-speed lines to the Internet.

An ADSL circuit connects an ADSL modem on each end of a twisted pair telephone line, creating three information channels

1. A high speed downstream channel
2. A medium speed duplex channel
3. A basic telephone service channel

The basic telephone service channel is splitoff from the digital modem by filters, thus guaranteeing uninterrupted basic telephone service, even if ADSL fails. To create multiple channels, ADSL modems divide the available bandwidth of a telephone line in one of two ways

:frequency-division multiplexing (FDM) or echo cancellation,as shown in Figure. FDM assigns one band for upstream data and another band for downstream data. The downstream path is then divided by time-division multiplexing into one or more high-speed channels and one or more low-speed channels. The upstream path is also multiplexed into corresponding low-speed channels. Echo cancellation assigns the upstream band to overlap the downstream, and separates the two by means of local echo cancellation, a technique. With either technique, ADSL splits off a 4-kHz region for basic telephone service using a splitter.

2.3 Wireless Access Technologies

2.3.1 Wi-Fi

Wi-Fi stands for Wireless Fidelity. As the words indicates, the system seeks to do away with-wires. This system is known as wireless LAN, as with Wi-Fi we can connect different computers in a LAN using radio waves.

2.3.1(a) Elements in Wifi Network

- **Access point:-** Access point (AP) is a device, which is acting as a bridge between the wireless client device and the wired network.
- **Wireless client device:-**Wireless client device can be a 802.11-enabled laptop/desktop (PC).The laptops available today are Wi-Fi supported with. As far as PC's are concerned, Wi-Fi can be enabled by installing Wi-Fi adaptor cards (PCMCIA card) in PC's or by connecting external USB adapt or cards and installing the driver software.

2.3.1(b) Operation

The Wi-Fi client devices are accessing the Access Point (AP) through the radio air interface. The AP is connected to IP network mainly through wired interface. The Wi-Fi client device is thus able to access the IP network through the AP. The geographic area served by the AP is defined as the hotspot .The Wi-Fi client device within the range of hotspot (up to 100m) can access the AP through the radio interface. In the 2.4 GHz system normally used in Wi-Fi, the frequency band is between 2.4GHz to 2.484GHz. Each channel is of 22MHz bandwidth. Normally an AP has 11 channels available and out of these channels 1,6,11 are non overlapping.This means that, these channels can be used in the same area without causing co-channel interference for better coverage and catering a good number of customers. The Wi-Fi network served by the service provider is indicated by the SSID (Service Set Identifier). In order to provide security to the network, the encryption mechanisms such as WEP (Wired Equivalent Privacy) and WPA (Wifi Protected Access) are implemented .WPA is a superior encryption method compared to WEP as it uses AES (Advanced Encryption Standard) for encryption.

2.3.1(c) Implementation in BSNL

As per Government policy on Broadband, the 2.4GHz frequency is delicensed for both indoor and outdoor implementation. BSNL is implementing 802.11 standard as a public access system. Access Points are installed in public places and customers who are having Wi-Fi enabled devices will be accessing Internet through the AP's provided in these locations. Depending on the places we are putting the AP's (hotspots), there are two types of hotspots namely hotspot A & hotspot B. Hotspots A-covers a small area and is having a single access point. Hotspot B is having a number of access point AG's. Customers are using prepaid cards for accessing Internet in these hotspots.

The following network elements are required for implementing Wi-Fi.

1. Access Points(AP's)
2. Access Gateway or Access Point Manager(AG) works as a DHCP server. Service to provide initial service screens.
3. Routers/Switchers for aggregating the traffic.
4. Operation Supports Subsystem(OSS) for Authentication/Authorization/ Accounting (AAA),Billing,Customer management, Network management & Service Provisioning.

2.3.2 Wi-Max

WiMAX is an acronym that stands for Worldwide Interoperability for Microwave Access, a certification mark for products that pass conformity and interoperability tests for the IEEE 8802.16 standards.(IEEE802.16 is working group number 16 of IEEE 802 specializing in point-to-multipoint Broadband wireless access).WiMAX covers wider, metropolitan or rural areas. It can provide data rates upto 75 megabits per second(Mbps) per base station with typical cell sizes of 2 to 10 kilometers. This is enough bandwidth to simultaneously support (through a single base station) more than 60 businesses with T1/E1-type connectivity and hundreds of homes with DSL-type connectivity. It will provide fixed, portable, and eventually mobile wireless broadband connectivity and also provides POTS services.

WiMAX actually provide two forms of wireless service:

1. **Non-line-of-sight**, WiFi sort of service, where a small antenna on your computer connects to the tower. In this mode, WiMAX uses a lower frequency range–2GHzto 11GHz

2. **Line-of-sightservice**,where a fixed dish antenna points straight at the WiMAX tower from a roof top or pole. Line-of-sight transmissions use higher frequencies, with ranges reaching a possible 66GHz.

Two key features of WiMax is the use of OFDM(Orthogonal Frequency Division Multiplexing) and Adaptive modulation techniques for achieving greater bit rates and stable connection.In OFDM,the data will be sent over narrow band carriers transmitted in parallel at different frequencies. These carrier frequencies are closely spaced and they are orthogonal. In adaptive modulation, depending on the signal to Noise ratio (SNR) value of the radio link, the modulations will the automatically changed and bit rates will be adjusted accordingly. This also ensures astable connectivity between the subscriber station and the WiMax base station.
The system consists of mainly 2 equipment's

1.WiMax basestation
2. WiMax CPE

WiMax base station supports single or multi RF carriers. These systems use either FDD or TDD. A modem, similar to the DSL modem can be used as WiMax CPE.This will ultimately be replaced by a pluggable card.
The WiMax Base Station can be connected to multiple Networks such as PSTN, video content server, Internet etc as per requirements. BSNL is planning to implement 3.5GHz WiMax systems.

2.3.2(a) APPLICATIONS

WiMax has the following applications:

1. It can be deployed for providing Broadband connectivity to areas where, provision of broadband through cable media is not feasible.
2. It can be deployed as the backhaul network for Cellular base station, by passing the PSTN.
3. It supports the backhaul connections to the Internet for Wi-Fi hotspots.

2.3.3 Local Multipoint Distribution Service (LMDS)

LMDS is a broadband wireless access technology that uses microwave signals operating between the 26GHz and 29GHz bands. It is a point- to-multipoint service, hence is typically deployed for access by multiple parties. Throughput capacity and distance of the link depends on the modulation method used-either phase-shift keying or amplitude modulation. Links upto 5 miles from the base station are possible.

L(Local)- denotes the propagation characteristics of signals in this frequency range limit the potential coverage area of a single cell site.

M(Multipoint)- indicates that the signals are transmitted in a point to multipoint or broadcast method.

D(Distribution)-refers distribution of signals which may consist of voice, data, internetand video.

S(Service)- implies the nature of relationship between operator and customer.Services offered through LMDS network are entirely dependent on the operator's choice of business.

2.3.3(a) FACTORS DETERMINING LMDS

1). **Line-of-sight**: LMDS requires direct line of sight.Tall buildings may obstruct line of sight and the solution is to divide area into smaller cells.
2). Antenna height placed on taller buildings can serve larger cells without obstructions

2.3.3(b) NETWORK ARCHITECTURE OF LMDS

1.Network Operations Centre (NOC)

•Contains Network Management System (NMS)
•NMS controls a number of Central Stations (CS) & Remote Stations (RS)
•NMS can configure, maintain and monitor both CS & RS

2.Fiber based infrastructure

•Interconnects the network node and the CS
•It consists of STM4/STM1links

3.Centralstation

i)**Central Controller Station (CCS):**Provides the interface to Network node.It can be connected to different networks such as PSTN/ATM/IP. It also has interfaces to accommodate STM1/STM4, 34Mbps, V5.2, for establishing connections to different networks.

ii)**Central Radio Station(CRS):** It consists of Microwave transmission and reception equipments. The height of the antenna should be such that it can provide LOS for the remote stations of targeted area. It uses sectored antennae for broadcasting towards remote stations with coverage range varying from 3 to 10kms. Depending up on the frequencies used.

2.3.4 REMOTE TERMINAL STATION

- **Roof Top unit**

  It uses a directional antenna to establish a M/W link with the Central station.

- **Network Interface Unit**

  NIU connects the RTU to CPE. NIU provides the gateway between RF components and in building appliances. NIUs are available in scalable and non scalable forms depending upon customer requirements.

  A scalable NIU is flexible and fully configurable.
  •It can support two way digital wireless voice, data and video communication for commercial and business use.
  •NIU is configured by the NO Cat the CS.
  •NIUs of this type allow N/W operators to meet customer's requirement efficiently. But is costly and is suitable for higher end users.

  Nonscalable NIU is not configurable, and provides a fixed combination of interfaces. It is cost effective and suitable for medium sized business and home segments.

- **Customer Premises Equipment**

2.3.4(a) Advantages

- Lower cost for both user and carrier than wired alternatives.
- Increased service area; network may be expanded one cell at a time.
- Capacity; with as much as 1,300 MHz of spectrum in a local market, carriers can support 16,000 telephone calls and 200 video channels simultaneously.

2.3.4(b) Disadvantages

- Requires line-of-sight between buildings; LMDS network is limited by surrounding objects
- Affected by precipitation; LMDS systems are susceptible to interference from rain and fog

2.3.5 Multichannel Multipoint Distribution System (MMDS)

Multichannel multipoint distribution service is a Broadband wireless technology and is used for general-purpose broadband networking. It is also known as wireless cable as it was initially used by cable TV operators for Satellite TV signal transmission. By using lower frequencies, MMDS signals travel longer distances and provide service to cells that are up to 35 miles across. The frequency range used is 2.1 to 2.7 GHz. (In US 2.5 to 2.7 MHz is used(200MHz Band width)). Maximum coverage area is about 70 Kms. and maximum transmitter power is about 100 watts.

Similar to LMDS, MMDS can transmit video, voice, or data signals at 1.5 Mbps downstream and 300 Kbps upstream at distances up to 35 miles. Mounted MMDS hub uses point-to-multipoint architecture. Pizza box (13 x 13 inch) directional antennas are mounted at receiving location & a cable runs from antenna to MMDS wireless modem, which converts analog signal to digital and may be attached to single computer or LAN.

2.3.5(a) Advantages

- Signal strength—low frequency MMDS RF signal travels farther and with less interference than high-frequency LMDS RF signals.
- Cellsize—seven times larger than area covered by LMDS transmitters.
- Cost—MMDS is less expensive than LMDS.

2.3.5(b) Disadvantages

- Requires direct line-of-sight makes installation difficult and eliminates locations blocked by taller obstructions.
- Shared signals—decreased speed and throughput since users share same radio channel.
- Security—Unencrypted transmissions may be intercepted and read.
- Limited markets—available in limited areas in USA

2.3.6 SATELLITE

Satellite broadband offers two-way internet access via satellites orbiting the earth about 22,000 miles above equator. The PC, through a special satellite modem broadcasts the requests to the satellite dish ,located on top of the roof/building which in trun transmits and receives signal from the satellites. But satellite broadband is slower in both uplink and downlink compared to any DSL technology.

At present we use VSAT (Very Small Aperture Terminals) & DTH (Direct To Home) terminals for satellite transmission. C, Ku & Ka bands are used for services involving fixed terminals and L band is used for mobile services. It offers data rates 9.6 Kbps for a handheld terminal and 60 Mbps for a fixed VSAT terminal at present.

Satellite broadband has got an advantage, that it can be deployed in every region in a country. Satellite explores the possibility of usage in rural areas where tough terrain conditions prevails. It provides an Always On Connection without dialling .It offers incredible reliability, better than 99.9%. and need not worry about dropped connections during critical transactions, or missed emails.

With the advent of new technologies in the field of communication which has brought the world closer and closer, the consumer will be in a better position to choose and reap the benefits, the broadband technology offers viz. High Speed Internet, Video Conferencing, Telemedicine, Video on Demand ,Internet Radio, Instant messaging, etc.

2.3.7 Free Space Optics(FSO)

Wireless Links at the Speed of Light

2.3.7(a) How Free Space Optics (FSO) Works ?

Free Space Optics (FSO) transmits invisible, eye-safe light beams from one "telescope" to another using infrared lasers. The beams of light in Free Space Optics (FSO) systems are transmitted by laser light focused on highly sensitive photon detector receivers. These receivers are telescopic lenses able to collect the photon stream and transmit digital data. Commercially available systems offer capacities in the range of 100 Mbps to 2.5 Gbps, and demonstration systems report data rates as high as 160 Gbps . A laser transmitter which is safe when viewed by the eye is designated IEC Class 1M. It is possible to design eye-safe laser transmitters at both the 800 nm and 1550 nm wavelengths but the allowable safe laser power is about fifty times higher at 1550nm. The only essential for FSO is line of sight between the two ends of the link.

2.3.7(b) Free Space Optics (FSO) Security

FSO laser beams cannot be detected with spectrum analyzers or RF meters. It requires a matching Free Space Optics (FSO) transceiver carefully aligned to complete the transmission. Interception is very difficult and extremely unlikely. The laser beams generated by Free Space Optics (FSO) systems are narrow and invisible, making them harder to find and even harder to intercept and crack. Data can be transmitted over an encrypted connection adding to the degree of security available in FSO network transmissions.
The following protocols have been wirelessly transmitted by laser communication:

- Ethernet, Fast Ethernet, Gigabit Ethernet
- FDDI
- ATM (OC-3, OC-12, OC-24)

Using WDM 160 Gbps in the lab
Free Space Optics uses the infrared portion of the electromagnetic spectrum between visible light and microwaves. Atmospheric effects such as fog, snow, rain, smog, sand-storms and scintillation (thermal shimmer) all cause attenuation of the infrared signal as it passes through the atmosphere.

2.3.7(c) TECHNICAL SPECIFICATIONS

Transmission rates :100 - 715 Mbps
Operational range : 3 dB/km: clear air: 400m to 5500m
10 dB/km: extreme rain: 400m to 2400m
Laser output power : 560 mW

Free-space wavelength :	1550 nm

2.3.7(d) <u>Advantages of FSO</u>

- Less expensive than fiber optic or leased lines
- Much faster installation, days or weeks compared to months for fiber optic cables.
- Transmission speed can be scaled to meet user’s needs; from 10 Mbps to 1.25 Gbps.
- Security is key advantage; not easy to intercept or decode(wide military applications).
- FSO systems offers a flexible networking solution.
- Freedom from licensing and regulation translates into ease, speed and low cost of deployment.
- Easily upgradable.
- No latency
- Compatible with WDM technology
- Low power consumption

2.3.7(e) <u>Disadvantages of FSO</u>

- Impact of atmospheric conditions on FSO transmissions Scintillation is temporal and spatial variations in light intensity caused by atmospheric turbulence that acts like prism to distort FSO signals. FSO overcomes scintillation by sending data in parallel streams from several separate laser transmitters separated by about 7.8 inches called spatial diversity.

Following are some of the solutions to overcome fog
· Increase transmitted power
· Customize distance and products based on weather statistics for particular cities
· Place FSO transceivers less than 500 meters apart in regions with heavy fog
· Use a backup system along with FSO Signal interference, such as birds, can block signal
· Solution is to block signal temporarily and then raise to full power when obstruction clears

The broader market for FSO-based technology did not emerge until late 2000 when it became clear that fiber-optic cable would not reach into every building in the near future. Today, it is increasingly finding its way into a range of enterprise and service provider applications. The costs and challenges associated with trenching fiber in metropolitan areas can be prohibitive, yet bandwidth demands are increasing, particularly in the "last mile." In many cities, these demands are outstripping service providers' ability to deploy fiber-optic cable. Combined with shrinking capital budgets, other gaps and applications in service providers' networks must also be addressed through viable alternatives such as FSO-based,
optical wireless products.

2.3.8 NATIONAL INTERNET BACKBONE-Phase II(NIB-II)

2.3.8(a) INTRODUCTION

National Internet Backbone-Phase II (NIB-II) conceived and implemented by BSNL provides infrastructure for providing number of value added services to broadband customers countrywide with guaranteed quality of service (QoS). This will help to accelerate the Internet revolution in India. Moreover the NIB-II will create a platform, which enables e-governance, e-banking, e-learning, etc. with the key point of Service Level Agreements & Guarantee in tune with Global standards and customer expectations.

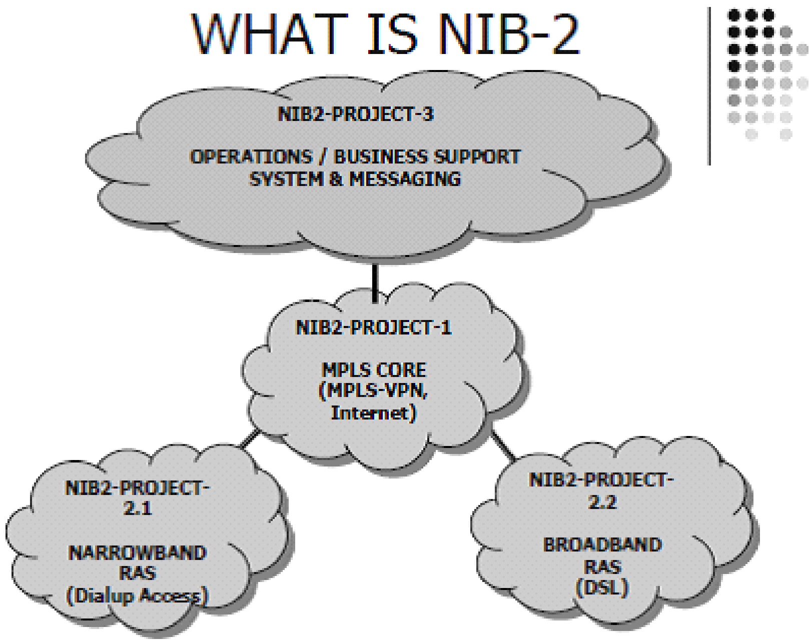
The Primary objectives in setting up the MPLS based IP network

- Building a common IP infrastructure that shall support all smaller networks and sub networks. The platform is intended to be used for convergent services, integrating data, voice and video and shall be the primary source of Internet bandwidth for ISPs, Corporate, Institutions, Government bodies and retail users.
- Making the service very simple for customers to use even if they lack experience in IP routing, along with Service Level Agreement (SLA) offerings.
- Make a service very scalable and flexible to facilitate large-scale deployment.
- Capable of meeting a wide range of customer requirements, including security, quality of service (QoS), and any-to-any connectivity.
- Capable of offering fully managed services to customers.

NIB-II has been grouped into following three major projects.

- **Project 1:** MPLS based IP Network infrastructure covering 71 cities.
- **Project 2:** Access Gateway platform This project is further classified as follows
  - 2.1 Narrowband Dialup Access
  - 2.2 Broadband Access
- **Project 3:** Messaging and Storage platform and Provisioning, Billing and Customer are and Enterprise management system.

This is as given in the diagram below



The network shall seamlessly integrate with the already existing network infrastructure comprising of the TCP/IP based NIB-Phase I and MPLS VPN network. The NIB-II project comprises of Technology solutions from different product manufacturers with the provision for future expansion.

2.3.8(b) <u>SERVICESPLANNEDINNIB-II</u>

a) Internet Access

i) Dial up access services/Leased Access Services.

ii) Digital Subscriber Line (DSL) access services: Broadband "always-on-internet" access over copper cables.

iii)Direct Ethernet access services: Broadband "always-on- internet" access using Fiber-to-the-building.

b) Virtual Private Network (VPN) services

i) Layer 2 MPLS VPN Services: Point-to-point connectivity between corporate LAN sites.

ii) Layer 3 MPLS VPN Intranet and Extranet Services: LAN interconnectivity between multiple Corporate LAN sites.

iii)Managed Customer Premises Equipment (CPE)Services

c) Value Added services

i) Encryption services: one of the end-to-end data security features.
ii) Firewall Services: one of the security features provided to customer.
iii)Network Address Translation (NAT)Services: Service that will enable private users to access public networks

d) Messaging services
e) Data Centre Services at Bangalore, Delhi and Mumbai

f) Broadband services through DSL & Direct Ethernet
i) Fast Internet Access services
ii) Terminating Dialup and DSL/Direct Ethernet customers on MPLS VPNs
iii)Multicast Video streaming Services
iv)Video on Demand services

2.3.9 NETWORK ARCHITECTURE :

The NIB-II consists of an integrated 2-layer IP and MPLS network. The Layer 1 network will constitute the high speed Backbone comprising of Core routers with built in redundancies supporting both TCP/IP and MPLS protocols with link capacities in accordance with the traffic justification. Its function will primarily be limited to high-speed packet forwarding between the core nodes. Layer 2 consists of Edge Routers for aggregation of Customer traffic and enforcing QoS and other administrative policies. This layer shall provide
customer access through following three mechanisms,

i. Dialup
ii. Dedicated Access
iii. Broadband access

2.3.9(a) IP Addressing

The IP address is an address assigned to every computer (also includes routers and switches and other devices) on the Internet to uniquely define them. No two computers can use the same IP address. However, one computer (or device) may have several IP addresses. A simple example would be a computer that serves as a host for multiple services in which case each service may have one or more IP addresses.

TCP/IP includes an Internet addressing scheme that allows users and applications to identify a specific network or host to communicate. An Internet address works like a postal address, allowing data to be routed to the chosen destination. TCP/IP provides standards for assigning addresses to networks, sub networks, hosts, and sockets, and for using special addresses for broadcasts and local loopback.

IP address is made up of a network address and a host (or local) address. This two-part address allows a sender to specify the network as well as a specific host on the network. A unique, official network address is assigned to each network when it connects to other Internet networks. IANA (Internet Assigned Number Authority) will assign the IP Address for your network when your network is connected to Internet.

Internet Addresses

The Internet Protocol (IP) uses a 32-bit IPV4 address , two-part address field. The 32 bits are divided into four *octets* as in the following:

01111101 00001101 01001001 00001111
These binary numbers translate into:
125 13 73 15

The two parts of an Internet address are the network address portion and the host address portion. This allows a remote host to specify both the remote network and the host on the remote network when sending information. By convention, a host number of 0 (zero) is used to refer to the network itself.
TCP/IP supports three classes of Internet addresses: Class A, Class B, and Class C. The different classes of Internet addresses are designated by how the 32 bits of the address are allocated. The particular address class, a network is assigned depends on the size of the network.
These addresses contains some key information. The first bits in the first octet always provides information as to what type of network the address belongs.
If the first bit is a “0” (in decimal notation, this would mean the first three digits from 0-127) then we have a class A network. This makes the first 8 bits the network address and the next 24 bits host addresses.
If the first two bits are “10” then we have a Class B network (in decimal 128-191). This makes the first 16 bits network addresses and the next 16 bits host addresses.
If the first three bits are “110” then we have a class C network (in decimal 192-223). This makes the first 24 bits network addresses and the next 8 host addresses.
If the first four bits are 1110 we have a class D. This is used for multicasting and is not used as network addresses. The decimal value would be 224-239. If the first bits are 1111 we have a class E network (in decimal 240- 255). These addresses are experimental and not used. Neither Class D or E network addresses can be used thus.

2.3.9(b) Multi Protocol Label Switching (MPLS)

Overview of MPLS Technology

MPLS is a hybrid technology model, which enables very fast forwarding at the core and slower conventional routing at the edges of a network. It combines the best of ATM’s circuit switching and IP’s packet-routing. Packets are assigned a label at the entry to a MPLS domain and are switched inside the domain by a simple look-up table. The MPLS domain is usually the core backbone of a provider’s network. These labels determine the quality of service rendered to the packet. At the egress router at the domain's edge, the packets are stripped off their labels and are routed in a conventional manner to their destination. In MPLS, packets are mapped to Forwarding Equivalence Classes (FECs) only once at the ingress router, and the FEC's corresponding "label" is assigned to the packet and is sent along with it. This label is of fixed length and is only locally significant. At later hops within the MPLS domain, this label is used as an index into the routing tables to determine the next hop, as well as the new value for the label. Unlike conventional IP routing, there is no complex processing of the packet header involved in MPLS. Compare this to conventional IP routing, where the next hop is determined on the basis of the packet's header, and also by running a network layer routing algorithm. The conventional routing is done using two mainfunctions, partitioning the complete set of possible packets into Forwarding Equivalence classes and mapping each FEC. to the next hop. This mapping of packets to FECs is done at every router in conventional IP routing and is a costly operation. MPLS is multi-protocol because this label assignment and label based switching can be used over any underlying network protocol. An MPLS based router is also called "Label-Switched Router" (LSR), and the path taken by a packet, after being switched by LSRs through an MPLS domain, is called "Label- Switched Path" (LSP). The LSR at the ingress and egress of the MPLS domain is called Label Edge Router(LER). A labeled packet usually carries multiple labels organized as a Last In First Out (LIFO) label stack. At a router, forwarding decisions are always based in the stack's topmost label, independent of the underlying labels. This label stack is useful to implement tunneling and hierarchy. The advantages of MPLS over conventional routing are evident in some situations, as given here. MPLS forwarding can be done by switches, because only a simple table lookup and label replacement is involved. A computationintensive large prefix search, as in conventional routing, is gainfully avoided. Incoming packets from different ports, or typified by any other headerindependent criteria, can be distinguished by the ingress router by assigning them to different FECs. This scores over conventional IP routing, where only the header information can be used for making routing decisions. MPLS allows packets to be differentiated on the basis of the ingress router used for entering the MPLS domain. This is difficult in IP routing, as the intermediate router addresses are not included in the packet's header. Since the mapping of labels to FECs at the ingress LSRs(LER) is a one-time activity, these mapping algorithms can be made as complex as desired. Unlike conventional IP-based source routing, where an extra set of address information is carried, the MPLS needs to only carry a label to specify fixed paths. A shim header is a special header placed between layer two and layer 3 of the OSI model. The shim header contains the label used to forward the MPLS packets Multi Protocol Label Switching (MPLS), is used by the service providers which can create IP tunnels throughout their network, without the need for encryption or end-user applications for speeding up network traffic flow and making it easier to manage.. In a way it is the ability to create end-to-end circuits, with specific performance characteristics, across any type of transport medium, eliminating the need for overlay networks or Layer 2 only control mechanisms. In MPLS network, incoming packets are assigned a "label" by a "label edge router (LER)". Packets are forwarded along a "label switch path (LSP)" where each "label switch router (LSR)" makes forwarding decisions based solely on the contents of the label. At each hop, the LSR strips off the existing label and applies a new label, which tells the next hop how to forward the packet.

2.4 Broadband Digital Loop Carrier (BDLC)

2.4.1 Overview of conventional DLC

The local loop is the physical connection between the user's premises to the main distribution frame (MDF) in the telecommunications network provider. Digital loop carrier (DLC) technology makes use of digital techniques to bring a wide range of services to users via twisted-pair copper phone lines. DLC is adigital transmission access product, which broadly consists of a central office terminal located in the exchange, and a remote terminal, located at or near the subscriber’s premises. DLC carries sub loop in digital form that is why it is called DLC.

2.4.2 Advantages of DLC

Reduces copper in the network thereby reducing associated problems
Provides multiple services on a common platform
Extends the service area of an exchange by 50 kms approximately
Easy & fast to deploy
Requires less space, less power.

DLC -COMPONENTS

Central Office Terminal (COT)
Remote terminal(RT)/ access terminal(AT)
Network Management System(NMS)

2.4.3 DLC-RT CONNECTION

The COT deployed at the exchange end consists of Channel Banks and an STM-1 Multiplexer. It provides various user interfaces to the exchange as required for the DLC operation. The remote terminal or access terminal deployed at the remote end consists of Channel Banks and a STM-1 Multiplexer. It provides the various complimentary user interfaces to the subscriber as per the exchange interfaces. A management system is provided at the COT for the operation, configuration and maintenance of the total system.There are two types of DLC’s 2W & V5.2 supported DLC. In 2W DLC’s, COT will have the full complement of channel banks and it will accept analog 2W interface lines from the exchange. In V5.2 type, COT will not have any POTS channel cards.

Working Principle

Subscriber lines are terminated in the MDF which is housed in the RT.
This is taken to the channel card/POTS card in the which it converts it into digital 64Kbps The E1 processor card in the channel bank, accepts data from the channel cards and multiplexes it into eight E1’s(2.048Mb/s) and transmits to the SDH for further processing. Here it multiplexes the several E1’s from the E1 processor card to form STM-1 format and transports it towards the COT. At COT, the SDH signal is received in the STM Multiplexer card where it is demultiplexed

to several E1’s and these E1’s are processed in the E1 processor cards. If it is 2W DLC, E1’s are demultiplexed into 64Kbps channels which in turn is converted into analog signals to be extended to the main exchange switch for actual switching, through 2w extended from the COT to switch. If it is V5.2 DLC, E1’s are directly extended to the switch after HDLC protocol conversion in the E1 processor card.
Two types of architecture are normally adopted. : Star configuration & Ring configuration. In ring configuration, it supports path redundancy. In case any one path fails, full connectivity is maintained through the alternate path. This is possible, as the connectivity is established through SDH format and this format accommodates protection switching bytes which enables it to switch to protection channel.

Chapter 3

NETWORK CONCEPTS

3.1 INTRODUCTION

A network is nothing more than two or more computers connected to each other so that they can exchange information, such as:

- e-mail messages or documents,
- Share resources, such as disk storage or printers.

The connection may be via electrical cables that carry electrical signals, or fiber-optic cables by using impulses of light. Wireless networks let computers communicate by using radio signals. A network, in addition to special hardware, also requires special software to enable communications. Network support is built into all major operating systems, including all current versions of Windows, Macintosh operating systems and Linux.
Small or large, all networks are built from the following basic building blocks:

- Client Computers
- Server Computers
- Network Interface Cards (NIC)
- Cables
- Hubs & Switches
- Wireless Networks

- Network Software

- **Client Computers**

The computers that end-users use to access the resources of the network. They usually run a desktop version of Windows along with application software such as Microsoft Office. Sometimes referred to as WORKSTATIONS.

- **Server Computers**

Computers that provide shared resources, such as disk storage and printers, as well as network services, such as e-mail and Internet access. Server computers typically run a specialized Network Operating System (NOS) such as Windows 2000 Server, NetWare, or Linux along with special software to provide network services. For example, a server may run Microsoft Exchange to provide e-mail services for the network, or it may run Apache Web Server so that the computer can serve Web pages.

- **Network Interface Cards (NIC)**

A card installed in a computer that enables the computer to communicate over a network. Almost all NICs implement a networking standard called ETHERNET. Every client and every server computer must have NIC (or built-in network port) in order to be a part of the network.

- **Cables**

Computers in a network are usually physically connected to each other using cable. The most commonly used cable today is called Twisted Pair, also known as 10BaseT. Another type of cable commonly used is Coaxial. For high-speed network connections, fiber-optic cable is used.

- **Hubs & Switches**

Each computer in a network is connected by cable to a device known as a hub or switch. The hub or switch in turn, connects to the rest of the network. Each hub or switch contains a certain number of ports, typically 8 or 16. Hubs and Switches can be connected to each other to build larger networks.

- **Wireless Networks**

In many networks, cables and hubs are making way for wireless network connections, which enables computers to communicate via radio signals. In a wireless network, radio transmitters and receivers take the place of cables.

Advantage: Flexibility
Disadvantage: It is inherently less secure than a cabled network.

- **Network Software**

What really makes a network work is software. Server computers typically use special Network Operating System (NOS) in order to function efficiently. Client computers need to have their network settings configured properly in order to access the network.

- **Network Categorization**

Based on the geographical size, its ownership, the distance it covers and its physical architecture, networks can be categorized as:

- LAN: Local Area Network
- MAN: Metropolitan Area Network
- WAN: Wide Area Network

LAN : Computers are relatively close together, such as within the same office or building. LAN can extend to several buildings on a campus – provided the buildings are close to each other.

WAN :A network that spans a large geographical territory, such as an entire city, region, or even an entire country. WANs are typically used to connect two or more LANs that are relatively far apart.

MAN :A network that that's smaller than a typical WAN but larger than a LAN. Typically, a MAN connects two or more LANs within a same city but are far enough apart that the networks can't be connected using a simple cable or wireless connection.

- **Network Topology**

The term network topology refers to the shape of how the computers and other network components are connected to each other. Several different types of network topologies:

- Bus Topology
- Star Topology
- Ring Topology
- Mesh Topology

3.2 Understanding Protocols & Standards

3.2.1 Understanding Protocols

Protocols & Standards are what make networks work together. Protocols make it possible for the various components of a network to communicate with each other. Standards also make it possible for network components manufactured by different companies to work together. A protocol is a set of rules that enable effective communications to occur. Computer networks depend upon many different types of protocols, which are very rigidly defined, in order to work. Various protocols tend to be used together in matched sets called protocol suites. The two most popular protocol suites for networking are: TCP/IP (Transmission Control Protocol/ Internet Protocol) and IPX/SPX (Internet Packet Exchange/ Sequenced Packet Exchange). TCP/IP was originally developed for UNIX networks and is the protocol for the Internet. IPX/SPX was originally developed for NetWare networks and is still widely used for Windows networks. A third important protocol is Ethernet, a low-level protocol that's used with both TCP/IP and IPX/SPX.

3.2.2 Understanding Standards

A Standard is an agreed-upon definition of a protocol. Standards are industry-wide protocol definitions that are not tied to a particular manufacturer. Many organizations are involved in setting standards for networking.

- ANSI: American National Standards Institute
- IEEE: Institute of Electrical & Electronics Engineers
- ISO: International Organization for Standardization
- IETF: Internet Engineering Task Force
- W3C: World Wide Web Consortiu

3.2.3 OSI Reference Model

Open Systems Interconnection Reference Model is a framework into which the various networking standards can fit. Open Systems Interconnection Reference Model is a standard of standards. The OSI Model breaks the various aspects of a computer network into seven distinct layers.

LayersFunctions	
APPLICATION	File Transfer, e-mail, Remote login etc.
PRESENTATION	ASCII Text, Sound
SESSION	Establish/ Manage Connection
TRANSPORT	End-to-End Communication: TCP
NETWORK	Routing, Addressing: IP
DTA LINK	Two party communication: Ethernet
PHYSICAL	How to transmit signal: Coding

3.2.4 Ethernet Protocol

The most popular set of protocols for the Physical and Data Link layers is Ethernet. The Ethernet is defined by the IEEE standard known as 802.3. The actual transmission speed of Ethernet is measured in Mbps.

Ethernet comes in three different speed versions:

- Standard Ethernet - 10-Mbps
- Fast Ethernet – 100-Mbps
- Gigabit Ethernet – 1-Gbps (or 1000-Mbps)

3.2.5 TCP/IP Protocol Suite

The TCP/IP, the protocol on which the Internet is built, is actually not a single protocol but rather an entire suite of related protocols. The TCP/IP suite is based on a four-layered model of networking that is similar to the seven-layer OSI Model.

The Internet provides three sets of services. At the lowest level is a connectionless delivery service (network layer) called the Internet protocol (IP). The next level is the transport layer service. Multiple transport layer services use the IP service. The highest level is the application layer services. Layering of the services permits research and development on one without affecting the others. Application-layer protocols are divided into two groups, first, those that provide a utility function to the
Internet (utility), and, second, those that provide a service directly to the user. The major applications protocols are categorized below by user service and utility.

User Service Application

User service applications include the following.

- TELENET – provides a remote logon capability
- File transfer protocol (FTP) – provides a reliable file transfer capability.
- Trivial file transfer protocol (TFTP) – provides an unreliable, simple file transfer capability.
- Hypertext Transfer Protocol (HTTP) – provides access to Web.
- Simple message transfer protocol (SMTP) – provides electronic mail capability.

Utility Applications

Utility applications include the following.

- Simple network management protocol (SNMP) – provides network management information.
- Domain name service (DNS) – provides a directory assistance for Internet addresses using local names.
- Address resolution protocol (ARP) – provides a physical address from an IP address.
- Reverse address resolution protocol (RARP) – provides an IP address from a physical device address.

The layer of operation classification of the utility protocols address resolution protocol (ARP), reverse address resolution protocol (RARP), Internet control message protocol (ICMP), Internet group management protocol (IGMP), exterior gateway protocol (EGP), border gateway protocol (BGP), interior gateway protocols (IGPs), and routing information protocol (RIP) is more complex than illustrated. The standard for Internet protocol defines the ICMP and IGMP as part of the IP. However, they receive data and control in the same manner as transport layer protocols user datagram protocol (UDP) and transmission control protocol (TCP), that is, by means of the protocol number in the IP header. The same situation is true with EGPs, and IGPs (excepting RIP). The RIP (an IGP) uses a port number in the UDP header to obtain data and control. Similarly, the BGP also uses a port number, but it is situated in the TCP header to obtain control and data.

In theory, all application protocols could use either the UDP or the TCP. The reliability requirements of the application dictates which transport layer protocol is used. For example, some applications, such as the domain name service (DNS), may either UDP or TCP. The UDP provides an unreliable, connectionless transport service, while the TCP provides a reliable, in-sequence, connection-oriented service.
Because the UDP is unreliable, many of the application layer protocols only use TCP, for example, FTP and TELNET. For the application layer protocols that do not require a reliable service, they use only UDP, for example, TFTP and SNMP. The Internet protocol (IP) is a connectionless, network protocol providing an end-to-end, datagram delivery service. The service is unreliable, and the datagrams may arrive at the destination host damaged, duplicated, out of order, or not at all. This is a major justification for having the transport layer service. Although there are many physical/link layer protocols, the most popular is Ethernet.

INTERNET PROTOCOL (IP)

The IP provides a connectionless delivery system that is unreliable and on a best-effort basis. The IP specifies the basic unit of data transfer in a TCP/IP internet as the datagram. Datagrams may be delayed, lost, duplicated, delivered out of sequence, or intentionally fragmented, to permit a node with limited buffer space to handle the IP datagram. It is the responsibility of the IP to reassemble any fragmented datagrams. In some error situations, datagrams are silently discarded while in other situations, error messages are sent to the originators (via the ICMP, a utility protocol.) The IP specifications also define how to choose the initial path over which data will be sent, and defines a set of rules governing the unreliable datagram service.

USER DATAGRAM PROTOCOL (UDP)

The UDP provides application programs with a transaction oriented, single shot datagram type service. The service is similar to the IP in that it is connectionless and unreliable. The UDP is simple, efficient and ideal for application programs such as TFTP and DNS. An IP address is used to direct the user datagram to a particular machine, and the destination port number in the UDP header is used to direct the UDP datagram (or user datagram) to a specific application process (queue) located at the IP address. The UDP header also contains a source port number that allows the receiving process to know how to respond to the user datagram. It effectively loads up one round with the entire, fixed-length message, aims it at the intended receiver (IP address and destination port number), fires one shot into the network, and ends. There is no acknowledgement, flow control, message continuation, or other sophisticated attributes offered by the TCP. The UDP operates at the transport layer and has a unique protocol number in the IP header (number 17). This enables the network layer IP software to pass the data portion of the IP datagram to the UDP software. The UDP uses the destination port number to direct the from the IP datagram (user datagram) to the appropriate process queue. The format of the UDP datagram is illustrated in Figure-6. Since there is no sequence number or flow control mechanism, the user of UDP must either not need reliability or self service. The reliability of UDP is characterized by phrases such as send and pray, used to describe its operation.

3.2.6 <u>IPX/SPX Protocol Suite</u>

Novell originally developed the IPX/SPX suite in the 1980s for use with their NetWare Servers. 8IPX/SPX also works with all Microsoft Operating Systems, with OS/2, and even with Unix and Linux. IPX stands for Internet Package Exchange. It’s a Network layer protocol that’s analogous to IP. SPX stands for Sequenced Package Exchange. It’s a Transport layer protocol that’s analogous to TCP. Unlike TCP/IP, IPX/SPX is not a standard protocol established by a standards group, such as IEEE.

Instead, IPX/SPX is a proprietary standard developed and owned by Novell. Both IPX and IPX/SPX are registered trademarks of Novell.

<u>NETWORK HARDWARE</u>

The building blocks of networks are network hardware devices such as servers, adapter cards, cables, hubs, switches, routers, and so on.

<u>Servers</u>

Server computers are the lifeblood of any network. Servers provide the shared resources that network users crave, such as file storage, databases, e-mail, Web services, and so on.

<u>Network Interface Cards (NIC)</u>

Every computer on a network, both clients and servers, requires a network interface card (NIC) in order to access the network. A NIC is usually a separate adapter card that slides into one of the motherboard expansion slots. However, some motherboards have a built-in network interface, so a separate card isn’t required.

<u>Network Cable</u>

We can construct an Ethernet network by using one of two different types of cables:

- Coaxial Cable

- Twisted Pair Cable (UTP/ 10BaseT)

Hubs & Switches

The biggest difference between using coaxial cable and twisted-pair cable is that when you use twisted-pair cable, you must also use a separate device called a hub. A switch is simply a more sophisticated type of hub.

Routers

A router is like a bridge, but with a key difference. Bridges are Data Link layer devices. A router is a Network layer device. A router is itself a node on the network, with its own MAC and IP addresses.

3.3 NETWORK OPERATING SYSTEMS

All network operating systems, from the simplest (such as Windows XP Home Edition) to the most complex (such as Windows Server 2003), must provide certain core functions.

Some of the core NOS features are:

- Network Support
- File Sharing Services
- Multitasking
- Directory Services
- Security Services

3.4 TRANSMISSION MEDIA AND INTER NETWORKING COMPONENTS

The networking can be done through wired or wireless media.

3.4.1 Wired media

Cable is the medium through which information usually moves from one network device to another. There are several types of cable, which are commonly used with LANs. In some cases, a network will utilize only one type of cable; other network will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network. The following sections discuss the types of cables used in networks and other related topics.

· Unshielded Twisted Pair (UTP) Cable.

· Shielded Twisted Pair (STP) Cable

· Coaxial Cable

· Fiber Optic Cable

· Wireless LANs

(a)Unshielded Twisted Pair (UTP) Cable

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for networks. The quality of UTP may vary from telephone-grade wire to extremely highspeed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices.

(b)Shielded Twisted Pair (STP) Cable

A disadvantage of UTP is that it may be susceptible to radio and electrical frequency interference. Shielded twisted pair (STP) is suitable for environments with electrical interference: however, the extra shielding can make the cables quite bulky. Shielded twisted pair is often used on networks using Token Ring topology.

(c)Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield the metal shield helps to block any outside interference from fluorescent lights, motors, and other computers. Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are: thick coaxial and thin coaxial.

(d)Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials .It transmits light rather than electronic signals, eliminating the problem of electrical interference. This makes it deal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

3.4.2 Wireless Media

Not all networks are connected with cabling; some networks are wireless. Wireless LANs use high frequency radio signals or infrared light beams to communicate between the workstations and the file server. Each workstation and file serve on a wireless network has some sort of transceiver/antenna to send and receive the data.. Information is relayed between transceivers as if they were physically connected. For longer distance, wireless communications can also take place through cellular

telephone technology or by satellite. Wireless networks are great for allowing laptop computers or remote computers to connect to the LAN. Wireless networks are also beneficial in older buildings where it may be difficult or impossible to install cables.
Wireless LANs also have some disadvantages. They can be very expensive, provide poor security, and are susceptible to electrical interference from lights and radios.

3.5 NETWORK CONFIGURATIONS

Two major network configurations are:

- Peer to Peer
- Client server.

3.5.1 Peer-to-Peer Networks

Peer-to-peer networks allow you to connect two or more computers in order to pool their resources. Individual resources such as disk drives, CD-ROM drives, scanners and even printers are transformed into shared resources that are accessible from each of the computers. They don’t have a file server or a centralized management. In this all computers are considered equal and they all have the same abilities to use the resources available on the network. Unlike client-server networks, where network information is stored on a centralized file server computer and then made available to large groups of workstation computers, the information stored over a peer-to-peer network is stored locally on each individual computer. Since peer-to-peer computers have their own hard disk drives that are accessible and sometimes shared by all of the computers on the peer-to-peer network, each computer acts as both a client (or node) and a server (information storage). In the diagram below, five peer-to-peer workstations are shown. Although not capable of handling the same rate of information flow that a client-server network would, all five computers can communicate directly with each other and share each other's resources.A peer-to-peer network can be built with 10BaseT , 100 Base Tx or with a thin coaxial (10Base2).

3.5.2 Client-Server Networks

In a Client Server network the functions and applications are centralized and managed in servers. The servers are the hearts of the system providing access to resources and security. The servers are loaded with a network operating system like Novel NetWare, Windows NT server, Windows2Kserver etc, provide the mechanism to integrate all the resource allocation to the work stations (clients). Though this type of expensive networks provides a handful of advantages failure of the whole network happens when the server fails.

3.6 WIRELESS LOCAL AREA NETWORKING

A Wireless Local Area Network (WLAN) is a computer network that transmits and receives data with radio signals instead of wires. WLANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. Increased mobility and the absence of cabling and other fixed infrastructure have proven to be beneficial for many users. Wireless users can use the same applications they use on a wired network. Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards. People use WLAN technology for many different purposes:

- Mobility
- Low Implementation Costs
- Installation and Network Expansion
- Inexpensive Solution
- Scalability

WiFi is the wireless way to handle networking. It is also known as 802.11 networking and wireless networking. The big advantage of WiFi is its simplicity. You can connect computers anywhere in your home or office without the need for wires. The computers connect to the network using radio signals, and computers can be up to 100 feet or so apart.

WiFi's Radio Technology

The radios used in Wi-Fi have the ability to transmit and receive. They have the ability to convert 1s and 0s into radio waves and then back into 1s and 0s. The Institute of Electrical and Electronics Engineers (IEEE) creates standards, and they number these standards in unique ways. The 802.11 standard covers wireless networks.

3.7 Network Security System Firewall

Consider the Internet to be fire of viruses, hackers and cyber criminals all looking for systems that they can invade. The firewall stops unwanted connections from entering your internal network.. Rather like the gate in the fortress wall the firewall allows only data and connections that meet certain criteria to pass through the wall to the internal network. A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It may be a hardware device (see Figure 1) or a software program (see Figure 2) running on a secure host computer. In either case, it must have at least two network interfaces, one for the network it is intended to protect, and one for the network it is exposed to. A firewall sits at the junction point or gateway between the two networks, usually a private network and a public network such as the Internet. The earliest firewalls were simply routers. The term firewall comes from the fact that by segmenting a network into different physical subnetworks, they limited the damage that could spread from one subnet to another just like firedoors or firewalls. A firewall examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped. A firewall filters both inbound and outbound traffic. It can also manage public access to private networked resources such as host applications. It can be used to log all attempts to enter the private network and trigger alarms when hostile or unauthorized entry is attempted. Firewalls can filter packets based on their source and destination addresses and port numbers. This is known as address filtering. Firewalls can also filter specific types of network traffic. This is also known as protocol filtering because the decision to forward or reject traffic is dependant upon the protocol used, for example HTTP, ftp or telnet. Firewalls can also filter traffic by packet attribute or state.

A firewall cannot prevent individual users with modems from dialing into or out of the network, bypassing the firewall altogether. Employee misconduct or carelessness cannot be controlled by firewalls. Policies involving the use and misuse of passwords and user accounts must be strictly enforced. These are management issues that should be raised during the planning of any security policy but that cannot be solved with firewalls alone. The arrest of the Phonemasters cracker ring brought these security issues to light. Although they were accused of breaking into information systems run by AT&T Corp., British Telecommunications Inc., GTE Corp., MCI WorldCom, Southwestern Bell, and Sprint Corp, the group did not use any high tech methods such as IP spoofing (see question 10). They used a combination of social engineering and dumpster diving. Social engineering involves skills not unlike those of a confidence trickster. People are tricked into revealing sensitive information. Dumpster diving or garbology, as the name suggests, is just plain old looking through company trash. Firewalls cannot be effective against either of these techniques.

Anyone who is responsible for a private network that is connected to a public network needs firewall protection. Furthermore, anyone who connects so much as a single computer to the Internet via modem should have personal firewall software. Many dial-up Internet users believe that anonymity will protect them. They feel that no malicious intruder would be motivated to break into their computer. Dial up users who have been victims of malicious attacks and who have lost entire days of work, perhaps having to reinstall their operating system, know that this is not true. Irresponsible pranksters can use automated robots to scan random IP addresses and attack whenever the opportunity presents itself.

There are two access denial methodologies used by firewalls. A firewall may allow all traffic through unless it meets certain criteria, or it may deny all traffic unless it meets certain criteria (see figure 3). The type of criteria used to determine whether traffic should be allowed through varies from one type of firewall to another. Firewalls may be concerned with the type of traffic, or with source or destination addresses and ports. They may also use complex rule bases that analyse the application data to determine if the traffic should be allowed through. How a firewall determines what traffic to let through depends on which network layer it operates at. A discussion on network layers and architecture follows.

CHAPTER 4

TRANSMISSION UNITS

4.1 Introduction

- The study of transmission units has a unique importance for a communication engineer who has to maintain and install telecommunication equipments achieving the standards set up by international consultation committees. In order to control the quality of wanted signal in the presence of many undesired signals, we should be able to specify the amount of wanted and unwanted signals at a point in the telecommunications network. The components used in the telecommunication circuit either give loss or gain to the signals they handle. There are certain specific operating conditions to be satisfied for various components without which the optimum performance cannot be obtained from these components. For this, it is essential to define conditions that control those operating conditions. This can be done only if the conditions are specified in terms of certain units of the quantity, which the components are to handle.

4.2 Transmission Impairments

With analog transmission systems using copper cable there are three major categories of impairments. They are attenuation, noise, and distortion.

- **Attenuation:** There are two commonly used processes to compensate (overcome) for attenuation or loss:
  - Repeaters are the most commonly used devices to compensate for "Loss." However, repeaters amplify the noise along with the signal resulting in a poor signal to noise ratio.

- Signal to Noise Ratio: The ratio of the average signal power (strength) to the average noise power (strength) at any point in a transmission path.

- **Noise:** Any random disturbance or unwanted signal on a transmission facility that obscures the original signal. Noise is generally caused by the environment in which the system is operating.
- **Distortion:** Inaccurate reproduction of a signal caused by changes in the signal's waveform, either amplitude or frequency.To compensate for distortion equalizers may be used. One type of equalizer used in the analog environment is the load coil. Load coils are used to flatten the frequency response.

Signal-to-Noise Ratio

It is popularly known as SNR. SNR is the ratio of signal power to the noise power at any point in a circuit. This ratio is usually expressed in Decibels (dB). For satisfactory operation of a channel the value of SNR should be sufficiently high i.e., the signal power should be sufficiently higher than the noise power. SNR at any point in a circuit is given as SNR = S/N = Signal Power / Noise Power Both powers are expressed in watts.

Expressing dBs: SNR = 10 $\log_{10}$ (S/N) dB.

4.3 DISTORTION IN TELECOMMUNICATION CIRCUITS

4.3.1 Introduction

A signal is said to have suffered distortion if, after passing through a network is not an exact replica of the original signal in respect of its amplitude or wave

Signal distortion is of two kinds.

a) Linear distortion

b) Non linear distortion

Linear distortion takes place in passive networks. Different types of linear distortion are;

1. Attenuation distortion
2. Phase distortion

Imperfect attenuation, frequency response and phase-frequency characteristic of a network cause attenuation and phase distortions respectively. Non-linear distortion takes place in active networks only and is caused by their excessive loading. Different types of non-linear distortion are;

a. Amplitude distortion

b. Frequency distortion

c. Inter-modulation distortion

- **Attenuation distortion**

The term attenuation distortion is employed to the case of a transmission system where here is variation of gain or loss with frequency. It is assessed with the system operated under steady-state condition by applying a series of sinusoidal waveforms at different frequencies. Fig.1

shows the amplitude- frequency characteristics of an open wire line. Curve A depicts an ideal open wire line with no attenuation distortion. Curve B pertains to the practical one.

- **Phase distortion (Envelope delay distortion)**

Phase distortion takes place when the time of propagation through a transmission system varies with frequency. Owing to the different relative phase relationships than existing, the output waveform may appear to be quite different from the input waveform, even though the same frequencies are available in the same relative amplitude.

- **Non-linear distortion**

"Non linear distortion" is the general name given to a certain type of distortion that occurs when the transmission properties of a system are dependent on the instantaneous magnitude of the applied signal. It is further sub-divided as under:

a) Amplitude distortion.
b) Harmonic distortion.
c) Inter-modulation distortion.

- **Amplitude distortion**

It is defined as the variation of gain or loss of a system with the amplitude of the input. It is measured with the system operated under steady- state conditions with an input of sinusoidal waveform.

- **Harmonic distortion**

It is due to the production of harmonics in the output when a sinusoidal input of specified amplitude is applied. It is expressed as the ratio of the RMS voltage of all the harmonics in the output, to the total RMS voltage at the output.

- **Inter-modulation distortion**

It is due to the production of combination frequencies in the output when two or more sinusoidal voltages of specified amplitude are applied at the input. For two parent frequencies p and q, the output may contain frequencies such as (p± q), (1p± q), (p± 2q) etc. in addition to the frequencies p and q.

4.4 CROSS-TALK IN TRANSMISSION MEDIA

4.4.1 Introduction

Any disturbing signal produced by transfer of unwanted power from one transmission path (called disturbing circuit) to another transmission path (called disturbed circuit) is known as cross talk. Cross talk may be produced by

- Galvanic, capacitive or inductive couplings between transmission media (Linear cross-talk) e.g. between pairs of a VF (voice frequency) cable system.
- Poor control of frequency response i.e. defective filters or poor filter design is the cause.
- Non-linear performance in analogue (FDM) multiplex systems. A signal transmitted on one circuit or channel of a transmission system (multichannel) creates an undesired effect in another circuit or channel (nonlinear cross talk)

4.4.2 <u>Types of cross talk</u>

Broadly speaking, cross talk is of six types.

1. Near-end cross- talk (NEXT).
2. Far-end cross talk (FEXT).
3. Intelligible cross-talk
4. Unintelligible cross-talk
5. Interaction cross-talk
6. Reflected cross-talk

- **<u>Near-end cross talk (NEXT)</u>**

Near-end cross talk occurs if the cross talk power in the disturbed channel propagates in the direction opposite to the propagation of useful power in the disturbing channel. Refer to figure for illustration of near-end cross talk. The terminals of the disturbed channel, at which the near-end cross talk is present, and the energized terminal of the disturbing channel, are usually near each other. The near-end cross talk is much stronger than far-end cross talk because the magnetic (or galvanic) and electrostatic inductions are additive in the case of nearend cross talk and the inducing current in the disturbing circuit is much stronger.

- **<u>Far-end cross-talk (FEXT)</u>**

It occurs if the cross talk power in the disturbed channel propagates in the direction of the propagation of the useful power in the disturbing channel. The terminals of the disturbed channel, at which the far-end cross talk is present, and the energized terminals of the disturbing channel, are usually remote from each other. Far-end cross talk is less effective in impairment of the original signal in the disturbed circuit because the magnetic and electrostatic inductions are subtractive. Also the inducing current in the disturbing circuit gets very much attenuated after it has travelled to the far end.

- **<u>Intelligible cross talk</u>**

The cross talk is intelligible when the whole or an important part, of the speech on the disturbing circuit is intelligible on the disturbed circuit. Between circuits transmitting the same frequency band or working without frequency translation (audio-frequency) only, intelligible cross talk can arise. As the secrecy of the conversation is affected by intelligible cross talk, steps should be taken to see that intelligibility of sentence articulation of the cross talk should be less than 10%.

- **<u>Unintelligible cross talk (also called noise)</u>**

The cross talk is unintelligible when the disturbing circuit gives rise only to noise in the disturbed circuit. It decreases the intelligibility but does not endanger the secrecy of conversation. Unintelligible cross talk occurs

1. Between carrier channels having different frequency allocations.
2. Between carrier channels having virtual carrier frequencies essentially differing from each other and
3. In consequence of non-linear distortion.

- **Interaction cross talk (Indirect cross talk)**

Interaction cross talk conveyed by a third circuit from the disturbing circuit to the disturbed circuit, where it causes far end cross talk (fig.3). This type of cross talk is also called double near-end cross talk. It occurs mainly in two-wire carrier systems fitted with intermediate repeaters.

- **Reflected cross-talk**

Indirect cross talk caused by reflection due to mismatch of the circuit is called reflected cross talk.

4.4.3 Causes of cross-talk

Cross talk is mainly caused by two types of induction viz., Magnetic and Electrostatic.

- **Magnetic induction**

It is well known that a change in magnetic lines of forces is associated with the flow of electric currents. The magnetic lines of forces due to currents flowing through circuit A will also embrace the wires of circuit B. As the current in circuit A alternates, the magnetic field also alternates, and according to Faraday' law it induces e.m.fs in the wires of circuit B.

- **Electrostatic induction**

Electrostatic induction occurs due to the capacitance between four wires of the two circuits that are built side by side. Practically it is noted that the current due to magnetic induction flows in one direction in the entire circuit, whereas that due to the electric induction flows through the two sections in opposite directions.

4.5 OPTICAL FIBRE CABLE

4.5.1 FIBRE OPTICS :

Optical Fibre is new medium, in which information (voice, Data or Video) is transmitted through a glass or plastic fibre, in the form of light, following the transmission sequence give below :

(1) Information is encoded into electrical signals.
(2) Electrical signals are converted into light signals.
(3) Light travels down the fibre.
(4) A detector changes the light signals into electrical signals.
(5) Electrical signals are decoded into information.

4.5.2 <u>ADVANTAGES OF FIBRE OPTICS</u> :

Fibre Optics has the following advantages :

(I) Optical Fibres are non conductive (Dielectrics)

- Grounding and surge suppression not required.
- Cables can be all dielectric.

(II) Electromagnetic Immunity :

- Immune to electromagnetic interference (EMI)
- No radiated energy.
- Unauthorised tapping difficult.

(III) Large Bandwidth (> 5.0 GHz for 1 km length)

- Future upgradability.
- Maximum utilization of cable right of way.
- One time cable installation costs.

(IV) Low Loss (5 dB/km to < 0.25 dB/km typical)

- Loss is low and same at all operating speeds within the fibre's specified bandwidth long, unrepeated links (>70km is operation).

(v) Small, Light weight cables.

- Easy installation and Handling.
- Efficient use of space.

(vi) Available in Long lengths (> 12 kms)

- Less splice points.

(vii) Security

- Extremely difficult to tap a fibre as it does not radiate energy that can be received by a nearby antenna.
- Highly secure transmission medium.

(viii) Security - Being a dielectric

- It cannot cause fire.
- Does not carry electricity.
- Can be run through hazardous areas.

(ix) Universal medium

- Serve all communication needs.
- Non-obsolescence.

4.5.3 <u>APPLICATION OF FIBRE OPTICS IN COMMUNICATIONS</u> :

- Common carrier nationwide networks.
- Telephone Inter-office Trunk lines.
- Customer premise communication networks.
- Undersea cables.
- High EMI areas (Power lines, Rails, Roads).
- Factory communication/ Automation.
- Control systems.
- Expensive environments.
- High lightening areas.
- Military applications.

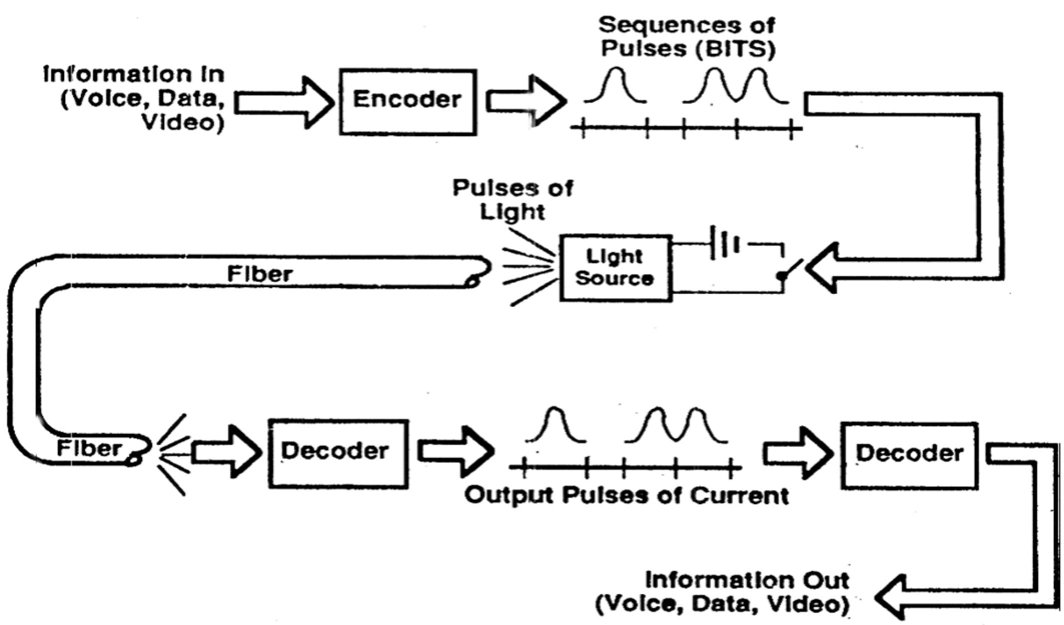
- Classified (secure) communications.

4.5.4 <u>Transmission Sequence</u> :

(1) Information is Encoded into Electrical Signals.
(2) Electrical Signals are Coverted into light Signals.
(3) Light Travels Down the Fiber.
(4) A Detector Changes the Light Signals into Electrical Signals.
(5) Electrical Signals are Decoded into Information.
- Inexpensive light sources available.
- Repeater spacing increases along with operating speeds because low loss fibres are used at high data rates.

4.5.5 <u>Principle of Operation - Theory</u>

· Total Internal Reflection - The Reflection that Occurs when a Light Ray Travelling in One Material Hits a Different Material and Reflects Back into the Original Material without any loss of Light.



<u>CHAPTER 5</u>

<u>DATA COMMUNICATION</u>

5.1 <u>INTRODUCTION</u>

Communication plays a very important part in our lives because we are almost always involved in some form of communication, e.g.

· Face-to-face conversation

· Reading a book
· Sending or receiving a letter
· Telephonic conversation
· Watching a film or T. V.
· Looking at paintings in an art gallery
· Attending a lecture

There are many other examples of communications and Data Communications is one specific area of whole field of communication. Aim of communication is to transfer some information from one point to another. In data communication, this information is generally called as Data or a message.

COMPONENTS

In order to send data/message from one point to another, following three components are essential:
1. Source
2. Medium
3. Receiver

These elements are the minimum requirement for any communication process. In data communication, source and receiver are called Data Terminal Equipment (DTE), e.g. A teleprinter or a computer terminal with keyboard. The medium may be a 2W telephone line or 2W/4W leased line.

5.2 TRANSMISSION DEFINITIONS

For understanding the data communication following terminology is discussed: -

- **Communication lines**
  The medium that carries the message in a data communication system, e.g. A 2W telephone line.

- **Communication Channel**

A channel is defined as a means of transmission. It can carry information in either direction but in only one direction at a time.E.g. A hose pipe. It can carry water in either direction, but the direction of flow depends on which end of pipe is connected to the water tap.

- **Simplex Transmission**
  1. Message always flows in one direction only.
  2. An input Terminal can only receive and never transmit.
  3. An O/P Terminal can only transmit and never receive.

- **Half Duplex Transmission**
  - A half duplex channel can transmit and receive but not simultaneously.
  - Transmission flow must halt each time and direction is to be reversed.
  - This halt is called the turn-around time and is typically 8 to 10 ms in the case of leased circuits and 50-500 ms in case of 2W telephone line through Public Switched Telephone Network (PSTN).

- **Full-duplex Transmission**
  It is both way communication. If we set up a communication line with two channels, we have the capability of sending information in both directions at the same time. This is called full duplex transmission system.

5.3 TRANSMISSION CODES

All data communication codes are based on the binary system (1s and 0s). A message can be encoded into a meaningful string of 1s and 0s that can be transmitted along a data line and decoded by a receiver. The string of 1s and 0s is meaningful because it is defined by a code that is known to both the source and the receiver. Code is limited by the number of bits (binary digits) it contains, e.g. one-bit code means that we can have 2 characters so that we can encode the letter A by '0' and B by '1'. Similarly, a 2 bit code will enable us to handle 4 characters. Thus, a n-bit code enables us to handle 2^n characters. Some commonly used codes are :

1. Baudot code
2. ASCII code
3. BCDIC code
4. EBCDIC Code

Baudot Code

This is also called International Alphabet no.2. This is used on International telex network and is often called telex code. It being a 5 bit code, we can represent 32 characters. This is not enough to handle a full alphanumeric character set. So two of the characters are designated as code extension characters. These are letter shift (LS) and figure shift (FS).

LS = 11111 represented by 1. (Downward arrow)

FS = 11011 represented by 1. (Upward arrow)

Pressing LS or FS indicates the receiver that next character will be a letter character or a figure character as the case may be. So we can double the number of characters that can be handled by this code.

Limitations

All the 5 bits are used for information and there is no inherent means for error detection.

ASCII Code (American Standard Code for Information Interchange)

It is an eight-bit code which consists of seven information bits and one bit for parity checking. This is the most widely used data code. Seven information bits gives us 128 combinations, which allows us to encode a full keyboard of the computer.

- 52 alphabets (capital and small).
- 0-9 (10 numbers).
- Punctuation marks
- Additional graphic and control characters.

Parity Bit is placed at the most significant bit position. Purpose of parity bit is to detect the errors. While transmitting on line, Least Significant Bit (LSB) is transmitted first and MSB last. e.g. H is transmitted on line as bit no. 1234567P i.e. 00010011assuming P=1(odd parity).

BCDIC (Binary Coded Decimal Interchange Code)

It is a six-bit code that is used as an internal code by some computers. With 6 information bits, we can have $2^6 = 64$ possible code combinations. For data transmission, code is implemented as 7-bit code containing 6 information bits and one parity bit.

EBCDIC (Extended Binary Coded Decimal Interchange Code)

It is a 8-bit code in which all the 8-bits are used for information (unlike ASCII), giving 256 possible code combinations. EBCDIC is used as an internal machine code in some of the computers.

5.4 DATA TRANSMISSION

(a) Parallel Transmission.
(b) Serial Transmission.

Parallel Transmission

In this method, all bits of encoded character are transmitted simultaneously which means that each bit of the code is having a dedicated channel.

Serial Transmission

It is the most commonly used method of communication. In this method, bits of the encoded character are transmitted one after the other along one channel serially bit by bit as well as character by character.

Bit Synchronization

Clock is used for synchronization. The source clock tells the source how often to put the bits on to the line and receive clock tells the receiver how often to look at the line, e.g. in Fig.9. If we wish to transmit at 100 bits/sec. we set the source clock to run at 100 bits/sec. which tells the source to put the bits on the line 100 times per second. At the receiving end, we would see a bit appearing at the input of the receiver every 1/100th of a second.

Character Synchronisation

Receiver can identify the character if it knows how many bits are there in the character and the speed at which the bits are coming down the line. Then it can count off the required number of bits and assemble the character once it has identified the first bit of a character. There are two ways to identify the first bit of a character.

1. Synchronous Transmission.
2. Asynchronous Transmission.

Synchronous Transmission

It is used to transmit whole blocks of data at once. Each block of data is preceded with a unique synchronising pattern. This makes use of SYN transmission control character. The SYN character has a bit pattern of 00010110 with odd parity. Receiver is designed to continuously look towards the 'SYN' character. When it receives the SYN character, it knows the first bit of the information character. But sometimes there is false synchronisation (Fig.11) where eight bits of two continuous characters could look like a SYN character.

5.5 CHARACTERISTICS OF DATA SIGNALS

Having organised the data into binary codes, the binary conditions have to be represented in the form of electrical signals suitable for remote transmission over communication lines. There are a number of ways by which digital symbols can be represented by electrical signals. Fig.13 shows a synchronous two valued (binary) data waveform. In each symbol interval, a condition of 'current' or 'no current' is transmitted. The two symbols are labeled '1' and '0'. In telegraph terminology, these are called MARK and SPACE. Each signal element has the same duration of T seconds and follows immediately after the preceding element, so that the signal element rate is 1/T bits per second.

The receiver under the control of its clock, properly phased with respect to the incoming data waveform, samples the wave at the middle of each symbol interval. If the amplitude is between half and full amplitude, the symbol is recorded as a '1' ; if between zero and half amplitude the symbol is recorded as '0'. The threshold of decision is the half amplitude level (normally). Instead of current and no current opposite directions or polarities of current can be used. Fig.14 shows a waveform having equal positive and negative amplitudes. In this case the decision threshold is zero. This type of signal is referred to as 'Polar' signal In the foregoing examples, there is no change in the signal if one of the symbols is repeated. It is sometimes desirable to have definite separation between two consecutive symbols as shown in Fig.15. This type of signal is called the "Return to Zero" signal as opposed to the 'Non return to zero' signals of the previous examples which used full bit length pulses.

5.6 CHARACTERISTICS OF A TRANSMISSION CHANNEL.

Information carrying capacity of a transmission channel is determined by the following two characteristics: -

1. Bandwidth (BW).
2. Signal-to-noise (S/N) Ratio.

5.7 NYQUIST–SHANNON SAMPLING THEOREM

The **Nyquist–Shannon sampling theorem** is a fundamental theorem in the field of information theory, in particular telecommunications. In addition to Claude Shannon and Harry Nyquist, it is also attributed to Whittaker and Kotelnikov, and sometimes simply referred to as the **sampling theorem.**

The theorem states the conditions under which the samples of a signal (e.g., a function of time) can be used to reconstruct the signal perfectly: When sampling a bandlimited signal (e.g., through analog to digital conversion) the sampling frequency must be greater than twice the signal's bandwidth in order to be able to reconstruct the original signal perfectly from the sampled version. Intuitively, if a signal is bandlimited prior to digitization, it cannot change very rapidly, so that the information obtained from the samples is enough to reconstruct the signal. As is seen more formally below, a greater sampling frequency is required if the bandwidth of the signal. If the conditions of the theorem are not satisfied, this phenomenon is called aliasing, which is undesirable in most applications because the signal has not be sampled fast enough.

5.8 SIGNAL ENCODING

We can represent bits as digital electrical signals in many ways. Data bits can be coded into following two types of codes :

(a) Non Return to Zero (NRZ Codes).

(b) Return to Zero (RZ Codes)

- **NRZ Codes:**In this type of codes, the signal level remains constant during a bit duration. There are 3 types of NRZ codes.
- **NRZ-L Coding:**Bit is represented as a voltage level which remains constant during the bit duration.
- **NRZ-M Coding:**A transition in the beginning of a bit interval whenever there is a 'Mark.
- **NRZ-S Coding:**A transition in the beginning of a bit interval whenever there is a 'Space'. Let us see the following bit stream 10100110 into three different types of NRZ codes.

5.9 TRANSMISSION AND COMMUNICATION

Let us now understand the difference between transmission and communication. Transmission means physical movement of information from one point to another. Communication means meaningful exchange of information between the communicating devices.

We have two types of communication :

(1) Synchronous Communication.

(2) Asynchronous Communication.

- **Synchronous Communication:** In Synchronous communication the exchange of information is in a well disciplined manner, e.g. if A want to send some information to B, it can do so only when B permits it to send. Similarly, vice-versa is true. There is complete synchronisation of dialogues, i.e. each message of the dialogue is either a command or a response. Physical transmission of data may be in synchronous or asynchronous mode already decided between A and B.

- **Asynchronous Communication:** In Asynchronous communication the exchange of information is in less disciplined manner, e.g. A and B can send messages whenever they wish to do so. Physical transmission of data may be in synchronous / asynchronous mode. Thus, we see that Simplex Transmission is one way communication (OW), Half Duplex Transmission is two way Alternate Communication (TWA), and Full Duplex Transmission is two way Simultaneous Communication (TWS).

5.10 TRANSMISSION OF DIGITAL DATA INTERFACES AND MODEMS

LOCAL AREA NETWORK (LAN)

A network of interconnected computers, which exists within a limited geographical area, such as a room, a building or a campus, is termed as a Local Area Network. A few characteristics of LAN are as below:

- Speed 4, 10, 16 up to 100MBPS
- Distance Few Kms (Typically 1.5Kms)
- Requires dedicated local wiring (Ethernet, Token Ring, FDDI, ATM)
- Shared access to medium

3.4 LAN TOPOLOGY

Common LAN topologies are Bus, Ring and Star, Network requirements of these topologies are:

- Flexible to accommodate
- Changes in physical location of the stations

- Increase in number of stations.
- Increase in LAN coverage
- Consistent with the media access method
- Minimum cost of physical media.

5.10.1 TRANSMISSION MEDIA FOR LAN

In a local area network, stations are interconnected using transmission media which can be a twisted pair cable or a coaxial cable or even an optical fiber cable. Choice of transmission media depends on several factors. While data rate and cost are prime considerations, physical and electrical characteristics of the media need also to be taken into account because they determine ease of installation, noise immunity, geographical coverage etc. In this chapter, popular physical transmission media are discussed. They are twisted pair, base-band and broadband coaxial cables and optical fibers. Their physical construction, characteristics and applicability to various medium access methods are described.

5.10.2 Considerations for Choice of Transmission Media:

The following features of the transmission media must be taken into consideration while choosing suitable media for local area networks.

- **Bandwidth:**Bandwidth of the transmission media determines the maximum data rates which can be handled by the media. Data rates are, of course, determined by the stations but the transmission medium should not become bottleneck in achieving the required data rate. It must be kept in mind that bandwidth of transmission media is function of the length of the media. For e.g. it may be possible to achieve very high data rates on a low cost twisted pair but then maximum length of one transmission segment is limited to not more than a few meters.

- **Connectivity:**Some transmission media are suitable for broadcast mode of operation and point to multi-point links, while others are better suited for point to point links. For example, the present status of technology, Optical fiber is suited for point to point links only.

- **Geographic Coverage:**In a LAN operating in broadcast mode on a bus, the electrical signals should reach from one end to the other without degradation in quality of the signals below the required limits. Attenuation and group delay characteristics of the medium determine overall distortion in the signals. These characteristics are function of distance and therefore determine the geographic coverage of the LAN. Propagation time, which is also dependent on the media characteristics, is an important consideration in that access mechanism where propagation delay determines the length of one segment of the media.

- **<u>Noise immunity</u>:**Ideally the transmission media chosen for LAN should be free from interference from outside sources, though practically it is not possible. Degree of immunity to interference varies from media to media. Susceptibility to interference is because LAN cabling is usually done in the same ducts which carry power cables also. Degree of noise immunity required depends on environment where a LAN is installed.

- **<u>Security</u>:**In some of the LAN topologies and access methods it is very easy to tap on the LAN & pick up the messages without generating any alarm. For considerations of data security, the transmission medium is to be so chosen that it may not be easily tapped.

- **<u>Cost</u>:**At present state of technology, cost of different media are different and are changing continuously. Metallic media is becoming costlier and optical fiber costs are going down. Cost of media is also related to the cost of equipment associated with the media. Therefore an overall view of cost structure is more important than media alone. In most of the instances, the LAN vendors specify the medium for which their products are designed. A look into the characteristics of media do help the user in becoming aware of the limitations of the transmission medium being supplied by the vendor.

5.10.3 MEDIA ACCESS CONTROL

The physical topology of local area networks can take shape of a bus or ring or a star but the network attributes in terms of delay, throughput, expandability etc. are determined by the mechanisms utilized for sharing the use of physical interconnecting media. There are many methods sharing the media and they are, in general, called Media Access Control methods. These methods can be categorized as :

- Access Centrally Controlled
- Distributed Access Control

In the former access to the media is controlled by a central controller. There are several ways in which the media is shared, e.g. Polling, demand assigned time division or frequency division multiple access, etc. However if the central controller fails, the entire network goes down. But in local area networks, distributed access control methods are more common and are described in the following sections.

<u>Distributed Access Control</u>

As name implies, there is no single controller for the shared media. A discipline is built up among the various stations (station refers to a LAN terminal/host/any other device) of the local area network so that a fair opportunity is given to each station to transmit its data which is in the form of frames. The basic advantage of distributed control over centrally controlled methods is that there is no single point of network failure. Distributed access control methods are available both for bus and ring topologies.

Media Access Control – Bus Topology

An interconnecting bus can be thought of as single data transmission channel to which all the stations of the network are connected. A bus can be a twisted pair cable, a coaxial cable or even an optical fiber cable. The bus operates in broadcast mode, i.e. all the stations are always listening to all the transmissions on the bus. Access control mechanisms are so designed that transmissions from different stations do not intermingle and all the stations get fair chance to transmit. There are two techniques which dominate the present day market :

Token passing and CSMA/CD.

5.10.4 DATA LINK CONTROL

The services provided by the physical layer are limited to conversion of bits into electrical signals and transmission of these signals over the interconnecting media. But it is not sufficient for reliable transmission of the bits. Disturbed line conditions of the media may introduce errors which must be taken care of. The basic function-error control and other associated functions are carried out by the second layer of the OSI model, data link layer. In the following sections, we shall discuss in general the mechanisms used for implementation of these functions in various data link protocols.

To transfer digital information from device A to B and in the opposite direction, we require :

- An interconnecting transmission medium to carry the electrical signals (e.g.copper wires).
- A standard interface between the device and the interconnecting transmission medium (e.g. RS-232-C).
- Services of the physical layer to convert bits (1s and 0s) into electrical signal.

These three elements provide only the capability for transparent exchange of bits over the physical connection. The electrical signal, however, may get corrupted by the noise encountered during transmission over the physical medium and this may result in introduction of errors in the data bits. Therefore, a mechanism to control the transmission errors is required. The bits could also be lost if the receiving device is not ready for the incoming bit stream. Therefore, a data flow control mechanism also needs to be implemented. Flow control also enables error control because an error is detected, the receiver should be capable halting further incoming flow of bits till the errors have been corrected.

Error control and flow control functions ensure reliable transfer of bits from one device to the other. These functions are not carried out by the physical layer but are implemented in the data link layer.

5.10.5 DATA LINK LAYER

The data link layer constitutes the second layer of the hierarchical OSI model. It incorporates certain data link control processes which carry out error control, flow control and the associated link management functions. The data link layers together with physical layers and interconnecting medium provide a data link connection for reliable transfer of data bits over imperfect physical connection.

5.10.6 DATA LINK PROTOCOLS

Protocols are rules and procedures governing the interaction between two peer (equal) entities. In the present context these entities are the data link control processes constituting the data link layers. There are many data link protocols developed by various manufacturers and organisations. While all the protocols broadly satisfy the basic requirements of the data link layer, the services offered are different.

Examples of data link protocols are :

- Binary Synchronous Data Link Control (BISYNC, BSC).
- Synchronous Data Link Control (SDLC).
- High Level Data Link Control (HDLC).
- Advanced Data Communication Control Procedure (ADCCP).

BISYNC and HDLC are the most commonly used protocols today, but HDLC is going to be the most important in future because it has been accepted as a standard. A data link protocol must specify :

- The format of the frames, i.e. the position and size of the various fields.
- The contents of the fields containing control bits.
- The sequence of the messages to be exchanged to carry out error control, flow control and link management functions.

Data link functions are implemented differently in different protocols. But they consist of similar set of processes which are described below.

FRAMING

The first and foremost task of the data link layer is to format the user data as series of frames each having a predefined structure. The frame format, in general, consists of three components as shown in Fig. 5.4(a).

- Header
- Data
- Trailer

The data field contains the data bits received from the next higher layer which are to be transmitted across the data link. The header and the trailer consist of one or more fields containing data link protocol control information. Note that header and trailer consist of several fields. The frame starts with a flag to identify the start of a frame. The flag is followed by an address field. The control field contains sequence number of the frame, acknowledgement of having received a good frame or other link control information. The trailer consists of Frame Check Sequence (FCS) containing error detection bits and a flag indicating end of the frame. It is not necessary that all frames contain all the fields. Some of the frames contain only the control information. These frames are used for link management, error and flow control functions.

FRAME FORMAT

A frame consists of number of fields and, therefore, its format is so designed that the receiver is able to

- locate the beginning of each frame.
- locate various fields in a frame.
- separate the data field.

For this purpose, some field identifiers and frame identifiers, are incorporated. For example, in the HDLC frame as shown in Fig.5(b), the flags identify the start and end of the frames. The other fields, address, control and FCS fields have fixed number of bits, so they can be easily separated, once flags have been identified. The remaining bits of the frame constitute the data field.

TRANSPARENCY

Problems may arise if the data field in a frame contains bit patterns similar to the bits in the header or trailer. For example, if the data contains a bit pattern same as the flag in a HDLC frame, the receiver may mistake it for end of the frame. Therefore, the frame format should be so designed that such situations are taken care of an no restrictions are placed on the user as to what bit patterns can/cannot be sent.

FLOW CONTROL

Flow control mechanisms are incorporated to ensure that the data link layer at the sending end does not send more data frames than what the data link layer at receiving end is capable of handling. Therefore, the receiver is to be provided with a control to regulate the flow of the incoming frames. This control is in form of an acknowledgement (ACK) which is sent by the receiver, the acknowledgement serves two purposes :

- It clears the sending end to transmit the next data frame.
- It acknowledges receipt of previous frame(s).

The two commonly used flow control mechanisms are STOP-AND-WAIT and SLIDING WINDOW.

5.10.7 DATA LINK ERROR CONTROL

Two types of errors can occur during transmission of frames from one device to the other.

- Content errors.
- Flow integrity errors.

Errors contained in a received frame are termed as content errors. Flow integrity errors refer to the lost/duplicate frames and acknowledgements. Error control involves three phases :

- Error Detection.
- Error Correction.
- Recovery.

Content errors are detected using parity check or cyclic redundancy codes. The parity bits or CRC check bits are added as the trailer in a frame at the sending end. The most common method of error correction is retransmission of the frame. The receiver informs the sending end of the error and the sending end retransmits. Note that it is essential for the sending end to retain a copy of the transmitted frame until it is acknowledged by the receiver. Recovery refers to how the system gets back into normal operating mode after a correction has been made. Generally, the sending end treats each retransmission ame as the first transmission and continues with the next frame. It keeps a historical record to detect if the link has become very noisy resulting in very frequent transmissions. In such an eventuality, it may initiate recovery procedures which may involve re-establishment of the link. For the flow integrity errors, the data link protocols specify the procedures to be adopted to detect and recover the missing frames and acknowledgements. It must be remembered that no error method is 100% effective. There will always be some undetected content and flow integrity errors. Residual Error Rate (RER) refers to the errors that still exist in the data stream after all error control procedures have been completed.

5.10.8 DATA LINK MANAGEMENT

The data transfer process between two devices can be viewed as consisting of the following phases

- Link establishment phase.
- Information transfer phase.
- Termination phase.

Link establishment includes processes required to initialise the data link, call/poll the other end, set mode of data transfer (synchronous/asynchronous) etc. Information transfer phase involves exchange of data and acknowledgements. Disconnection phase consists of those processes associated with relinquishing control of the link. Control is normally returned to the master/primary station. Data link protocols define a set of control symbols and procedures to execute the above mentioned functions. These symbols and procedures are specific to a data link protocol and, therefore, cannot be generalised.

DATA LINK PROTOCOL

High Level Data Link Control (HDLC) was developed by ISO and has become the most widely accepted data link protocol. It offers a high level of flexibility, adaptability, reliability and efficiency of operation for today as well as tomorrow's synchronous data communication needs. ADCCP developed by ANSI is almost similar to HDLC, IBM'S SDLC is a proper subset of HDLC and level 2 of X- 25 is a permissible option of HDLC. In this chapter, we shall study the basic features and operation of HDLC protocol. Certain liberties have been taken in the level of completeness of description so as not to cloud the overall picture with the details.

GENERAL FEATURES

HDLC is a bit oriented data link control protocol which satisfies wide variety of data link control requirements including :

- Point-to-point and point-to-multipoint links.
- Two way simultaneous communication over full duplex circuits.
- Two way alternate operation over half duplex or full duplex circuits.
- Synchronous and asynchronous communication.
- Communication between primary stations and between primary and secondary stations.
- Full data transparency.

5.11 NETWORK ESSENTIALS

5.11.1 FUNDAMENTALS OF NETWORKING

Information does not exist in a vacuum. Just as the need to share in formation between desktop computers in an office has forced the proliferation of LANs, the need to share information beyond a single workgroup is forcing the adoption of LAN to- LAN links, host gateways, asynchronous communication servers, and other methods of communicating with other systems.

5.11.2 LAN COMPONENTS

Local Area Network is a high speed, low error data network covering a relatively small geographic area. LAN connects workstations, peripherals, terminal and other devices in a single building or other geographically limited area. LAN standard specifies cabling and signaling at the physical and data link layers of the OSI model. Ether. FDDI and Token ring are widely used LAN technology. In LAN technology to solve the congestion problem and increase the networking performance single Ethernet segment is to divide into multiple network segments. This is achieved through various network components. Physical segmentation, network switching technology, using full duplex Ethernet devices, fast Ethernet and FDDI available bandwidth may be maximized.

- **REPEATERS:** Repeaters are devices that amplify and reshape the signals on one LAN& pass them to another. A repeater forwards all traffic from one LAN to the other. Repeaters are usually used to extend LAN cable distances or connect different media type. Repeaters connect LANs together at the lowest layer, the Physical layer, of the OSI model. This means that repeaters can only connect identical LANs, such as Ethernet/802.3 to Ethernet/802.3 or Token Ring to Token Ring. Two physical LANs connected by a repeater become one physical LAN. Because of this, the proper use and placement of repeaters is specified as part of LAN architecture’s cabling parameters.

- **HUB:** As its name implies, a hub is a center of activity. In more specific network terms, a hub, or concentrator, is a common wiring point for networks that are based around a star topology. Arcnet, 10base-T, and 10base-F, as well as many other proprietary network topologies, all rely on the use of hubs to connect different cable runs and to distribute data across the various segments of a network. Hubs basically act as a signal splitter. They take all of the signals they receive in through one port and redistribute it out through all ports. Some hubs actually regenerate weak signals before re-transmitting them. Other hubs retime the signal to provide true synchronous data communication between all ports. Hubs with multiple 10base-F connectors actually use mirrors to split the beam of light among the various ports.

- **PASSIVE HUBS:** Passive hubs, as the name suggests, are rather quiescent creatures. They do not do very much to enhance the performance of your LAN, nor do they do anything to assist you in troubleshooting faulty hardware or finding performance bottlenecks. They simply take all of the packets they receive on a single port and rebroadcast them across all ports--the simplest thing that a hub can do. Passive hubs commonly have one 10base-2 port in addition to the RJ-45 connectors that connect each LAN device. 10base-5 is 10Mbps Ethernet that is run over thick-coax. This 10base-2 connector can be used as network backbone. Other, more advanced passive hubs have AUI ports that can be connected to the transceiver to form a backbone that may be more advantageous. Most passive hubs are excellent entry-level devices that can be used as starting pointsinin the world of star topology Ethernet. Most eight-port passive hubs are cheaper.

- **ACTIVE HUBS:** Active hubs actually do something other than simply re-broadcasting data. Generally, they have all of the features of passive hubs, with the added bonus of actually watching the data being sent out. Active hubs take a larger role in Ethernet communications by implementing a technology called store & forward where the hubs actually look at the data they are transmitting before sending it. This is not to say that the hub prioritizes certain packets of data; it does, however, repair certain "damaged" packets and will retime the distribution of other packets. If a signal received by an active hub is weak but still readable, the active hub restores the signal to a stronger state before re-broadcasting it. This feature allows certain devices that are not operating within optimal parameters to still be used on your network. If a device is not broadcasting a signal strong enough to be seen by other devices on a network that uses passive hubs, the signal amplification provided by an active hub may allow that device to continue to function on your LAN. Additionally, some active hubs will report devices on your network that are not fully functional. In this way, active hubs also provide certain diagnostic capabilities for your network. Active hubs wil also retime and resynchronize certain packets when they are being transmitted. Certain cable runs may experience electromagnetic (EM) disturbances that prevent packets from reaching the hub or the device at the end of the cable run in timely fashion. In other situations, the packets may not reach the destination at all. Active hubs can compensate for packet loss by re-transmitting packets on individual ports as they are called for and re-timing packet delivery for slower, more error-prone connections. Of course, re-timing packet delivery slows down overall network performance for all devices connected to that particular hub,but sometimes that is preferable to data loss--especially since the re-timing can actually lower the number of collisions seen on LAN. If data does not have to be broadcast over and over again, the LAN is available for use for new requests more frequently. Again, it is important to point out that active hubs can help you diagnose bad cable runs by showing which port on your hub warrants the retransmission or retiming.

- **INTELLIGENT HUBS:** Intelligent hubs offer many advantages over passive and active hubs. Organizations looking to expand their networking capabilities so users can share resources more efficiently and function more quickly can benefit greatly from intelligent hubs. The technology behind intelligent hubs has only become available in recent years and many organizations may not have had the chance to benefit from them; nevertheless intelligent hubs are a proven technology that can deliver unparalleled performance for LAN. In addition to all of the features found in active hubs, incorporating intelligent hubs into your network infrastructure gives you the ability to manage your network from one central location. If a problem develops with any device on a network connected to an intelligent hub, it can easily identify, diagnose, and remedy the problem using the management information provided by each intelligent hub. This is a significant improvement over standard active hubs. Troubleshooting a large enterprise-scale network without a centralized management tool that can help you visualize your network infrastructure usually leaves you running from wiring closet to wiring closet trying to find poorly functioning devices.

5.11.3 NETWORK SERVICE TYPES

There are two types of Network Services one is known as Connectionless (or Datagram) and the other is Connection-Oriented (or Virtual Circuit).

- Connectionless Service

In connectionless service the end node transmits with every piece of data the address to which the data should be delivered. Every piece of data called packet is independently routed, so the network can't guarantee that all the packets will reach the destination in the transmitting order since the packets can be delivered through morethen one path.

- Connection-Oriented Service

In connection-oriented service the end node first informs the network that it wishes to start a conversation with another end node. The network sends its request to the destination that accepts or rejects the request. If the destination refuses, connection fails, otherwise connection is established. Connection-Oriented service usually has the following characteristics:

- The network guarantees that all packets will be delivered in order without loss or duplication of data.
- Only a single path is established for the call, and all the data follows that path.
- The network guarantees a minimal amount of bandwidth and this bandwidth is reserved for the duration of the call.
- If the network becomes overly utilized, future call requests are refused.

Following are few examples of applications, which need the connection-oriented service or connectionless service.

- File transfer and remote terminal protocols will not tolerate loss of data, and require the packets to remain ordered. This kind of application dictates a connection-oriented service.
- Electronic mail do not requires that packets remain ordered. Speech conveying systems can tolerate a modest percentage of lost packets. In packet voice, receiving delayed packets is actually useless. This kind of application dictates connectionless service.

5.11.4 TCP, SUBNETTING AND SUPERNETTING

In the mid-1990s, the Internet is a dramatically different network than when it was first established in the early 1980s. There is a direct relationship between the value of the Internet and the number of sites connected to the Internet. Over the past few years, the Internet has experienced two major scaling issues as it has struggled to provide continuous and uninterrupted growth. The eventual exhaustion of the IPv4 address space The ability to route traffic between the ever increasing number of networks that comprise the Internet The first problem is concerned with the eventual depletion of the IP address space.

TCP

TCP is a connection-oriented transport protocol that sends data as an unstructured stream of bytes. By using sequence numbers and acknowledgment messages, TCP can provide a sending node with delivery information about packets transmitted to a destination node. Where data has been lost in transit from source to destination, TCP can retransmit the data until either a timeout condition is reached or a successful delivery has been achieved. TCP can also recognize duplicate messages and will discard them appropriately. If the sending computer is transmitting too fast for the receiving computer, TCP can employ flow control mechanisms to slow data transfer. TCP can also communicate delivery information to the upper-layer protocols and applications it supports. Figure below shows the relationship of the Internet Protocol Suite to the OSI Reference Model.

SUBNETTING

In 1985, RFC 950 defined a standard procedure to support the subnetting, or division, of a single Class A, B, or C network number into smaller pieces. Subnetting was introduced to overcome some of the problems that parts of the Internet were beginning to experience with the classful two-level addressing hierarchy: Subnetting attacked the expanding routing table problem by ensuring that the subnet structure of a network is never visible outside of the organization's private network. The route from the Internet to any subnet of a given IP address is the same, no matter which subnet the destination host is on. This is because all subnets of a given network number use the same network-prefix but different subnet numbers. The routers within the private organization need to differentiate between the individual subnets, but as far as the Internet routers are concerned, all of the subnets in the organization are collected into a single routing table entry. This allows the local administrator to introduce arbitrary complexity into the private network without affecting the size of the Internet's routing tables. Subnetting overcame the registered number issue by assigning each organization one (or at most a few) network number(s) from the IPv4 address space. The organization was then free to assign a distinct subnetwork number for each of its internal networks. This allows the organization to deploy additional subnets without needing to obtain a new network number from the Internet.

The router accepts all traffic from the Internet addressed to network 130.5.0.0, and forwards traffic to the interior subnetworks based on the third octet of the classful address. The deployment of subnetting within the private network provides several benefits: The size of the global Internet routing table does not grow because the site administrator does not need to obtain additional address space and the routing advertisements for all of the subnets are combined into a single routing table entry. The local administrator has the flexibility to deploy additional subnets without obtaining a new network number from the Internet. Route flapping (i.e., the rapid changing of routes) within the private network does not affect the Internet routing table since Internet routers do not know about the reachability of the individual subnets - they just know about the reachability of the parent network number. Extended-Network-Prefix Internet routers use only the network-prefix of the destination address to route traffic to a subnetted environment. Routers within the subnetted environment use the extended-network- prefix to route traffic between the individual subnets. The extended-network-prefix is composed of the class full network prefix and the subnet-number. The extended-network-prefix has traditionally been identified by the subnet mask. For example, if you have the /16 address of 130.5.0.0 and you want to use the entire third octet to represent the subnet-number, you need to specify a subnet mask of 255.255.255.0. The bits in the subnet mask and the Internet address have a one-to-one correspondence. The bits of the subnet mask are set to 1 if the system examining the address should treat the corresponding bit in the IP address as part of the extended network- prefix. The bits in the mask are set to 0 if the system should treat the bit as part of the host-number.

The standards describing modern routing protocols often refer to the extended network-prefix- length rather than the subnet mask. The prefix length is equal to the number of contiguous one-bits in the traditional subnet mask. This means that specifying the network address 130.5.5.25 with a subnet mask of 255.255.255.0 can also be expressed as 130.5.5.25/24. The /<prefix-length> notation is more compact and easier to understand than writing out the mask in its traditional dotted-decimal format.

5.11.5 ROUTING PROTOCOLS

Hosts and Gateways are presented with datagram addressed to some host. Routing is the method by which the host or Gateway decides, where to send the datagram. It may be able to send the Datagram directly to the destination if it is connected to that n/w or gateway directly. If the destination is not directly reachable, then it will try to send the datagram to a gateway that is nearer to the destination. The goal of routing protocol is simple: It supplies the information that is needed to do the routing. There are many type of Routing protocols used, but for the NIB nodes following are the routing protocols recommended:

- RIP
- OSPF
- BGP4

ROUTING: INTERNAL (INTEREOR) AND EXTERNAL

Internal routing is the art of getting each router in your network to know how to get to every location (destination) in your network. You can do this simply, with static routes, or in a more complicated but robust way, with active internal routing protocol such a s RIP, RIPv2, OSPF and IS-IS. It’s obviously critical that any box inside your network know how to get (directly or indirectly) to any other box inside your network. Before your invite people to send data to your network, you’ve got to have a running and happy network to take the data. If your default route into one or more providers, external routing is not something you have in your network. But if you do want to “peer’ with someone – or to “multi-home” to multiple providers and have a little bit more control over where your data goes on the internet, you will be taking at least some external routes into your network and will do so with BGP.

5.11.6 X.25 PACKET SWITCHING

Switching technique is used for communication of information from one end to other end. These switches are hardware and /or software devices capable of building connections between one or more devices linked to the switch. There are three methods of switching the information – Circuit switching, Packet switching and Message switching. Circuit switching is designed for the real time applications (voice) and dedicated connection path between source and destination. Communication path is not fully utilized in circuit switching and not shareable. Communication of data and other application, which desired more throughputs, cannot be multiplexed to adjacent channel even they are available and not used to carry any information. Packet switching uses the virtual circuit as carrier to carry the packets. Packet switching was first theorized in the early 1960s by the pioneers of ARPANET, the first computer network. In the early 1970's there were many data communication networks (also known as Public Networks), which were owned by private companies, organizations and governments agencies. Since those public networks were quite different internally, and the interconnection of networks was growing very fast, there was a need for a common network interface protocol. In 1976, X.25 was recommended as the desired protocol by the International Consultative Committee for Telegraphy and Telephony (CCITT) called the International Telecommunication Union (ITU) since 1993. X.25 is a packet switched data network protocol which defines an international recommendation for the exchange of data as well as control information between a user device (host), called Data Terminal Equipment (DTE) and a network node, called Data Circuit Terminating Equipment (DCE).

5.11.6(a) <u>CONCEPT OF PACKET SWITCHING</u>

The packet switching concept was first discovered by Paul Baran in the early 1960's, and then independently a few years later by Donald Davies. Leonard Kleinrock conducted early research in the related field of message switching, and in 1969 helped build the ARPANET, the world's first packet switching network. Packet switching is the mode of communication in which the transmission bandwidth is dynamically allocated and permitting many users to share the same transmission line. A packet is a unit of data that is transmitted across a packet switched network. A packet-switched network is an interconnected set of networks that are joined by routers or switching routers. The concept of a packet-switched network is that any host connecting to the network can, in theory, send packets to any other hosts. The network is said to provide any-to-any service. The network typically consists of multiple paths to a destination that provide redundancy. Packets contain header information that includes a destination address. Routers in the network read this address and forward packets along the most appropriate path to that destination. There are two types of Packet switching - Connectionless packet switching and Connection oriented packet switching.

5.11.6(b) <u>CONCEPT OF X.25</u>

X.25 utilizes a Connection-Oriented service which insures that packets are transmitted in order. X.25 is a packet switched data network protocol which defines an international recommendation for the exchange of data as well as control information between a user device (host), called Data Terminal Equipment (DTE) and a network node, called Data Circuit Terminating Equipment (DCE). The user sees the network as a cloud through which each packet passes on its way to the receiving DTE. Although X.25 is an end-to-end protocol, the actual movement of packets through the network is invisible to the user.

5.11.8 <u>FRAME RELAY</u>

Frame relay is a virtual circuit Wide Area Network. Earlier virtual circuit switching network called X.25 was performing switching at the network layer. X.25 has several drawbacks

- X.25 has a low 64-Kbps data rate.

- X.25 has extensive flow and error control at DLL & Network layer. It was designed in 1970s when the transmission media were more prone to errors. Flow and error control at both layers
- Organization started their own private WAN by leasing T-1 or T-3 lines. A T-1line is designed for a user who wants to use the line at a consistent 1.544 Mbps. It is not suitable for bursty data, which requires bandwidth on demand.
- Frame Relay is a Wide area network with the following features:
- It operates at higher speed 1.544 mbps to 44.376 mbps.
- It operates at physical layer & data link layer.
- It allows bursty data.
- It allows a frame size of 9000 byte, which can accommodate all LAN frame sizes.
- It is less expensive than other traditional WANs.
- It has error detection at DLL only. There is no flow control or error control. If a frame is damaged it is silently dropped.
- It is designed for those protocols that have flow & error control at the higher layers.
- Architecture
- Frame relay provides SVC & PVC.
- Frame Relay does not provide flow or error control. they must be provided by the upper-layer protocols.

CHAPTER 6

INTERNET

6.1 OVERVIEW OF INTERNET

The Internet is a global computer network made up of smaller computer networks; it has been called a "Network of Networks."

These smaller networks include:

Local Area Networks (like networked offices or computer labs, and campus-wide networks) _ Wide Area Networks (like city-wide networks)

_ State and Regional Networks (including regional service providers and others) _ National and International Networks

There is no one inventor of the Internet. The Internet was created in the 1960s as a huge network linking big university and government computers. The science behind the Internet was invented during the Cold War, when the United States was in competition against Russia for weapons and technology. So the Internet is actually pretty old—around forty years. Much of Internet's initial development was supported by American governmental research and network development (beginning with the American military's ARPANET in 1969)

In fact, email has been around since 1972! In 1989 that Tim Berners-Lee, a scientist at the European Laboratory for Particle Physics in Geneva, proposed the World Wide Web. Now Internet Service Providers (ISPs) offer Internet access to their clients, at costs ranging from Rs 150/- per 6 months to hundreds of rupees per year, depending on the types of service they offer.

6.1.1 <u>What are the uses of the Internet?</u>

There are three fundamental uses of the Internet:
Communication
Information Retrieval
Presentation of Information

- **Communication:** The Internet is used both for one-to-one communications (email and real-time "chat" programs) and one-to-many.
- **Information Retrieval:** The Internet allows access to public domain information, bibliographic databases, libraries, and entertainment services, as well as to proprietary information services .
- **Presentation of Information:** Any organization connected to the Internet can provide access to its own in-house information (library catalogs, faculty information, etc.) to millions of people world-wide. Individuals can also develop and provide their own information packages via their own home pages.

6.1.2 <u>Internet Addresses</u>

Every computer, file of information, and person on the Internet is identified by a unique "address."

<u>Computer Addresses</u>

Computer addresses are made up of three parts (or, in some cases, two parts), separated by "dots," like this:
computer-name, institution, domain
The computer name is a name given locally to identify a particular computer; it is, in some cases, omitted from the address. The institution name is the name (or an abbreviation) of the name of the school, company, or other institution housing the computer. The domain name specifies either the type or the geographic location of the computer.

6.1.3 <u>Domain Names</u>

There are several possible "domain" names, including some that identify the type of institution, and some that identify a geographical location. They include:
edu educational institution
com commercial and profitable organizations
org non-profitable organizations
net Internet infrastructure and service providers
gov governmental agency/department
mil American military agency

int International organizations.....

6.1.4 Personal Addresses

A person's address (or their email address) places the user's "username" (or "login") and the symbol "@" before the computer address. For example, a user whose username is "sundar", who is accessing email from the "bsnl" server of India, would have the following address:
sundar@bsnl.in

6.1.5 Uniform Resource Locators (URL)

Sources of information that are on the World Wide Web or FTP server are identified by an extended address called a "Uniform Resource Locator" (URL). Here is a typical URL: http://www.win.org/workshops/internet.shtml

The first part of the URL ("http://") identifies the type of information or protocol (in this case, it is a hypertext document, available from a HyperText Transport Protocol (http) server on the World Wide Web). The middle part ("www.win.org") is the basic address, as described above. The final part ("/workshops/internet.shtml") identifies the directories within which the document resides ("workshops"), as well as the exact name of the document ("internet.shtml").

6.2 Internet Services

"Internet services" serve more sophisticated and multi-purpose purposes, and increasingly make the Internet a truly useful information resource.

- **EMAIL:**It is the Internet's version of the postal service. Using the Internet, it provides the ability to send a message, reply to a message, send a file created in another program and/or even send the same message to a group of people. Some **benefits** of Email are:

  Speed: A message can be sent from Chennai to Australia in a matter of seconds. ·

  Cost: Emails are cheap. You are usually charged only for the telephone call time (local call rate) for sending the message into the Internet, and not the cost associated with transferring the message across the Internet.

  Flexibility: It is easy to send duplicates of your messages to other people or groups for the cost of a single message.

  Record keeping: Messages sent and received can be easily stored for future reference.

  In order to use Email, you will need Internet access arranged through an Internet Service Provider (ISP), who will allocate you one or a number of Email accounts. To be able to retrieve and send mail from these addresses, a user will need what is known as Email client software and your ISP usually provides this although nowadays most computers come with it pre-installed.

  Mail Lists: These use email to support discussion groups on a wide range of specific subjects. Once you are becoming a subscriber of a mailing list, you will receive lot of emails related to the subject covered by the mailing list.

- **FTP :**FTP was the original Internet mechanism for the storage and retrieval of information. There are still many FTP Sites around the Internet, although many of them have been melded into the World Wide Web. In computer science, FTP stands for "File Transfer Protocol," which is a way of transferring files between computers. A file can be anything -- a spreadsheet, a word document, a song, or a picture. When someone says "Please FTP me that file," for instance, that means "Please transfer that file from your computer to mine." To FTP, you usually need to download a special program, or application. You also usually need a password to be able to access or send information to someone else's computer.
- **Gopher :**Gopher was developed at the University of Minnesota, primarily to support its own Campus Wide Information Server (CWIS). It provides access to information available either locally or elsewhere on the Internet by means of a simple series of uniformly designed menus.
- **Instant Messaging (IM)**:IM is a way for you to communicate instantly with your friends over the Internet. That might not sound so different to email. Have you ever noticed how cumbersome it is to have a brief conversation via email? You have to click Reply to each message, then find the right spot in the message to type something new, then send it. Then you have to wait for the next message to arrive! IM lets you to have a conversation almost as naturally as on the phone or face to face, by typing messages into a window shared between you and your friend's screens.

  Another difference between IM and email is that with IM you can see your friends presence, that is, whether they are actually on-line at the same time as you. This lets you send messages truly instantly, instead of sending off a mail and having to wait for your friend to check their mailbox. An IM message pops up on the other person's screen as soon as you send it. Of course, if you'd rather not be interrupted, you can change your own presence so others will know not to disturb you. There are lots of other fun and useful IM features you can explore, like group chats, file transfers, voice calls, video conferencing and emoticons that reflect your mood.
- **IRC**:IRC stands for "Internet Relay Chat". It has been used in many countries around the world. IRC is a multi-user chat system, where people meet on "channels" (rooms, virtual places, usually with a certain topic of conversation) to talk in groups, or privately. There is no restriction to the number of people that can participate in a given discussion, or the number of channels that can be formed on IRC.
- **Newsgroups:**The Internet has a place where we can gather, question, and discuss our experiences within a wide variety of topics. It's called Usenet News. Some users also call it Net News. Think of Usenet News as a giant, worldwide bulletin board. Anyone can freely post something on this bulletin board. Everyone else can read the posted items and add their own items. These voluntary contributions and free exchange of information are the foundation of the Internet. Usenet News allows people on the Internet to share their opinions and experiences, openly and freely, on a level playing field. No one has priority or seniority over anyone else. Usenet News gives everyone an equal opportunity to participate in the discussions. When you send an e-mail message, the only people who can read it are the recipients (for the most part). When you post an article on

Usenet News, every person on the Internet could read it and respond to it. Not that they ever would, but they could. That's a lot of people and a lot of opinions, and only a few of them come from true experience. There are tens of thousands of newsgroups. Some of them are applicable to a global audience; others are more applicable to a country, city, or organization. Most of the newsgroups are available to everyone on the Internet. However, some of the newsgroups have a limited audience.

- **Voice over IP:** Voice over IP (Voice over Internet Protocol or "VoIP") technology converts voice calls from analog to digital to be sent over digital data networks. In Voice over IP, or VoIP, voice, data, and video all travel along the network.
- **World Wide Web (WWW):** The newest information application on the Internet, the WWW provides standardized access to Gopher, FTP, Telnet and more by means of home pages designed either by institutions or by individuals. By means of the HyperText Markup Language (HTML), it allows users to "point" at highlighted terms following "links" to whatever information interests them. It is a multimedia environment, allowing Internet users access to audio and video materials. There are a number of client software packages (or browsers), including Lynx (a textonly browser), Netscape, and Microsoft's Internet Explorer, (which are multimedia browsers).

6.3 TYPES OF INTERNET CONNECTIONS

The options for providing user connectivity to the Internet are given below:

1. Terminal Dialup/Modem (Shell connection)

- Most common option
- User requirements limited to modem and communications software
- Text-only access
- Shell accounts were more popular before the advent of the Web. A shell account lets you use your computer much as if it were a virtual console associated with a remote computer. You can type commands, which are interpreted by the remote computer, and view the resulting output on your computer. Although a few web browsers, such as Lynx, can operate via a shell account, they don’t generally support the highly graphical, multimedia pages which web surfers have come to expect.

2. SLIP (Serial Line Internet Protocol)

- Computer is treated as though it were directly connected for the period it is online
- Utilizes telephone lines
- User must have modem, TCP software, SLIP software, & software for Internet applications
- Multimedia access

3. PPP (Point-to-Point Protocol)

- Computer is treated as though it were directly connected for the period it is online
- Utilizes telephone lines

- User must have modem, TCP software, PPP software, & software for Internet applications
- Multimedia access
- While your computer is connected to the Internet, you can use it to surf the Web with your favorite browser. If your ISP allows, you can even run a web server, providing pages that can be viewed by others around the world.

4. <u>ISDN (Integrated Services Digital Network)</u>

- Most often used to connect remote telecommuters to office LANs
- Requires ISDN phone line access
- Faster than analog terminal dialup/modem service
- User must have ISDN phone line, ISDN card, communications software, TCP software & SLIP or PPP software multimedia connectivity

5. <u>DIAS</u>

The DIAS offers a wire-line solution for high speed symmetrical Internet access on the existing telephone lines. It provides an "always on" internet access that is permanently available at customer's premises. DIAS combines voice and internet data packets on a single twisted pair wire at subscriber premises that means you can use telephone and surf internet at the same time.

6. <u>Cable Modem</u>

The term “Cable Modem” is quite new and refers to a modem that operates over the ordinary cable TV network cables. Basically you just connect the Cable Modem to the TV outlet for your cable TV, and the cable TV operator connects a Cable Modem Termination System (CMTS) in his end (the Head-End).

Actually the term “Cable Modem” is a bit misleading, as a Cable Modem works more like a Local Area Network (LAN) interface than as a modem.

In a cable TV system, signals from the various channels are each given a 6-MHz slice of the cable’s available bandwidth and then sent down the cable to your house. When a cable company offers Internet access over the cable, Internet information can use the same cables because the cable modem system puts downstream data – data sent from the Internet to an individual computer – into a 6-MHz channel. On the cable, the data looks just like a TV channel. So Internet downstream data takes up the same amount of cable space as any single channel of programming. Upstream data – information sent from an individual back to the Internet – requires even less of the cable’s bandwidth, just 2 MHz, since the assumption is that most people download far more information than they upload.

Putting both upstream and downstream data on the cable television system requires two types of equipment: a cable modem on the customer end and a cable modem termination system (CMTS) at the cable provider’s end. Between these two types of equipment, all the computer networking, security and management of Internet access over cable television is put into place.

7. <u>Digital Subscriber Line (DSL) connection.</u>

DSL is a very high-speed connection that uses the same wires as a regular telephone line.

Here are some advantages of DSL:

1. You can leave your Internet connection open and still use the phone line for voice calls.
2. The speed is much higher than a regular modem
3. DSL doesn't necessarily require new wiring; it can use the phone line you already have.
4. The company that offers DSL (e.g. BSNL) will usually provide the modem as part of the installation.

But there are disadvantages:

1. A DSL connection works better when you are closer to the provider's central office.
2. The service is not available everywhere.

Other types of DSL include:

1. **Asymmetric DSL** (ADSL) line – The connection is faster for receiving data than it is for sending data over the Internet
2. **Very high bit-rate DSL (VDSL)** – This is a fast connection, but works only over a short distance.
3. **Symmetric DSL (SDSL)** – This connection, used mainly by small businesses, doesn't allow you to use the phone at the same time, but the speed of receiving and sending data is the same.
4. **Rate-adaptive DSL (RADSL)** – This is a variation of ADSL, but the modem can adjust the speed of the connection depending on the length and quality of the line.

8. Direct Connection (Leased circuit)

Most often used to connect sites within a specific organization; such as a university or business requires owning or leasing of cable (from 64 kbps to 45 Mb) users typically connected via Ethernet LANs multimedia connectivity at its fastest.

9. Satellite connections

This connection allows you to download Internet files via a satellite connection. This is an efficient method for receiving large Web graphics and other items, but you still need a modem connection for other features. You must purchase the connection hardware as well as subscribe to the service.

10. Wireless connections

Pagers, cellular phones and personal digital assistants (PDAs) now allow varying levels of Internet access, from notification of E-mail to limited Web connections. Many of these services remain in the experimental stage. The PPP connection is called as TCP/IP connection or PSTN dial-up connection. ISDN connection is called as ISDN dial-up connection. Cable Modem, DSL and Direct Connection are always-on connection. The words "connection" and "account " related to Internet are interchangeable.

6.4 Comparisons of Internet accounts

You can compare the two types of Internet accounts - shell and PPP - with two kinds of postal service. Imagine that no mail carrier actually comes to your home to pick and deliver mail.

Instead, every time you want to conduct postal business, you go to the post office. This resembles a shell account: The computer that connects you to the Internet is remote, and every time you want to do something on the Internet you must open a terminal, or telnet, session to that computer. PPP, on the other hand, is like home delivery: The Internet comes right to your doorstep, and your computer is literally placed on the Internet by the machine at our ISP that you connect to. Under Microsoft Windows, you use hyper terminal to access a shell account and Dial- Up Networking to access a PPP account. Under Linux, you can choose from among several programs that let you access a shell account. The most commonly used programs are minicom and seyon. To access a PPP account under Linux, you use the PPP daemon, pppd.

If you are one of the first users to connect to the Internet through a particular cable channel by using Cable Modem Internet connection, then you may have nearly the entire bandwidth of the channel available for your use. As new users, especially heavy-access users, are connected to the channel, you will have to share that bandwidth, and may see your performance degrade as a result. It is possible that, in times of heavy usage with many connected users, performance will be far below the theoretical maximums. The good news is that this particular performance issue can be resolved by the cable company adding a new channel and splitting the base of users. Another benefit of the Cable Modem for Internet access is that, unlike ADSL, its performance doesn't depend on distance from the central cable office.

ADSL is a **distance-sensitive technology**: As the connection's length increases, the signal quality decreases and the connection speed goes down. The limit for ADSL service is **18,000 feet** (5,460 meters), though for speed and quality of service reasons many ADSL providers place a lower limit on the distances for the service. At the extremes of the distance limits, ADSL customers may see speeds far below the promised maximums, while customers nearer the central office have faster connections and may see extremely high speeds in the future.

6.5 Choosing an Internet Connection

(Modem, ISDN, Cable, DSL - ASDL/SDSL)

As the Internet becomes increasingly popular with every day that passes, it is now considered as one of the best ways to do business (e-commerce), network (by email), and build partnerships (on-line collaboration). It is arguably, some would say, the most efficient way of gathering information for a wide range of business uses and to interact with customers. One of the main issues today is what is the best way to connect to and use the Internet to its full potential with a view to speed and reliability?

Unfortunately, because of the poor quality of the existing telephone network that connects us to the Internet, the speed at which information (web pages, images etc) appears on your screen is slow compared to the latest technology available. Ultimately, DSL (see below) will be the solution that will provide us all with a connection up to ten times faster than the speed at which information arrives to you with a regular modem.

As new technology becomes available almost every week, the awareness of the difference between the performance (speed), costs and availability is still unknown to many people and consequently we face problems deciding which connection is best for our business needs.

(i) PC Modem- up to 56kbps The PC Modem is the standard way of connecting to the Internet but is now the slowest.
The fastest type of standard modem is 56kbps, these are included as standard with all new PC's; but if you do not have one they can be bought from around £15-20 upwards. If you are currently using a modem below 56k (which is unlikely) then the difference in speed will be very noticeable. There is nothing negative about using standard PC modems but the speed may be a crucial factor if time is valuable to your business or I downloading large or numerous files (images, emails, etc) is what you require.

(ii) ISDN (Integrated Service Digital Network) - 64/128kbps ISDN provides a solution by offering two high-speed lines capable of running at 64kbps each through your existing phone network. The advantage of this is that each line can be connected to a different source (e.g. two computers, a computer and a telephone/fax or two telephones). Another feature that may interest you is that the lines can be used simultaneously from a single computer giving a speed of 128kbps. This would be useful should you need the extra speed to work quicker over the Internet at a specific time, or for downloading large images and files.
This service requires you to remove your existing modem (if you have one) and replace it with an ISDN card that can be found from most large PC stores. ISDN appears expensive in comparison to ADSL/broadband, but the two phone lines that come with it can be invaluable to a small business. If ADSL is not available in your area, then ISDN offers an effective solution.

(iii) Cable Modem- up to 600kbps
Cable offers greater speeds but has the initial problem of availability. Just like Cable TV, you can only receive the service if you live within a cable operator's franchise area. Should you find that you are one of the 'chosen few' you may consider this over ADSL (see below) because of the cheaper operating costs; although you should check carefully because prices are always changing. In cable Modem connection, speeds of up to 2Mbps can be achieved in the future.
In order to use cable you will need two things: A cable modem and a Network Interface Card (Sometimes referred to as NIC's). You do have to bear in mind the future and consider the following: Once all subscribers in your area have all been connected to the Cable Modem connection, the speed of the service will run at slower rates (kbps). This is because the amount of information that the Cable can carry at one time is shared with all those connected to it. However, you could also consider that there may be further advances in the technology to change this.

(iv) ADSL - Over 256 kbps
This connection improves the speed at which you can download/upload dramatically compared to the standard PC modem. ADSL uses your existing phone line but gives you he added advantage of being able to use the phone/fax at the same time as being connected to the

Internet: the connection time to the Internet is instant as ADSL is "always on" meaning that you can start surfing the net as soon as you turn on your computer.

Using such a connection will involve extra hardware such as a box that fits to your wall that you plug a USB modem (also needed) into which will then connect to your computer. When you connect to ADSL you also get a new phone line, which can be beneficial to many small businesses. The use of this line does not affect the ADSL connection either. Broadband is available in all cities. However, you should check availability in your area before discounting ISDN or 56k. DSL gives faster downloading speeds (receiving) than uploading speeds (sending).

(v) **SDSL**- upto 2Mbps

This service was released in early 2004 -- aimed at businesses -- allowing users to enjoy the same uploading (sending) speeds as it was capable of downloading (receiving). This service is beneficial to businesses that frequently send large files via the internet: the current connection may be causing the network to suffer huge strain when transporting such files.

Subscribers can sign up for speeds varying from 256kbps to 2Mbps, depending on preference. This service is much more expensive than ADSL broadband and should only be considered if there is an instant need for the service.

6.6 MODEM

6.6.1 MODEM fundamental

Acronym for *MODulator / DEModulator* which describes the method used to convert digital data used by computers into analog signals used by the phones and then back into digital data once received by the other computer. The above pictures help represent a digital signal and an analog signal. All computer data is stored and transmitted within the computer in digital format 1s and 0s. In order for this data to be transmitted over analog phone lines the data must be transmitted into an analog signal which is the noise you hear when connecting to another computer. Once the other computer receives this signal it will translate the signal back into its original digital format. Typical modems are referred to as an *asynchronous* device. Meaning that the device transmits data in a intermittent stream of small packets. Once received the receiving system then takes the data in the packets and reassembles it into a form the computer can use.

6.6.2 Proxy Servers

A proxy is a device which allows connection to the Internet. It sits between workstations on a network and the Internet, allowing for a secure connection, allowing only certain ports or protocols to remain open. When a client requests a page, the request is sent to the proxy server, which relays it to the site. When the request is received from the site, it is forwarded back to the user. Proxy servers can be used to log internet use and block access to prohibited sites. Some home networks, corporate intranets, and Internet Service Providers (ISPs) use **proxy servers** (also known as **proxies**). Proxy servers act as a "middleman" or broker between the two ends of a client/server network connection. Proxy servers work with Web browsers and servers, or other applications, by supporting underlying network protocols like HTTP.

Key Features of Proxy Servers

Proxy servers provide three main functions:

1. Firewalling and filtering
2. Connection sharing
3. Caching

The features of proxy servers are especially important on larger networks like corporate intranets and ISP networks. The more users on a LAN and the more critical the need for data privacy, the greater the need for proxy server functionality.

6.7 E mail

6.7.1 What is email?

Email is the method of electronically sending messages from one computer to another. You can send or receive personal and business-related messages with attachments, such as pictures or formatted documents. You can even send music and computer programs. Email is the one of the popular services offered by Internet. It is the replacement of Postal mail. Postal mail is known as Snail Mail because it is very slow. Email is cheaper and faster than Postal Mail, less intrusive than a phone call, less hassle than a FAX. Because of its speed and broadcasting ability, Email is fundamentally different from paper-based communication. Using email, differences in location and time zone are less of an obstacle to communication.

Through Email you can exchange:

- Ideas,
- Agendas,
- Memos,
- Documents and
- Attachments

Just as a letter makes stops at different postal stations along its way, email passes from one computer, known as a mail server, to another as it travels over the Internet. Once it arrives at the destination mail server, it's stored in an electronic mailbox until the recipient retrieves it. It is Store and Forward System. Copies can be sent automatically to names on a distribution list. Sends delivery confirmation message to sender when the recipient opens message. This whole process can take seconds, allowing you to quickly communicate with people around the world at any time of the day or night. To receive email, you must have an account on a mail server. This is similar to having an address where you receive letters. One advantage over regular mail is that you can retrieve your email from any location. Once you connect to your mail server, you download your messages to your computer.

6.7.2 Types of Email

There are two basic types of email accounts: paid and free.

· A paid account includes a mailbox and access to the Internet. You pay an Internet Service Provider (ISP) like BSNL, AOL for this service.

· A free account includes only a mailbox. Companies like Yahoo and Hotmail provide free mailboxes; in return, you will see advertising. To use a free mailbox, you have to be able to get on the Internet. This type of mail is called as **web-mail**.

Accessing the two types of Email Accounts

If you want to send an Email you should have 2 things.

• An Email address.

• Email Programme at the client side.

To access your email account, you must be on the Internet. You can send and receive email messages through an email program like Outlook Express or through a browser like Internet Explorer. If you go through a browser, you are using ***web-mail***. Most email accounts can be accessed either way. 72

· If you access your mail through an email program, the messages are downloaded to your computer and removed from the company's mail server.

· If you access your mail through a browser (web-mail), the messages remain on the company's mail server until you delete them. Most web-mail accounts have a maximum storage space. When your mailbox is completely filled, you will not be able to receive any additional messages. You must regularly delete some messages *and* empty the trash in order to free up storage space.

6.8 DNS

While DNS is one of the least necessary technologies that make up the Internet as we know it, it is also true that the Internet would never have become as popular as it is today if DNS did not exist. Though this may sound like a bit of a contradiction, it is true, nonetheless. DNS stands for two things: Domain Name Service (or Domain Name System) and Domain Name Servers. One acronym defines the protocol; the other defines the machines that provide the service. The job that DNS performs is very simple: it takes the IP addresses that computers connected to the Internet use to communicate with each other and it maps them to hostnames. Sounds pretty simple, doesn't it? Well, it is. But just because it's simple doesn't make it any less important. Human beings tend to have a difficult time remembering long strings of seemingly arbitrary numbers. The way that our brains work, it's difficult to make information like that stick. And that is where DNS comes in. It allows us to substitute words or phrases for those strings of numbers. Words are a lot easier for people to remember than numbers, especially when they can be tied to a specific idea that is linked to the website.

But how does DNS work? What makes it operate? How did it start?

6.8.1 Web site address

Before we get into DNS, let's start off with breaking down a web address. It essentially gives where the web page is, and how you need to talk to it. Lets use the example of:

http://www.bsnl.co.in/pages/cellone.htm The first part is "http://", and that tells your PC what protocol (what language so to speak) to use talking with this site. In this case, you are using HTTP (HyperText Transfer Protocol). Another very common one for web designers to use is "ftp://" or File Transfer Protocol. You would use it to connect to your web server to put the web pages you created onto the server. You also see "https://" quite commonly. This simply means that the connection between you and the web server is secure (meaning the information being sent back and forth is encrypted). You should see "https://" when you are checking out, especially when they are entering credit card information. The next part,"www.bsnl.co.in" is called the *Domain Name*. The "www" used to be more significant than it is today. Today, the "www" is, for the most part, assumed and you can get to the same page regardless of whether or not you type in "www" your browser. The part "/pages/cellone.htm" tells the web server to look in the directory called "pages" and send the file called "cellone.htm" to your browser. It is just like the directories on your PC. The “in” of the Domain Name “www.bsnl.co.in” is called as Top Level Domain (TLD). It is the right extreme portion of the domain name. For example the TLD of www.yahoo.com is com.

6.8.2 <u>IP address</u>

Before we get into DNS, we need to explain what an IP address is. Every PC and server has an IP address on the Internet. It has the format of 4 numbers, separated by periods, and looks like "61.1.137.84". Each number should be between 0 and 255. Think of it as your phone number on the Internet, it must be unique. It would be bad to have 2 different houses with the same phone number, and it would be bad to have 2 different machines (more properly known as hosts) that have the same IP address on the Internet.

6.8.3 <u>Why DNS needed?</u>

For most people, it is much easier to remember "www.bsnl.co.in" than it is to remember "61.1.137.84". When you enter a URL into your browser, you usually use the easy to remember name. How does your PC know where to find "www.bsnl.co.in? Remember that each machine has a IP address? There is a way to translate from the easy to remember domain name, and the hard to remember IP address. Enter DNS. DNS is an acronym for "Domain Name Service". Its whole purpose in life is to translate between the friendly "www.bsnl.co.in" and the not-so-friendly 61.1.137.84. It handles this translation for web sites, email, FTP servers, database servers, or any machine within a domain name. Let's dig into the process of how that works. DNS means Domain Name Service. It is actually a service that can keep large number of machines’ IP addresses for huge network communication. Now the question arises why is this needed. Let’s understand this with the help of an illustration. ***Example:*** Let’s say rose1, rose2, rose3, rose4, and rose5 are the 5 machines in a network, then for communication between each machine, each machine’s /etc/hosts in Unix (or hosts.txt in Windows) file should have all the five entries of the machine name. Within this small network there would be no problem if you add another machine say rose6 inthe network. But for this too, the network administrator has to go to each machine, add the rose6 in /etc/hosts file and then comeback to the new comer rose6 machine and add all the ther entries (rose1...rose5) including its own name also in /etc/hosts (or hosts.txt) file. But what if the network is setup with say 60 machines and a 61st machine has to be added? Then administrator will have to go to each machine again and write the new machine’s name at /etc/hosts/ (or hosts.txt) file and again comeback and write all the 60 machines name on the 61st machine’s etc/hosts file which is a tedious and time taking job .

Thus, it is better to keep a centralized server, where all the IP addresses will stay and if a new one does enter into the network then the change will have to be done at the server and not on the client's machine.

6.8.4 The Origin of DNS

Like almost everything else originally associated with the Internet, DNS traces its origins to ARPANET. Alphabetic hostnames were introduced shortly after its inception as a means of allowing users greater functionality, since the numeric addresses proved difficult to remember.
Originally, every site connected to ARPANET maintained a file called 'HOSTS.TXT which contained the mapping information for all of the numeric addresses used there. That information was shared through ARPANET. Unfortunately, there were many problems that arose from that setup. Errors were commonplace and it was inefficient to make changes considering they needed to be made on each and every copy of the HOSTS.TXT file.
By November of 1983, a plan was laid out in RFCs 881, 882, and 883, also known as 'The Domain Names Plan and Schedule,' 'Domain Names -- Concepts And Facilities,' and 'Domain Names -- Implementation And Specification.' These three RFCs defined what has developed into DNS as we know it today. Surprisingly, not a whole lot has changed since that time
.

6.8.5 Understanding DNS

DNS organizes groups of computers into *domains*. These domains are organized into a hierarchical structure, which can be defined on an Internet-wide basis for public networks or on an enterprise-wide basis for private networks (also known as intranets and extranets). The various levels within the hierarchy identify individual computers
organizational domains, and top-level domains. For the fully qualified host name omega.microsoft.com, *omega* represents the host name for an individual computer, *microsoft* is the organizational domain, and *com* is the top-level domain. Top-level domains are at the root of the DNS hierarchy and are therefore also called *root domains*. These domains are organized geographically, by organization type, and by function. Normal domains, such as microsoft.com, are also referred to as *parent domains*. They're called parent domains because they're the parents of an organizational structure. Parent domains can be divided into sub-domains, which can be used for groups or departments within an organization. There are three types of TLDs. They are:
1. Generic or Organization based TLD (e.g com, edu, gov, mil, net, org, int, aero, museum, etc)
2. Geographical or country based TLD (e.g. in, us, au, etc). These TLDs are having
2 letters.
3. Inverse (e.g. arpa). This TLD is to find domain name from IP address. Sub-domains are often referred to as *child domains*. For example, the fully qualified domain name (FQDN) for a computer within a human resources group could be designated as jacob.hr.microsoft.com. Here, jacob is the host name, *hr* is the child domain, and *microsoft.com* is the parent domain.
Domain Name System (DNS) is an Internet service that translates domain names into IP addresses. DNS provides a database that stores a list of host names and their corresponding IP address. This process is called name resolution or mapping. Name resolution occurs when a program on a local computer requests a remote host for resources. The local computer sends

the host name of the server as part of the request. By using the host name as an index, the DNS database is searched to resolve the IP address of the host.

6.8.6 Domain Name Space Hierarchy

DNS is organized in a hierarchical tree structure. Each branch in the tree represents a domain and each sub-branch in the tree represents a sub-domain. DNS consists of multiple levels of domains. The domains are identified based on the level at which they are placed in the hierarchical tree structure. The various levels of domains in a domain name space hierarchy are:

· Domain root: This is the node at the highest point of the hierarchical DNS tree. In a DNS domain name, a trailing period represents the domain root tree (.). It is also shown as two empty quotation marks representing a null value.

· Top-level domain: This is the next level in the hierarchical tree structure. It represents the region or the type of organization to which a domain belongs. A top-level domain name contains two or three letters such as com, edu, and mil.

· Second-level domain: This is a domain name registered under a specific top-level domain, such as organizations based on type and geographical locations. The Second-level domain names have names with variable length. For example, example.com is a second-level domain name.

· Sub domain: This is a domain created under a second-level domain. Organizations need to create additional domains to represent organizational hierarchy and various functional groups. A second-level domain also contains a name with variable length.

· Host or resource: A host or resource computer is the last in the DNS hierarchy. It helps find the IP address of the computer based on its host name.

CHAPTER 7

OVERVIEW OF WLL & CDMA

7.1 CDMA system description

Wireless communications can be traced back to 1898 when the first wireless telegram was produced. The history of wireless communication service can be traced back to the 1920s when police car wireless communication was first put in use in the Detroit Public Security System of the US. The wireless communication system put into real commercial services can be traced to the 1940s when Bell laboratories of the US conducted commercial mobile wireless communication systems tests and the 1960s when a new type of mobile telephone system called for modified mobile telephone services. However, as technologies were relatively underdeveloped in those days, mobile communications did not find extensive developments. Since the last 20 years, the largescale integrated circuit and computer technologies have paved the way to the rapid development of the commercial applications of mobile communications. In fact, the wireless mobile communication technologies have basically been developed based on exploring new mobile communication frequency bands, reasonable use of frequency resources and minimization, portability and multifunction of mobile stations. Ever since the “cellular” theory was put forward in the 1970s, cellular mobile ommunications have found extensive applications. Theoretically, the principle of a cellular system is the repeated use of wireless channels, namely frequency-division multiplexing. A service area is divided into abstract hexagonal cellular cells, and two non-adjacent cells can use the same frequency, with the sizes of cells depending on the user density. This greatly improves the frequency spectrum utilization, and thus effectively improves the system capacity. In addition, owing to the development of microelectronic technology, computer technology, communication network technology, signal coding technology and digital signal processing technology, mobile communications have made quite great progress in various aspects such as switching, signaling network mechanism and wireless modulation coding technology etc., and thus the cellular mobile communication system has come through changes from analog to digital, from FDMA to TDMA and CDMA, which represent the evolution from the first generation cellular mobile communication system to the third generation cellular mobile communication system. The following paragraphs will first make a simple retrospect of these three generations of cellular mobile communication systems, then describe related system technology principles and features, and, lastly, discuss the prospect of the third generation cellular mobile communication system.

7.2 History of wireless cellular mobile communications

7.2.1 First generation cellular mobile communication system

In the late 1970s, the first generation cellular mobile communication system characterized by frequency division multiple access (FDMA) and analog frequency module (FM) came into being, pioneering the commercialization of cellular mobile communication systems. The major modes in this phase include TACS of the UK, AMPS of the US and NMT of north Europe. This phase featured defects such as low frequency utilization, small system capacity, no united international standard, very complicated equipment, high cost, requirement of certain protection bands, no effective anti-interference and anti-attenuation measures, poor voice quality, low security etc., as well as limited number of subscribers and incapability of non-voice services and digital communication services. With the development of services, the first generation cellular mobile communication system became unable to satisfy the market requirement. Furthermore, in the transmission system, the voice transmission was implemented in the analog mode, while signaling gateways adopted the digital mode, resulting in ineffective control of network management.

7.2.2 The second generation cellular mobile communication system

In mid 1980s, the second-generation cellular mobile communication system featuring TDMA, CDMA and digital modulation (QPSK, p/4-QPSK and GMSK) appeared. The major modes in this phase include GSM of Europe, DAMPS of the US and the CDMA system put forward by Qualcomm of the US. At that time, since some critical techniques in the CDMA system were not properly solved, the development of the CDMA technology was relatively slow. However, since

the GSM system adopted the TDMA technology, which was mature at that time, the utilization of frequency spectrum was increased, and the shortcomings of the analog system were well solved. Therefore it gained wide support from telecom operators and equipment manufacturers of the world, and the globally united GSM system standard was made up. However, for the very reason that this kind system used the TDMA mode, the anti-interference and ant attenuation capability of this kind of system was still unsatisfactory, certain protection time slots were required, and the system capacity was unable to meet the growing requirements of the users. Besides, the design of this kind of system is very complicated, the frequency utilization was not high, and the hard handoff mode was adopted for intercell handoff, which tended to cause call drops, and was unable to satisfy the users' growing fast data transmission and broadband video multimedia service requirements. evertheless, since the CDMA technology involves multiple critical technologies, it has many unique performances, which largely increases the system capacity (analyses show that its system capacity is ten times that of FDMA, and over four times that of TDMA), and it does not require protection bands and timeslots. The CDMA technology itself has provided the basis for the realization of soft handoff and software capacity. Furthermore, the frequency classification in the CDMA system has become relatively simpler, and its anti-interference and anti-attenuation capabilities are also better the former two ones. In a word, the overall performances of the CDMA cellular mobile communication system are all superior to those of all the other currently existing cellular mobile communication systems.
It is because CDMA has the all the above-mentioned merits, and it is more because Qualcomm has solved some of the critical technologies, that the CDMA has attracted extensive attention from the world's telecom businesses, which makes all believe that CDMA is the most prospective communication technology in the future wireless technology development, thus making it an outstanding one among the digital cellular mobile communication systems. The development of CDMA has been a progressive process, and the commercial products on the current market are basically all based on the IS-95A narrow-band N-CDMA technology. It is presently the development direction of CDMA to realize low-cost, high-quality, inter-connective and inter-working, and IPsupporting and data-supporting services and wireless intelligent network (WIN) services, aiming at providing users with convenient and effective communication services, on the basis on the existing narrow-band N-CDMA. From the point of view of the communication technologies and people's requirements, the future wireless communication world will be a broadband, comprehensive ata and multimedia network. The broadband CDMA technology will be an import pillar supporting this network.

7.2.3 <u>The third generation cellular mobile communication system</u>

7.2.3(a) <u>The drive for the development of the third generation cellular mobile communication system</u>

The first generation cellular mobile communication system represented by AMPS and TACS has solved the people's calling-while-moving problem, and greatly satisfied the users' requirements. However, as the first generation mobile system had such problems as poor voice quality, low frequency spectrum utilization, poor security etc., it was soon replace by the digital second generation cellular mobile communication system represented by GSM and IS95. Compared with the first generation, the second generation cellular mobile communication system been greatly improved in aspects such as voice quality, frequency utilization, security and privacy, and has satisfied the people's requirement within a period of time. Along with the development of mobile communication technologies and the growth of the scale of mobile communications, the shortcomings of the second generation cellular mobile communication system have been gradually uncovered.

1. Scanty Wireless Frequency Resource

The rapid growth of the number of mobile subscribers has caused the frequency resource of the second generation cellular mobile communication system to become relatively insufficient. The fastness of the mobile communication development has gone far beyond people's expectation. Today, China has over 60 million mobile subscribers, and the number is growing at a speed of 10 to 20 million per year. It is believed that China will have 350 million mobile subscribers by the year 2010. As a result of system capacity expansion, cells of certain major cities have shrunk to less than 500 meters, and the system capacity can hardly be further increased by means of cell splitting. On the other hand, the small cell ranges are causing frequent handoffs and serious interference, which greatly lower the voice quality. Low frequency utilization is another reason for the scanty frequency resource. Compared with the first generation mobile communication system, the second generation cellular mobile communication system that uses digital technology has greatly improved the frequency utilization. However, when compared with the third generation cellular mobile communication system that uses the CDMA technology as its kernel, its frequency utilization is still low.

2. Unable to Satisfy the Requirements of New Services

The second generation cellular mobile communication system adopts the voice-oriented design. To provide high-quality and high-efficiency voice services is the main objective of the second generation cellular mobile communication system. Along with the development of the Internet and e-business, data services will take the dominating position. In the future, ultimedia services with the medium- and high-speed data services as the bearer will become he application most frequently used by the users,

5and, as second generation cellular mobile communication system with voice services as its main design objective can hardly provide high-speed data services, and therefore it is doomed to be replaced by the new generation.

7.2.3(b) Brief descriptions of the third generation cellular mobile communication system

The third generation cellular mobile communication system (3G) is also called IMT- 2000, implying that the system's working frequency band is 2000MHz, and its maximum service rate can be as high as 2 Mbit/s. Its technical basis is broadband WCDMA, characterized mainly by multimedia and intelligent features. It can improve the multi-element transmission rate, and realize the general integration of ground cellular system, cordless system, cellular mobile communication system and satellite system - the real global services. It provides a unified platform for the combination and distribution of various services. Although the third generation cellular mobile communication system still has room for perfection, the general framework has been defined. It has the following tree major features:

Seamless global roaming.

High-speed transmission.

High-speed mobile environment: 144kbit/s; walking lowspeed mobile environment: 384kbit/s; Indoor static environment: 2Mbit/s; Seamless service transfer. That is, interworking is available in fixed networks, mobile networks and satellite services. The technology of 3G is the multimedia communication system that uses the IP technology as bearer to realize end-to-end IP and provide multiple serviced. Although the development of 3G and the formulation of its standard have been held up due to different technical, political and commercial interests, and there are as many as ten commercial standards for 3G have been put forward up to now, yet the basis for the transmission mode of all these standards is CDMA. The following paragraphs will present a simple description of the 3G system structure.

1. System Vertical Layers

Bearer Layer

Located at the bottom of the structure is the bearer layer. The IP technology-centered bearer layer is responsible for the transmission and routing of all the data applied on the upper layer, including voice, data and video frequency etc. As the corner stone of the future third generation cellular mobile communication system, the IP protocol should have major progresses in various aspects such as security, efficiency, address space etc., should be ble to provide end-to-end QOS guarantee, and should be able to use multiple transmission mechanisms, such as IP Over ATM, IP Over SDH and IP Over DWDM. High speed, high efficiency and flexibility will its main features.

Switching Layer

The second layer is the switching layer. In this layer contains multiple servers with concentrated functions, that is each server implements a certain specific function. For example, the CSCF call status control server is responsible for call establishment, maintenance and release, the RADIUS server performs subscriber identity authentication, the HSS (Home Subscriber Server) stores various subscription and location information of the subscribers and takes part in the mobility management, and the VOD server provides the VOD server. By coordinating with one another, these servers can provide some basic services. For example, by cooperation with other entities, the CSCF server can provide the basic voice service.

Application Layer

the highest layer is the application layer, which is equivalent to the SCP layer in an intelligent network. The functional entity of this layer work in coordination with various unctional servers of the switching layer to control the connection flow of subscriber calls and quickly generate various new services to satisfy the users' requirements.

2. System Lateral Layers

3G mobile Station

The 3G mobile stations should completely support the IP protocol and various applications on the IP protocol, such as Web browsing, VOD etc. It should become the center of the future personal office work and entertainment.

Full-IP Radio Access Network

The RAN system of 3G supports all-roundly the high-speed packet services, and can perform transparent transmission of IP data. RAN is also responsible for wireless resource management, including the distribution, maintenance and release of the subscriber resources, and implements the mobility management by coordinating with other entities.

Full-IP Core Network

The kernel network is responsible for the subscribers' call control, multimedia data flow transmission, routing etc., so as to provide abundant multimedia services for the subscribers. The core network of 3G is connected with other networks through various media gateways. For example, it is connected with the PSTN via signaling and transmission gateways, with the Internet via PDSN, and with the traditional second generation networks through roaming gateways.

7.3 Process of evolution from 2G to 3G

As mentioned above, there are presently mainly two research and development directions, and the evolution from the IS-95A-based narrow-band N-CDMA system to 3G is shown in Fig. 1-1.

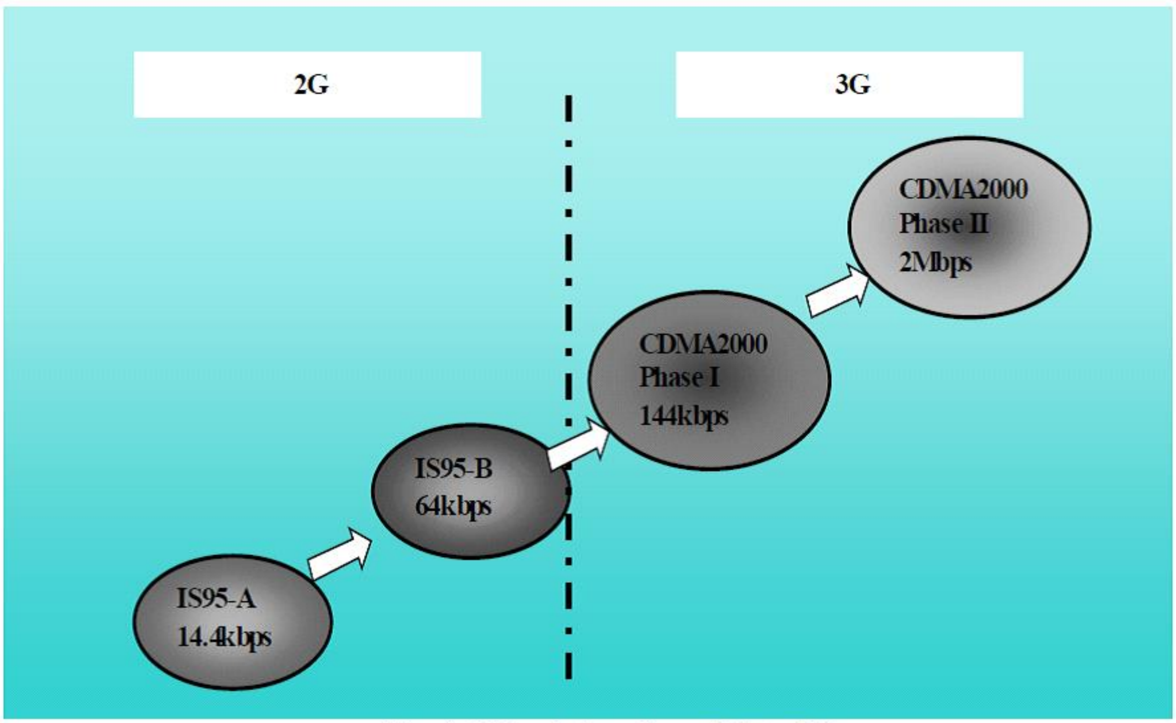


Fig. 1-1 Evolution from 2G to 3G

In Fig. 1-1, IS95-A integrates the IP protocol in the mobile phone, and it is not necessary to include the IP layer in the network's packet transmission layer. As the result, the hardware is compatible with all the IP-based standard networks in the future. The data transmission rate of the IS95-A network is 14.4kbit/s; IS95-B increases the data transmission rate to 64kbit/s by upgrading the core network and wireless network, and makes CDMA a packet mode network by adding a data basis device through the base station controller; as the first phase of CDMA2000, 1XRTT doubles the voice capacity, 8

and increases the data transmission rate to 144kbit/s, and it is estimated that the typical rate available for the subscribers is 130kbit/s; 1XEVDO can provide high-speed packet data service on a carrier frequency. If the subscribers require voice or any other real- time service, the 1XEVDO system will automatically returns to 1XRTT, and execute and complete that service, and this process is transparent to the subscribers; 1XEVDV is the second phase of CDMA2000, with its object being integrating the capability on the first phase to the same carrier frequency, while keeping the capability of transmitting packet data services on separated carrier frequency. This phase provides real-time, non- real time, mixed real-time/non-real-time service modes, and a data transmission rate as high as 2Mbit/s.

7.4 Basic concepts of CDMA wireless transmission system

7.4.1 Wireless multiple access communication

As we all know, it is a primary issue that must be considered in any transmission system how to establish channel links among subscribers within the network in the radio wave coverage area in the environment of wireless communication. In fact, the essence of this question is a question of multiple address mobile communication. The wireless multiple access modes currently in use include: FDMA in analog systems, and TDMA and CDMA in digital systems. The theoretical basis for the realization of multiple access connections is the signal division technology. That is, suitable signal design is made at the transmitting end so that the signals sent from different stations are different; the receiving end has the signal identifying capability, and can choose the corresponding signal from mixed signals. When multiple access mobile communication is established based on the difference of carrier frequencies of the transmission functions, the multiple access mode is called Frequency Division Multiple Access (FDMA); when multiple access mobile communication is established based on the difference of signal existence time, it is called Time Division Multiple Access (TDMA) mode; when the multiple access mobile communication is established based on the difference of transmission signal code forms, it is called Code Division Multiple Access (CDMA) mode. Fig. 1-2 gives a schematic diagram of the time domains and frequency domains of FDMA, TDMA and CDMA transmission processes.

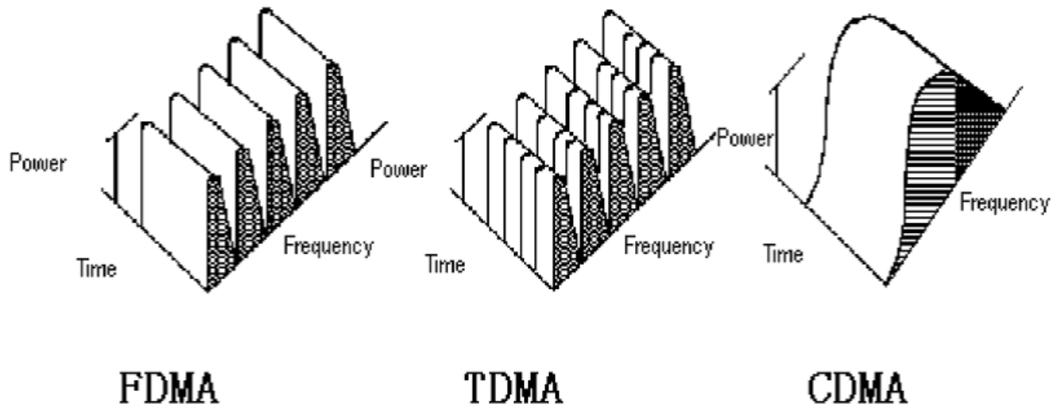


Fig. 1-2 Schematic diagram of time domains and frequency domains of FDMA, TDMA and CDMA

7.4.2 <u>Concept of CDMA</u>

The so-called CDMA refers to such a technology that the transmitting end modulates the signals that it sends using mutually different and (quasi) orthogonal pseudo-random address codes, and the receiving end detects the corresponding signals by demodulating the mixed signals using the same pseudo-random address codes.

7.4.3 <u>Concept of spread spectrum communication</u>

A spread spectrum technology is adopted in CDMA transmission systems. The so-called spread spectrum technology refers to such a technology that the original signals are converted to transmission signals with much wider bandwidth the original, so as to achieve the anti-interference purpose of the communication system. Its mathematic model is the Shanon equation in the information theory. That is, under the condition of noise interference, the channel capacity is:

$C = B \log2 (1 + S / N)$

Where, B is the channel bandwidth, S is the average signal power, N is the average noise power, and C is the channel capacity. From the above equation, we can see: when S/N decreases, the purpose of high quality communication can be achieved without reducing the system capacity, as long as the bandwidth B is increased.

7.4.4 <u>Technical features of CDMA</u>

Based on the above analysis, it can be deduced that CDMA has the following technical features:

1. Invisibility and security;
2. Strong anti-interference and anti-multi-path ability;

3. Realization of multiple access technology, increase of capacity and improvement of frequency reuse pattern;
4. Wide frequency band seizure, increased system complicity and high synchronization requirement.

7.4.5 Principle of CDMA transmission system

7.4.5(a) CDMA wireless transmission system structure

In CDMA communication systems, the pseudo random address codes are periodic code series with strong self-correlation but 0 or very small mutual correlation. Based on the different signal modulation modes, CDMA systems can be divided into DS-CDMA system and MC-CDMA system. In a DS-CDMA system, i.e. the so-called direct spread code division multiple access stem, specific spread spectrum codes are used at the transmitting end to perform time domain spread spectrum processing to the original signals, and the same spread codes are used at the receiving end for the signal demodulation to obtain finally the required useful signals. In a MC-CDMA system, i.e. the so-called multi-carrier code division multiple assess system, specific spread spectrum codes are used at the transmitting end to perform frequency domain spread spectrum processing to the original signals, and the same method is used at the receiving end for the signal demodulation to obtain finally the required useful signals. Since the MC-CDMA system works in frequency domain, the fast Fourier transformation (FFT) technology must be employed at the transmitting end, while inversed Fourier transformation (IFFT) technology must be used at the receiving end.
In a commercial CDMA cellular mobile communication system, CDMA is mainly combined with the direct spreading technology to form the DS-CDMA system. The system's transmission in both forward and backward directions is sketched in Fig. 1-3.

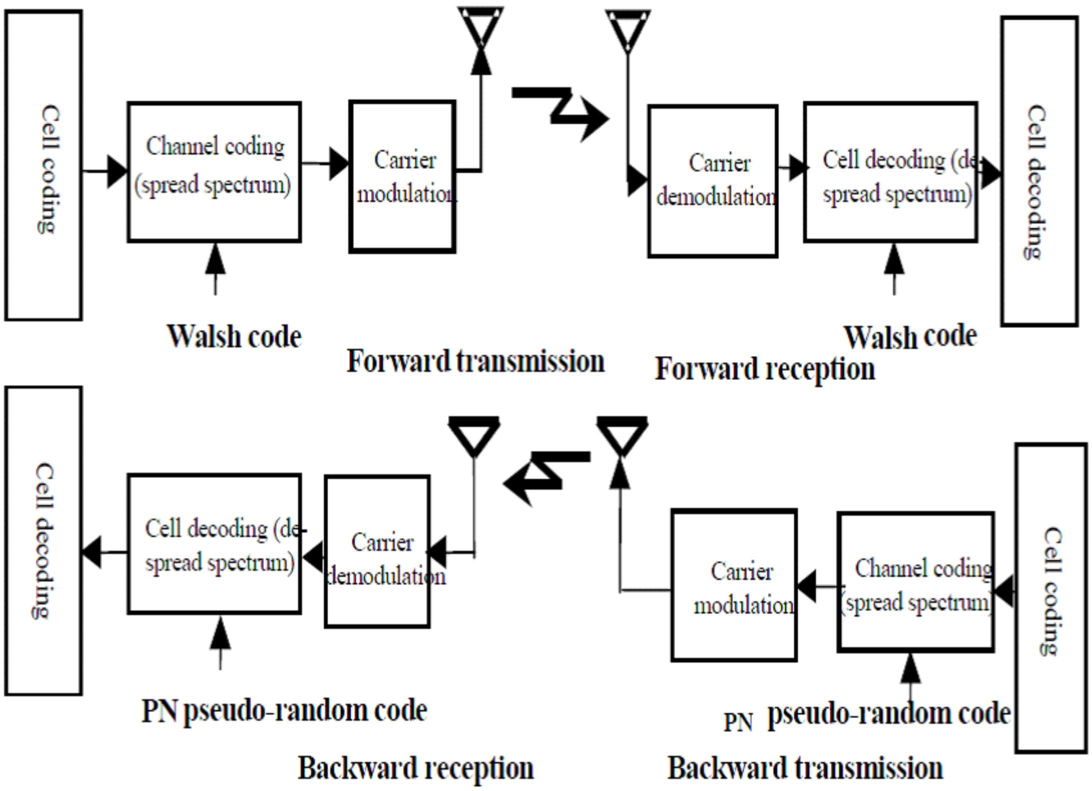


Fig. 1-3 Sketch of forward and backward transmission and receiving in CDMA transmission system

7.4.5(b)Communication Standards for CDMA Wireless Transmission System

The main standards used in the CDM process are as follows:

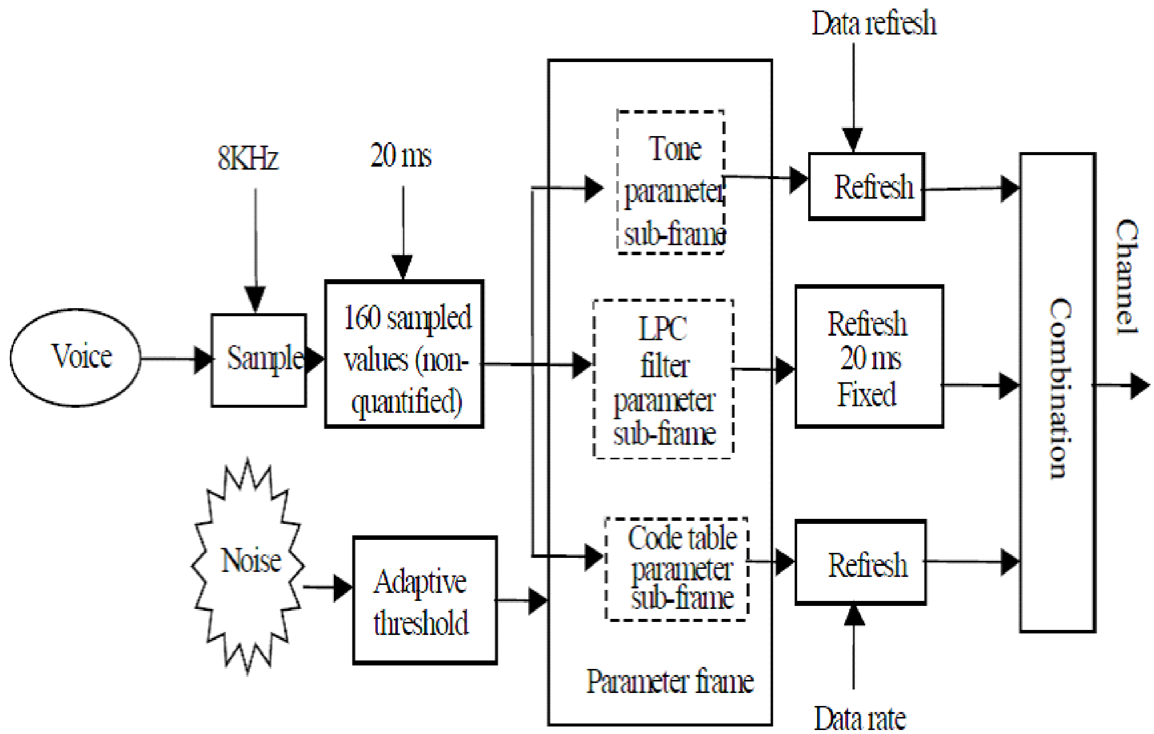
1. Either in forward or backward direction, the signals have to be pre-coded first, and corresponding decoding processing is to be performed in the respective receiving process;
2. Frequency division duplex (FDD) mode is adopted as the transmission mode;
3. Qualcom variable rate code-excited linear prediction (Q-CELP) mode is used for voice coding;
4. The convolution coding and block interleaving combination mode is adopted for channel error correction;
5. QPSK is adopted for forward modulation, and p/4-QPSK is adopted for backward modulation;
6. The spread spectrum signal rate is 1.2288Mbit/s;
7. Frequency bands: 824-849MHz (backward channels/BS receiving), 869-894MHz (forward channels/BS transmission);
8. Carrier separation: 1.25MHz.

7.4.6 Critical technologies in CDMA wireless transmission system

Several new technologies are used in the CDMA wireless transmission system to improve the system's safe and stable operation, and thereby the system's service quality has been largely enhanced. The following paragraphs will present a brief introduction of the major critical technologies.

7.4.6(a) Voice coding technology

The CDMA wireless transmission system adopts Q-CELP variable rate vocoder technology. The purpose is to lower the data transmission rate as much as possible hile keeping the communication quality at a certain level. Q-CELP mainly uses code table vector quantification differential signals, and then generates a variable output data rate based on the voice activation level. Generally speaking, for a typical two-party call, the average output data rate is almost twice, or more than twice, lower than the maximum data rate. The implementation process is briefly described as follows: The input voice signals are sampled at 8kHz first, then they are divided into many 20ms-long frames to generate sub-frames - parameter frames containing three types of parameters (linear prediction code filter, tone parameter and code table parameter). The three types of parameters are constantly updated, and the updated parameters are transmitted to the receiving end according to a certain frame structure. Of these parameters, the linear prediction code filter parameter is updated once per 20ms (one frame) under any data rate, while the tone parameter and code table parameter change with the selected data rate. The implementation sketch is shown in Fig. 1-4.



Q-CELP variable rate vocoder block diagram

7.4.6(b) Voice activation technology

Generally, the mobile subscriber voice activation unremittance probability is 35%. In the CDMA transmission system, making use of this feature, when all subscribers share the same wireless channel and at the instance when there is no information transmission among the subscribers, the vocoder output rate controller transmitting power is reduced or stops transmission, thus the system capacity is increased by nearly 3 times.

7.4.6(c) Synchronization technology

In the CDMA transmission system, the importance of synchronization lies in the system's full application of orthogonality of spread spectrum codes. It is due to the introduction of synchronization technology, the signals of various channels are orthogonal to one another rather than introducing interference (in fact, synchronization error may introduce some interference, but with a very small level). The realization of synchronous CDMA includes three processes: synchronization detection, synchronization establishment and synchronization holding.

7.4.6(d) Power control technology

In the CDMA transmission system, the condition for the separation of the signals of different mobile stations using the CDMA method is that the powers of the received signals of various channels are basically the same, and the method to ensure the same power of various signals is to control the transmitting power of the base stations and mobile stations. The power control technologies include forward power control technology and backward power control technology. The backward power control technology can be further divided into mobile station-involved backward loop control technology and mobile station and base station jointly involved closed loop and outer loop control technology. No matter forward power control technology or backward power control technology, this rule must be followed: power decrease should be fast and power increase should relative slow.

7.4.6(e) <u>Soft handoff technology</u>

In the CDMA transmission system, soft handoff technology refers to the inter-cell handoff using "connecting the new cell before disconnect the original one" mode, and it may occur in the following three cases: between different sectors with the same BTS, between different BTSs within the same BSC, and between different BSCs within the same MSC.

7.4.6(f) <u>Diversity technologies</u>

In order to thoroughly eliminate the signal attenuation phenomenon caused by multi-path attenuation, the CDMA transmission system has introduced the diversity technologies. In the CDMA transmission system, three types of diversity technologies have been introduced: time diversity, frequency diversity and space diversity.

7.4.6(g) <u>Multi-access technology</u>

<u>1. Walsh Codes</u>

Differentiating forward channels: In the CDMA system, each forward code division channel uses 64-level Walsh functions of the bit rate of 1.2288Mbit/s for spectrum spreading, so that the forward code division channels are mutually orthogonal.

<u>2. PN Codes</u>

<u>215-1 short code</u>: To differentiate base stations;

<u>242-1 Long code</u>: To differentiate mobile stations backward, and used for scrambling forward. In the CDMA system, two m series are used, one is 242-1 (r=42) long and the other is 215-1 (r=15) long. In forward channels, the m series with length of 242-1 are used to scramble the service channels, and the m series with the length of 215-1 are used for orthogonal modulation of the forward channels. Different base stations use m series with different phases for modulation, with the minimum phase difference being 64 bits. Thus, there can be up to 512 phases available.

In backward channels, the series with the length of 242-1 are used for direct spectrum spreading, with each subscriber allocated with phase of one m series. Calculated by the users' ESN, these m series phases are randomly distributed and non-repeated, and these users' backward channels are basically orthogonal to one another. The PN code with the length of 215-1 is also used for orthogonal modulation of backward service channels

However, as it is not necessary to differentiate the base stations on backward channels, the m series of the same phase is used for all mobile stations, with its phase offset being 0.

7.4.7 RAKE receiver

The forward channel receiver (mobile station) in the CDMA transmission system is equipped with three correlators and one searching correlator. The signals modulated by QPSK are sent these three correlators, which implement the separation and reception of the signals of these three paths. The searching correlator is used to give the time delay values t1, t2 and t3 of the related address codes, and then the receiving system performs comparison between the delay data and the code elements to determine the path to be received and the correct sampling and judgment of the weight circuit, and finally obtain end maximum output signal signal-to-noise ratio. In the backward channel receiver (within base station), the signal processing mode is basically the same with that in the forward channel receiver, but with an additional space diversity receiving circuit.

7.5 Network and control technologies

The important effect of mobile communication cannot be brought into full play until a huge network is built up. Therefore, the network and control technologies appear vitally important, and that is why the modern digital mobile communication technology includes not only the latest development of wireless and wired communications, but also the computer control technologies and network technologies. Similarly, the CDMA 16 system system's many supreme features are realized by means of the extremely complicated but flexible and reliable network and control technologies in the system. The initial control is implemented on the wireless interface (i.e. the Uı interface between the mobile station and the base station) through the pilot channel, synchronizing channels and paging channel in the forward channels, and the access channel in the backward channels. After the establishment of communication, the control is implemented only by means of the signaling service multiplexed in the service channel between the forward channels and backward channels (such as inter-cell handoff, power control technology etc.). In addition, complex interface, signaling, network, maintenance and management (OMC) and control technologies exist between a base station's BTS and BSC (Abis interface), between a BSC and MSC, and between BSCs in the same MSC. Especially, the interface, signaling, network and control technologies at the MSC are the most complicated. This is the very reason that effective control must be exercised on the network in order for the safe operation of the network.

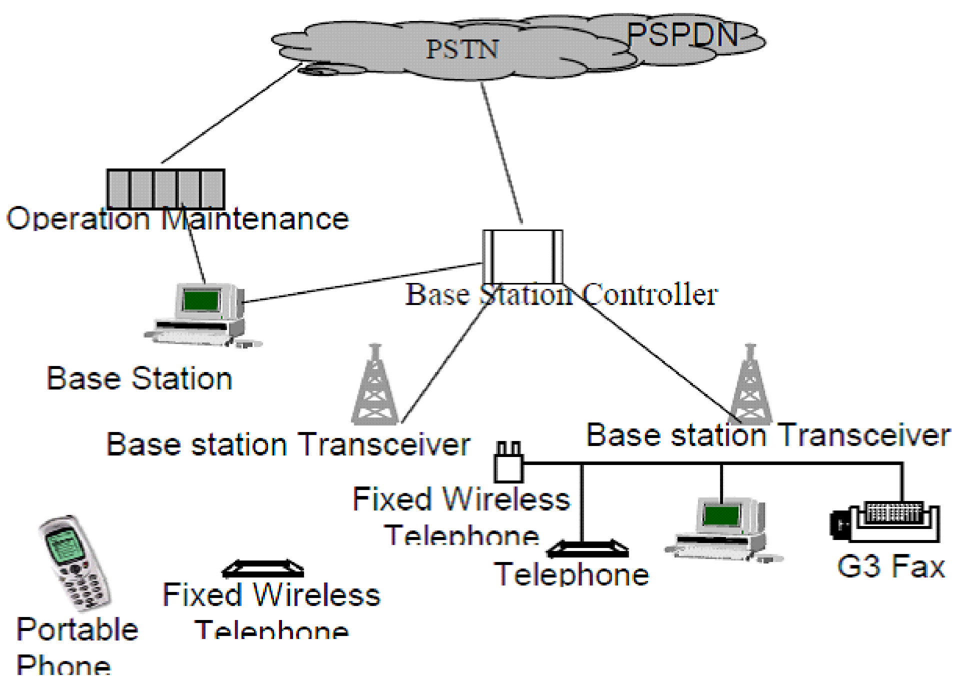
7.5.1 System Overview

WLL (Wireless Local Loop) system is a digital wireless local loop system based on most recent international specifications and CDMA technology, which has been accumulated through the installation and operation of commercial systems. The system has evolved from the existing wired and CDMA digital cellular system. In the wireless local loop (WLL), the telephone lines, interface between the existing PSTN switching systems and subscribers;

have been replaced with a wireless system. It can provide subscribers with the service quality equal to that of the wired system. For the successful development, cutting-edge technologies of computers, semiconductors, communications and software sectors are utilized widely for the system enough to provide the highest quality in all the applications including exterior size, optimal performance, service flexibility and network environment applicability. The system that employs the cellular technology makes it possible to configure the network more economically. The reason is why it covers a wider service area by using the same network as that of cellular phone or PCS (Personal communications service) system in common. In addition, it is subject to less restrictions and transmission loss in a free service area than the cellular phone system. Moreover, since it is operated in a fadeless state, its data transmission rate can be increased rather dramatically compared to the case where other system is used. It has been developed based on CDMA technology having a greater subscriber capacity with the use of wireless interface mode.

7.5.2 Network Configuration

The Network components are Base Station Controller (BSC), Base station Transceiver Subsystem (BTS), Fixed Subscriber Unit (FSU), and Base Station Manager (BSM). Additionally, the system is equipped with inter-working function (IWF) for data service. The network configuration diagram is shown below .



WLL Network Configuration

7.5.2(a) <u>Base Station Controller (BSC)</u>

The Base Station Controller (BSC) interfaces with the BSC and PSTN LE (Local Exchange) in order to support the establishment/release of originating/terminating calls. It performs the trans-coding between QCELP (Qualcomm Code Excited Linear Predication) in wireless sections, PCM (pulse code modulation) in wire network. Also it has an echo canceling function by traffic delay, and interface function between the BTS and PSTN LE. It utilizes R2, No. 7, and V.5.2 signaling system for the interface with PSTN LE.

7.5.2(b) <u>BTS (Base Station Transceiver Subsystem)</u>

The Base station Transceiver Subsystem (hereinafter, referred to as BTS), located between FSU and BSU, controls the calls and carriers out the maintenance function. That is, it enables the wireless FSU to acknowledge the BTS first, sends down required data, allocates the traffic channels to call requests, and open call paths.

7.5.2(c) <u>BSM (Base Station Manager)</u>

The functions of Base Station Manage (hereinafter, referred to a BSM) include initialization, downloading, status management, configuration management, performance statistics, and subscriber authentication on the BSC and BTS. Since the BTS operating device accommodates several subsystems, it has the minimum effect on the system operation and maintenance when faults occur.

7.5.2(d) <u>FSU (Fixed Subscriber Unit)</u>

Fixed Subscriber Unit (hereinafter, referred to as FSU), placed between BTS and subscriber provides the wireless interface function. It can be classified into various forms depending on how many antennas, lines and applications it has. It can also provide voice services, voice bandwidth data and digital data services.

7.6 <u>System based on CDMA Technology</u>

CDMA (Code Division Multiple Access) is one of modulation and multiple access modes. It is based on spread spectrum communications widely used nowadays. Currently, it is used for latest cellular mobile and advanced wireless communications. The CDMA has a capability to resolve the capacity problems resulted from the growing demand of mobile communication service. For long-term benefits, it continues to provide an economical and effective wireless communication environment, with the functions and features described below.

- **<u>Large Capacity</u>**

The site test on CDMA under various types of environment conditions indicates that CDMA system has capacity of 10~20 times as much as analog system has. The system capacity may increase for any quality of service of call traffic.

- **Availability and Cost-effectiveness**

In the perspective of network equipment and subscriber equipment, the price of CDMA system is about the same as that of analog system. However, its capacity can be 20 increased with much less number of cells compared to the analog and TDMA system. Accordingly, the user can reduce the installation and maintenance cost.

- **High-Quality Service**

The variable bit rate voice coder can reproduce digital voice and high quality voice. Accordingly, the system can silence the background noise even under the overload. Moreover, the independent tracing on each multi-path reduces greatly the fading effect. CDMA soft handoff technology can handle dully the call handoff. Such a technology excludes the possibility of call disconnect and reduces the system load.

- **Call Confidentiality**

Since CDMA signals are scrambled, the system has an advanced call confidentiality that allows the CDMA digital system to prevent wireless illegal access.

7.6.1 Various Supplementary Services

The system provides data service and subscriber management function under the wireless environment. It is capable of providing the following types of supplementary services.

- **Subscriber Authentication**

Authentication is a subscriber management process that handles the information exchanged between the network and WLL FSU to identify the WLL FSU. Its has a powerful security function to confirm whether a subscriber is valid, and prevent unauthorized or illegal subscriber from access to the network.

- **Data Service**

Asynchronous Data Service (Maximum of 14.4 Kbps) IS-707 A.4
14.4 Kbps G3-Fax Data Service (Maximum of 14.4 Kbps) – IS-707 A.4/IS-707 A.7
Packet data service (Maximum of 64Kbps) – IS-707 A.5 (14.4Kbps), IS-707 A.9 (64Kbps)

7.6.2 Supplementary Services

CHD (Call Holding), CF (Call Forwarding), CT (Call Transfer), CW (Call Waiting), CLIP (Call Line Identification Presentation), CLIR (Calling Line Identification Restriction), CC (Conference Calling), TWC (Three-Way Calling), and etc.

7.6.3 Mobility (Optional)

In all areas where the WLL system covers and control, the services can be provided to support subscribers' mobility. It can also provide the handoff function among sectors or cells. On the contrary, any mobility added to the WLL system (that is, if WLL provides the hybrid (mobile/fixed) service), will be implemented from trade-off among mobility, service quality, and network cost.

- Limited mobility in BSC coverage
- Soft Handoff (between BTSs)
- Soft Handoff (between sectors)

7.6.4 PSTN Interface

The system has the following type of interface in accordance with the requirement of PSTN LE interface.

- **R2/No. 7**

R2/No. 7 type STAREX-WLL system is used as the local exchange for PSTN LE instead of AN (Access Network) for PSTN LE. The system itself can provide a call processing, supplementary services, and billing functions.

- **V.5.2**

V5.2 type system is used and AN for PSTN LE which provides all the supplementary services and billing functions except data service. In this case, the WLL system can provide a transparent service for services provided by LE.

7.6.5 System Features

1. BSC

The BSC, located between PSTN LE and BTS, has BTS status management of BTS and wireless resource management function. In addition, it trans-codes between QCELP mode voice packet data and PCM data and performs an echo canceling function used to remove echo caused by the time delay of vocoder block while being connected to the wire subscriber. The BSC that accommodates up to 48 BTS is made up of a high-speed traffic packet router, selector for voice data processing, vocoder, call control processor, and trunk interface unit.

The major functions that it provides are as follows.

- Call Processing Function
- Transparent Service Provision
- Voice Coding
- Optimal Voce Quality Selection
- Provision of Supplementary Services
- Message Distribution Function
- Call Resource Management
- PSTN Interface
- Operation and Maintenance Function
- Network Inter-working Function

Call Processing Function

By inter-working with the BTS and PSTN, the BSC can support the set up/release function of wireless-wire, wire-wireless, wireless-wireless calls that have entered the Base Station Controller. It also supports the G3 Fax, non-voice circuit data, and packet data call processing function.

Transparent Service

Also provided is the message processing function for transferring BTS-BSC-PSTN LE transparent messages used for location registration and supplementary services while busy.

Voice Encoding

It cross-converts IS-95A/ANSI J-STD-008 traffic data to PCM and voice versa in order to handle the voice traffic packets at an interval of 20ms per call. For the processing of voice traffic, 14.4Kbps (Rate Set2) vocoder for an excellent voice quality is provided as well as 9.6 Kbps (Rate Set1) vocoder.

Optimal Voice Selection

This function is to select the best packet among those arrived via a maximum of three multipaths for preventing the call disconnect. It has two functions, that is, transcoding them into PCM data; as reverse function, sending out voice traffic packets converted from the PCM data via a maximum of three paths.

Supplementary Services

Messages related to various types of supplementary services are processed.

- **Message Distribution**

This function is used to carry out a routing function promptly on the traffic packets and control message between several BTSs and BSC.

- **Call Resource Management**

This function is used to distribute and select the load of vocoder resources needed for call set up, and it carries out the collecting function during the call releasing. During the load sharing, the staggered frame control function by frame-offset value is applied.

- **Operation and Maintenance**

The processor status management, device status management, configuration management, measurement and statistics processing, test processing, fault processing, and overload control functions are carried out for the operation and maintenance of BTS and BSC. The operator interface for the operation and maintenance is processed at a workstation connected to the system.

- **Network Inter-working**

Since the CDMA cellular system based on the IS-95A/B and J-STD-008 Recommendations codes voice signals into low rate vocoder data, it cannot send out asynchronous data/fax modulation signals used on the wire network via a wireless interface. Therefore, it is required to directly transfer asynchronous data/fax binary data information to wireless digital channel section. A modem function capable of interworking with these data should be installed at the end of mobile communication network to transfer them to the asynchronous data/fax modem of wire network. The data networking function (IWF) explained later is a device used to carry out the above modem functions.

- **PSTN Interface**

R2/CCS No. 7/V5.2 signaling is used for the PSTN network interface.

2. BTS

The BTS interfaces with the subscriber side in the wireless mode and BSC via E1. It carries out the channel management and power control function between the wireless interface sections. The BTS provides the following types of main functions.

- Call Processing Function
- Wireless Resource Management
- Software Downloading
- Operation and Maintenance Function
- Fault Management
- Testing Function
- Overload Control Function
- Statistics and Measurement Function

Call Processing

BTS interworks with the BSC and subscriber to process the setup/release function and mobile, mobile-land, and mobile-mobile calls in the BTS. Also it performs the Markov
Call processing function for the test call set up.

Wireless Resource Management

Channel elements for call set up are selected and then are collected during channel resource load distribution and the call release.

Software Downloading

The BTS downloads OS (Operating System) and Application software from the BTS Controller for each processor. In case the same version of OS and application code are downloaded, the system only has to receive the loading from the flash memory (nonvolatile memory) for execution, instead of receiving the loading again. This shortens the initialization time of BTS since it removes any unnecessary loading time.

Operation and Maintenance

For the operation and maintenance of BTS, the processor status, configuration information, and operation information management are executed throughout the BTS by inter-working with BSC and BSM. The equipment status is evaluated periodically for maintenance and then, the results are reported to the system operator. In addition, maintenance commands are executed through an operator's terminal in order to check the status of specific equipment.

Testing Function

For channel elements (particularly, traffic channels), available resources are tested periodically in real time for higher resource reliability. Depending on the testing results, whether to use the testing results as call resources or to initialize them again is determined. On-demand test by operator's request is possible as well. Two types of CE related tests are available: the function of testing the hardware of CE itself and the function of carrying out the test using the Markov call of BTS.

- **Overload Control Function**

It can be divided into minor, major, and critical depending on the processor load. Then, necessary actions are taken after classifying them into terminating call inhibition (minor), terminating/originating call inhibition (major), and call connection inhibition (critical).

- **Statistics and Measurement Function**

The information on the collection and reporting on various types of statistics information (traffic statistics, hand-off statistics, and paging statistics) are processed.

Mobility Support

The handoff can be performed between BTS sectors (softer handoff) or cells (soft handoff) in order to support the subscribers' mobility.

3. Operation and Maintenance System (BSM)

The main functions of operation and maintenance system are as follows.

- Configuration Management
- Performance Management
- Fault Management
- Security Management
- Operator Interface Function
- Software Downloading

Configuration Management

As part of configuration management, the system authentication is carried out. In addition, system configuration and re-configuration are performed and controlled. Moreover, related information is collected and the system is initialized, activated, and reactivated. Moreover, the corresponding information is provided to the system for service continuation or termination.

Performance Management

Performance Management provides the function of evaluating and improving system operation or the efficiency of network and network elements. For this purpose, statistics data related to various types of QoS are collected from the network elements.

Fault Management

During the fault management process, the abnormal operations of wireless subscriber line components are detected, isolated, and corrected.

Security Management

General computer security functions are carried out. In addition, the functions related to system operator/system authentication are executed.

· Authorization facilities – for system operators
· Access control
· Security recording

Man-Machine Interface Function

This is a function used for Man/Machine Interface. The commands of system operator are analyzed, executed, and controlled. In addition, command execution results are 28 reported to the system operator. Moreover, for the multi-processing of inputs/outputs, a window management function for partitioning the screen is carried out as well. Moreover, the function of managing message history is carried out as well.

Software Downloading Function (BSC and BTS)

A new function is added onto the existing software. In addition, the function of loading software onto the network elements during the installation of network elements and reactivation is carried out.

The operation and management function enables the system operator to find out the service status easily. It also provides data required for billing. Moreover, it provides various types of functions to the system operator so that various types of services can e
provided to the subscribers.

8. ACKNOWLEDGEMENT

We would like to ackowledge Prof. K. R. Chandrasekharan Pillai, Principal, NSS College of Enginering, Palakkad for making our inplant training a success. We express our sincere thanks to Prof. Abdul Kareem, Head of the Dept. of ECE, for granting permission for attending the training and his support throughout.

We would like to thank BSNL, Eranamkulam for conducting the inplant training. We wish to express our gratitude to General Manager, BSNL, Eranamkulam for his assistance and support throughout the session. We also thank all others whose contributions made this training possible.