TELECOMMUNICATIONS NETWORK

Dianthy Marya
Martono D. A.
M. Nanak

CERDAS
ULET
KREATIF
www.cerdas.co.id

Telecommunications Network

Copyrights © 2022. All Rights Reserved
Hak cipta dilindungi undang-undang

Penulis:
Dianthy Marya
Martono D. A.
M. Nanak

Penyunting:
Dhega Febiharsa

Desain & Tata Letak:
Tim Penerbit Cerdas Ulet Kreatif

ISBN :
Cetakan Pertama : **2022**
Penerbit :
Cerdas Ulet Kreatif
Jl. Manggis 72 RT 03 RW 04 Jember Lor - Patrang
Jember - Jawa Timur 68118
Telp. 0331-4431347, 412387 Faks. 4431347
e-mail : info@cerdas.co.id

Distributor Tunggal:
Cerdas Ulet Kreatif
Jl. Manggis 72 RT 03 RW 04 Jember Lor - Patrang
Jember - Jawa Timur 68118
Telp. 0331-4431347, 412387 Faks. 4431347
e-mail : info@cerdas.co.id

Undang-Undang RI Nomor 19 Tahun 2002
Tentang Hak Cipta

Ketentuan Pidana
Pasal 72 (ayat 2)

Barang Siapa dengan sengaja menyiarkan, memamerkan, mengedarkan, atau menjual kepada umum suatu ciptaan atau barang hasil pelanggaran Hak Cipta atau hak terkait sebagaimana dimaksud pada ayat (1), dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp. 500.000.000,00 (lima ratus juta rupiah).

FOREWORD

First of all, praise be to Allah SWT, through whose assistance the author completed the textbook entitled Telecommunication Network.

This textbook serves as a reference for the fourth-semester Telecommunication Network course. The fundamentals of a telecommunications network, including network classification, signaling, and switching, are covered in this book. In addition, this book discusses private branch exchange, grounding on a telecommunications network, network quality of service, and how to manage the network in telecommunication.

Our profound gratitude goes out to all of our colleagues who assisted us and genuinely offered moral support throughout the entire process of creating this book.

Finally, we'd like to offer you a nice reading experience and, of course, remind you that we always welcome feedback and improvement recommendations.

Malang, July 2022

Authors

TABLE OF CONTENTS

CHAPTER 1
INTRODUCTION

A. What is Telecommunication Networks?

A telecommunications network is a collection of nodes connected by a telecommunications link for the purpose of exchanging messages. The primary goal of telecommunications networks is to send data in any format from one user to another on the networks. To transmit data messages and signals, telecommunications lines can use a variety of technologies based on switching approaches (circuit switching, message switching, or packet switching). Messages can be forwarded from the origin node to the target node through many network hops if numerous nodes work cooperatively. Each node in the telecommunication network must be able to communicate with other nodes correctly.

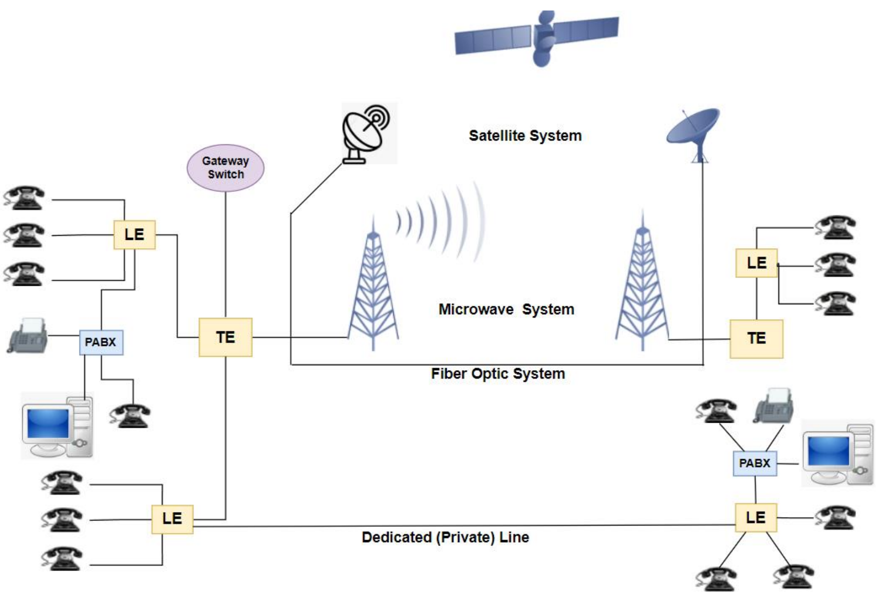

Figure 1. A typical telecommunication networks

The telecommunications network is made up of numerous networks that provide various services such as data, fixed, and cellular. Customers can connect to the network via a variety of network technologies, such as fixed telephones or mobile/cellular telephones. Computer networks, the Internet, the PSTN, worldwide Telex networks, aviation ACARS (Aircraft Communications Addressing and Reporting System) networks, and cellular telephone networks are all examples of telecommunications networks. The telephone network is an example of a public networks. The users of public networks are called subscribers.

B. Basic Telecommunications Network

A telecommunication network is a telecommunication system that allows many users to share information. The telecommunication network is perhaps the most complex infrastructure deployed by humankind. It spans a wide geographical area and is composed of different types of equipment (Lannone, 2012). The telecommunications network consists of three main parts, namely transmission system, switching system, and nodes or terminals as shown on figure 2.

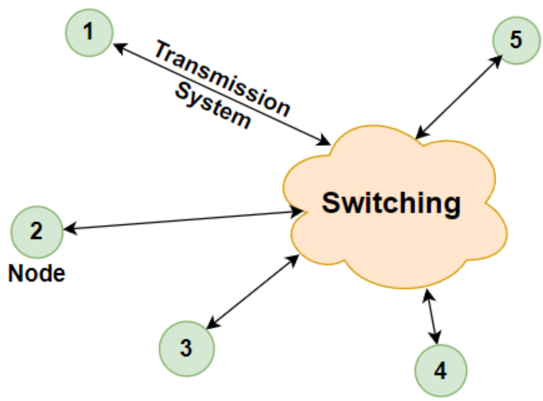

Figure 2. Three main parts of telecommunications network

1. Transmission

Transmission is the process of transporting information between end points of a system or a network (Anttalinen, 2003). The transmission systems interconnect exchanges and, taken together, in a telecommunications network. There are three part or element on basic concept of transmission system as you can see on the figure 3, such as transmitter, transmission channel or media, and receiver.

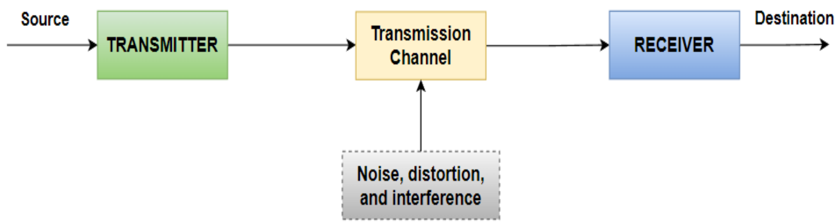

Figure 3. Basic concept of transmission system

a) Transmitter

The transmitter decodes the input signal and generates a transmitted signal that is suitable for the characteristics of the transmission media or channel. Encoding and modulation are frequently used in signal processing for transmission. In the case of optical transmission, the transmitter converts an electrical signal format to an optical signal format. An example of transmission system on radio transmitter mainly consists of the following parts:

1) Power supply is the energy source used to power the device and create the energy for broadcasting. Power supply circuit transform the input electrical power to the higher voltages needed.
2) Electronic oscillator generates a wave called the carrier wave where data is imposed and carried through the air.
3) Modulator adds the information into the carrier wave by varying some aspect of the carrier wave. The information is provided to the transmitter as an electronic signal called the modulation signal. The modulation signal may be an audio signal, a video signal, or for data in the form of a binary digital signal. Different types of transmitters use different modulation methods to transmit information.
4) Radio Frequency (RF) amplifier increases the power of the signal in order to increase the range where the waves can reach.
5) Antenna or impedance matching circuit is a device that matches the impedance of the transmitter to the impedance of the antenna (or the transmission line to antenna) in order to transfer the power efficiently to the

antenna and prevent a condition called standing waves when the impedances are not equal.

b) Transmission Channel or Media

The transmission channel is an electrical medium that bridges the distance from the source to the destination (Anttalinen, 2003). Transmission systems use two basic media for information transfer from one point to another:

1) Guided Transmission Media

   The waves are guided along a physical path or solid medium such as twisted pair cables, coaxial cables, and optical fiber.

   i. Twisted Pair Cable

      A twisted pair cable consists of two insulated copper wires. The two wires twisted together to reduces external electrical interference as well as interference between pairs in the same cable. This cable is symmetrical and the difference in voltage. An example of twisted pair cable is telephone cable. It has transmission speed of 2 million bytes per second to 100 million bytes per second.

   ii. Coaxial Cable

      The core of a coaxial cable is made of strong copper wire that is surrounded by insulating material and a cylindrical conductor surrounds the insulator. The outside conductor is protected by a plastic sheath. The coaxial cable's structure provides a nice combination of high bandwidth and strong noise immunity. Coaxial cables are used in LANs (the original 10-Mbps Ethernet), broadcast radio and TV antenna systems, high-capacity analog and digital transmission systems in telecommunications networks.

   iii. Optical fiber

      Optical fiber is the most recent transmission medium. It has a strong immunity to external electrical interference, a large bandwidth, and low attenuation. In all industrialized countries and high capacity, fiber optic cables are the primary medium for long-distance communication. Optical fibers have the disadvantage of being more difficult to install than copper connections.

2) Unguided or Wireless Transmission Media
Unguided (Wireless) transmissions are methods that allow the transmission of data without the use of physical means to define the path it takes. Unguided media provide a means for transmitting electromagnetic waves but do not guide them; examples propagation through air (free space) such as satellite communication and cellular systems. Examples of unguided or wireless transmission include microwave, satellite, radio or infrared. Microwaves operates at high frequencies, including UHF, SHF and EHF. Infrared that used for short distance communication, with a speed of 4 Mbps.

Transmission systems interconnect exchanges and, taken together, in a telecommunications network. It called the transmission or transport network. It is worth noting that the number of speech channels required between exchanges is substantially lower than the number of customers.

c) Receiver

Receiver takes the signal from the channel and converts it back into usable information. Radio receiver is the opposite of a radio transmitter. It uses an antenna to capture radio waves, processes those waves to extract only those waves that are vibrating at the desired frequency, extracts the audio signals that were added to those waves, amplifies the audio signals, and finally plays them on a speaker.

2. Switching

In theory, all telephones might still be connected to each other by wires, as they were at the firs of telephony. However, as the number of telephones increased, operators realized that switching signals from one wire to another was necessary. Because the number of concurrently active calls is far lower than the number of telephones, just a few cable connections were required between exchanges. The switching device or system built and placed between customers on the telephone network is known as an exchange. The first switches were not automatic, so switching was done manually using a switchboard. Exchanges were previously a complex sequence of electromechanical selectors, but in recent decades they have evolved into software-controlled digital exchanges. Modern exchanges typically have a vast capacity (tens of thousands of customers), and thousands of them may have calls running concurrently. A basic telecommunications network show on the figure 4.

Switching is defined as a mechanism for connecting the input channel to the output channel so that information (telecommunication traffic) can be streamed from the sender to the receiver. In a data communication network, the switching device can be a switch or a router. Switching system on a computer network is referred to as Packet Switching, and on a telephone network it is called Circuit Switching. An example of switching system on a computer network show on the figure 5.

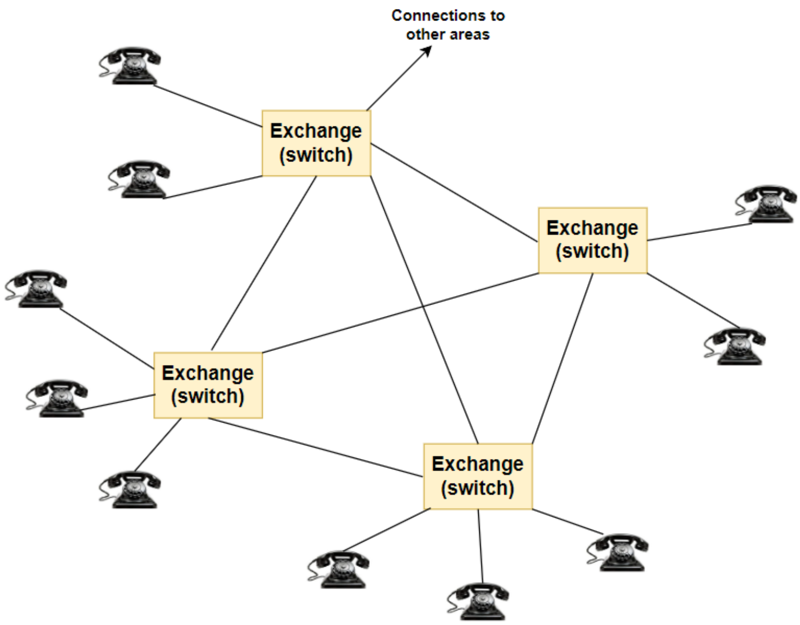

Figure 4. A basic telecommunications network

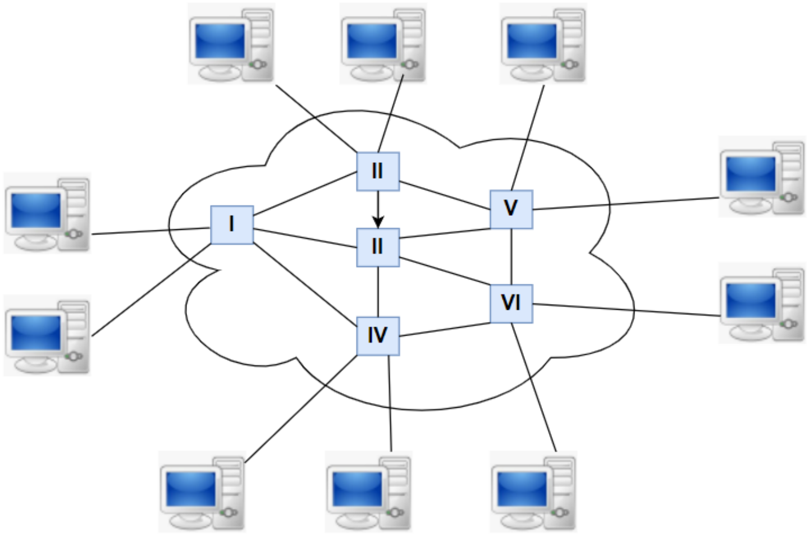

Figure 5. Switching system on a computer network

Switching system used to receive control signals, information, and conversations, which are subsequently forwarded to the data recipient with any necessary changes. Switching basic functions are interconnections, control, detect connection requests, receive information, sending information, holding a busy test, supervise the conversation.

3. Signalling

The IEEE defines signaling as the exchange of information specifically concerned with the establishment and control of connections and the transfer of user-to-user and management information in a telecommunication network. Conventional signaling has evolved with the telephone network. Signaling is accomplished by the use of specific signals or messages that inform the opposite end of the connection what is expected of it. There are three examples of signaling to customers:

- Off-hook condition: When the exchange recognizes that the subscriber has raised the telephone hook (the dc loop is connected), it sends the subscriber a dial tone.
- Dial: When a subscriber dials digits, the central office or exchange receives them.

- On-hook condition: When the exchange detects that the subscriber has terminated the call (the subscriber loop has been severed), it disconnects the connection and ceases invoicing.

In a telecommunications network, signaling is a highly complex process. Signaling is divided into three functional areas:

- **Supervisory**
  Supervisory signaling provides information to the switch about the condition of the line or circuit whether the circuit (internal to the switch) or trunk (external to the switch) is busy or idle, when the called party and the caller are off-hook or on-hook.
- **Address**
  Address signaling directs telephone calls to the called subscriber. The local switch receives these numbers and, using the information contained in the numbers, directs the call to the called subscriber.
- **Call progress: audible-visual**
  provide some kind of audio-visual means of informing the subscriber being called that a telephone call is waiting. Example; ring back tone and busy back.

Signaling is also required between exchanges because most calls must be connected via more than one exchange or switch. For the connectivity of various exchanges, many different signaling protocols are utilized. The other signaling are subscriber signaling and inter-switch (inter-register) signaling. Inter-switch (inter-register) signaling is required between switches when more than one switch is involved in setting up a call. Inter-register signaling is the process of sending addresses between switches.
The local exchange control unit receives subscriber signaling from the subscriber line, such as dialed numbers, and performs the appropriate actions based on its program. Typically, the call is routed through several exchanges, and signaling information must be transferred from one exchange to the next. This can be accomplished using two types of signaling either channel associated signaling (CAS) or common channel signaling (CCS).

There are two classifications on signaling based on signaling area. First, signaling between subscriber and exchange. And second, signaling between exchanges. A more complete explanation of signaling classifications is in chapter 3.

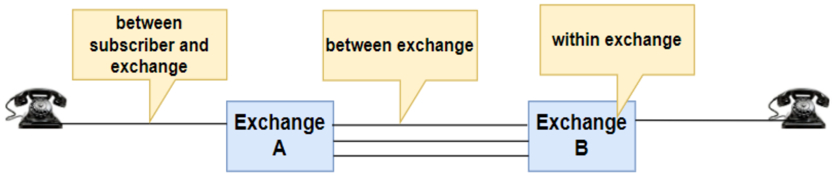

Figure 6. Switching area

Consider an international mobile phone subscriber turning on his phone in Korea. He can receive calls aimed to him in about 10 seconds. Hundreds of signaling messages carry information for this purpose between exchanges in international and national networks.

C. Telephone Numbering

An international telephone connection from any telephone to any other telephone is made possible by unique identification of each subscriber socket in the world (Anttalinen, 2003). Each telephone set has a unique identification number in mobile telephone networks. The numbering is hierarchical, with the highest level having an internationally standardized country code. As a result, country numbering schemes are independent of one another.

The telephone number hierarchy structure consists of international prefix, country code, trunk or area code, and subscriber number. For international calls, an international prefix or an international access number is used. It informs the network that the connection will be forwarded to another country via an international telephone exchange. Although the international prefix varies by country, it is gradually being standardized. For example, 00 is used throughout Europe; elsewhere, it may be different.

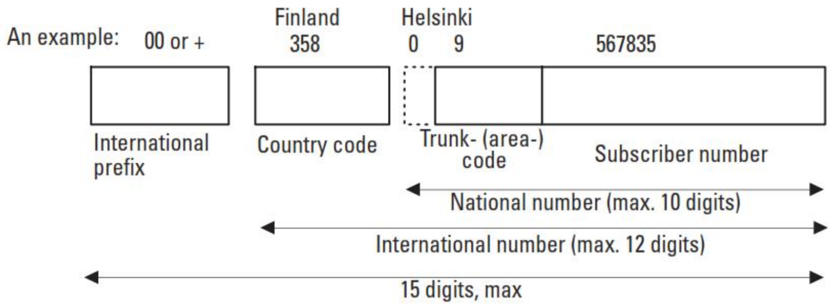

Figure 7. The structure of the telephone number hierarchy

Source: (Anttalinen, 2003)

An international number is a phone number that includes the country code and has a maximum length of 12 digits. The country code contains one to four numbers that identify subscriber's country. ITU has created various country codes, ranging in length from one to four digits. Consider the following country codes as examples: 385 for Finland, 62 for Indonesia, 7 for Rusia, 60 for Malaysia, and 1 for the US and Canada. For national calls, country codes are not required because their purpose is to make subscriber identity unique over the world.

The trunk code specifies the location inside the country to which the call will be routed. The first digit is a long-distance call identification number, and the remaining numbers identify the location. The trunk code is used to identify the subscriber's home network rather than the location on cellular service.

In a fixed telephone network, the subscriber number is a unique identification of the subscriber within a geographical area. To reach a certain subscriber, dial the same number from anywhere in the area. Due to the numbering system, the subscriber component of one subscriber's telephone number may be the same as that of another subscriber in another location.

D. Network Topologies

A network is a collection of nodes and linkages. There are numerous examples of networks observed in daily life. Networks can also exist on a much smaller scale, such as the electrical circuitry in a television set, with real cables or printed circuit rails connecting the nodal electronic components. Similarly, numerous communications networks are comprised of a range of nodal functions and transmission links. The pattern of links between the nodes in a network, that is, its topology, determines the possible routeings between any two nodes – either direct if a link between the two nodes exists or connected through one or more intermediate nodes, known in general as a 'tandem routeing' (Valdar, 2017).

A topology is essentially a map of a network. The most basic telecommunication network topology format is point-to-point, which is the direct connection of two devices, or nodes. This network type was essentially the original telephony system solution. As the number of devices increases, they can be linked in in star and ring topologies. The figure 8, shows the possible set of network topologies.

Star topology allows communication between specific groups of nodes in such a way that other nodes are not aware of the communication. It provides a direct link between all nodes. The security of star topology is more secure than in ring topology because if one leg of the network is damaged, the rest of the network will continue to function normally. A local network with dependent exchanges linked to the parent exchange is an example of a star topology that may be used to achieve minimum link costs.

A ring topology represents the broadcast type as the traffic is routed via all the nodes. In the ring architecture, transmission occurs only in one direction, around the network's closed loop.

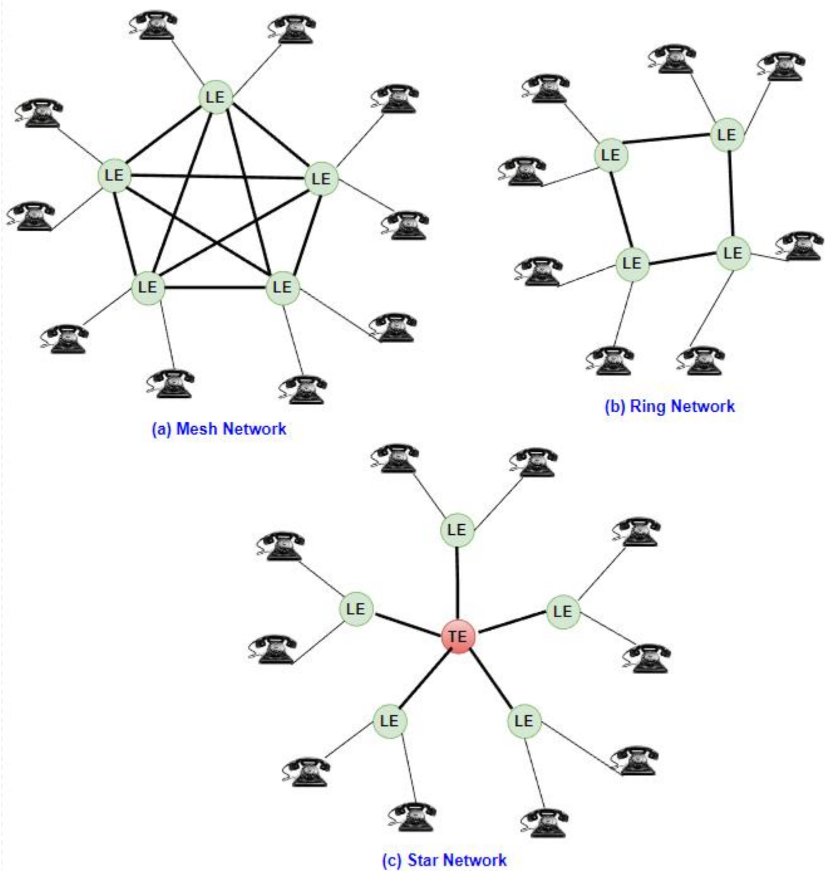

Figure 8. Network Topologies

In fact, telecommunication networks are typically made up of a combination of topologies in order to reduce costs while maintaining an appropriate amount of resilience. A star network, for example, may be utilized to achieve low connection costs, but some meshing between specific nodes would be included to offer the network some resistance to link failures.

Review Questions

Q1. What is telecommunication network?

Q2. What are the main parts of telecommunications network?

Q3. Switching system on a telephone network is referred to as………

Q4. Give an example of international telephone number from Indonesia and explain the structure of that number!

Q5. Draw some of telecommunication network topologies!

CHAPTER 2
TELECOMMUNICATION NETWORK AND TERMINAL

A. Introduction to Telecommunication Network

Telecommunications are today widely understood to mean of communicating over a distance. The first form of telecommunication networks was the telegraph. Telecommunications are now global and include not only telephony over fixed and mobile networks, but also data – the World Wide Web, e-mail, broadcast TV, video, social networking, etc. In setting out how all of this works it is helpful to understand how the basic telephone networks are structured since they form the basis of all today's telecommunications networks (Valdar, 2017).

B. Telecommunication Network

Telecommunication networks can be classified based on several things such as classification based on how signals are transmitted and received. There are three types of telecommunications networks based on how signals are transmitted and received, namely:

1. Broadcast networks
   In broadcast network, signals transmitted by one end-user device simultaneously automatically heard by all other end-user equipment. Example: AM/FM radio, and television.
2. Switched networks
   In switched network, signal must be routed through network nodes or switched to desired route. Example: telephone network.
3. Hybrid
   This type of telecommunications network is a combination of broadcast and switched networks. for example: Ethernet segment (broadcast) connected to Routers.

Telecommunications networks can also be classified based on network customers and service availability. Public networks and private or dedicated networks are the two basic types or classifications based on network customers and service availability. Furthermore, telecommunication networks can be classified based on the type of information (Voice/Speech/Audio, Data, and Video), transmission mechanism (Analog, Digital, Radio, Satellite), topology (Mesh, Ring, Star), data rate and response speed (Broadband vs Narrowband).

1. Public Networks

Public networks are owned and managed by telecommunications network operators that have a license to provide telecommunications services. Any customer can be connected to the public telecommunications network if he has the correct equipment and an agreement with the network operator (Anttalinen, 2003). PSTN, mobile telephone network, internet, radio and television network are all examples of public networks.

a) Telephone Network

The ubiquitous telephone networks that are available all over the world are outstanding examples of public telecommunication networks known as Public Switched Telephone Networks (PSTN). PSTN refers to the global circuit-switched telephone networks that are linked via switching centers. PSTN is a classic circuit-switched telephone network run by national, regional, or local telephony’s operators that provides infrastructure and services for public communications. The PSTN is the global communications infrastructure that transports voice and data locally, nationally, and globally. The vast majority of voice calls are routed through the PSTN. PSTN service is sometimes referred to as POTS to distinguish it from other services supplied by telecommunications networks today. The PSTN is made up of local networks connected by a long-distance network as shown in Figure 9.

PSTN's main characteristics are:

- ✓ the network is fixed so the network's mobility is severely constrained with a bandwidth of 64 kbps,
- ✓ analog access with a frequency of 300-3400 Hz,
- ✓ circuit-switched
- ✓ It can be connected with other networks such as ISDN, PLMN, and PDN.

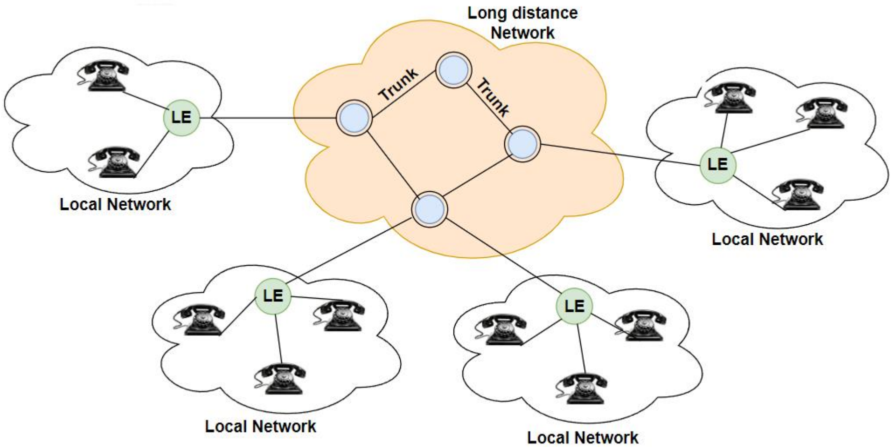

Figure 9. PSTN overview

PSTN is divided into three main parts:

1. The backbone networks
   Backbone Network is the core network that supports the PSTN, which is a network that connects central telephone. It has capabilities to link two interconnected users (switching), provide user identification (numbering), provide call details, the conversation, and the conclusion of the conversation (signaling).
2. The access networks
   A network that connects the central to the customer is known as an access network. The Access Network is divided into four sections: local access network that uses copper cable as the transmission medium, a local access network that uses air as a transmission medium and antennas as information signal transmitters and receivers, local access network that transmits data through optical cable, and Hybrid Fiber Coaxial (HFC) is a local access network that uses both fiber optic and coaxial cable transmission media. In its early stages, the HFC network can be used for three services: analog services (analog services), digital services (digital services), and data services (data services).
3. The interconnection networks

The interconnection network is a private center with features such as a public center used by an institution/company in serving the company's internal communications.

The overview of the modern public switched telecommunications network is presented in Figure 10.

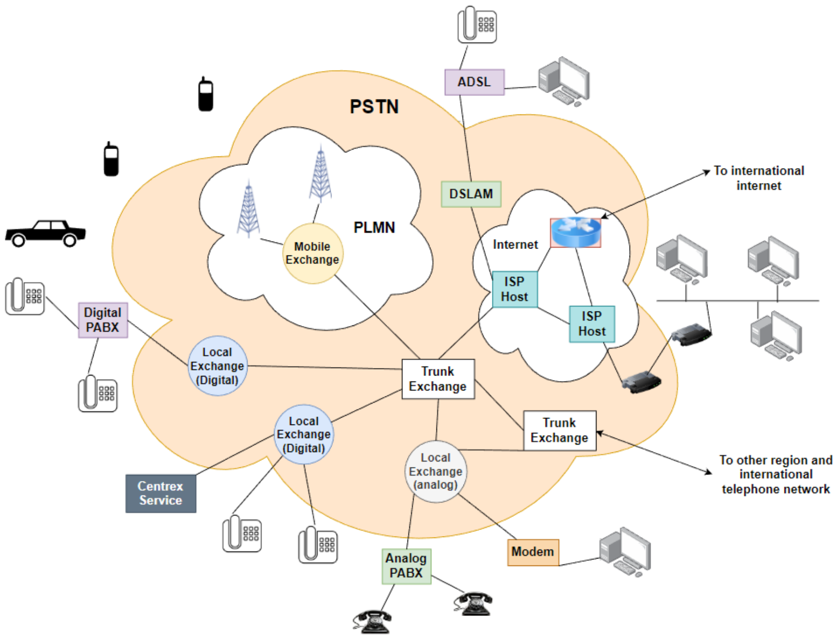

Figure 10. Overview of the modern PSTN

Network Component

The components on Public Switched Telephone Networks are Telephone Central, Main Distribution Frame (MDF), Primary cable, Cable House, Secondary cable, Distribution Point (DP), and Boundary Terminal Box (BTB) as shown on the figure 11.

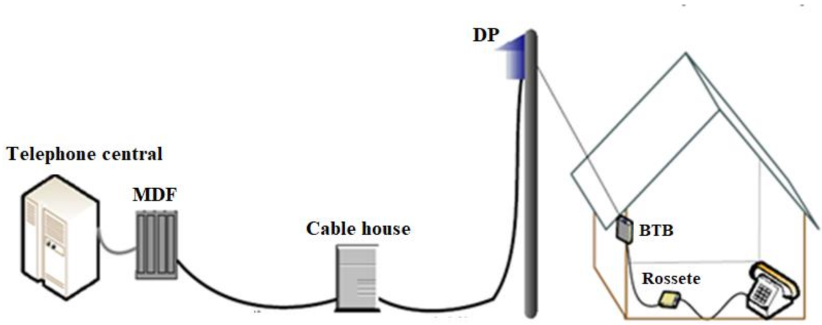

Figure 11. PSTN network component

- ✓ The center for managing the relationship between telephone subscribers are on Telephone Central.
- ✓ Main Distribution Frame (MDF) is in the form of an iron frame to place horizontal and vertical terminal blocks which are connected by using a jumper wire, namely polyethylene copper cable.
- ✓ Primary cable is cable that connects MDF with cable house.
- ✓ Cable house is terminal for primary and secondary cable termination.
- ✓ Secondary cable is which connects between cable house and distribution point.
- ✓ Distribution Point (DP) is cable terminal where the secondary cable is connected to the drain line.
- ✓ Boundary Terminal Box (BTB) is the terminal box in the house is attached to the wall as a continuation of the termination of the distribution point.
- ✓ Socket / rosette is cable terminal connecting the house to the telephone.

Hierarchy

Telephone connections are carried out locally, regionally, nationally, and worldwide. The telephone network structure or topology must have tiers known as the hierarchy. The hierarchical structure of the network helps operators manage the network and it makes the basic principle of telephone call routing straightforward (Anttalinen, 2003). The call is routed up in the hierarchy by each exchange if the destination subscriber is not located below this exchange.

b) Mobile Telephone Networks

Since the first analog networks were deployed, the popularity of mobile communications has expanded at an exponential rate. The concept of publicly available radio coverage for wireless communications regardless of place or time has resulted in higher mobile penetration figures, with more mobile subscribers than landline subscriptions. The area of a mobile network is divided into small cells of only a few kilometers or less across.

The first mobile phone networks appeared in the 1970s, using analog technology and a fairly restricted service. TACS (Total Access Communication Network), AMPS (Advance Mobile Phone System), NMT (Nordic Mobile Telephone), RadioCom2000, and NetzC are early examples of analog mobile phone technology. It uses analog networks, which do not inherently facilitate data transfer. Users could buy modems to transmit data or send faxes, but they were expensive and slow. The handsets were frequently large and had little battery life.

Second generation (2G) mobile phone system development had begun. 2G was executed under the term GERAN (GSM/GPRS/EDGE). The systems are digital, which improves service quality and expands the number of services that networks can serve. GSM (Global System for Mobile Communications), D-AMPS: Digital AMPS (IS-54, IS136), CDMAOne (IS-95), and PDC are examples of digital mobile phone technologies (Public Digital Cellular). Operators of 2G networks have updated their technology to facilitate more efficient data delivery. It is commonly referred to as packet data. 2.5G is the new designation for these technologies, which have enabled operators to offer numerous new and diverse services to subscribers. Third generation (3G) networks were developed in the 1990s and are now being installed all over the world. The fundamental distinction between 2G and 3G networks is the degree of service that a 3G user can expect. Later, the 3G term UMTS was also developed, the packet data services being the primary indicators for the enhanced 3G: HSDPA (High Speed Downlink Packet Access), HSUPA (High Speed Uplink Packet Access), and the combined evolution version of these, HSPA (High Speed Packet Access) (Pentinen, 2015). Further enhancements of

HSPA are indicated by the term HSPA+. Mobile phone technology has always advanced swiftly, and a 4G network has now been installed all across the world. Figure 13, shows the idea of mobile systems generations.

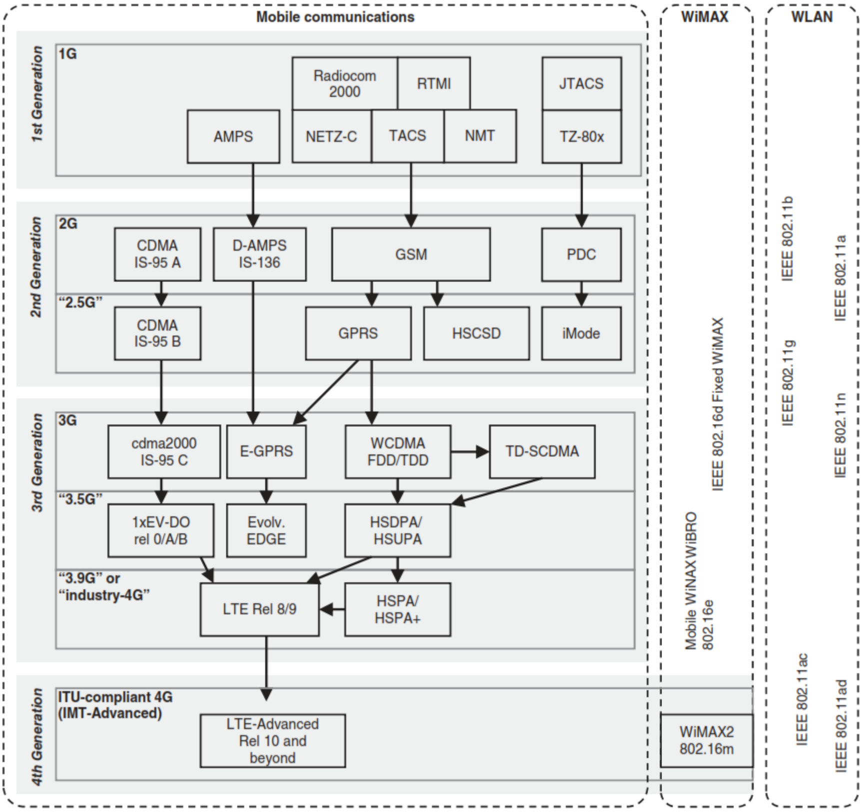

Figure 12. The contents of the 2G, 3G and 4G of mobile communications

Source: (Pentinen, 2015)

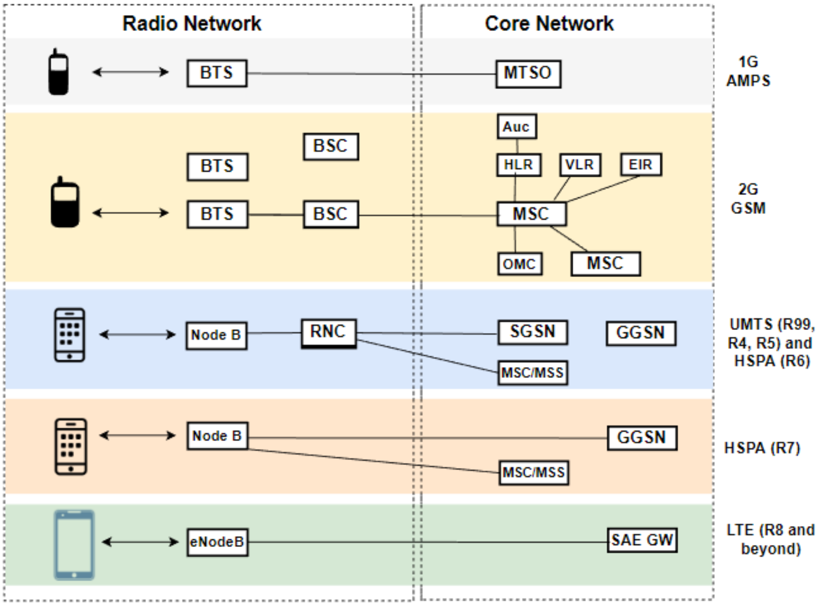

Figure 13. The evolution of network architectures

c) Telex Networks

Telex, or Teleprinter exchange, is the earliest type of data transfer, invented during the Second World War and utilized as a safe and dependable long distance communication method. Telex networks are telegraph networks that connect teleprinters using special dedicated switches. Telex's bit rate is quite modest, 50 or 75 bps, which makes it incredibly robust. It was previously widely utilized, but its significance has diminished as newer messaging systems, such as electronic mail and facsimile, have eroded its market share. The internet today is founded on numerous original telex functions for direct intercountry contact, desktop message, and the Internet Chat type facility.

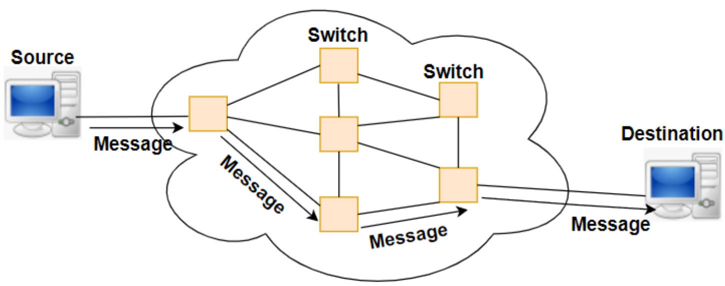

Figure 14. Telex Networks

d) Paging Networks

Paging is a method of sending a message to someone whose exact location is uncertain via a public or private communications system or radio signal. Paging networks can only communicate in one direction. Pagers are low-cost, lightweight wireless communication technologies that allow you to contact customers without speaking. Simple pagers just beep, whereas complex pagers may receive vast quantities of text and show the e-mail message on a screen. The importance of paging systems has decreased in countries where cellular networks, which provide text-messaging services, are widely used.

Paging systems provide four fundamental forms of messaging services: tone, numeric, text, and voice. One-way and two-way paging systems can both provide messaging services. One-way paging systems can only transfer messages from the system to the pager. Two-way paging systems enable for message confirmation and response from the pager to the system.

e) Public Data Networks

Public data networks offer leased point-to-point connections, circuit-switched connections, and packet-switched connections. Leased point-to-point lines are frequently an economical method for connecting the LANs of regional corporate offices. Data transmission circuit-switched networks are not frequently utilized anymore. The X.25 network provides global packet-switched data service. These networks were designed to provide commercial data transmission services, and they have pricing capabilities, allowing the customer's fee to be calculated depending on the amount of data transferred. Because of the growth of the Internet, the importance of these networks has diminished. X.25 e-mail has given way to Internet e-mail. To provide data services to mobile consumers, public wireless data networks such as general packet radio service (GPRS) have been created. Another method used to provide data service in hot locations, such as airports, is wireless LAN (WLAN).

f) Internet

The Internet is a global packet-switched network that evolved from the ARPANET, which was created in the late 1960s by the United

States Defense Department. The ARPANET grew until it became a wide-area computer network called the Internet, which was used in the 1970s and 1980s mainly by academic institutes such as universities (Pentinen, 2015). The Internet does not have charging capabilities, and client pricing is often dependent on the access data rate and a fixed monthly charge. The user-friendly graphical user interface WWW was launched in the early half of the 1990s. The use of the Internet has grown at a remarkable pace after that.

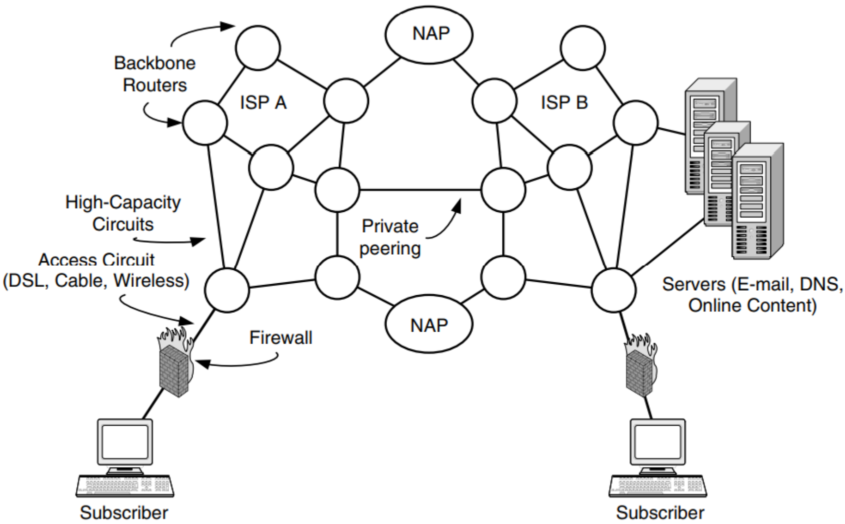

Figure 15. Internet configuration
source: (Green, 2006)

The Internet is now the world's largest information network, and many Internet service providers (ISPs) have sprouted up to provide Internet services to both businesses and consumers. The Internet's growth continues, and expanding commercial services (such as electronic shopping), new access technologies, and integrated audio and video services will all contribute to its future relevance. The figure 15, show illustrates how the Internet is configured.

g) ISDN

ISDN is an abbreviation of “Integrated Services Digital Network”. Basically, ISDN is a way to provide higher speed data transfer over regular telephone lines. ISDN allows data transfer rates up to 128kbps. ISDN is classified into two types:

1. The Basic Rate Interface (BRI) is made up of two full-duplex 64 kbps B-channels and a full-duplex 16 kbps D-channel. This configuration is known as 2B + D. Due to the additional framing, synchronization, and other overhead bits required on the channel, the overall bit rate on a basic access link is 192 kbps. the ISDN-BRI was built as the maximum amount of data that could flow over conventional cable.
2. The Primary Rate Interface (PRI) has 23 B-channels and one D-channel (US) or 30 B-channels and one D-channel (International) (Europe). The primary rate interface (PRI) was designed as the greatest amount of data that could flow over a T-1/E-1 carrier. The ISDN-PRI is primarily used for large-scale voice services. Many private branch exchange (PBX) systems come with their own ISDN hardware and can take a PRI from the phone operator.

The original version of ISDN used baseband transmission. Another version, called B-ISDN, uses broadband and supports data rates of up to 1.5 Mbps. B-ISDN requires fiber optic cables. ISDN technology has been available for some time, but due to expensive tariffs in the past, its use has been limited. Higher rate access technologies, such as xDSL and cable modems, on the other hand, give superior performance and have slowed the rise of ISDN.

h) Radio and Television Networks

For mass communications, radio and television networks are typically unidirectional radio distribution networks. Historically radio and television networks operators did not offer dial-up bidirectional telecommunications services. Cable TV networks created by cable TV providers already provide access to these networks in urban areas. As the telecoms industry has deregulated, these operators have expanded into additional telecommunications services, including landline telephone service and high-data-rate Internet access.

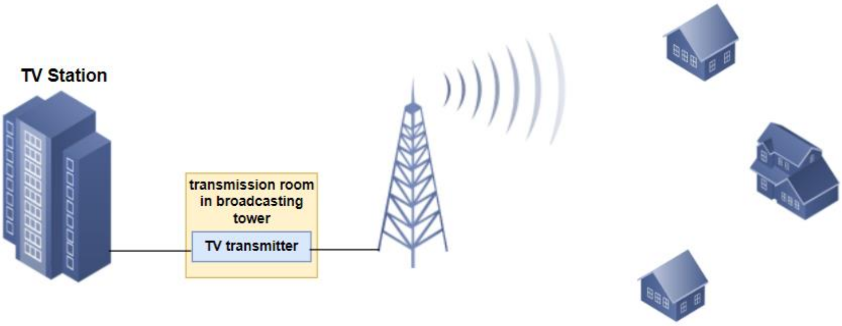

Figure 16. TV broadcast

2. Private or Dedicated Network

Private or dedicated networks are established and designed to meet the communication demands of certain businesses. The networks usually own and operate by themselves. The nature of private network communication is point-to-multipoint or group communication. The services provided are a customized blend of voice, data, and, for example, unique control information.

a) Voice Communication Networks

Private dedicated voice networks are utilized by the police and other emergency services, as well as taxi companies. They are referred to as private or professional mobile radio (PMR). Typical PMR is point to multipoint operation or group working. Old days, train firms also have private fixed telephone networks that run alongside the tracks through cables. Currently the communication system for train is growing with the presence of digital network technology wireless.

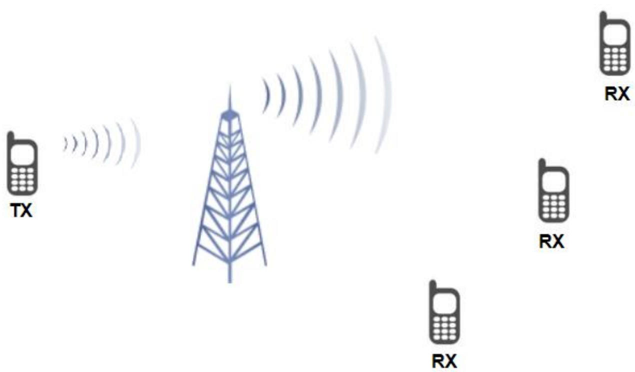

Figure 17. Typical PMR point to multipoint operation

b) Data Communication Networks

Today, data networks serve as the foundation for a large portion of telecommunications services. The transition from circuit switched, analog telephony systems to digital and packet-based systems has been dramatic. Data communication networks are dedicated networks especially designed for the transmission of data between the offices of an organization (Pentinen, 2015). They can integrate LANs (Local Area Network) with mainframe computers that transmit data to branch offices. Banks, hotel chains, and travel agencies, for example, each have their own data networks. The LAN can be physically built with twisted pair cable, coaxial cable, or optical fiber cable and configured as a single bus or as a series of buses in a tree, ring, or star topology, posing issues for transport network dimensioning.

A MAN is a corporate network that consists of numerous interconnected LANs at various locations within a 3–30 miles radius. The interconnection of LANs, often referred to as the sub-network, can be accomplished by the use of leased lines or a public data service provided by the network operator, such as ATM, Frame Relay, or SMDS. Another notion is the WAN, which connects widely distant LANs and MANs (usually over lengths of more than 30 miles).

3. Virtual Private Networks

Virtual Private Network (VPN) has a variety of meanings, but it usually refers to speech or the Internet. Virtual Private Network (VPN) provides a service similar to an ordinary private network, but the systems in the network are the property of the network operator (Pentinen, 2015). Setting up and maintaining an organization's own private network is prohibitively expensive, VPNs provide another way for businesses to lease resources from public network operators. The public switched telephone network provides all connectivity within the virtual private network, with full network element sharing by the 'private network' and public traffic. VPN technology is utilized for phone services such as corporate PBX/PABX networks. The primary idea behind a VPN is to establish a secure, point to point connection over the network between communicating organizations. A VPN tunnel employs encryption and authentication to ensure that communications are unreadable even if they are intercepted.

An important application of VPN is intranet use. An intranet is a private data network that uses open Internet technology. Physically, an intranet may be made up of many LANs at different sites. To interconnect these LANs, a VPN is established to provide data transmission between sites through the public Internet network (Pentinen, 2015). In an intranet, firewalls are deployed at the interface between each LAN and the public Internet. The firewalls authenticate communicating parties and encrypt and encapsulate data for transmission from one office to another over the public Internet.

C. Network Terminals

A terminal in the context of telecommunications is a device that becomes an end-user in a telecommunications system and serves as an information source interface between the user and the system. The terminal has the ability to call and receive alternately, as well as call and receive only. Telephones, fax machines, radios, televisions, printers, and modems are examples of terminal equipment.

(a) Telephone (b) Cell Phone (c) Fax (d) Computer

Figure 18. Some of end instrument

There are some terminals classifications based on the type of information or signal: terminal for both text and images are fax machines, terminal for voice is radio and telephone, terminal for video is television, terminal for data is modem, and terminal for multimedia is computer.

1. Voice Terminals: Radio and Telephone

Radio is one type of one-way communication device whose role is to receive messages (news, information and entertainment) from the transmitter. The radio is classified into two types based on the type of modulation used, namely AM radio if the modulation used is amplitude modulation, which has the feature of modifying the amplitude of the modulated signal in response to the fluctuation of the amplitude of the information signal. FM radio is the second type of radio if the modulation utilized is frequency modulation, which means that the frequency modulated signal fluctuates in response to changes in the amplitude of the information stream.

The telephone is a type of communication device that is used to send voice messages (especially messages in the form of conversations). Most telephones work by sending electrical signals through the telephone network, allowing users to converse with one another. Along with the rapid development of technology, mobile phones have now been developed. A mobile phone, also known as a handphone or a cellular phone (cellphone), is an electronic communications device that has the same basic characteristics as traditional telephones but can be taken everywhere (portable) and does not require a network connection.

2. **Video Terminals: Television**

   Monochrome television was developed prior to World War II. Televisions were first sold commercially since the 1920s. However, it did not achieve significant market penetration until several years after the war. Television is a telecommunication device that functions as a receiver for broadcast images and sound in monochrome (black and white) or in color. The word television is a combination of the word ‘tele’ from the Greek which means ‘far’ and ‘visio’ from Latin which means vision. So that television can be interpreted as a long-distance communication tool that uses visual media. Televisions were first sold commercially since the 1920s. TV broadcasting is mostly spread via VHF and UHF radio waves.

3. **Data Terminals: Modem**

   The term modem is an acronym for modulation/demodulation. Modems are critical components of data communications networks. It’s required to support long-distance digital communications. Modem convert digital signals from data terminal equipment to analog signals for transmission across analog communications facilities, and then reverse the process. Modem architecture can be divided into four major functional units: data pump that in charge of carrying out the two basic tasks of a modem (modulation and demodulation), Controller is frequently referred as the modem's CPU that handles the terminal's command interface and various other supervisory and ancillary functions, Data Access Arrangement (DAA) containing the analog circuitry that electrically isolates the modem from the telephone network as well as the physical interface to connect to a plain old telephone system (POTS) line, and the asynchronous serial interface between the modem and the terminal is known as the terminal interface.

Figure 19. Role of Modem

4. **Text and Pictures Terminals: Fax**

   Facsimile or fax sometimes known as telecopying or telefax (short for telefacsimile), is the telephonic transfer of scanned printed information (including text and images), typically to a telephone number linked to a printer or other output device. The original document is scanned with a fax machine or telecopier, which interprets the contents in text or images as a single fixed graphic image, converts it to a bitmap, and then transmits it as audio-frequency tones over the telephone network. The receiving fax machine decodes the tones and reconstructs the image on paper. Fax machines were used in office contexts in the 1980s and 1990s, but Internet-based technologies such as email and the World Wide Web progressively rendered them obsolete.

Review Questions

Q1. Explain telecommunications networks classified based on data rate and response speed?

Q2. What is network terminal for data and multimedia?

Q3. The telephone network structure or topology must have tiers known as ………

Q4. Explain the two types of ISDN!

Q5. Draw the 4G network architectures!

CHAPTER 3
SIGNALING

A. Definition of Signaling

Signalling is the process of sending control information over landline and mobile networks to monitor, control, route, and set up sessions between devices (Dodd, 2019). Signalling is utilized in public landline, mobile, and Internet networks, as well as for intercarrier communications and billing. The main functions of signalling are connection establishment (call setup), channel monitoring (supervision), and connection disconnection (path disconnection). Signalling in current signalling systems, such as Common Channel Signalling (CCS7), incorporates extra activities such as network administration, application of additional features (supplementary service), operation and maintenance functions, and so on.

B. Signaling Classification

Signaling can be classified into several types based on the classification or classification point of view. Signaling classification or signaling classification based on the following are:

1. Based on the utilization of voice or data channels and signaling channels, signaling is classified into:
    a. Channel Associated Signaling (CAS)
    b. Common Channel Signaling (CCS)
2. Based on its function, signaling is classified into:
    a. Line Signal or Supervisory Signal are signals whose function is to monitor channel conditions and control channels. For example: idle, blocking, seizure, clear forward, forced release, etc.
    b. Signal registers are signals whose function is to carry information about the telephone number being called or caller, class or category of the caller, the caller's free or busy condition and control signals (reverse direction) for controlling the signaling register process. Sub-classification of signal registers in forward direction, contains information of the destination number is called Group I, calling line category is called Group II, and the number of the caller is

called Group III. Sub-classification of signal registers in the backward direction, contains the information of control over the forward signal (called Group A), and condition of the called customer (called Group B).

3. Based on the mode of transmission, signaling can be distinguished:
   a. Link-by-link
      The transmission of a signal block (complete) from the originating center is carried out through one or more transit centers by relay (link-by-link) to the destination center.

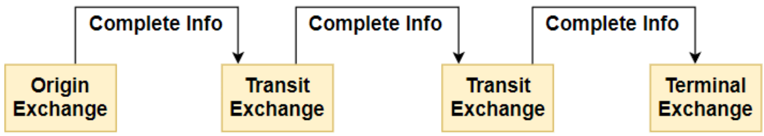

Figure 20. Link-by-link signaling mode

   b. End-to-end
      The originating center sends only part of the information (necessary for routing) to each transit center through which it passes. After the origin center is connected to the destination center, then the routing info is sent.

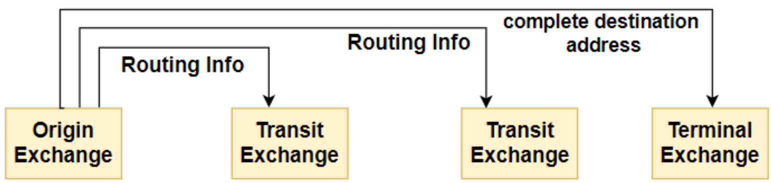

Figure 21. End-to-end signaling mode

   c. Enblock
      Same as link-by-link mode, where the complete signal is sent in a relay. The terms enbloc is only known in CCS.

   d. Overlap
      The transmission mode is like link-by-link where the signal information is sent not all at once (complete) but gradually (partially). The terms overlap is only known in CCS.

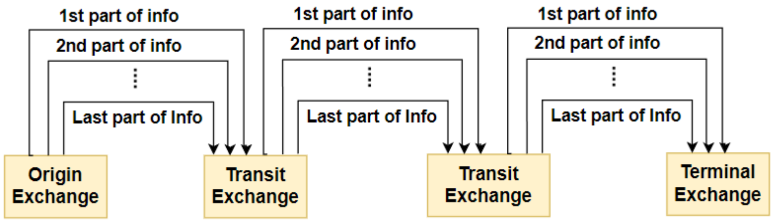

Figure 22. Overlap signaling mode

4. Signaling based on delivery direction is classified into forward signal and backward signal. The forward signal is sent in the forward direction, that is, the direction from the caller to the called (destination). And for backward signal is sent in the backward direction, that is, from the direction called to the caller.
5. Signaling based on the shape (curve) of the signal is classified into DC and AC. DC signals contain only positive or negative components or 0 volts or can be in the form of a polarity reversal (reverse polarity). Furthermore, when viewed from the timing: it can be continuous, a certain duration of time, or in the form of a series of pulses. AC signals containing positive and negative components periodically (frequency).
6. Signaling based on signal characteristics is classified into analog, and digital.
7. Signaling based on network segments is classified into:
   a. Subscriber Signalling
      Subscriber signalling classified as CAS. An example of subscriber signalling on analog channel is Z Interface (Loop Signalling, Address Signalling, Decadic Pulse, and Dual Tone Multiple Frequency). Then an example of subscriber signalling classified as CCS on digital channel is DSS1 (Digital Subscriber Signalling No.1).

   b. Inter-exchange Signalling
      An example of inter-exchange signalling classified as CAS are R Series (R1, R2) and C Series (C1 up to C5). C6 and C7 (CCS6, CCS7) are example of inter-exchange signalling classified as CCS. The C7 signalling system is often referred to as CCS7 or SS7.

8. Signaling by area scope is classified into:
   a. Regional scope for the dominant signaling system used in the scope of some international regions (regional/continental) such as the standard signaling system with the notation R (R1, R2).
   b. The international scope is the dominant signaling system used in the entire international area, such as the standard signaling system with the notation C (C1, C2).

C. Channel Associated Signaling (CAS)

Channel Associated Signaling (CAS) is a signaling system in which each voice or data channel has its own (associated) signaling channel. This means that each signaling channel is owned by each voice or data channel exclusively/monopoly and cannot "borrow" from each other. Speech information and signaling information flow through the same path. Several kinds of CAS Signaling are carried out simultaneously on the speech channel (DC signaling, in-band). Signaling is carried out on the same channel as speech but uses a different frequency (out-band).

Signaling in CAS is divided into two types: signaling between central systems and signaling on subscriber lines. CAS signals on subscriber lines can be divided into three groups, namely: Line Signals, Address Signals, and Audible Signals. The signal sharing scheme in the three groups can be shown in the figure 24.

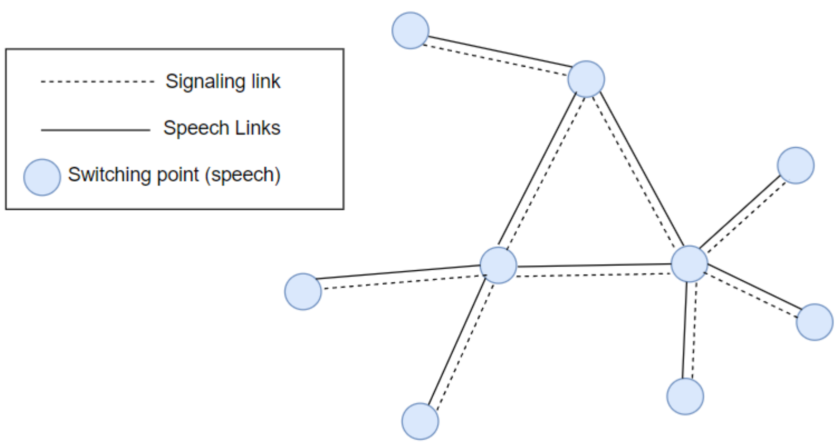

Figure 23. CAS

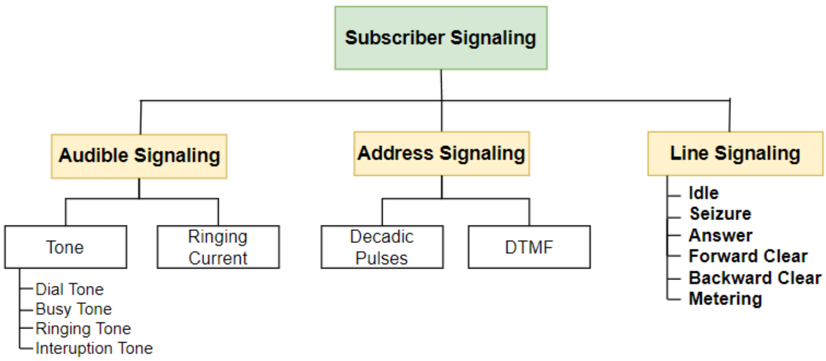

Figure 24. Signal sharing scheme on analog subscriber lines

In signaling between central CAS systems, there are Line Signals and Signal Registers which are an inseparable pair. The functions of line signal is to monitor and control the channel while the signal register carries information related to the relationship building process such as destination address, caller class or category, free or busy status of the called subscriber, signaling process control messages, etc. We can see the schematic types of inter-central signaling in CAS in the figure 25.

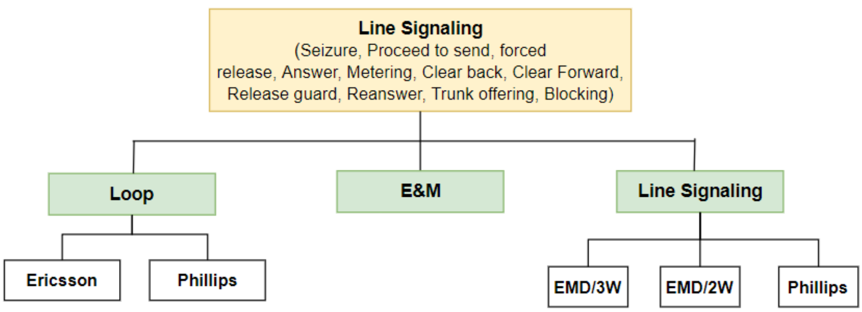

Figure 25. The schematic types of line signaling in CAS

D. Common Channel Signaling (CCS)

Common Channel Signaling (CCS) is a signaling system in which a number of signaling channels are shared (common) by a number of voice or data channels. Common-channel signaling became possible after the introduction of stored-program controlled exchanges (Bosse, 2002). CCS signaling is more powerful, flexible, and also faster than CAS signaling. Signaling uses a separate channel from the channel to transfer information on CCS. There is a separate signaling network as shown on figure 26.

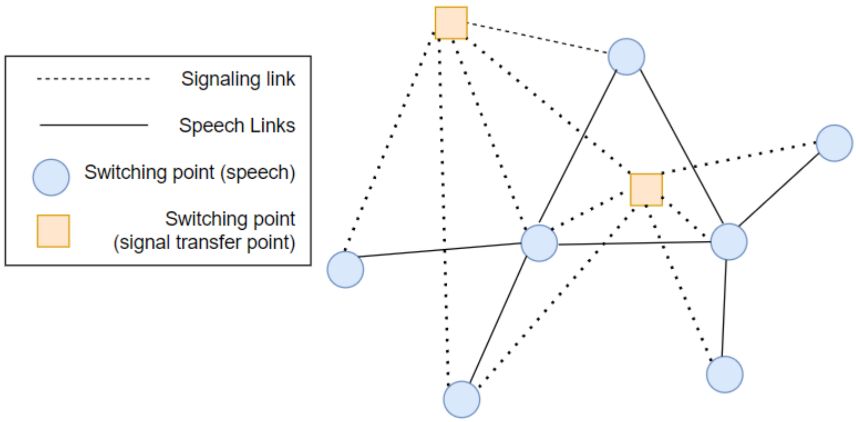

Figure 26. CCS

1. Terminology in SS7 Network

C6 or CCS6 is the first common channel signaling system recommended by CCITT on 1980. The revision of C6 is C7 often referred to as CCS7 or SS7. The overall goal of SS7 is to provide an internationally standardized general purpose common channel signalling system to meet the information transfer requirements of inter-processor transactions with digital communications networks for call control, remote control, network database access and management, and maintenance signalling. It ensures that information is transferred in the correct order, without loss or duplication.

The SS7 network is made up of signalling points (nodes) known as Signalling Points (SP) and Signalling Link transmission lines. The nomenclature used to name elements in the SS7 network is as follows:

- ❑ Signaling Points (SP)

  Signaling Points (SP) are any network nodes that can control/process signaling messages. Examples of Network Signaling Points: Switching Center, Operation & Maintenance Center (OMC), Service Control Points (SCP), Signaling Transfer Points (STP), Etc.
- ❑ Signaling End Point (SEP)

Signaling End Point (SEP) are a Signaling Point that is only able to process signaling messages that are directly addressed to it, but does not have the ability to transfer SS7 messages addressed to other SPs. In some discussions, the term SEP is often written as SP, so that in the network there are only two signaling point terms, namely SP and STP.

- Signaling Transfer Point (STP)
  It is a signaling point that can send signaling messages to other signaling points.
- Signaling Transfer Termination Point (STEP)
  It is a Signaling Point with STP and SEP (combined) capabilities.
- Signaling Link
  Signaling Link is a conduit for transmitting signaling messages between two Signaling Points.
- Link set
  Link set is a number of signaling links that connect two signaling points directly.
- Link Group
  Link group is a collection of links in a link set that have the same or identical characteristics.

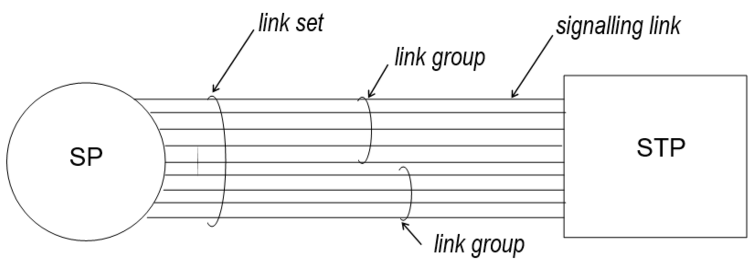

Figure 27. Signaling link, link set, and link group

- Originating Points (OP)
  Originating Points is the Signaling Point or the origin of the signaling message sender.
- Destination Points (DP)
  Destination Points is the Signaling Location or the signaling message's final destination point.
- Route signaling

Route signaling is a predefined message path. The path consists of STP and a signaling link between the Originating Point (OP) and Destination Point (DP).

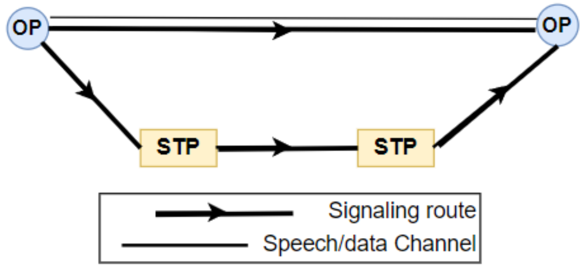

Figure 28. Signaling Route

2. Signaling Mode

There are two signaling modes based on the setup of the data/speech channel and the signaling link, namely Associated and Non-Associated. Non-Associated Mode can be either partially or completely non-associated.

a. Associated Mode

In associated mode, the signaling message is transferred via a signaling link whose path is the same as that of the speech circuit group.

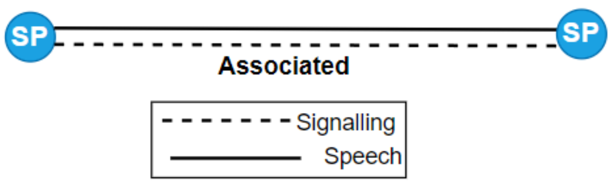

Figure 29. Associated mode

b. Non-Associated Mode

In this mode, the signaling message between two SPs is routed through one or more STPs, taking a different path than the voice/data circuit group. There are two types of non-associated modes:

- Quasi Associated

  In quasi associated mode, the message path is predetermined.

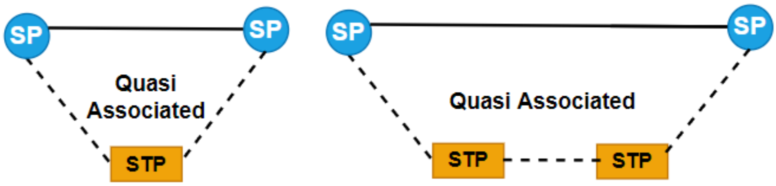

Figure 30. Quasi Associated

- Fully Non-Associated
  In this mode, messages are transferred over any available path in the network and cannot be predefined.

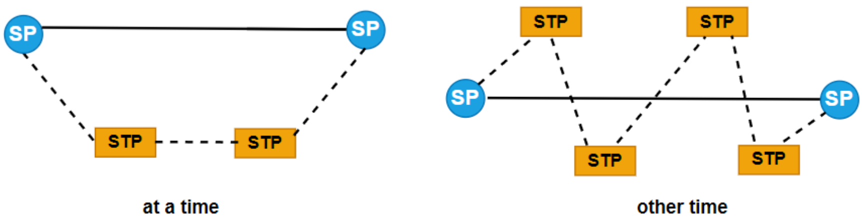

Figure 31. Fully Non-Associated

In practice, because the MTP feature of SS7 does not have the ability to rearrange the order of received messages and other problems such as dynamic routing, etc., the Fully Non Associated mode cannot be applied, so the Associated and Quasi Associated modes are commonly used.

Associated and Quasi Associated Mode configuration examples shows on the figure 32.

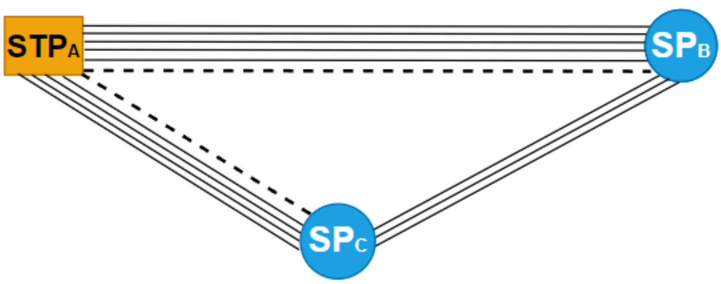

Figure 32. Associated and Quasi Associated Mode

3. Signaling Points (SP) Numbering

Signaling Point (SP) in the SS7 network must be allocated an identification or numbering called a Signaling Point Code (SPC). In SS7, the central identity of the origin (sender) is known as the Originating Point Code (OPC), and the central identity of the destination is known as the Destination Point Code (DPC). This information is stored in the SIF (Signaling Information Field) field of the signaling message frame. The following must be considered when designing the SP numbering:

- Easy to use
  For this purposes numbering uses a widely known or common code, i.e. decimal code instead of binary or other codes.
- Systematic
  In certain ways, related to the area code and the Office Code.
- Adaptable
  This ensures that future expansions will be simple to adapt without fundamentally altering the numbering pattern or framework.

ITU-T (in Q.704) regulates two things in terms of numbering SPC:

a. Signaling Point Code (SPC) length: 14 bits (in decimal = 00000 – 16384 5 digits).
b. Network Indicator (NI): 2 bits.
   That is, the information in the SS7 message (in the SSF field) indicating the network scope, is allocated as follows:
   - 00 (decimal = 0) : International Center
   - 01 (decimal = 1) : reserve for international
   - 10 (decimal = 2) : National Center
   - 11 (decimal = 3) : reserve for national

The SP that requires to be issued a numbering code in the PSTN or ISDN network are the Local Exchange (LE), Local Tandem (LT), and Toll Exchange (TE). While on the IN network, it is the Service Control Point (SCP) and Service Switching Point (SSP) that require a numerical code.

4. SS7 Architecture

Because the SS6 architecture is solely meant for connection-oriented services, it cannot be developed with the existing network structure due to the constraints of the applications that it can handle. In other words, SS6 cannot provide data communication services at OSI layers 4 through 7. To overcome this, corrections were made to SS6 in 1984 by inserting additional functional elements, namely SCCP (Signaling Connection Control Part) and TCAP (Transaction Capabilities), the results of which are known as Signaling System 7 (CCS7), the architecture of which is shown in the figure 33.

SS7's components are structured in a four-level hierarchy. A higher-level part is said to be a user of services offered by a lower-level part. This arrangement is similar to the seven-layer structure of the open systems interconnection (OSI) protocols for data communications (Bosse, 2002). For call setup, charging, and supervision information, SS7 employs a separate packet switched network.

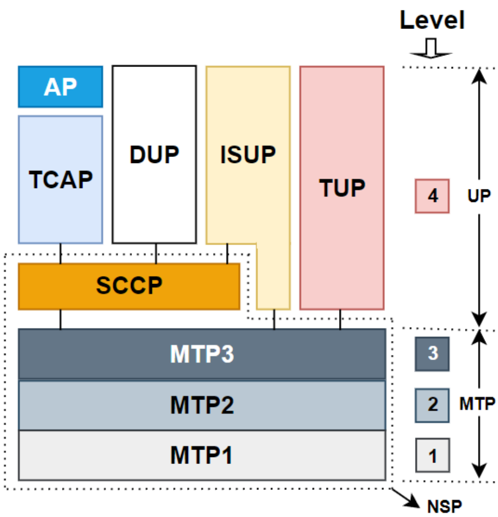

Figure 33. SS7 Architecture

Review Questions

Q1. The SS7 layer, which is responsible for routing, is……………

a) Link Function

b) Network Function
c) SCCP
d) Data Link Function
e) TCAP

Q2. The classification of signaling based on network segment are..............

a) Subscriber signaling and Inter-exchange signaling
b) Regional signaling and International signaling
c) Line signaling and Register signaling
d) CAS and CCS
e) Link-by-link and end-to-end

Q3. Signaling Point that is only able to process signaling messages that are directly addressed to it, but does not have the ability to transfer SS7 messages addressed to other SPs is called as …………

a) Signaling Points (SP)
b) Signaling End Point (SEP)
c) Signaling Transfer Point (STP)
d) Signaling Transfer Termination Point (STEP)
e) Signaling Link

Q4. The SS7 layer that functions to perform routing is .... What are the main functions of signalling?

Q5. What is the routing pattern that is utilized for reliability?

CHAPTER 4
SWITCHING

A. Definition

Switching, or the capacity to convey a signal from its source to the correct destination by selecting a suitable network path, is another important feature of a telecommunication network. Switching is defined as a mechanism for connecting the input channel to the output channel so that information (telecommunication traffic) can be streamed from the sender to the receiver. Definition of switching based on the ITU is the establishing, on demand, of an individual connection from a desired inlet to desired outlet within a set of inlets and outlets for as long as required for the transfer of information. Switching can also be interpreted as the process of transferring information from one point to another. In general, switching refers to the process of establishing a relationship between two telephone users so that they can communicate with one another.

B. Switching Elements

A switching element is a network component that sends data packets from the input terminal to the output terminal. A terminal can be defined as a point included within a switching element. Signaling, control, and crosspoint are examples of switching elements. Each switching element has a specific function.

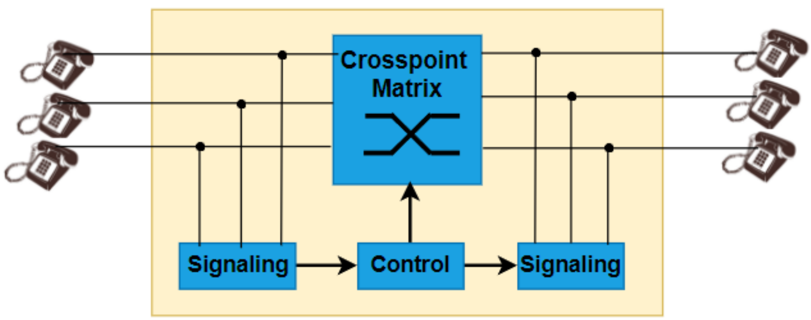

Figure 34. Switching Elements

The function of signaling on switching are to receive requests from callers and checking the status of the caller (idle or busy). When control is to determine which channel should be connected. And the function of crosspoint is to establish a connection between two points (make a connection between the caller and the called).

C. Switching System

Switching System is combination of regulated and controlled switching elements so that they can establish a communication link between 2 separate nodes over long distances. Switching systems have evolved through five generations, each providing additional functionality that were either prohibitively expensive or impossible to implement with their predecessors.

Manual switching was the first switching mechanism used in communications networks. Both telegraph and telephone networks used it. An operator on a manual switchboard set up telephone connections by connecting a patch cord into the appropriate jacks. The switchboard that can be used in this system are the Magneto Board or Local Battery (LB) and the Central Battery Connection Board (Common Battery, Central Battery, CB). The LB switchboard is connected to the subscriber's telephone set through a subscription circuit and has a primary cell for voice and a buzzer current generator for calls to the dial board. Because of its ease of servicing and maintenance, the CB junction board is preferred over the LB junction board. Manual switching was replaced by automatic switching on 1991. There are two types of automatic switching systems:

1. Electromechanical

   Initially, electromechanical switching technology was used in automatic switching offices. In the telephone network, three types of electromechanical switching systems were deployed. The first one employed A. B. Strowger's automated telephone selector, which was patented in 1889. Keith and Erickson later invented the Strowger selector in 1899, which was widely used in telephone offices for many years. After the way the selection worked, these systems were dubbed step-by-step switching systems.

   The connecting process is carried out digit by digit (step by step) by each selector level in a step-by-step automatic center. The advantage of this step-by-step approach is that if one of the control sets is disrupted (damaged), it will not have a substantial impact on the overall central job because each switching set includes a control set. Meanwhile, the disadvantage is that switching equipment and control units must be given in big quantities since they are still in use throughout the connection; a large space is necessary to accommodate a large number of equipment; and programs for particular facilities are difficult to accomplish. Due to its limited capabilities, step-by-step switches are only used for telephone exchanges with small capacities.

The last types of electromechanical switching systems were common control. The common control automated central is a type of central electromechanics in which the pulses are initially stored in a register before being connected to the selectors, as in the step-by-step system. The selector will only work on contacts, if the selected channel is free. The benefit of a common control central system is that the number of control units required is less than the number of switching units, and the space required is less than that of a step-by-step system. The disadvantage common control is that if there is a disturbance or damage to the control unit, it will interfere with the smoothness of the connection, because only one control unit is used to supervise several control sets.

2. Electronic

   The control function of the electronic switch system is performed by a "stored computer program", although the switching function is still electromechanical. SPC is divided into two categories: analog and digital.

   - ❑ A semi-electronic SPC (SPC Analog) central, in which the connection process is controlled by a program stored in the processor (SPC), while subscriber interactions remain analog.
   - ❑ Digital full-electronic SPC automatic center, in which the connection process is controlled by a program stored in the processor (SPC), and the processor and the cross-section of the customer interaction are already digitally operating.

   The speed with which this SPC system connects is one of its most notable features. If the unit of time in an electromechanical automaton is milliseconds, the connecting procedure in an SPC center is measured in microseconds.

The following figure is the summary of the classification of switching systems.

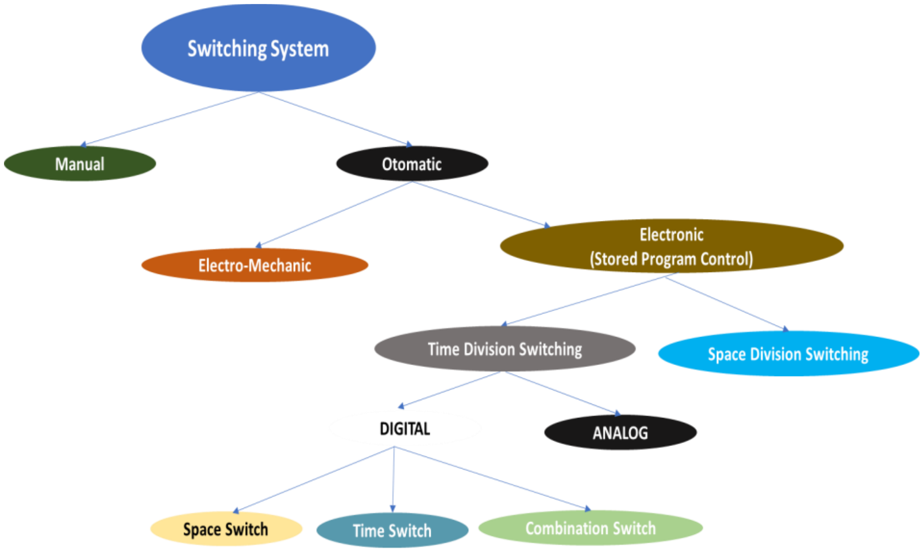

Figure 35. The classification of switching systems

NOTE: The switching system must meet certain requirements, including: switching system must have high availability, must have a fast response to switching and network devices, has a low failed time, and high security.

D. Switching Techniques

Based on the premise of how the communications circuit between the communicating devices is created, we can split data connections over a telecommunications network into distinct groups. Within the switched category there are two subcategories, circuit- and packet-switched networks, both of which are utilized for data transfer.

1. Circuit Switching

Circuit switching occurs when two nodes connect with each other across a dedicated communication path. There must be a predetermined path from which data will be sent, and no other data will be allowed. Setting up on circuit switch connection requires three steps: link setup, link hold-up, and link release. To put it another way, in circuit switching, a data transfer circuit must be constructed before data can be sent.

Circuit-switched networks provide fixed bandwidth and very short and fixed delay (Anttalinen, 2003). Circuit-switched is the most widely used technology for voice telephone, video telephone, and video conferencing. It has inflexible for data communications that need for transmission data rate is far from constant and varies greatly over short time periods. PSTN and ISDN are two examples of circuit-switched services.

2. **Message Switching**

   The message are store and relay from one switching center to the next center which is known as message switching. Rather than using circuits only for messages, messages are sent via the store-and-forward mechanism. It also known the term STORE and FORWARD. Message switching was the forerunner to packet switching, in which whole messages were routed. Message switching is commonly used in today's data networks, whether they be packet-switched or circuit-switched. Email messaging is an example of message switching.

3. **Packet Switching**

   Packet switching is a digital networking communication mechanism that divides all sent data into packets and sends them via a shared media. A header and payload are the two parts of a packet. The header contains data that the network hardware uses to route the packet to its intended destination. The application program extracts the payload at the destination and uses it.

E. Switching Hierarchy

The switching office, also known as an exchange, was once placed at a central location in a service area and supplied switched connections to all customers in that area. As a result, central offices are still commonly referred to as switching offices. As telephone density increased and subscribers demanded longer-distance connections, trunks connecting the central offices were needed to connect the individual service areas. New switches were needed to interconnect central offices as traffic grew, and a second level of switching, trunk or transit exchanges, emerged. National networks now feature many switching levels. The actual implementation of the hierarchy and the number and names of switching levels differ from country to country (Anttalinen, 2003).

The network's hierarchical structure aids network management and simplifies the basic premise of telephone call routing: if the target subscriber is not situated below this exchange, the call is routed up the hierarchy by that exchange. This fundamental basic idea of routing up and down in the switching hierarchy is supported by the structure of the telephone number. The following figure shows an example of a possible network hierarchy.

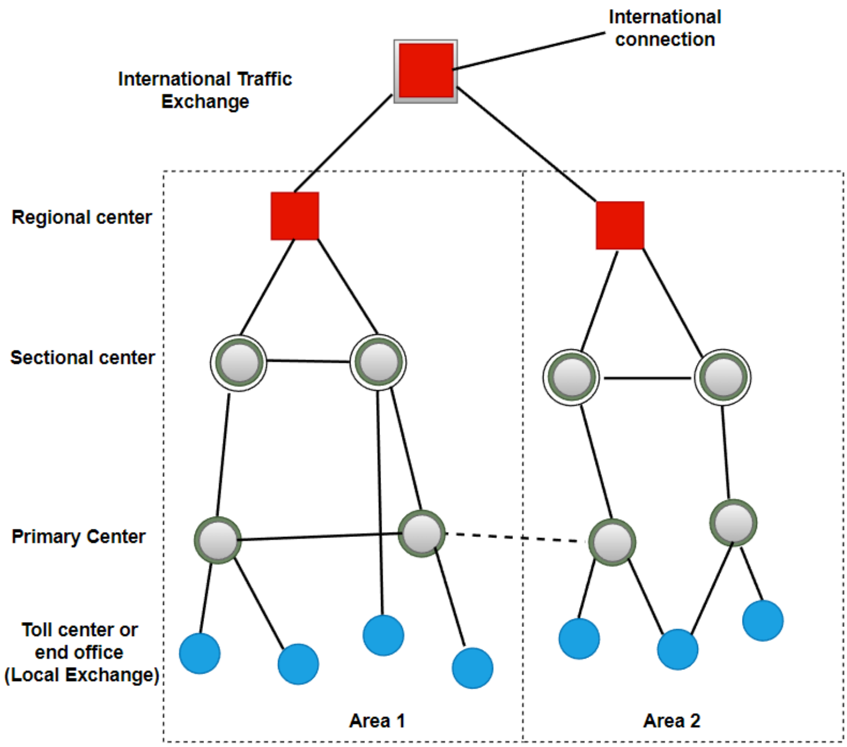

Figure 36. An example of switching hierarchy

Above local exchanges, the national switching hierarchy contains numerous tiers of switches. A simplified network layout in which higher levels than local exchanges are represented by a single level of trunk exchanges. Local exchanges are linked to trunk exchanges, which provide a network of connections from each client to any other subscriber in the country.

F. Softswitch

Softswitch is a general term for a new approach to telephone switching that has the ability to connect circuit networks with packet networks, including fixed telephone networks (PSTN), IP-based internet, cable TV and cellular networks. The advantages of implementing a softswitch include lower costs, improved service supply, and easier migration to IP networks.

A softswitch's architecture is variable and varies depending on the manufacturer. Softswitch is made up of numerous component, including:

1. **Media Gateway Controller (MGC) or Call Agent (CA)**
   Media Gateway Controller (MGC) is often refer to as a Call Agent (CA) is used in centralized architectures. The Media Gateway Controller (MGC) is responsible for managing all service and communication sessions, regulating the interactions of other network elements, and bridging networks with various characteristics, such as PSTN, SS7, and IP networks.
2. **Media Gateway (MG)**
   Stations in a softswitch network connect to an MG. Under the direction of a MGC, it manages supervision, provides ringing and dial tone, plays tones, opens ports, and initiates and releases connections. All of the call-processing elements of a circuit switch must be present in the softswitch, but they may be located on different servers. Except for the option of solo capabilities, the MG has little intelligence. The MG can be set up to play audio or video messages as well as provide advanced services such as interactive voice response and multimedia conferencing.

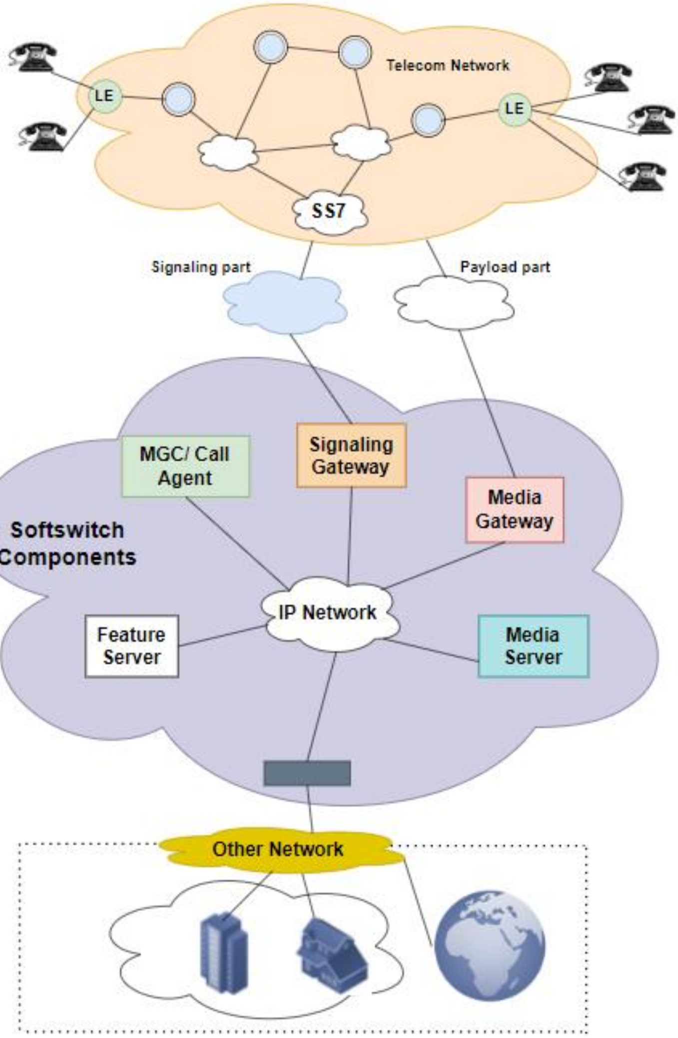

Figure 37. Softswitch component

3. **Signaling Gateway (SG)**
   The Signaling Gateway (SG) is an MGC-controlled bridge between the SS7 network and the IP network. SG only handles SS7 signaling.
4. **Feature Server (FS)**
   A feature server is a server that hosts a series of business services at the application level. A business application server is another name for this.
5. **Media Server (MS)**

The Media Server (MS) is responsible for providing media capabilities to the softswitch. The media server, for example, will be in charge of responding to voice responses.

Switching, control, signaling, and interface are just a few of the features available in softswitch. The softswitch's first switching function is to link IP nodes; in addition, the softswitch can connect and disconnect IP-PBX and PSTN to handle traffic in the form of data, voice, and video. The Media Gateway Controller is in charge of controlling and signaling (MGC). MGC is responsible for routing, validating, and providing access to users, as well as creating PSTN signaling routes. The last function is the interface function by the Application Programming Interface (API) which makes it possible to add or develop servers that are used to add new services.

Review Questions

Q1. A network component that sends data packets from the input terminal to the output terminal is called…………….

Q2. The switching technique that store and relay from one switching center to the next center which is known as ………………..

Q3. What are the requirements that switching system must fulfill?

Q4. Asynchronous Transfer Mode (ATM) is a type of switching ....

Q5. Explain some of softswitch component!

CHAPTER 5
QoS

A. Introduction to QoS

A network operator's or service provider's principal goal is to offer the quality of service (QoS) to its clients or users. Of course, users want the highest possible QoS, but operators must weigh the labor and equipment expenses of meeting specific requirements against the price that customers are willing to pay. QoS encompasses both network-related and non-network-related factors. Time between receiving an order and providing a service to a new customer, time to repair issues, and billing accuracy and convenience are examples of the latter. The performance of the network affects network-related elements (for example, congestion and call clarity). The interrelationships of the elements impacting QoS are illustrates in Figure 38, which shows non-network and network-related components.

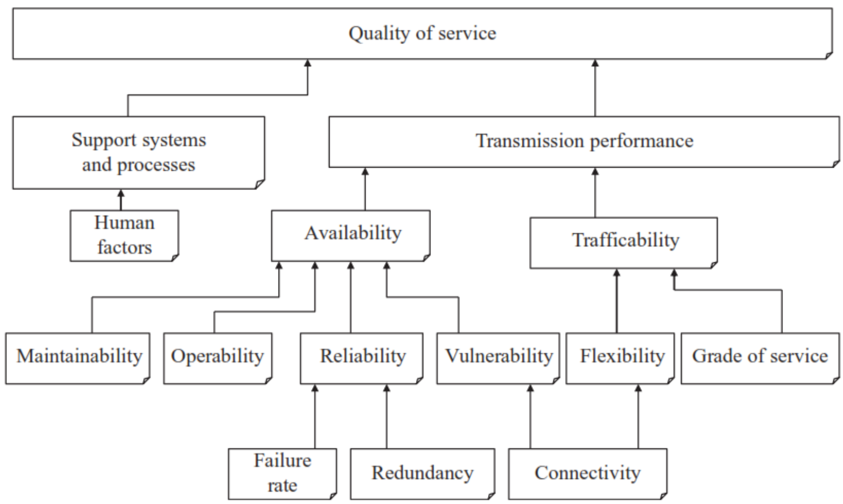

Figure 38. Factors affecting quality of service
source: (Valdar, 2017)

The first factor affecting network performance is the extent to which the network is available for service. The so-called 'trafficability,' which is a measure of how easily telephone calls, data packets, or even permanent transmission pathways for leased lines may be routed across the network, is another key aspect determining network performance. Measures such as grade of service (GoS), which indicates the likelihood of calls failing due to network congestion, determine the level of trafficability for telephone service.

B. QoS Definition

In the world of telecommunications, quality of service (QoS) is described as a collection of particular needs delivered by a network to users that are required to achieve. The users specify their performance requirements such as delay or packet loss, and the network bandwidth. Each service model has its own set of quality-of-service parameters. In the corporate world, the quality of a service can make a difference. Its parameters and metrics are required to provide an indicator of how well a service or product is doing, and hence should be considered when comparing services provided by other service providers. When service features and prices are comparable, quality becomes the differentiator for consumers, and service providers can utilize quality to have an image of well-thought-of provider. Simply said, put, QoS is the combination of network performance and non-network performance.

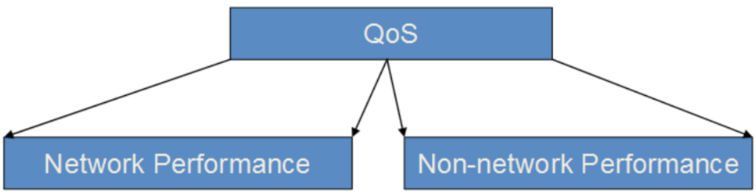

Figure 39. QoS
Source: ITU

ITU-T (Recommendation E.800 [ITU-TE.800]) and ETSI [ETSI-ETR003] basically defines Quality of Service (QoS) as “the collective effect of service performance which determine the degree of satisfaction of a user of the service” (Marchese, 2007). IETF considers QoS as the ability to segment traffic or differentiate between traffic types in order for the network to treat certain traffic flows differently from others. The term QoS has a variety of connotations, ranging from a user's experience of a service to a set of connection characteristics required to reach a specific level of service quality. Depending on the application field and scientific scope, the meaning of QoS varies.

General QoS terminology, as defined in ITU-T E.800, includes the following:

- QoS requirements of user/customer (QoSR): A statement of QoS requirements by a customer/user or segment/s of customer/user population with unique performance requirements or needs.
- QoS offered/planned by service provider (QoSO): A statement of the level of quality planned and therefore offered to the customer by the service provider.
- QoS delivered/achieved by service provider (QoSD): A statement of the level of QoS achieved or delivered to the customer. These parameters should be the same as specified for the offered QoS so that the two can be compared to determine what was actually achieved in order to assess the level of performance obtained.
- QoS experienced/perceived by customer/user (QoSE): A statement expressing the level of quality that customers/users believe they have experienced. Perceived QoS is assessed by customer surveys and from a customer's own comments on levels of service.

C. Telecommunication QoS Characteristics

Telecommunication is the process of sending data or voice over a long distance. There are a variety of communications technologies available, ranging from legacy networks to all-IP networks. Basic telephony services, satellite communications, and the Internet, and so on are just a few examples.

Best-effort service is used in today's global Internet service. When a packet is sent to the Internet for delivery to a target host, the network makes no guarantees about delivery time, delivery speed, available capacity, or even if the packet will be dropped if the network is congested. When considering the delivery of an email message, when seconds or minutes have a minor impact on the end user, delay is not an issue. However, if a voice-over-IP (VoIP) call's transmission delay is excessive, or if delays vary too much, or if too many packets are missed, the quality will deteriorate.

The Public Switched Telephone Network (PSTN), often known as the basic telephony service, is regarded as a gold standard for voice quality and meets all user expectations. Because this network is Circuit Switched (CS), a dedicated circuit (or channel) has been been aside for the call. On the one hand, it gives excellent quality, but it is less efficient than IP networks, which make better use of available bandwidth. Of course, the network can have issues delivering Quality of Service, such as noise on the circuit or the right volume levels.

It's critical to remember that the service's QoS is unique. A set of parameters unique to each service can be used to express it. Jitter is a parameter used in packet switched networks, whereas Cell Loss Ratio (CLR) is used in circuit switched analog networks. Another feature is that QoS is an end-to-end problem. This indicates that all entities in the path between the parties are interested about providing the service, and all segments are involved in the QoS guarantee process.

D. The four viewpoints of QoS

The service providers and the customers are the two main parties involved in management. Customers points of view are their requirements for QoS and their perceptions of received performance. The perspectives of the service provider are the QoS that are planned and the QoS that are actually achieved or delivered. For any service, the QoS stated is the end-to-end experience of the customer. The network or service provider would be most interested in network element performance, but not necessarily the user. Figure 40 depicts the aforementioned concept.

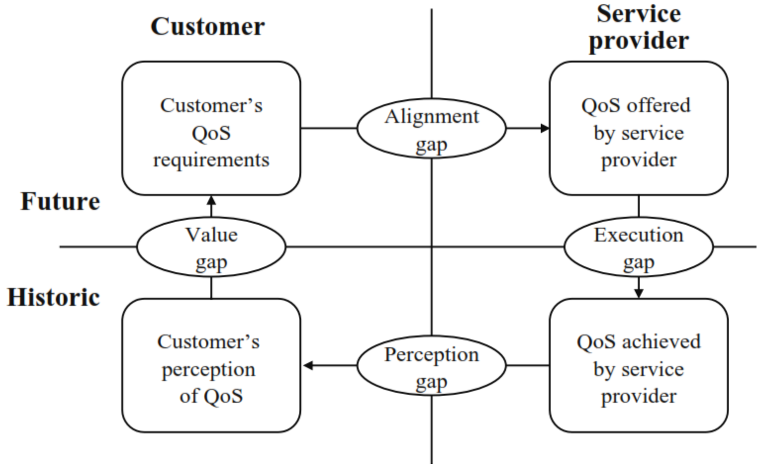

Figure 40. The four QoS viewpoints or the quality cycle
Source: (Antony Oodan, 2009)

The customer's QoS needs are a declaration of the level of quality of a certain service. The customer's level of quality might be described in technical or non-technical terms. A typical consumer is simply interested with the end-to-end service quality, not with how a particular service is delivered or with any aspect of the network's internal design. Customers want a variety of telecommunications service quality requirements, including: speed, accuracy, availability, reliability, security, simplicity, and flexibility.

The provider's quality of service (QoS) is a statement of the degree of quality that the service provider expects to give to the client. Values assigned to QoS parameters are used to express the quality level. When appropriate, the service provider may explain the provided QoS in non-technical language for the benefit of customers, as well as in technical terms for internal usage.

To make the most use of its resources, the service provider must specify the parameters to satisfy the majority of its consumers and specify variants for specific customers. There is no generally agreed-upon definition of 'provided quality.' As a result, each service provider will present its own set of quality parameter based on which network-related and non-network-related performance standards can be specified. The only exclusions will be technical, quality-related performance limits specified by ITU-T and ETSI recommendations.

E. QoS Parameter

Three classes of parameters determine the user experience are customer interface parameters, network infrastructure parameters and service functionality parameters. Quality of service parameters (also known as QoS metrics, QoS indicators, QoS measures, or QoS determinants) describe the quality of a service and its level of customer satisfaction. Objective and subjective measurement methods can be used to derive QoS parameters. Physical properties of circuits, networks, and communications are measured to obtain objective QoS criteria. Conducting well-designed customer opinion surveys yields subjective QoS parameters. Although QoS parameters are user-oriented and give useful input into the network design process, they are not always straightforward to translate into relevant network technical requirements.

Depending on the application and management architecture, QoS is measured using characteristics such as latency, jitter, packet loss, throughput, and many more. The following are the most important general QoS parameters in packet switching networks.

1. Jitter

Jitter is a delay fluctuation that is caused by the packet's fluctuating transmission delays through the network. This can happen due to the behavior of routers internal queues in specific conditions, routing modifications, and so on. This setting has a significant impact on the quality of streaming audio and/or video. To handle jitter, packets must be collected and held for long enough until the slowest packets arrive on time, then rearranged to be played in the correct order. When using video or music streaming services, jitter buffers can be seen. They are designed to compensate for jitter caused by the internet, allowing for uninterrupted playback of data transmitted over the network. When you click a link to watch a video, buffering begins before the media stream begins. Its cause additional delay, but it is required for jitter-sensitive applications.

2. Packet Loss

When one or more packets of data being transmitted through the internet or a computer network fail to reach their destination, this is known as packet loss. Wireless and IP networks cannot guarantee that packets will be sent at all, and some packets will be dropped if they arrive after their buffers have been filled. Other factors that can cause packet loss include signal degradation, high loads on network links, corrupted packets being discarded, and network element defects. Wireless networks have a higher risk of loss due to the air interface (e.g., interference from other systems, many impediments in the path, multipath fading, and so on). Delivery control is achieved in some transport protocols, such as Transmission Control Protocol (TCP), by obtaining acknowledgements of packet receipt from the receiver. If packets are missed during transmission, TCP will automatically resend the parts that were not acknowledged, lowering the connection's overall performance.

3. Throughput

Throughput refers to the amount of data sent or received by a network or entity, or the amount of data processed in a given amount of time. Bits per second (bit/s or bps) are the basic units of throughput measurement. Due to system losses and delays, the throughput may be lower than the input. Throughput is a good indicator of a communications link's channel capacity. A bandwidth meter is an example of a throughput measurement (which is used for measuring the real transfer rate that a DSL connection has). The Bandwidth Meter calculates the rate at which a test file is transmitted to the computer for a specific Server to determine the current throughput of a DSL connection. When you pay for a 1000kbps DSL connection, the bandwidth available for this connection on the access network is limited to 1000kbps. A bandwidth meter tool accurately evaluates how quickly a user may receive data from specific servers. However, it is possible that it does not reflect consumers' experiences downloading specific sites from the Internet. Regardless of the connection type, several factors influence the rate at which webpages and files download.

F. Network performance

The technical capabilities of the network in terms of the performance of specific combinations of items of equipment used to deliver services is referred to as network performance. It makes a significant contribution to the network's quality of service (QoS). Network performance is objectively assessed by characteristics that are significant to network operators, but have a shaky link with QoS as perceived by customers in many circumstances.

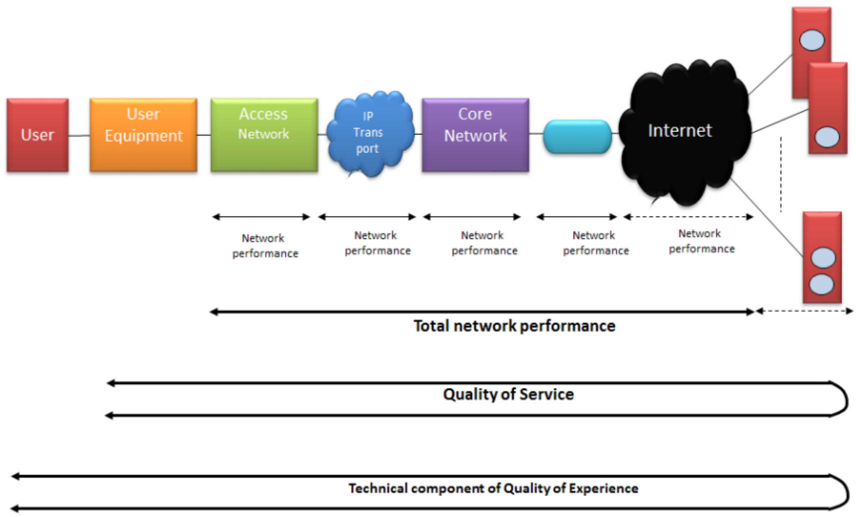

Figure 41. Network Performance, QoS, and QoE

Source: ITU

Several network performance metrics may, in some situations, contribute to the same customer-perceived impairment. There are also specific important criteria that have a significant impact on the quality of each network service, such as error performance for data services and delay for voice services. The following are some of performance parameters for transmission network.

1. Echo

There's also the issue of echo routes being set up, in addition to the screeching effect generated by unattenuated circulating signals. When the propagation delay between directly sent and breakthrough circulated speech signals grows significant, it becomes bothersome for telephone customers. There are two sets of paths: the talker echo-path and the listener echo-path. In most cases, the loss added at the subscriber line card for stability purposes, as discussed above, reduces the level of both types of echo signals sufficiently to provide acceptable telephony service quality.

Talker echo refers to the signal reflected to the speaker's end, whereas listener echo refers to the signal reflected to the listener's end. The echo delay time is equal to the time it takes for a signal to propagate through a connection and return, and is thus connected to line length, switching system delay, regeneration, and signal processing. The loss between equirelative level points at a 4-wire interface, from the receive to send ports, calculated as a weighted quantity in the frequency region 300–3400 Hz is known as 'echo loss.'

2. Delay

Propagation delay is defined as the time it takes for a signal applied at the input of an equipment (or connection) to reach the output of that equipment. Propagation delay is an unavoidable consequence of transmitting signals over long distances. Excessive lag not only increases the likelihood of echo, but it also makes communication more difficult. Because of the reaction latency, it causes confusion in speech, causing a speaker to repeat his sentence while the other party responds. Retransmission may occur for data and signaling where the protocol needs a quick response, resulting in a communication breakdown. Except in extraordinary situations, the ITU-T advises that the maximum one-way delay for an international connection not exceed 400 milliseconds.

In telecommunications and computing systems, latency is the time difference between transmitting and receiving a signal. For designers of communication systems that use geostationary satellites, latency has long been a major concern. Because of the time it takes for a radio signal to travel to and from the satellite, this is the case (GEO satellite orbit is at 35,787 km). Latency is also a concern for packetized networks on the ground, such as the Internet. In the case of the Internet, latency is caused by the amount of time spent routing packets at routers, rather than by distance. When there is a human interface to the information, such as a person making a phone conversation, using a multimedia program, or watching TV, latency can be a serious issue. The key factors of the QoS are latency and bit error rate.

3. Crosstalk

The existence of undesired signals linked from a source other than the connection under investigation is known as crosstalk. The disturbing signal is supplied via one channel, and the disturbed channel is measured. Even though low-level crosstalk is unintelligible for speech, it might give the user the sense of a lack of confidentiality, which is an undesired drop in service quality. Capacitive coupling between the pairs causes crosstalk in multi-pair wires in the local loop. Crosstalk is primarily affected by:

- the level of signal, which, if high, is more likely to cause crosstalk into another channel;
- the frequency of interfering signal, which, as it increases, is more likely to cause crosstalk;
- the balance of the circuits around earth, which, if each wire in a cable has equal capacitance to earth and to each other, will result in zero crosstalk between pairs. Unbalance, as well as the impedance terminating the line's balance to earth, increases the likelihood of crosstalk;
- the quality of the screening between circuits.
- the frequency of the interfering signal, which is more likely to generate crosstalk as it increases;
- the circuits' balance around the ground; if each wire in a cable has the same capacitance to the earth and to each other, crosstalk between pairs will be zero. Unbalance, as well as the impedance terminating the line's balance to earth, increases the likelihood of crosstalk;
- the quality of the screening between circuits.

G. QoS Measurement

The QoS measurement system and the statistics obtained from the measurement should: be well defined (non-ambiguous) and easily understood by service providers and customers; be relevant to customer applications; enable service providers to diagnose issues and anticipate capacity requirements; be independently repeatable, that is, multiple service provider measurements taken at the same time yield the same result; be independently verifiable by customers; and be independently repeatable by service providers.

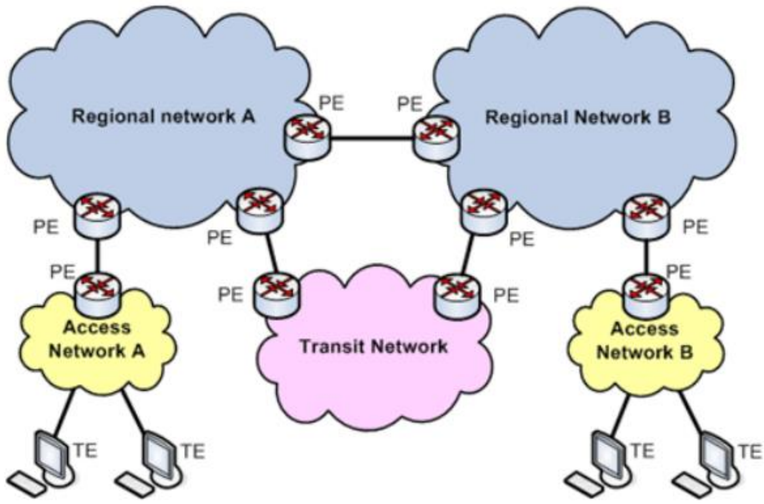

Figure 42. Basic network model for measurements
Source: based on ITU-T Y2173

There are two sorts of approaches for assessing QoS:

- Passive measurement (using test packets)
  Performance measures including as delay, jitter, and packet loss are measured while test packets are transmitted from management systems. This approach is frequently used for troubleshooting.
- Active measurement
  Probes are put on network elements and user devices in the form of software agents or network appliances (for the software agent case). The probes' measurements provide a very accurate state of the devices at any given time.

In addition to definitions and standards for QoS characteristics and their assessment through measurements, the following metrics should be defined:

- Operators will find this useful: The NRA's measurements for QoS monitoring must be practicable for operators to deploy at a reasonable cost and within a reasonable timeframe using consistent measurement and audit techniques.

- Customers care about: For the most common services used by clients, measurements must be taken.
- Comparative analysis of operators: Before they can be settled, the details of measurement methods may need to be debated between operators.

Review Questions

Q1. General QoS terminology, as defined in ITU-T E.800, includes the following, except............

a) QoSO
b) QoSE
c) QoSR
d) QoSD
e) QoE

Q2. The main purposes of QoS regulation are ....

a) Making sure networks work well together
b) Controlling the QoS in presence of competition
c) Helping customers be aware of the Quality of service, and operators to achieve fair competition
d) Checking claims by customer

Q3. The latency category is said excellent when the delay value...............

a) > 450 ms
b) < 150 ms
c) 150 – 300 ms
d) 300 – 450 ms

Q4. Why we need QoS?

a) To improve performance for applications that are sensitive to delays
b) To minimize the use of existing network investment

c) To respond traffic in the network
d) To give priority to common applications on the network

Q5. Availability is one of Seven QoS criteria. which one is the example of availability on QoS criteria?
a) ease of change in contract
b) coverage
c) ease of software updates
d) speech quality

CHAPTER 6
NETWORK MANAGEMENT

A. Introduction to Network Management

As the size and complexity of the telecommunications network has risen, so has the necessity of network management. Efficient network management is a critical instrument for assisting a network operator in improving services and increasing their competitiveness. Operation and maintenance (O&M) systems have traditionally been used to describe systems that handle control and supervisory functions in a telecommunications network. Now, the term network management system since the functions performed by network management systems are far more extensive than those supported by traditional O&M systems.

The task for network management is frequently delegated in a hierarchical structure. The public network operator is responsible for managing the public network in order to offer clients with dependable service. Most of public network operator have their own dedicated and incompatible network management systems, which are usually organized geographically, and the integration of these systems is a key future concern.

Early management systems were only responsible for detecting faults. Other administration duties became necessary as the networks grew larger and the number of users rose. Fault, account, configuration, performance, and security management are the five management services available today. These functions are linked to network resources, which are referred to as managed objects.

Telecommunication Management Network (TMN) and OSI standards are used to manage wireless telecommunication networks nowadays. The OSI model is widely used to manage the majority of IP-based network parts. The TMN model lays up the foundation for a layered architecture and management functional areas. For the managing system and the management system, the OSI model offers the management framework.

B. What is Network Management

Network management is defined in a variety of ways, depending on one's point of view. Normally, network management is defined as the execution of the set of functions required for controlling, planning, allocating, deploying, coordinating, and monitoring the resources of a telecommunications network or a computer network, including performing functions such as initial network planning, frequency allocation, predetermined traffic routing to support load balancing, cryptographic key distribution authorization, configuration management, fault management, security management, performance management, and accounting management (Ding, 2010). User terminal equipment is not typically included in network management. Monitoring is the process of querying the values of managed objects' major properties or general operating parameters (for example, layer identification, timer identifier, and window limit). Controlling is the process of setting them to desirable values based on specified conditions. Controlling a single managed object is distinct from controlling all other managed objects in the network. Monitoring and controlling are based on communication between the agent and the manager, a particular host responsible for management duties (sometimes also referred to as the management station).

Network management occurs between two categories of systems: those in command, known as managing systems, and those that are observed and regulated, known as managed systems. The majority of management systems are referred to as Network Management Systems (NMS). Generically, an NMS consists of three elements: managed devices, agents, and management workstations (Green, 2006). Agents are software modules that exist on managed devices, also known as network elements. The managed network connects the managed devices to the NMS. The network management software that runs on management workstations is at the heart of the system. The workstation can be a PC running Microsoft Windows management software or a UNIX workstation running an application. Management workstations can create network maps and serve as the interface between managed devices and the operator. In most circumstances, the workstation communicates with agents via the controlled network; however, if the network is unavailable, it may be required to contact some devices over the dial network.

C. Telecommunication Management Network (TMN)

The term TMN was introduced by a standard called as ITU-T as an abbreviation for Telecommunications Management Network. The concept of a TMN was defined by recommendation M. 3010. According to this recommendation telecommunication management network is a conceptually different network from the communication network. This management network interfaces with the communication network at multiple places and helps manage the underlying communication network efficiently.

TMN provides management functions for telecommunication network and the services. It basically not only provides the management functions but offers communication between itself and the other networks. TMN also provides the organized architecture to achieve the integration between different waves. TMN layers are frequently portrayed as a pyramid-like structure, with the levels from bottom to top being: the physical network elements, network management, service management, and, at the top of the pyramid, the layer for business process management.

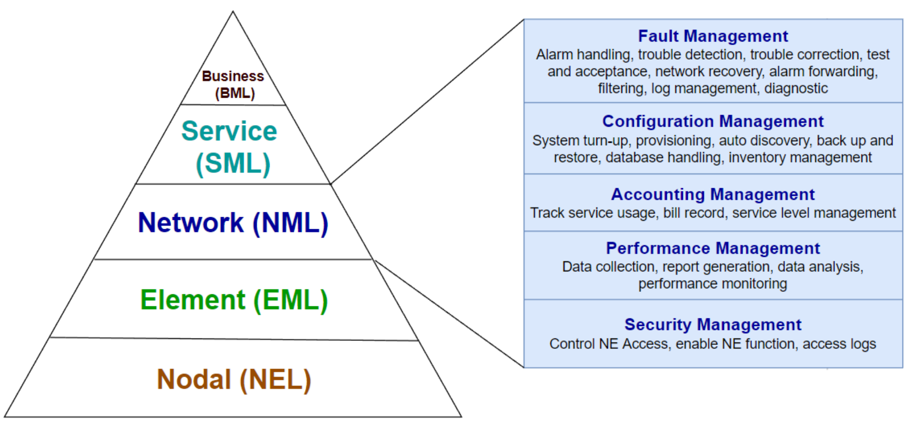

Figure 43. Layered architecture of the TMN

The element management layer's job is primarily to monitor and configure network elements as well as to discover faults via alert collecting and filtering. The Network Management Layer is responsible for managing the network's logical configuration, or network pathways (Path configuration, Path monitoring, and Path

tiering). The service layer oversees the services given to the end customer, including authentication and billing, as well as storing the consumer profile in terms of service fruition history in its database. This layer is also in charge of the mechanism for introducing new services into the network. The Business Management Layer is the most abstract layer, whose function would be to handle the network's business features, such as costs and service-related revenues, up to the evaluation of a network profit-and-loss sheet.
The managing systems are part of the network management layer, while the managed systems are part of the element management layer. This framework must support the following functional areas. These are also known as the FCAPS (Fault, Configuration, Accounting, Performance, and Security management).

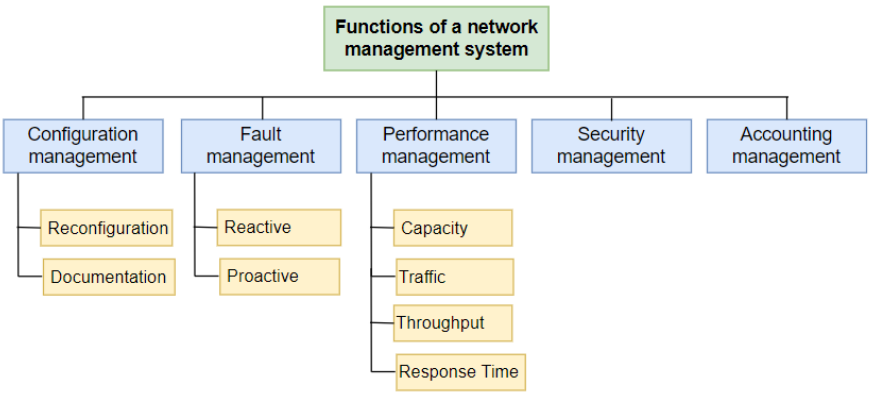

Figure 44. Function of a network management system

1. **Fault Management**

   Fault management is a set of functions that allows for the identification, isolation, and correction of abnormal telecommunications management network. There are two types of fault management: reactive fault management and Proactive fault management. The reactive fault management system is in charge of eliminating, isolating, rectifying, and documenting errors. A reactive fault management system's initial step is to pinpoint the exact location of the malfunction. A fault is defined in the system as an abnormal circumstance. When a malfunction occurs, the system either stops working properly or generates excessive errors. The reactive fault management system's next step is to isolate the fault. When a defect is isolated, it usually only impacts a few users. Following isolation, affected users are alerted immediately and given an anticipated time of rectification. The third step is to fix the problem. It may be necessary to replace or repair the defective components. After the error has been corrected, it must be documented. The record should include the precise location of the fault, the likely cause, the action or acts done to rectify the fault, the cost, and the time it took to complete each step. The issue may return so the documentation is very important. Documentation will assist current and future administrators in resolving similar issues. The occurrence of the same type of failure on a regular basis indicates a severe problem in the system. If a failure occurs frequently in one component, it should be replaced in order to avoid using that component.

Proactive fault management attempts to avoid the occurrence of defects. Although this is not always practicable, certain types of failure can be predicted and avoided. For instance, if a manufacturer specifies a lifetime for a component or a component part. Then replacing it before that period is a wise plan.

2. **Configuration Management**

   Configuration management discovers the location and name of controlled items and records them in the Management Information Base (MIB), together with their operating data. Configuration management functions include name management, data collecting, parameter setting, and initialization. Network planning and engineering, software installation, status and control checks, service planning and negotiation, and provisioning are all part of configuration management. In other words, configuration management includes the addition of new programs, new equipment, modifications to existing systems, and the removal of obsolete systems and programs. Configuration management is organized into two subsystems:

   1. Reconfiguration

      Reconfiguration, or the modifying of network components and functionalities, can be a frequent occurrence in big networks.

Hardware reconfiguration, software reconfiguration, and user account reconfiguration are types of reconfiguration.

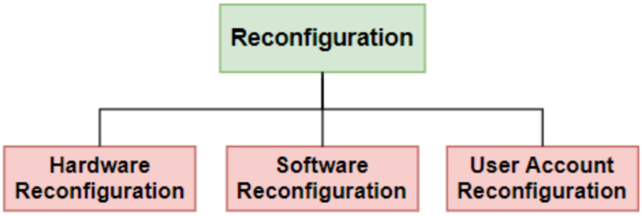

Figure 45. Types of reconfiguration

All changes to the hardware are covered by hardware reconfiguration. A desktop computer, for example, may require replacement. A router may need to be relocated to another network segment. A subnet can be added or removed from the network. All changes to the program are covered by software reconfiguration. For instance, new software must be deployed on servers or clients. Most software reconfiguration can, thankfully, be automated. For example, an application update on some or all clients can be downloaded electronically from the server.

User account reconfiguration entails more than just adding and deleting users on a system; it also takes into consideration user privileges. For example, a user may have read and write permissions for some files but only read permissions for others.

2. Documentation

The initial network configuration, as well as any later changes, must be thoroughly documented. It implies that documentation for hardware, software, and user accounts is required. Typically, hardware documentation consists of two types of documents are maps and specifications. Maps track each piece of hardware and its network connection. Every piece of software must be documented. Most operating systems offer a program for documenting user accounts and their privileges, which includes information such as software type, version, time installed, and license agreement. Management must ensure that the files containing this information are up to date and safe.

3. **Account Management**
   Account or accounting management is concerned with the cost of components such as resources and service prices, tariffs to reduce the cost of managed item consumption, and the detection of any account frauds. Account management is also responsible for the gathering and review of billing information. This helps to reduce operational costs by making the best use of the available systems. Account management is also in charge of ensuring that users are properly billed. Accounting is a particularly difficult issue in crosscontinent wired and wireless networks.

4. **Performance Management**
   Performance management manages managed items in terms of cost efficiency. Its duty is to collect and analyze statistical data in order to monitor and correct the network's behavior and efficacy, as well as to aid in planning, provisioning, maintenance, and quality assessments. To achieve the best overall performance, performance management logs attribute values and monitors response times. It allows for customizable network configurations and collects network performance information.
   A performance management, which is closely related to fault management, attempts to monitor and control the network in order to ensure that it runs as efficiently as possible. Performance management attempts to quantify performance through the use of measurable quantities such as:
   a) Capacity
      The network capacity is one component that must be monitored by a performance management system. Every network has a limited capacity, and the performance management system must ensure that this capacity is not exceeded.
   b) Traffic
      Traffic can be assessed in two ways. The number of packets traveling within the network is used to calculate internal traffic. The exchange of packets outside the network is used

to calculate external traffic. If there is high traffic during peak hours when the system is widely used, blockage may occur.

c) Throughput

We can measure the throughput of a single device (such as a router) or an entire network segment. Throughput is monitored by performance management to ensure that it does not fall below acceptable standards.

d) Response Time

Typically, response time is measured from the time a user requests a service to the time the service is granted. Other factors such as capacity and traffic can all have an impact on response time. The average response time is monitored by performance management.

5. Security Management

Security management is concerned with the protection of managed assets through the distribution and management of security services. Security services for communications, as well as security incident detection and reporting, are among its tasks. The communications security services provide services for authentication, authorization, access control, data confidentiality, data integrity, and non-repudiation that may occur during any communications between systems, between customers and systems, and between internal users and systems. The function of security event detection and reporting reports any behavior that may be regarded as a security violation to higher layers of security.

Review Questions

Q1. What layer does the FCAPS management function?

a) Service Management Layer (SML)
b) Network Management Layer (NML)
c) Business Management Layer (BML)
d) Element Management Layer (EML)

Q2. The quality of the overall acceptance of the application or service that is subjectively perceived by the end user is the definition of ....

a) Quality of Experience
b) Key Performance Indicators
c) Network Performance
d) Quality of Services

Q3. The network management standard for telecommunications networks recommended by ITU-T is ....

a) SNMP
b) TMN
c) COBRA
d) OSI/CMPI

Q4. Interpreting management information to human users via the g interface is a function of ....

a) Mediation Function (MF)
b) Network Element Function (NEF)
c) Operation Systems Functions (OSF)
d) Work Station Function (WSF)
e) Q Adapter Function (QAF)

Q5. The performance management in telecommunications networks includes ....

CHAPTER 7
ROUTING

A. Network Routing: An Overview

Network routing refers to the ability of an electronic communication network to send a unit of information from point A to point B by determining a path through the network, and by doing so efficiently and quickly (Deepankar Medhi, 2007). Address routing algorithms, routing protocols, and architecture are all part of the broad scope of network routing, with architectures containing multiple distinct features for efficient routing.

In telephone networks, the term routing also refers to the inbound and outgoing processing of calls. The term routing refers to the pathfinding of information or data streams from their source to their destination in telecommunications. It is most commonly used in the context of data networks and defines the transmission and delivery of data packets via individual network nodes (routers). The router accomplishes this by knowing either individual links or entire network topologies and selecting the optimum network node to forward the data packet to next depending on its destination address and other parameters. The decision is made using routing techniques and protocols. In telephone networks, the term routing also refers to the inbound and outgoing processing of calls.

B. IP Addressing

If you need to send data to any host on the Internet, you'll need to be able to uniquely identify all of them. As a result, a global addressing scheme is required, with no two hosts having the same address as we know as IP Address. The first feature that should be included in an addressing system is global uniqueness.

The IP address is separated into two types throughout development: IPv4 and IPv6. IPv4 addressing is written in a bit format from left to right, with the left-most bit being the most significant bit with the length of an IP address allocated to a host is 32 bits. The hierarchy in IP addressing is reflected through two components, a network part and a host part, referred to as the pair (netid, hostid). The host part (hostid) identifies a host on that network, whereas the network part (netid) identifies the network to which the host is connected. The IP prefix is another name for the network element. The network part of an IP address is shared by all hosts connected to the same network, but the host part must be unique. For networks and hosts, the IP address space was originally separated into three classes: Class A, Class B, and Class C, as shown in Figure 46. The first few bits of a 32-bit address were used to distinguish each class.

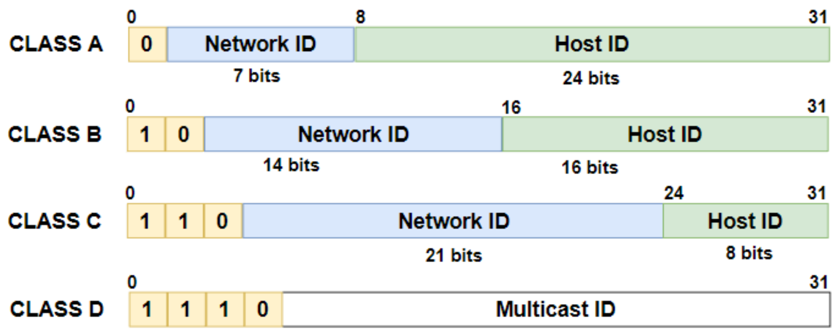

Figure 46. Classful IP addressing scheme

IPv6 is a more powerful version of IPv4. IPv6 (Internet Protocol version 6) is a 128-bit variant of an IP address. It is made up of eight sets of numbers and letters, each of which represents 16 binary digits in decimal form. An example of IPv6 is 2001:cdba:0000:0000:0000:0000:3207:9602. Or, it can be written shorter 2001:cdba::3207:9602. It can have a combination of up to 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses with a 128 bit system.

C. Routing Algorithms: Shortest Path and Widest Path

Shortest path algorithms are beneficial for IP networks, while widest path algorithms are useful for dynamic call routing and quality-of-service-based routing in telephone networks.

A communication network is made up of nodes and links in general. Nodes have different names depending on the type of network. In an IP network, for example, a node is known as a router, whereas in a telephone network, a node is either an end (central) office or a toll switch. A node in an optical network is an optical or electro-optical switch. In an IP network, a link connecting two routers is commonly referred to as an IP trunk or simply an IP link, whereas the end of a link originating from a router is referred to as an interface. In a telephone network, a link is referred to as a trunk group, an inter machine trunk (IMT), or simply a trunk.

Diverse types of communication networks have different goals, but they are commonly divided into two categories: user-oriented and network-oriented. User-oriented means that a network must give excellent service to each user so that traffic can flow rapidly from the source to the destination. Thus, instead of delivering the "best" service to a specific user, a network-oriented approach focuses on how to offer efficient and equitable routing so that the majority of users obtain decent and acceptable service. Because a network's resources, such as network capacity, are limited, such a perspective is necessary.

Next, we'll look at two crucial algorithms that have a significant impact on data networks, particularly Internet routing. In terms of the aforementioned broad classifications, these two algorithms, known as the Bellman–Ford algorithm and Dijkstra's algorithm, can be classed as user-oriented. Both are referred to as shortest path routing algorithms. It's a path-finding method whose purpose is to find the shortest path between two nodes. The shortest path can be defined in terms of distance in road networks, which is a straightforward approach to grasp it. However, conceptions other than the traditional distance-based measure, such as the time taken to travel between two cities, may be applicable as well. Distance does not always have to be measured in terms of physical distance; it can also be measured in terms of time. Each network link A generic word for a distance measure in communication networks is cost, link cost, distance cost, or link metric.

A network can be represented as a graph by mapping each node to a unique vertex in the graph, with edges linking the corresponding vertices representing links between network nodes. Each edge can have one or more weights, which might represent cost, delay, bandwidth, and other factors. The following figure shows a network made up of a graph with six nodes and ten links, each with its own link cost/weight.

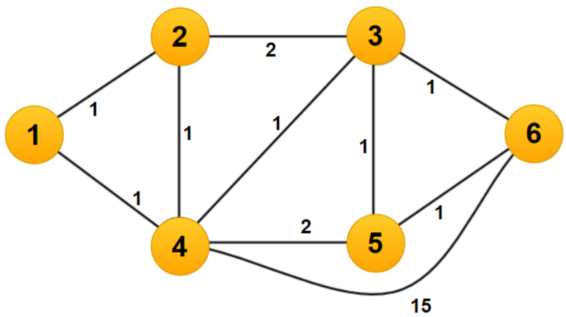

Figure 47. A six-node network

1. Bellman–Ford Algorithm

The Bellman–Ford algorithm computes the shortest path between two nodes in a centralized manner using a simple principle. The Bellman-Ford algorithm is quite similar to Dijkstra's algorithm in terms of finding the shortest path in a weighted graph, but it can accept negative weights. The Bellman-Ford Algorithm is a modification of Dijkstra's Algorithm. It is true if and only if the graph does not contain cycles with negative weights obtained from the source. The Bellman Ford algorithm operates by overestimating the length of the path between the starting and ending vertices. It then relaxes those estimations iteratively by discovering new paths that are shorter than the previously overestimated paths. We can ensure that the outcome is optimized by repeating this process for all vertices.

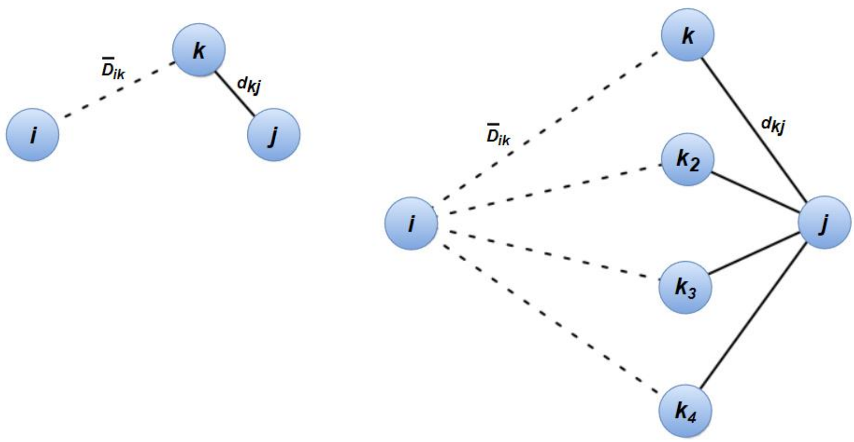

Figure 48. Centralized Bellman–Ford Algorithm

2. **Dijkstra's Algorithm**

Another well-known shortest path routing algorithm is Dijkstra's algorithm. Dijkstra's method is not the same as the Bellman–Ford algorithm or the distance vector technique in terms of its underlying concept. Dijkstra's algorithm is a solution to the problem of determining the shortest path from a network to each positive or negative vertex. Dijkstra's algorithm finds the shortest path by determining the least weight of a weighted graph, the shortest distance between two or more graph nodes, and the total value obtained is the smallest value. In a weighted network, the weight is a positive number, therefore it is not traversed by negative nodes. Dijkstra is one of the most often used algorithm versions for handling difficulties involving the optimization problem of finding the shortest path between vertex a and z. Negative nodes cannot traverse a weighted network since the weight is a positive amount. If this is the case, however, the given solution is infinity. Nodes are employed in Dijkstra's Algorithm because it employs a directed graph to discover the shortest path route.

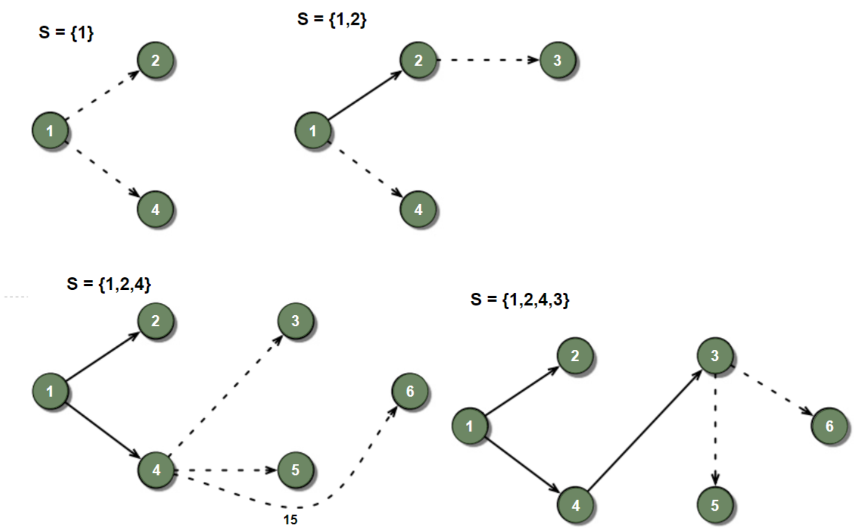

Figure 49. Iterative view of Dijkstra's algorithm

D. Routing Protocol

There are three classes of routing protocols: distance vector, link state, and path vector. Distance Vector Routing historically known as the old ARPANET routing algorithm or known as Bellman-Ford algorithm. Consider the Routing Information Protocol (RIP), which is based on the distance vector protocol concept and uses the distance vector ("distributed Bellman–Ford") algorithm for computing the shortest paths; similarly, the Open Shortest Path First (OSPF) protocol is based on the link state routing protocol concept and uses Dijkstra's shortest path first routing algorithm. However, in a networking environment that supports MPLS or GMPLS, OSPF/IS-IS is used as a routing protocol, but Dijkstra's shortest path first algorithm is not necessary. Consider real-time network routing (RTNR), which is used in the telephone network for dynamic call routing. RTNR uses a link state protocol, but the actual routing computation differs significantly from Dijkstra's algorithm. Finally, there are routing settings in which no information sharing is performed in order to select/compute routes; while this may appear strange, adaptive algorithms that function (and work effectively) without the paradigm of information exchange exist. While the actual routing computation differs from Dijkstra's algorithm, the state protocol is used. Finally, there are routing settings in which no information sharing is performed in order to select/compute routes; while this may appear strange, adaptive algorithms that function (and work effectively) without the paradigm of information exchange exist.

E. Routing in the PSTN

In the worldwide switched telephone network, routing is a crucial function. The switched telephone network's routing architecture is based on a half-century-old concept of hierarchical routing, and the hierarchical concept as it was conceived is still present in the overall global switched telephone network architecture. In addition, in the last 25 years, dynamic call routing schemes that can work in this hierarchical architecture have been established.

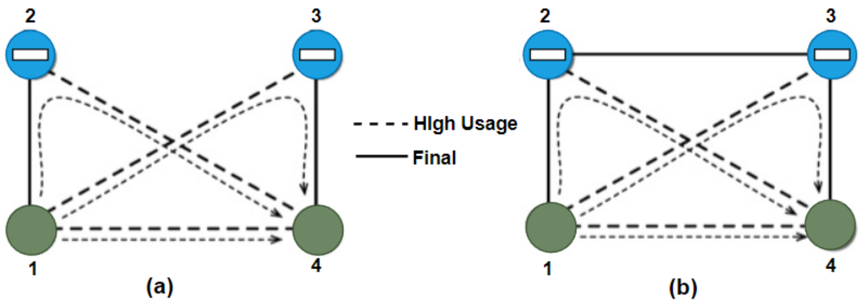

Figure 50. Hierarchical routing example

In a hierarchical routing context, the key rules for routing (while avoiding looping) can be described as follows:

- In a nested fashion, a switch in a higher level must have the switching function of the lower level. The many switching function rule is what this is called.
- Calls must be routed via the direct switch hierarchy at both the originating and destination switches. This is referred to as the two-ladder limit rule.
- A HU trunk group from a switch in the originating area to a switch at the next higher level in the destination area is preferred over the final trunk group to the switch at the level directly above it for a call from one area to another. This is referred to as the ordered routing rule. In other words, when several routes exist, the route order of attempts is predefined and constant, and is based on the level and placement of switches in different locations.

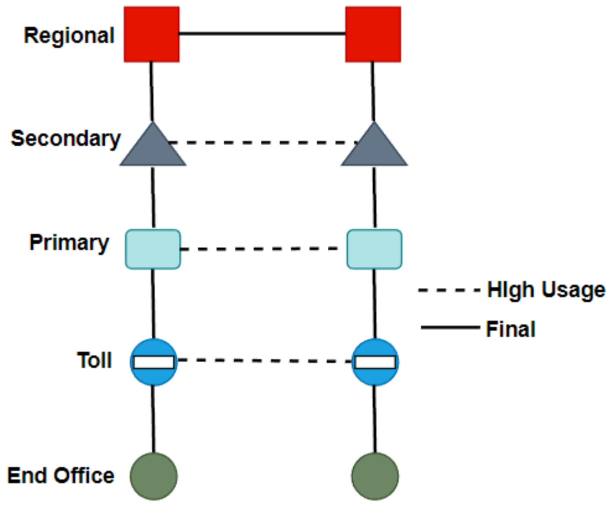

Figure 51. Switching hierarchy in hierarchical routing

Another switching level is defined above the regional switching center in the hierarchical routing topology to connect trunk groups from one country to another country. Hierarchical routing can so be briefly summarized as follows: A call can move up a trunk group from a lower-level switch to a higher-level switch unless the call is going directly from a higher-level switch to the final destination switch; a call can also go from one switch to another in the same level if the second switch is in the "destination region."

The restrictions of hierarchical routing necessitate the usage of dynamic routing. Remember that while hierarchical routing addressed the looping problem by employing creative usage of nodes at various levels and a set of rules, it also resulted in circumstances where some trunk groups were unable to be used for routing despite having sufficient capacity.

Progressive call control (PCC) is used in hierarchical routing. This means that the call control is forwarded from one switch to the next until it reaches its destination, unless the call cannot locate an outgoing trunk at an intermediate trunk, in which case it is dropped. To put it another way, the call is not returned to the originating switch to try a different routing.

Assume we could transfer call control from an intermediary switch to the originating switch. This indicates that the network supports originating call control (OCC); crank back refers to the functionality of returning a call to the originating switch and trying a different path. The topic of whether the network should provide PCC or OCC, as well as whether it should give crankback, has arisen since the introduction of dynamic call routing.

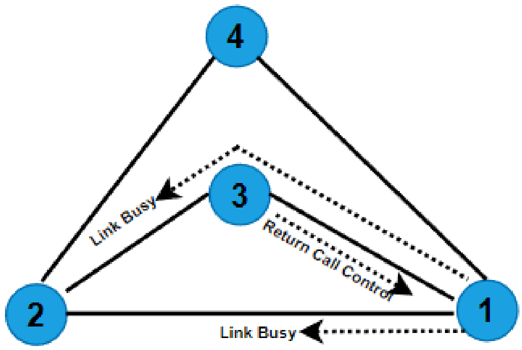

Figure 52. Illustration of crankback

All dynamic routing techniques for telephone networks allow for a maximum of two links per call. The network is frequently entirely or nearly totally integrated. Furthermore, trunk reservation is included in all designs. They differ in the following ways:

- Crankback and progressive or originating call control
- Time-sensitive or adaptive
- Off-line or near-online computation.
- Calculation of routing.
- Make a connection between the information used and how it is used.

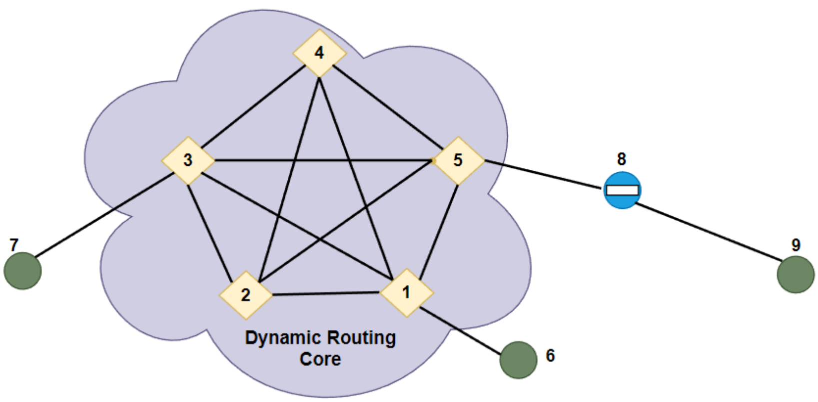

Figure 53. Dynamic call routing in conjunction with hierarchical routing

The first dynamic routing strategy to be implemented was Dynamic Nonhierarchical Routing (DNHR). This means that the number of routes available (and their sequence) varies depending on the time of day. The 24-hour time period spanning a 7-day week was divided into 15 load set periods in the case of DNHR: 10 for weekdays and 5 for weekends. Understanding traffic patterns was used to establish the varying amount of load set times. Due to low traffic flow, the same routing pattern can be employed from midnight to 8 a.m., for example. DNHR, like the other dynamic routing methods, allows just two links for a call within its network. DNHR is built on OCC and supports crankback. DNHR makes use of trunk reservation. It is a time-dependent routing method in which some routes ("designed paths") are computed ahead of time off-line, while other routes ("real-time paths") can be computed and appended in near real-time when congestion develops.

DCR is an adaptive routing strategy that can be modified frequently (often every 10 seconds) dependent on the status of network links. A centralized route processor was used to compute the routes to be cached. Routes require no more than two links to complete a call, and crankback is not supported in this scheme. Thus, if a call is blocked on the second leg of a two-link call, the call is lost, and the user must attempt again. DCR has two fall-back mechanisms: (1) if the route processor is down, cannot compute routes in a timely manner, or does not communicate back to the switched nodes in a timely manner, DCR continues to operate using the last known routing table; and (2) if a switch loses dynamic routing functionality for some unknown reason, the network can still operate as a two-level hierarchical routing system in which certain nodes are labeled ahead of time as nodes.

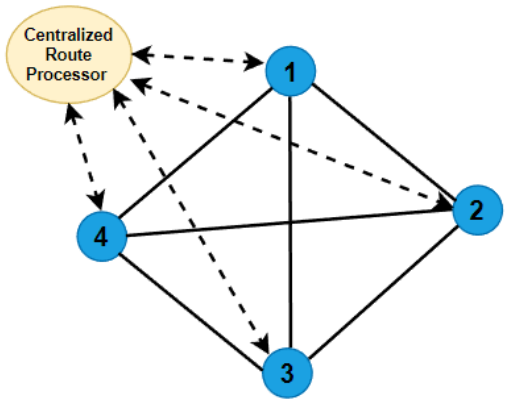

Figure 54. DCR architecture

Inbound routing in telephone systems
Incoming calls are assigned to specific individuals, phone lines, or groups based on predetermined information. When gathering information about a caller, voice response systems are frequently used. They allow the caller to be more specific about their request. The telephone system routes the caller to a member of staff who is qualified to handle the caller's concern based on predetermined criteria. This feature-based routing improves call agent availability while also increasing call processing efficiency.

Outbound routing in telephone systems
Finding the most cost-effective telephone provider for individual calls is an example of how outbound routing can be employed in telephone networks. Least Cost Routing is the technical phrase for this. The method often employs the Call-by-Call feature, which compares pricing tables automatically. Every call can be routed via the call provider that offers the cheapest rate for that individual call by using a call prefix number that is automatically pre-selected by the system. However, the user's own telephone company must support and enable call-by-call. The Least Cost Routing function can be implemented using software or new hardware in a telephone system.

Review Questions

Q1. The first dynamic routing strategy applied to the telephone network was ....

a) DCR
b) PCC
c) AHR
d) DNHR

Q2. An example of a routing protocol that uses a distance vector algorithm is...........................

a) Inter-Domain Routing Protocol (IDRP)
b) Routing Information Protocol (RIP)
c) Exterior Gateway Protocol (EGP)
d) Open Shortest Path First (OSPF)
e) Border Gateway Protocol (BGP)

Q3. An adaptive routing strategy that can be modified frequently (often every 10 seconds) dependent on the status of network links is....................

a) DCR
b) PCC
c) AHR
d) DNHR

Q4. The following is a routing classification in adaptive routing, except ....

a) Flooding
b) Isolated
c) Distributed
d) Centralized

Q5. A managed object (MO) is defined by ....

CHAPTER 8
PBX

A. Definition of PBX

The term PBX refers to a private branch exchange. The term "private" refers to equipment that serves private groups rather than providing public service. The term "branch" refers to a multi-station arrangement that allows for the sharing of central office lines. Its major function, which is to swap phone calls internally and outside, is reflected in the name Exchange.

A private branch exchange (PBX) is a telephone system that is only utilized within a company. A PBX is used by most medium to big businesses since it is less expensive than adding an external phone line to each employee's phone. Internal calls are also easier to make within a PBX because they can usually be done with three or four digits.

B. History of PBX

The Bell Company established the first simple operator-controlled switchboards in 1878, serving 21 subscribers. There have been various generations of PBXs since then. These can be categorized into one of five separate generations. First generation PBXs had patch panels for operator control. Second generation PBXs had automatic dialing and space division multiplexing and were based on step-by-step (Strowger) and crossbar switches (SDM). Third generation is a term use semiconductor switches under stored program control, and the features of the second generation PBXs were retained. Computer-based fourth-generation PBXs contain features such as automatic call distribution and voicemail. They also employ time division multiplexing, which allows voice and data to be combined on T-1 and ISDN lines. 5. 'Fifth generation' PBXs have LAN and Internet connectivity (i.e., IP support) as well as support for WAN technologies like as ATM. They can also be managed using a simple network management protocol

(SNMP). Fifth-generation PBXs provide LAN and Internet connectivity (i.e., IP support) as well as support for WAN technologies like as ATM. They can also be managed using a simple network management protocol (SNMP).

Components of the PBX aside from line and trunk interfaces. A typical PBX has three key components: a programmable CPU, memory, and a switch matrix. The CPU controls the switch matrix, which switches using either space division switching or time division switching. Advanced PBXs are designed to work across huge locations that span several kilometers.

C. Function of PBX

Because the PBX originated from operator-controlled switchboards used on public telephone networks, the basic operations of a PBX are quite similar to those of a Central Office switch. A PBX provides three basic roles via control signaling:

1. It establishes end-to-end connections among subscribers on the network, or to remote subscribers off the network, in response to a call request, via intermediate nodes such as other PBXs or PSTN Central Office switches. Because the call is made using circuit switched technology, the linked path is dedicated to the user for the duration of the call.
2. It monitors the circuit and detects signaling such as a call request, a response, a busy signal, and a disconnect signal.
3. It disconnects the circuit after the call is finished, allowing other users to access the resources. For every 8–10 users, one trunk line is usually allowed. Some of these trunks are then assigned as incoming lines, while the rest are assigned as outgoing lines, depending on the organization's call habits.

D. PBX Components

Numerous sets of station, some of which may have fully functional electronic terminals, are served by PBXs. Although wireless applications are frequently offered as an alternative, PBXs typically service voice terminals on a wired basis. The majority of PBXs were built using a modular architecture. PBXs are made up of cabinets, shelves, printed circuit boards, power supply, and other components, just like conventional computers. Power supply, common control, memory, switching matrix, trunk interfaces, line interfaces, and terminal equipment make up the majority of a PBX's physical and logical parts.

1. **Common Control**

   A system's actions and all of its different components are controlled by a common set of stored program logic known as common control. The manufacturers describe it as being so secure that it is bulletproof, but in reality it is made up of many microprocessors working with a stored software. The control processor is made up of memory, input/output hardware, bulk memory hardware, and software, just like any other computer.

   Microprocessors called Central Processing Units (CPUs) manage how the system functions. Although they might be centralized, for efficacy, efficiency, and durability reasons, they are typically dispersed among cabinets, shelves, or even cards (printed circuit boards). The most expensive and complicated board is typically the CPU board. The CPUs manage processes such call setup, call maintenance, call release, performance monitoring, system diagnostics, and the archiving of operational data for report analysis and display. Contemporary PBXs frequently have processor redundancy. Numerous PBXs have hot standby processors, which are instantly available in case a primary processor fails. These processors are in addition to the multiple microprocessors that do the processing tasks at the cabinet, shelf, and card levels. Notably, traditional PBXs are extremely closed, proprietary computer systems.

2. **Trunk and Line Interfaces**

   The PBX switch is interfaced with the trunks linking it to other switches using trunk interfaces, which take the physical form of specialized circuit boards. Trunks can be one-way outgoing, one-way incoming, or two-way by nature because they are directional (combination). In order to serve different specific applications, to improve system performance, and to guarantee a minimally acceptable level of both incoming and outgoing network access, a PBX frequently uses all three types.

   Trunks are typically multichannel, but single-channel trunks are used for applications including foreign exchange (FX) service and power failure transfer. High-capacity, multichannel trunks typically offer significantly better value since they can accommodate several conversations. Examples of multichannel trunk capabilities include T-Carrier, E-Carrier, and ISDN Primary Rate Interface (PRI), commonly known as Primary Rate Access (PRA). Trunk groups are collections of trunks with a common directional kind and use. Using a predetermined, user-definable hunt sequence, the PBX will search for available channels inside a trunk and for trunks within a trunk group.The following specific types of trunks can be accessed through trunk interfaces:

- Central Office Trunks: Connect the PBX to the neighborhood CO exchange. These trunks provide access to the local calling area and to all other areas served by the local telco, or Local Exchange Carrier (LEC). Additionally, they provide switched access to IntereXchange Carriers (IXCs) for long distance calls via the LEC.
- Interexchange Trunks Bypassing the LEC CO switch, allow direct access to an IXC. These trunks are typically solely meant for long-distance network access to locations beyond of the LEC's local calling area. CO trunks can be used for switched access in the event of an interexchange trunk facility failure, offering an extremely effective level of redundancy.
- Foreign Exchange (FX or FEX) Trunks: Link up with a foreign CO directly. They are utilized to provide more affordable access to and from a remote location where a lot of traffic starts and ends. A user organization with a lot of traffic may decide to build an FX trunk in order to avoid paying long-distance calling rates. The user organization avoids long-distance fees thanks to the FX trunk's flat-rate, mileage-sensitive pricing (the distance between the city centers is around 35 miles). Small- to medium-sized system environments use FX lines with critical systems.
- Direct Inward Dial (DID) Trunks: Exclusively designed for incoming traffic. A DID number that generally relates to the internal station is given to each station. The CO recognizes that a call is being placed to a seven-digit DID number and connects the call via a dedicated DID trunk. By virtue of a unique signaling and control arrangement that exists

between the PBX and CO, the DID number is transmitted to the PBX prior to the call. With that knowledge, a smart PBX with the appropriate generic software load may route the call automatically and direct it to the station without the need for an attendant. DID numbers are rented by the service provider to user organizations in sets or blocks, such as 50, 100, or 250.

- Tie Trunks: In a private network architecture, directly interconnect or tie together PBXs. The systems will route calls between offices across leased-line tie trunks using ARS software, eliminating toll fees in the process. Tie lines are used to connect key systems when they are used in tandem with or behind PBXs.
- Wide Area Telecommunications Service (WATS) Trunks: These provide bulk long-distance access at a subsidized rate. Special-purpose WATS trunks are extremely uncommon today because they have been replaced with subsidized long-distance billing plans that are not dependent on trunk infrastructure.
- Incoming WATS calls are handled by INward WATS (INWATS) Trunks. The called party is responsible for paying the fees at a reduced rate per minute or fraction thereof. The INWATS are used outside of the US.
- ISDN Trunks: Support bonding, commonly known as dynamic bandwidth allocation, and N 64. With the use of this functionality, an application that needs more than a narrowband channel can be served by the ISDN-compatible PBX dynamically allocating, or bonding, additional contiguous 64 kbps channels.
- Direct Inward System Access (DISA) Trunks: These allow for generally toll-free remote access to the PBX system. The caller can enter authorization codes to gain access to associated resources (such as email servers, voice processors, computer systems, and outgoing toll lines) when the PBX answers the call.
- Analog Trunks: Required to support analog devices. The most popular fax machines are simpler and less expensive, and they only have analog line interfaces, despite the fact

that more advanced fax machines and fax servers are built with digital line and trunk interfaces. An analog line port is necessary for such equipment.

3. Station Interfaces

Station interfaces take the form of printed circuit boards that can handle numerous stations of the same general kind through multiple ports on a single interface card. For instance, analog line cards with analog ports can support analog voice sets, in which case a codec at the line card level digitizes the signal. Digital line cards can be used with digital telephones, in which case a codec included into the station set digitizes the analog signal. Computer workstations, printers, and other digital devices are all directly supported by digital line cards as well. Usually, line cards can support 4, 8, 16, or 32 ports.

4. Terminal Equipment

The user terminal equipment often takes the shape of a telephone set because PBXs are built primarily to facilitate voice traffic. Data terminals are also frequently included in terminal equipment, though. Examples of terminal equipment include the following:

- Telephone sets
  There are two types of telephone sets: generic and proprietary.
- Attendant consoles
  Incoming and outgoing calls can be answered and extended, operators can help incoming callers, and conference calls can be set up using attendant consoles. To improve attendant effectiveness and lower associated expenses, attendant consoles and attendants are frequently centralized in large, private network scenarios. Manufacturers of sizable, network-capable PBX systems provide the Centralized Attendant Service (CAS) capability.
- Maintenance and Administration Terminals
  PCs connected to the system are known as Maintenance and Administration Terminals (MATs). Although the modern

way of connecting is often over an Ethernet LAN, the MATs may be directly linked to a maintenance port on the system via an RS-232 connection. In most cases, remote maintenance can be carried out via the PSTN using a modem connection.

E. PBX Technical Details

Starting with the connection to the outside world, it can be done using a variety of technologies and protocols. Copper, optical fibers, and wireless technologies like WiFi, infrared, and microwave can all be utilized as the medium. Other nodes can be joined in PBX networks, typically using proprietary or specific universal interconnection protocols. Naturally, the media choices are the same as for connections to the outside world.

A network of cables and distribution frames is required for the PBX to be connected to the public network, to another PBX, or even to its internal users. All internal and external lines are connected to the PBX through the main distribution frame. It is positioned close to the PBX and has two sections, one for lines entering from the PBX and the other for lines exiting for the users and the outside network. For internal users, cables can be terminated in intermediate distribution frames that placed in racks in every floor of the building. The physical location where the PBX is actually located is the next physical PBX parameter. There are numerous instances where the PBX is put in a building's basement or the hallways, behind unsecured doors.

The PBX's telephone extensions are its primary users. If the appropriate boards are present, numerous sets can be connected in a PBX. A typical illustration of a list of sets along with their calling numbers. There are certain extensions-numbers on the PBX board, which is placed into a slot. Its extensions are given spatial-geographical IDs, each of which is assigned a specific extension number. One pair of cables, two pairs of cables, an optical link, or even a distance extension device can be used to connect the boards to the sets.

A PC or server running any O/S can serve as the administration or management station on PBX. Larger PBXs often incorporate the software in their own operating system, however smaller PBXs typically require the program to be placed in the external administrative server. The software in use may be a closed, proprietary operating system or one that is based on a general-purpose operating system that has been specially tailored for PBXs. The management suite enables the delivery of the PBX as well as controlling its operation, configuring, activating, and customizing features, as well as carrying out maintenance duties and other operations.

The PBX's internal database can be accessed using utilities. In fact, all essential PBX setup and operation data is kept in a database that is accessible from the management session or directly from the operating system. Although risky, this functionality is crucial for conveying changes inside a PBX network. The management suite's changes to the settings are reflected in the database.

Now let's talk about features and services. A wide range of services and features are available with modern PBXs. From basic call forwarding to cutting-edge multimedia teleconferencing, there are literally hundreds of services that can be provided. Depending on the service provider, they are either provided on an internal-local level or as network features. As was already mentioned, there is a great deal of complexity and systems interaction. Therefore, it makes sense that a method cannot be done with 100% success, including a comprehensive testing of all potential scenarios and parameters that could result in vulnerabilities.

F. System Capacity and Configuration

Physical and traffic are some dimensions that must be considered in the PBX capacity. Physical capacity is a measurement of the quantity of lines and trunks that can be supported by additional line and trunk cards and cabinets. Every system has a practical or finite limit on the total number of shelves, cabinets, circuit boards, and, eventually, ports that it can accommodate.

The amount of simultaneous discussions that may be accommodated is known as traffic capacity. This measurement is crucial, especially when switching between speech and data. You must take into account the processors' and buses' capacity. The maximum number of Busy Hour Call Attempts (BHCAs) and Busy Hour Call Completions (BHCCs) that the system can support is used to describe the processor capacity. According to empirical traffic research, the busiest time of the day is the hour that is considered to be the busy hour.

PBXs are typically set up as centralized systems, with all cabinets and auxiliary equipment placed close together for simple administration. A business with a vast campus environment may choose to use a decentralized strategy, with many intelligent cabinets placed in different campus quadrants and connected by high-capacity circuits. The capacity to connect several PBXs to a private tie-line network through tie trunks may be necessary for very big enterprises with numerous, widely scattered locations. A Virtual Private Network (VPN) is an alternative that can do the same thing. Even while dedicated leased connection trunks are not necessary, a VPN offers a lot of the features of a truly private network.

G. PBX Enhancements and Trends

The PBX is being positioned by manufacturers more and more as a communications server for voice, data, video, and image communications. In October 1995, the PBX team at Lucent Technologies created the first fully integrated multimedia PBX. The MultiMedia Communications eXchange (MMCX) Server allowed interfaces to Ethernet, ATM, and ISDN networks as well as all standard PBX telephone functions on multimedia calls containing any mix of voice, data, image, and video. The PBX innovations and trends as follow:

- By utilizing the same cable and wire infrastructure for both computer and telephone terminals, such linkages allow users to access computer programs over the PBX. ISDN or Ethernet lines can be used to connect the PBX to a host computer or local area network. In general, phone communications continued to be handled by the PBX, while data communications continued to be handled by the LAN. In actuality, voice has started moving to the LAN domain.
- Manufacturers of PBXs have long enabled modem sharing and slow data transmissions via terminal interfaces. Manufacturers are supporting high-speed connections to ATM and Ethernet LANs. Again, data connections through a PBX often proved to be too ineffective and expensive, so over time, this strategy received little genuine support. Rather, data continued to be

sent through the LAN and voice continued to be switched through the PBX. Voice is now moving to the LAN domain, which is the change in the opposite direction.

- Through a unique PBX wireless, a certain group of users can access wireless communications. A large office complex or campus can enable wired connections to antennas via special PBX ports. As long as they stay inside the antennas' constrained range, certain mobile users can utilize specific cordless telephones to stay in touch as they move around the company. The benefits of using wireless PBX technology include greater mobility, higher call completion rates, lower call-back costs, and higher productivity because fewer voicemails are being left. The disadvantages include rising costs, a lack of feature content, and security worries.
- Fax messaging is supported by several manufacturers. The user can access the fax message onscreen at a workstation. Due to the decline in demand for fax messaging with the introduction of e-mail and the high cost of the Application Programming Interface (API), this upgrade was never very well-liked in the traditional PBX.
- The integration of voice, data, and video via a single set of access and transport facilities, or access through a single high-capacity local loop to a single packet- switching broadband WAN, is another benefit of IP telephony, or VoIP.

H. IP PBX

Since the internet's widespread use, traditional Private Branch Exchange (PBX) telephone networks have undergone significant transformation. Businesses are gradually transitioning away from analogue systems and toward IP PBX alternatives.

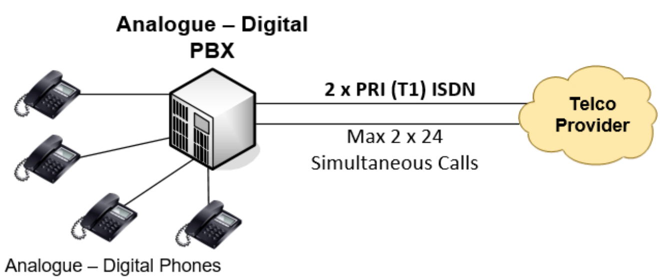

Figure 55. A typical Analogue-Digital PBX with phones and two ISDN PRI lines

Source: https://www.firewall.cx/general-topics-reviews/ip-pbx-unified-communications/1188-how-ip-pbx-work-best-free-voip-systems-advanced-unified-communications.html

In an IP-based system, intelligence is distributed over one or more microprocessor-based telephony servers and databases across several database servers. The telephones themselves are intelligent terminals and can take the form of either hardphones (hardware-based telephones) or softphones (software - based telephones residing on desktop, tablet, laptop, or other computer platforms).
The TDM technology created for voice communications is entirely disregarded by a pure IP PBX, or IPBX. A pure IPBX is built using a distributed client/server architecture, which is often deployed on a switched Ethernet LAN that has a speed of at least 100 Mbps. Client software that is installed on intelligent IP hardphones and softphones communicates with one or more servers that may be dispersed throughout a company, possibly in several locations. Each and every call control operation, including call creation and teardown, is handled by one or more telephony servers.

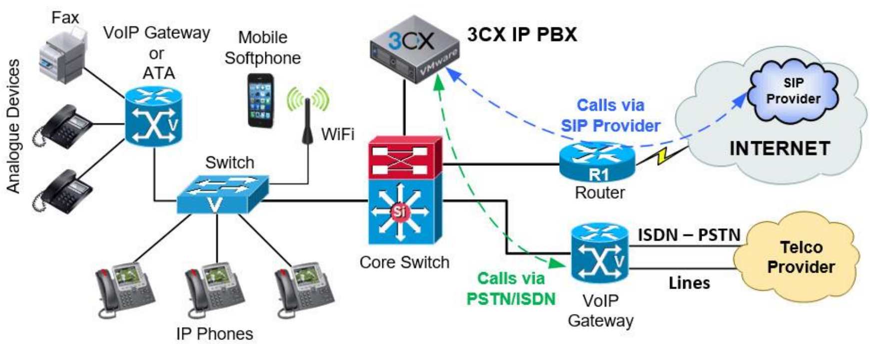

Figure 56. IP PBX and VoIP Components

Source: https://www.firewall.cx/general-topics-reviews/ip-pbx-unified-communications/1188-how-ip-pbx-work-best-free-voip-systems-advanced-unified-communications.html

Windows is the primary operating system for the IP PBX. The widely used SIP protocol is used for communication with the gateways and service providers for sip phones. Cisco and Microsoft are two well-known companies that support the open SIP standard. SIP phones, which can be hardware- or software-based, are communicated with by the IP PBX on one side.

Hardware-based sip phones function and appear exactly like regular phones. Software-based phones connect via USB via the computer's built-in headset. The IP PBX must then be able to make calls to external numbers. This can be done using VoIP gateways or VoIP service providers for gateways, which convert regular PSTN lines' analog data into digital signals that can be handled by the IP PBX and transmitted through a computer network.

PBXs has a sizable feature set that have long been present on digital PBXs, some of them have been improved. IP PBXs are the only devices with the following major features:

- Shared Infrastructure: The IPBX inevitably uses shared transmission infrastructure, which may include servers, routers, Ethernet switches, and other devices. Costs associated with administration and maintenance are also decreased thanks to this shared infrastructure.
- Scalability: A lot of IPBXs include modular design. Another system module can be installed at a reasonable cost as memory, port, or traffic capacity runs out and more capacity is needed.
- Networking: IPBXs make it easier to connect many sites to the internet.
- Redundancy and Resiliency: The Internet is highly resilient and redundant by nature. In general, IP networks tend to have these characteristics. VoIP call control can be either dispersed over several sites or consolidated at one location, with various backups and mirrored databases.
- User Interface: IPBXs in particular and CT systems in general both offer enhanced user interfaces. IP hardphones often have alphanumeric and softkey screens. Softphones are widespread and come with a user-friendly, well-known, and even intuitive GUI that is simple to operate with a mouse, keyboard, and touch screen.
- Voicemail, e-mail, IM, and even fax mail are all highly and simply accessible through a single user interface on a single softphone for messaging.

- Presence: Much like with instant messaging, users can control their own presence, or available status. To put it another way, a user can advertise his or her availability by saying that they are online and available for email or instant messaging but unavailable for phone calls, unavailable for IM or phone calls, out to lunch, or otherwise unavailable.
- Find me or follow me Call forwarding allows users to set their own rules, with special options for friends and family, coworkers, and clients, for instance. Calls from one class of callers may go immediately to voice mail in the event of a no-answer situation, whereas calls from another class may go to a mobile phone or home phone.
- Multimedia Conferencing: A user can schedule a conference using a calendaring tool with the added option to control which conferencing features are available to each participant at any given time. By doing so, the presenter is better able to adapt a multimedia presentation to the audience's needs, both individually and collectively. There may be voice, video, text, graphics, and whiteboarding available as media options.
- Voice/Data Integration: Since speech and data infrastructure is shared and IP softphones are intelligent, multitasking, voice-enabled computer workstations, it is simple to access data while on a voice call.
- Moves, Adds and Changes: Just like in a data-only Ethernet context, MAC action is simple to do in an IPBX setting. In instance, moves are frequently plug'n play. Through a password-protected intranet interface, the system administrator or even the end user can carry out numerous other MACs.
- Mobility and portability: Users of softphones can move them wherever in the organization where an Ethernet port is accessible, plug them in, and nearly instantaneously be online.
- Remote Access: Softphones are portable enough to allow for simple Internet connections to the IPBX from a variety of locations, including homes, hotels, coffee shops, and other public spaces. IPBX technology offers excellent support for teleworkers, or telecommuters, provided they have internet or cable modem connections and the hardware and software required to create a VPN tunnel to the main office.

The benefits of IP PBX technology are:

- ✓ Lower communication expenses - compared to analog PBXs, Internet-connected PBXs can offer substantially higher cost savings. Both metered and unmetered trunking services are provided by VoIP service providers.
- ✓ Reliability in the cloud - Connect your current PBX to the cloud's dependable history. For stable performance, a trustworthy VoIP service will have many data centers. They can divert calls elsewhere even if your PBX is unavailable.
- ✓ Maintains existing hardware - By continuing to use the hardware that is already connected to the PBX.
- ✓ Minimal change - Many firms find change to be unsettling. Consider SIP trunking as a starting point for realizing the benefits of a VoIP phone system. we may easily increase the number of voice channels as the business expands.

Review Questions

Q1. The type of PBX that can be installed with analog, digital and IP phone types is ....

Q2. The majority of PBXs were built using a ………………

Q3. What are the benefits of IP PBX technology?

Q4. What are some dimensions that must be considered in the PBX capacity?

Q5. Draw a telephone network that uses at least 2 different types of PBX that are connected to each other!

CHAPTER 9
GROUNDING & BONDING

A. Basic Concept

This chapter will cover the term "Ground," which is frequently used but also sometimes misinterpreted. Ground is known by many different names. There are many different types of ground, including earth, earth ground, neutral, common ground, analog ground, digital ground, and instrument ground, to mention a few as shown on the following figure.

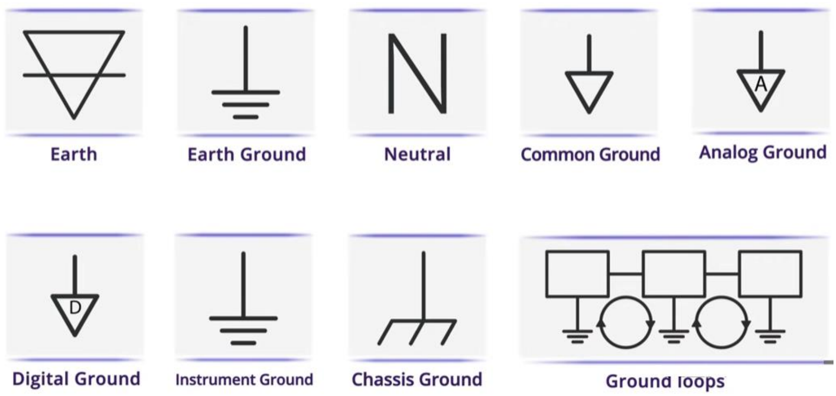

Figure 57. Types of grounding

Source: https://www.youtube.com/watch?v=YO-Dnk6ZKrI

Ground can signify many different things to various individuals. An electrician's definition of "Ground" may differ from an electronic engineer's definition. There are numerous explanations for grounding. All electrical systems and installations must have proper grounding as a vital safety precaution.

In order to prevent internal wire failures from dangerously raising the voltage potential of these exposed electrical parts, we ground them. Current flow requires the completion of every electrical circuit. The act of grounding acts as a circuit return path in various applications. As an illustration, the chassis of your car serves as a single ground for all battery return current.

So let's examine some of the various perspectives on the ground. That Earth and Earth Ground are the same thing is generally a given.

The reference point in an electrical circuit that is directly and physically connected to the earth is known as "earth ground." The ground you walk on is called earth ground. True zero volts exist on Earth Ground. It is the true zero reference for any and every electricity discussion.
There is earth ground proof everywhere you look. A copper rod in the ground with a thick wire attached to it may be visible. This Earth Ground wire travels to your electrical panel before connecting to all of the Ground terminals on each outlet in your home as shown on the following figure.

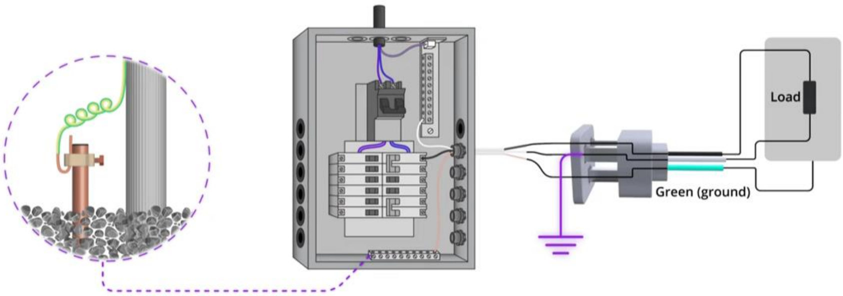

Figure 58. Grounding
Source: https://www.youtube.com/watch?v=YO-Dnk6ZKrI

The fact that a wire from the Neutral terminal also connects to Earth Ground at the end. Take note of the electrical symbol we've used to represent Earth Ground. Electrical schematics commonly use this symbol incorrectly more than any other. The International Electrotechnical Commission document IEC 60417 Graphical Symbols for Use on Equipment contains the symbols used to denote ground terminals. The symbol for Earth Ground is 5017. Every electrical circuit must be finished in order for current to flow, as we mentioned earlier. In numerous applications, the common denominator serves as the return route. For instance, the chassis of your car serves as a common ground for the return current to the negative terminal of the battery. On electronic schematics, the Earth Ground sign may occasionally be used erroneously. The goal is to represent a Common Ground, which may or may not be related to Earth Ground.
The following figure is a typical illustration of a little component of a sizable electronic circuit encased inside a metal chassis. There are four symbols for the ground that might or might not be related to the

earth's surface. However, they are meant to highlight a Common Ground point. We do know that the voltage will be +15 volts if we measure it from Point A to any of these common ground points.

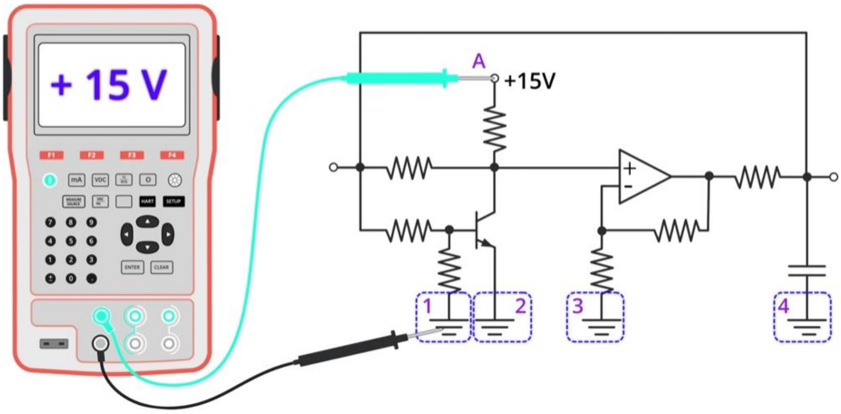

Figure 59. A typical illustration of a little component
Source: https://www.youtube.com/watch?v=YO-Dnk6ZKrI

All return paths to the power source should be connected together at one point in the circuit, as shown in the ideal wiring diagram. Sadly, this is frequently not feasible. It would be more acceptable to use the symbol IEC 60417 5020 if points 1 through 4 are connected to a Common Ground rather than to Earth Ground. This symbol implies that the points are wired to a chassis or frame terminal.

B. The Necessity Grounding and Bonding for Telecommunication Systems

Telecommunications grounding and bonding have grown to be a more lucrative market for electrical contractors due to the rise in demand for computer network installations. It has been difficult to comprehend the vocabulary and unique concerns used in the telecommunications industry, even if comparable basic principles apply.
Networks and equipment used for telecommunications should be grounded to the electrical service, just like with conventional electrical grounding. But when it comes to dealing with telecommunications systems, just grounding to structural steel is insufficient. The telecommunications cabling and power must be effectively equalized due to the sensitivity of the electronic

equipment in order to prevent loops or transients that could harm the equipment. Creating a comprehensive grounding and bonding system that goes beyond the fundamental "green-wire" concept is necessary to accomplish this.

C. Grounding and Bonding Definition

The safety circuits for electrical systems' branch circuits and feeders are bonding and grounding. Bonding and electrical grounding are two defensive processes that take place simultaneously. Grounding and bonding have traditionally been thought of as the major means of shielding equipment, buildings, and people from electrical shock and fire risks while also providing a number of benefits for system operation.

These two procedures lower the risk of shock while simultaneously performing crucial protective duties for machinery and other property. Potential differences between electrical systems and equipment and the earth are reduced by the process of grounding a system or piece of electrical equipment. The phrase "grounding" refers to a path of connection to the earth. The goal of earthing is to provide a way to let line-to-earth fault current flow through a system at a high enough level to operate the protective device inside the allowed disconnection window.

There is a connection when there is bonding. Bonding serves the purpose of joining conductive items together. Bonding is the electrical connection of two or more conducting things, making them into one. Bonding is the process of joining two electrically conductive items so that they operate as one unit, eliminating possible differences between them and lowering the risk of electric shock. We also can say that bonding is a connection method that balances electrical potential differences or permits current to flow back to its source.

Bonding reduces potential (voltage) differences between connected conductive elements. Conductive components are connected as a result of bonding. As a result, bonding takes place and grounds electrical equipment when it is grounded and connected to other equipment (the connection to the Earth). Bonding is necessary because electrically conductive components, including structural steel, metal cable trays, and metallic supporting structures, could activate themselves in the case of coming into touch with lightning, line surges, or unintended contact with high voltage lines.

D. Grounding Systems for Telecommunications

Every telecommunications room (TR) in the building is connected physically to the building's grounding electrode system by the telecommunications grounding and bonding system. The following elements are typically found in a telecommunications grounding system that adheres to the ANSI/TIA/TIA-607 standards:

- Telecom Entrance Facility (TEF)
  The telecoms entrance facility (TEF) consists of the area where the backbone facilities for the inter- and intra-building join as well as the access point to the telecommunications service. The TEF may house electrical components and antenna entrances for telecommunications.
- Telecom bonding conductor.
  All communications bonding conductors must comply with the ANSI/EIA/TIA-607 standard, which mandates that they be listed for their intended use and approved by a nationally renowned testing laboratory like UL or ETL. Bonding conductors must always be made of insulated wires. Bonding conductors must also be formed of copper metal, as specified by the specification. The ANSI/EIA/TIA-607 standard forbids the use of other metal types as bonding conductors. All bonding conductors must also be at least #6 AWG in size.

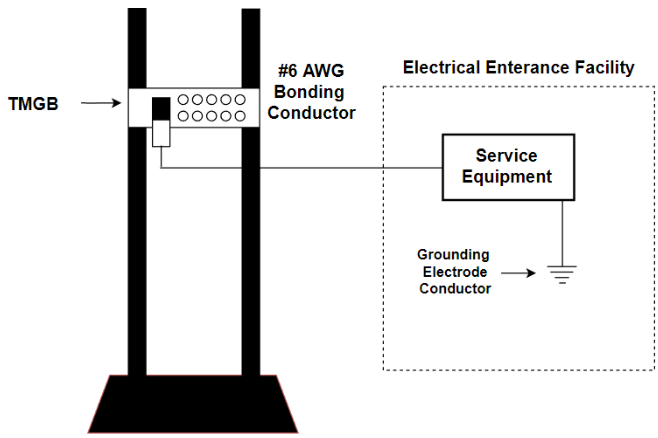

Figure 60. Telecom Bonding Conductor

The ANSI/EIA-TIA-607 standard forbids using bonding conductors in an iron-based metallic conduit. According to this standard, bonding conductors must be bonded at both ends of iron conduits that are longer than 1 m (3 ft). The bonding conductor must be connected with wires that are at least #6 AWG in diameter.

- Telecom main grounding busbar (TMGB).

  The TMGB is a specifically designed addition to the building grounding electrode system for the communications network. The TMGB need to be simple for telecommunications staff to access since it serves as the main attachment point for TBBs and equipment.

  The TMGB is predrilled copper busbar with standard NEMA bolt holes of the appropriate size and spacing for the intended lug connection. It should have adequate space to meet current needs and allow for expansion in the future. 100 mm in width and a minimum thickness of 6 mm are needed. There are many different types of ground bars, some of which are available as kits that can be tailored to match the particular needs of the application. Prewelded Cadweld pigtails are available with insulated or bare conductors, in a range of conductor lengths, and are prepared to be fastened to the building ground.

  The primary method for reducing resistance is electrotin plating. The mating surfaces must be fully cleaned if they are not plated. The alternating current equipment ground bus (or a metallic enclosure) must be bonded to the TMGB/TGB where telecommunications panelboards are located with the TMGB. While positioning TMGBs as close to the panelboards as possible, the necessary clearances must be kept in place.

  Exothermic welds should be used for connections to the TMGB or lugs. Exothermic welds offer a connection that aids in preserving the grounding system's long-term integrity.

- Telecom bonding backbone (TBB).

  All TGBs are connected to the TMGB through the TBB, which acts as a conductor. Potential disparities between the telecommunications systems to which it is linked are decreased or equalized. The only conductor that offers a ground fault current return channel shouldn't be the TBB.

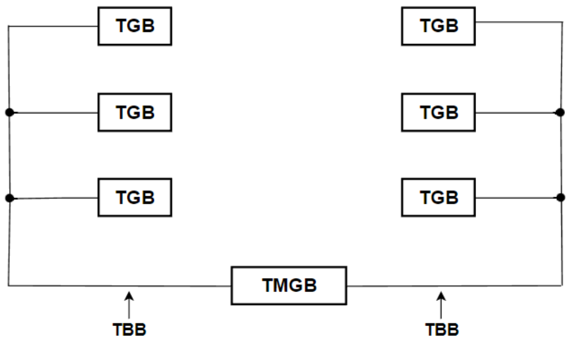

Figure 61. Telecom Bonding Backbone

Through telecommunications backbone channels, the TBB loops around the entire building starting from the TMGB. Every telecommunications closet and equipment room in the building has a TGB connected to it. Depending on the size of the building and the number of TGBs inside, multiple TBBs can be required. The backbone for telecommunications bonds should not be made of water pipes or iron cable shield.

Each TBB should be made of an insulated copper conductor that is at least No. 6 AWG in size and may even be as large as 750 kc mil, which is frequently used by telecommunications and phone companies. A TBB interconnection bonding conductor (TBBIBC) must be located on the top floor and at least every third floor of a multi-story building when more than one TBB is being used.

- Telecom grounding busbar (TGB).

TGBs are centrally connected systems and equipment that are served by a communications closet and have predrilled copper busbars with typical NEMA bolt hole sizes. It must be at least 50 mm wide and 6 mm thick. Similar to the TMGB, the TGB needs to be cleaned or electrotin-plated before the conductors are connected to the busbar. The TBB to TGB bonding conductor should be continuous and run in the shortest amount of time.

The TGB is frequently mounted to the panelboard's side. Each TGB should be connected to the structural steel in the same room with a No. 6 AWG conductor once the building's structural steel is effectively grounded. In the grounding system, always employ the shortest distance possible.

- Telecom bonding backbone interconnecting bonding conductor (TBBIBC).
  When two or more TBBs are put vertically in the intrabuilding backbone pathway, they must be linked together according to the ANSI/EIA/TIA-607 standard. The element utilized for this purpose is the telecommunications bonding backbone interconnecting bonding conductor (TBBIBC) (see the figure above).

The TBBIBC must be put at least every third story and on the top floor in accordance with the ANSI/EIA/TIA-607 standard. The TBB conductor size must be smaller than the minimum size of the TBBIBC.
The TBBIBC could also be used to connect many TGBs that are placed in the same TR. The TGBs installed in several TRs located on the same floor of the building are also bound together via the TBBIBC. The requirements for this connection would be the same as bonding multiple TBBs at the top floor and at least every third story.
The system starts at the electrical service entry, proceeds to the TMGB, then loops back to each TGB, which are located in separate telecoms closets on each floor of the building structure.

SUMARY

The term "telecommunications grounding and bonding" refers to additional grounding and bonding that has been built expressly for telecommunications. This is usually included to address the performance of telecommunications systems; it is not a replacement for the grounding and bonding requirements set forth by the National Electrical Code (NEC).
A thorough set of regulations for both electrical and communication cabling is found in the NEC. Communication cable installation for phone systems, telegraph systems, burglar alarm systems, and other central station systems is covered by Article 800.

Review Questions

Q1. What is grounding?

Q2. What is the purpose of grounding in telecommunication?

Q3. Why is bonding necessary?

Q4. A specifically designed addition to the building grounding electrode system for the communications network is called …………

Q5. What is Telecom grounding busbar (TGB)?

GLOSSARY

Analog: A transmission mode in which information is transmitted by converting it to a continuously variable electrical signal.

ANSI (American National Standards Institute): The national standards development body in the USA.

Bandwidth: The range of frequencies a communications channel is capable of carrying without excessive attenuation.

Basic rate interface (BRI): The basic ISDN service consisting of two 64-kbps information or bearer channels and one 16-kbps data or signaling channel.

Battery: A direct current voltage supply that powers telephones and telecommunications apparatus.

Bit error rate (BER): The ratio of bits transmitted in error to the total bits transmitted on the line.

Bit rate: The speed at which bits are transmitted on a circuit; usually expressed in bits per second.

Bit: The smallest unit of binary information; a contraction formed from the words BInary digIT

Broadband: A term used to describe always-on access to the Internet by cable, DSL, or satellite. Also, a form of LAN modulation in which multiple channels are formed by dividing the transmission medium into discrete frequency segments. Also, a term used to describe high bandwidth transmission of data signals.

Broadcast: A transmission to all stations on a network.

Byte: A set of eight bits of information equivalent to a character. Also called an octet.

Central office (CO): A switching center that terminates and interconnects lines and trunks from users.

Central processing unit (CPU): The control logic element used to execute instructions in a computer

Channel: A path in a communications system between two or more points, furnished by a wire, radio, lightwave, satellite, or a combination of media.

Circuit switching: A method of network access in which terminals are connected by switching together the circuits to which they are attached. In a circuit-switched network, the terminals have full real-time access to each other up to the bandwidth of the circuit.

Circuit: A transmission path between two points in a telecommunications system.

Coaxial cable: A single-wire conductor surrounded by an insulating medium and a metallic shield that is used for carrying a telecommunications signal.

Common channel signaling (CCS): A separate data network used to route signals between switching systems.

Common control switching: A switching system that uses shared equipment to establish, monitor, and disconnect paths through the network. The equipment is called into the connection to perform a function and then released to serve other users.

Crosstalk: The unwanted coupling of a signal from one transmission path into another.

Data: Digitized information in a form suitable for storage or communication over electronic means.

Dedicated circuit: A communications channel assigned for the exclusive use of an organization. Also known as a private line.

Delay: The time required for a signal to transit the communications facility; also known as latency.

Digital: A mode of transmission in which information is coded in binary form for transmission on a network.

Downlink: The radio path from a satellite to an earth station.

Download: To send information from a host computer to a remote terminal.

E & M signaling: A method of signaling between offices by voltage states on the transmit and receive leads of signaling equipment at the point of interface.

Echo: The reflection of a portion of a signal back to its source.

Electronic mail: A service that enables messages and file attachments to be transferred across a communication network.

Error: Any discrepancy between a received data signal from the signal as it was transmitted.

Ethernet: A proprietary contention bus network developed by Xerox, Digital Equipment Corporation, and Intel. Ethernet formed the basis for the IEEE 802.3 standard.

ETSI (European Telecommunications Standardization Institute)

Facsimile: A system for scanning a document, encoding it, transmitting it over a telecommunications circuit, and reproducing it in its original form at the receiving end.

Frequency: The rapidity, measured in cycles per second or Hertz (Hz), with which an alternating current varies from peak to peak.

Gateway: Circuitry used to interconnect networks by converting the protocols of each network to that used by the other.

Hybrid: A key telephone system that has many of the features of a PBX. Such features as pooled trunk access characterize a hybrid. Also, a multiwinding coil or electronic circuit used in a four-wire terminating set or switching system line circuits to separate the four-wire and two-wire paths.

Integrated services digital network (ISDN): A set of standards promulgated by ITU-T to prescribe standard interfaces to a switched digital network.

Interface: The connection between two systems. Usually hardware and software connecting a computer terminal with peripherals such as DCE, printers, etc.

International Telecommunications Union (ITU): An agency of the United Nations that is responsible for setting telecommunications standards.

Internet protocol (IP): A connectionless protocol used for delivering data packets from host to host across an internetwork.

Jitter: The variation in arrival intervals of a stream of packets. Also, the phase shift of digital pulses over a transmission medium.

Latency: The time it takes for a bit to pass from origin to destination through network; also known as delay.

Leased line: A nonswitched telecommunications channel leased to an organization for its exclusive use.

Link: A circuit or path joining two communications channels in a network.

Local area network (LAN): A narrow-range data network using one of the nonswitched multiple access technologies.

Local loop: See Subscriber loop.

Main distributing frame (MDF): The cable rack used to terminate all distribution and trunk cables in a central office or PBX.

Message switching: A form of network access in which a message is forwarded from a terminal to a central switch where it is stored and forwarded to the addressee after some delay.

Microwave: A high-frequency, high-capacity radio system, usually used to carry multiple voice channels.

Modem: A contraction of the terms MOdulator/DEModulator. A modem is used to convert analog signals to digital form and vice versa.

Modulation: The process by which some characteristic of a carrier signal, such as frequency, amplitude, or phase is varied by a low-frequency information signal.

Mobile telephone switching office (MTSO): The electronic switching system that switches calls between mobile and wireline telephones, controls handoff between cells, and monitors usage. This equipment is known by various trade names.

Network: A set of communications nodes connected by channels.

Node: A major point in a network where lines from many sources meet and may be switched. Noise: Any unwanted signal in a transmission path.

Off-hook: A signaling state in a line or trunk when it is working or busy.

On-hook: A signaling state in a line or trunk when it is nonworking or idle.

Packet switching: A method of allocating network time by forming data into packets and relaying it to the destination under control of processors at each major node. The network determines packet routing during transport of the packet.

Packet: A unit of data information consisting of header, information, error detection, and trailer records.

Prefix: A three-digit (in North America) code that is the third tier in the E.164 numbering plan, after country code and area code.

Primary rate interface (PRI): In North America a 1.544-mbps information-carrying channel that furnishes ISDN services to end users. Consists of 23 bearer channels and one signaling channel. In Europe a 2.048-mbps channel consisting of 30 bearer and two signaling channels.

Private automatic branch exchange (PABX): A term often used synonymously for PBX. A PABX is always automatic, whereas switching is manual in some PBXs.

Private branch exchange (PBX): A switching system dedicated to telephone and data use in a private communication network.

Propagation delay: The absolute time delay of a signal from the sending to the receiving terminal.

Protocol: The conventions used in a network for establishing communications compatibility between terminals and for maintaining the line discipline while they are connected to the network.

Public data network (PDN): A data transmission network operated by a private telecommunications company for public subscription and use.

Public switched telephone network (PSTN): A generic term for the interconnected networks of operating telephone companies.

Quality of service (QoS): A measure of parameters such as delay, jitter, and packet loss that affect isochronous transmissions.

Register: A device in a switching system that provides dial tone and receives and registers dialed digits.

Response time: The interval between the user's sending time of the last character of a message and the time the first character of the response from the host arrives at the terminal.

Router: A device that operates at layer 3 in the OSI hierarchy to forward packets between devices across a network.

Routing: The path selection made for a telecommunications signal through the network to its destination.

Signaling System #7 (SS7): An out-of-band signaling protocol between public switching systems.

Signal-to-noise ratio: The ratio between signal power and noise power in a circuit.

Network Management Protocol (SNMP): A management protocol for monitoring and controlling network devices.

Telecommunications grounding busbar: A grounding point for telecommunications services and equipment in each telecommunications equipment room and closet.

Telecommunications main grounding busbar (TMGB): The central grounding point for telecommunications equipment rooms and closets. The TMGB is bonded to the electrical ground and to the building's metal framework.

Telecommunications: The electronic movement of information.

Terminal: A fixture attached to distribution cable to provide access for making connections to cable pairs. Also, any device meant for direct operation over a telecommunications circuit by an end user.

Throughput: Information bits correctly transported over a data network per unit of time.

Time division multiplexing (TDM): A method of combining several communications channels by dividing a channel into time increments and assigning each channel to a time slot. Multiple channels are interleaved when each channel is assigned the entire bandwidth of the backbone channel for a short period of time.

Topology: the architecture of a network or the way circuits are connected to link the network nodes.

Transmission Control Protocol (TCP): A protocol for providing reliable end-to-end delivery of data across an internetwork, usually used with IP.

Transmission: The process of transporting voice or data over a network or facility from one point to another.

Trunk: A communications channel between two switching systems equipped with terminating and signaling equipment.

Uplink: The radio path from an earth station to a satellite.

Virtual private network (VPN): An IP network that is defined over a carrier's IP network, providing security by authentication and encryption.

Voice mail: A service that allows voice messages to be stored digitally in secondary storage and retrieved remotely by dialing access and identification codes.

Wireless: A radio or infrared-based service that enables telephone or LAN users to connect to the telecommunications network without wires.

INDEX

BIBLIOGRAPHY

Dodd, A.Z. 2019. *The Essential Guide to Telecommunications 6th Edition*. New York: Addison Wesley.

Green, J., H., 2006. *The Irwin Handbook of Telecommunications 5th edition.* USA McGrawHill.

Lannone, E. 2012. *Telecommunication Networks*. Boca Raton: Taylor & Francis Group.

Marchese, M. 2007. *QoS Over Heterogeneous Networks.* England: John Wiley & Sons Ltd.

Medhi, D., Ramasamy, K. 2007. *Network Routing: Algorithms, Protocols, and Architectures.* San Francisco: Elsevier Inc.

Oodan, A., Ward, K., Savolaine, C., Daneshmand, M., & Hoath, P. 2009. *Telecommunications Quality of Service Management: from legacy to emerging services.* A.P. Oodan (Ed.). London: The Institution of Engineering and Technology.

Pentinen, T.J. 2015. *The Telecommunications Handbook: Engineering Guidelines for Fixed, Mobile, and Satellite Systems.* United Kingdom: John Wiley & Sons Ltd.

Tarmo, A. 2003. *Introduction to Telecommunications Network Engineering 2nd edition*. Norwood: Artech House Inc.

Valdar, A. 2017. *Understanding Telecommunications Networks 2nd Edition*, London: The Institution of Engineering and Technology.

Wright, E., Reynders, D. 2004. *Practical Telecommunications and Wireless Communications for Business and Industry.* Burlington: IDC Technologies.

AUTHOR'S BIOGRAPHY

Dianthy Marya, S.T., M.T. The author completed her postgraduate education at Telkom University, Faculty of Electrical Engineering, Master of Telecommunications Electrical Engineering. Currently the author works as a lecturer at the Polytechnic State of Malang, Department of Electrical Engineering, Digital Telecommunication Network Study Program since 2019. The author can be contacted via email dianthy@polinema.ac.id.

Martono Dwi Atmadja, Ir., MMT. The author completed his postgraduate education at Sepuluh Nopember Institute of Technology. Currently the author works as a lecturer at the Polytechnic State of Malang, Department of Electrical Engineering, Digital Telecommunication Network Study Program since 1987. The author can be contacted via email martono.dwi@polinema.ac.id

M. Nanak Zakaria, S.T., M.T. The author completed his postgraduate education at Brawijaya University. Currently the author works as a lecturer at the Polytechnic State of Malang, Department of Electrical Engineering, Digital Telecommunication Network Study Program since 1999. The author can be contacted via email nanak_zach@polinema.ac.id