Empirical Study on Network Management of Asia Pacific Communication Ltd.

By

Md. Imran Hossan

ID: 153-19-1815

This Internship Report is presented in partial fulfillment of the requirements of the Degree of Bachelor of Science in Electronics and Telecommunication Engineering.

Supervised By

Engr. Md. Zahirul Islam
Assistant Professor
Department of ICE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY
DHAKA-1207, BANGLADESH
December, 2018

APPROVAL

This Internship Report Titled "**Empirical Study on Network Management of Asia Pacific Communication Ltd**" is submitted by Md**. Imran Hossan** to the Department of Information & Communication Engineering, Daffodil International University, has been accepted as fit for the partial fulfillment of the condition for the Degree of B.Sc. (Hon's) in Information & Communication Engineering & approved as to its style and guts. The Presentation will be held on October, 2018.

BOARD OF EXAMINERS

Md. Taslim Arefin Chairman
Associate Professor & Head
Department of ICE
Daffodil International University

Prof. Dr.A.K.M Fazlul Haque Internal Examiner
Professor
Department of ICE
Daffodil International University

Dr. Engr. Quamruzzaman Internal Examiner
Professor
Department of ICE
Daffodil International University

S.K. Aditya
Dr. Subrata Kumar Aditya External Examiner
Professor
Department of EEE
University of Dhaka

APCL ASIA PACIFIC COMMUNICATION LTD.

☎ +880 2 9862364-5 ✉ info@apclbd.net www.apclbd.net Siraj Tower (Level 5), House # Ta-114/1
Badda Link Road, Gulshan-1, Dhaka-1212

Date: Dec 23 2018

TO WHOM IT MAY CONCERN

This is to certify that, Md. Imran Hossan, S/O- Md. Golam Mostofa and Amina Begum, an undergraduate student of Daffodil International University under the department of Electronics and Telecommunication Engineering, successfully completed Three months (From 1st Sep 2018 to 1st Dec 2018) long internship at this Company.

His internship activity includes understanding the implementation, operational and maintenance activities of the data communication network of the company.

During the period of his internship program with us he had been exposed to different process was found punctual, hardworking and inquisitive.

We wish him every success in his life and career.

Khalid Pervez
Director
Asia Pacific Communication Limited
Phone:029862365
Contact: 01712011071
Email: khalid@apclbd.net
Web: www.apclbd.net

Khalid Pervez
Director
Asia Pacific communication Ltd.

Acknowledgement

At First, I am like to convey my gratitude to the Almighty for charitable me the right path while trying the duty. The real sprit of achieving a goal is finished the way of quality and austere castigation. I would have never thrived in effecting my task without the teamwork, help and support provided to me by many personalities. This internship report would not consume been possible without the provision and direction of **Engr. Md. Zahirul Islam, Assistant Professor,** Department of Information Communication Engineering, Daffodil International University, Dhaka, under whose direction I chose this topic. I would like to rapid my heartiest gratitude to **Md. Taslim Arefin, Associate Professor and Head,** Department of Information and Communication Engineering, for his kind help to surface our thesis and also to other faculty participants, the staffs of the ETE Department of Daffodil International University must grant with due esteem the perpetual support and endurance of my family members for final this internship.

Abstract

Network management is challenging. To operate, maintain, and secure a communication network, network operators must grapple with low-level vendor-specific configuration to implement complex high-level network policies. Despite many previous proposals to make networks easier to manage, many solutions to network management problems amount to stop gap solutions because of the difficulty of changing the underlying infrastructure. The Asia Pacific Communication Limited (ACPL) has been one of the remarkable companies among all the large enterprises of Bangladesh. This practicum report is focus on the main branch. In this report the network infrastructure, communication, support, maintenance, security and development ACPL studied thoroughly. The existing network is well formed and up to date. But there are few limitations are there which may overcome which is also addressed in this report.

Table of Contents

Chapter 1 Introduction

Chapter 2 Organization overview

Chapter 3 overview of data communication and networking

Chapter 4 Overview of IP addressing

Chapter 5 ISP Network of APCL

Chapter 6 Upgradation of APCL Network

Chapter 7 Design of Upgraded Network of ACPL

Chapter 8 Conclusion

List of Figures

List of Table

Chapter 1

Introduction

1.1 Introduction:

Data communication and Computer networking is a most important part of the information technology. Today every business in the world needs a computer network for smooth operations, flexibly, instant communication and data access. Just imagine if there is no network communication in the university campuses, hospitals, multinational organizations and educational institutes then how difficult are to communicate with each other. Modern world scenario is ever changing. Data Communication and network have changed the way business and other daily affair works. Now, they highly rely on computer networks and internetwork. A set of devices often mentioned as nodes connected by media link is called a Network. A node can be a device which is capable of sending or receiving data generated by other nodes on the network like a computer, printer etc. These links connecting the devices are called Communication channels. Computer network is a telecommunication channel using which we can share data with other computers or devices, connected to the same network. It is also called Data Network. The best example of computer network is Internet.

The report is prepared for the purpose of the fulfillment of practicum as the graduation requirement of Electronics and Telecommunication Engineering in Daffodil International University, under the Asia Pacific Communication Ltd from September 15th, 2018 to December 15th, 2018. This is a great pleasure to work with the APCL, on their Data Center Migration along with the networking system. Through this work, it was possible to gain practical knowledge about the computer networking implementation and network infrastructures during the internship period. . At first, the review of PC arrange framework, hierarchical data, APCL organize structures and usage, and security and support are talked about. In the wake of concentrate the entire system of Data focus, APCL Ltd, a thought is proposed to encourage the server farm organize framework. The prevalent bundle following programming named as CISCO parcel tracer rendition 7.2 is used to demonstrate the execution of the current system of APCL and proposed work.

1.2 Asia Pacific Communication Ltd (APCL)

Asia Pacific Communication Limited (APCL) is a nationwide internet service provider in Bangladesh. We provide nationwide broadband connectivity with maximum availability. To ensure high availability we use fiber optic cable with diversify path through different NTTN. Customer gets high availability and committed information rate with consistent throughput. We use MPLS-VPN to serve our customers to ensure maximum security. The network is monitored by proper monitoring tools so that we can find out any fault of a circuit very quickly and able to rectify it within the Service Level Agreement (SLA) of customer. We are continuously expanding our network to reach customer doorsteps for quicker delivery. We research new product and services for continuous improvement.

1.3 Vision of APCL

To become the most adorable organization in serving of choice in serving the Nation as a progressive and Socially Responsible financial institution by supplying tools& support together for profit and sustainable growth. Its hares a significant portion of the ISP’s sector by utilizing available manpower and also state of the art technology for maximizing the shareholder’s wealth.

1.4 Mission of APCL

The missions of APCL are set out as follows:

1. Delivering excellent financial support to our communities based on strong customer relationship.

2. Providing long lasting solutions that combining our cutting-edge technology, experience and financial strength to our clients and stakeholders.

3. Creating a cohesive and friendly environment where customers and our people can excel.

1.5 Address of APCL

Corporate Office:
Day-Night Siraj Tower,
Ta-114/1 (Level 5),
Gulshan Link Road,
Dhaka-1212

Email: info@apclbd.net
Phone: +880 2 9862365
NOC: +880 2 9862364

Chapter 2 Organization overview

2.1 Company Profile

Asia Pacific Communication Limited (APCL) is a nationwide internet service provider in Bangladesh. We provide nationwide broadband connectivity with maximum availability. To ensure high availability we use fiber optic cable with diversify path through different NTTN. Customer gets high availability and committed information rate with consistent throughput. We use MPLS-VPN to serve our customers to ensure maximum security. The system is checked by legitimate observing apparatuses so we can discover any blame of a circuit rapidly and ready to amend it inside the Service Level Agreement (SLA) of client. We are consistently growing our system to achieve client doorsteps for snappier conveyance. We investigate new item and administrations for nonstop enhancement.

2.2 Objectives of APCL

The objectives of APCL are set out as follows:

- Provide uninterrupted excellent quality of Service
- Maximum pay off from current TCO (Total Cost of Ownership)
- Excellent support for ultimate comfort
- To facilitate high speed, dedicated broadband connectivity directly to client’s premises over a radio/wireless and Optical Fiber link.
- To provide data connectivity almost anywhere in the country through its

2.3 Corporate Information of APCL

Asia Pacific Communication Limited (APCL) is a notable ISP spend significant time in coordinated security and innovation arrangements. They convey to its customer’s finish IT arrangements. They generally say to you "Give Your Hand and Take the World in It." They would love to associate every client to the Internet, and give them a stage to Communicate and collaborate.

Asia Pacific Communication Ltd is delivering internet service for all business clients. A major % of the high class bandwidth sale is based on the corporate clients. APCL is always grateful to them and they try their best to serve them the best. They can have here WAN Connectivity, VPN etc. Here you will find the widest network to serve you no matter where you work or live.

2.4 APCL Services

As a commercial organization, APCL provides all internet services to people. More over it presents a good number of innovative services and products for the clients. The services offered by APCL are shown below:

- Internet Service.
- Data Service.
- System Integration
- IPLC Circuit: International Data Service
- Security Surveillance
- Unified Threat Management.

(a)Internet Service

A reliable internet connection opens the enormous window of opportunities in front of the businesses. Subscription to APCL business internet service provides customers the access to a vast number of options to get benefit from its hosted services as their business requires.

Their internet service has features that include:

- Redundant Transmission.
- Internet Router with proper functionality.
- Installation and Commissioning of Internet Router.
- Provisional Acceptance Test(PAT): QoS Testing.
- Final Acceptance Testing After one-month Service Period: QoE Testing.
- 24×7 Customer Service (Mobile Apps and IVR Facility).

- Additional Service for Google Caching, Web filtering and Unified Thread Management.
- Knowledge based Support.
- Training and High Level Topology Sharing.

(b)Data Service

They provide:

- Redundant Transmission.
- Transmission Router.
- Installation and Commissioning of Transmission Router.
- Provisional Acceptance Test(PAT): QoS Testing.
- Final Acceptance Testing After one-month Service Period: QoE Testing.
- 24×7 Customer Service (Mobile Apps and IVR Facility).
- Additional Service for P2P or P2M GRE Tunnel, IPSec Tunnel, MPLS L2VPN and L3VPN.
- Knowledge based Support.

- Training and High Level Topology Sharing.

(c)System Integration

Their service portfolio is completed with the following solutions:

- Integrated full-range Networking Solution for SOHO.
- DNS Configuration.
- Proxy and caching Server Configuration.
- Mail Server Configuration.
- IP Phone and IP PBX Solution.

(d)IPLC Circuit: International Data Service

While the Internet provides a very cheap superhighway to connect offices and people worldwide, it is certainly not the most secure and sage pathway. For organizations who demand the ultimate in data communication security, International Private Leased Circuit (IPLC) provides a dedicated clear channel from "point A to point B". While IPLC may be "the" solution for complete security and ultimate quality of service, it is also quite expensive. Latest technologies, such as MPLS VPN provides a far more cost effective solution with comparable performances as IPLC.

Their features are:

- Redundant Transmission @local loop.
- Transmission Router for TDM, L2 or L3 Service.
- Installation and Commissioning of Transmission Router.

- Provisional Acceptance Test (PAT): QoS Testing.
- Final Acceptance Testing After one-month Service Period: QoE Testing.
- 24×7 Customer Service (Mobile Apps and IVR Facility).
- Additional Service for P2P or P2M GRE Tunnel, IPSec Tunnel, MPLS L2VPN and L3VPN.
- Knowledge based Support.
- Training and High Level Topology Sharing.

(e)Security Surveillance

They give IP camera security answer for our client. In the market, there have numerous arrangements however we furnish future evidence and strong arrangement with important preparing so client can keep up everyday task.

Their solution includes:

- IP Camera
- Video Storage
- Large Display
- Networking along equipment
- Camera View over the Internet with secure pipe
- Complete turnkey solution

(f)Unified Threat Management

Organizations today are struggling with viruses and malicious attacks that are incredibly complex, and are deployed with a multifaceted approach to obtain their desired result. These new blended threats package a combination of virus and worm technology into an extremely elusive attack vehicle. In addition to security threats from blended attacks, administrators also face increased network slowdowns and a lack of prioritization of traffic moving throughout the network that impedes effectiveness. Unified Threat Management is an emerging trend in the firewall appliance security market. Unified Threat Management is the evolution of the traditional Firewall into a Swiss Army product that not only guards against intrusion but performs content filtering, spam filtering, intrusion detection and anti-virus duties traditionally handled by multiple systems.

Key points of UTM

- Network Auditing.
- Find out Security breach of the existing network.
- Recommendations.
- Product and Protocol selection for ensuring security.
- Full proof deployment.
- Reporting.

2.5 The Technology of APCL

APCL has some technologies which they are uses:

- IP/MPLS
- Metro Ethernet
- SDH

(a)IP/MPLS

We have nationwide coverage of MPLS Layer-3 and Layer-2 VPN solution. MPLS is now considered as the most advanced, robust and most secured solution for data-connectivity.

The following are some of the advantages of MPLS network:

- Provide a diversified range of Secured and encrypted VPN services (MPLS Layer 3 VPNs) to meet the requirements of the entire spectrum of customers from small and medium to large business enterprises and financial institutions.
- Make the service very simple for customers to use even if they lack experienced in IP routing.
- Make the service very scalable and flexible to facilitate large-scale deployment.
- Provide a reliable and amenable service, offering SLA to customers.
- Capable of meeting a wide range of customer requirements, including security, traffic engineering (TE), quality of Service (QOS), class of service (CoS) and any-to-any connectivity.
- Capable of offering fully managed services to customers.
- MPLS is a scalable tunneling architecture used for forwarding packets, based on label stacking.

(b)Metro Ethernet

APCL use metro Ethernet technology at access network to connect home and corporate offices. Metro Ethernet network gives us maximum flexibility to connect customer with single and double tag vlan marking. We use service provider tag where customer already have tag based network. We use Ethernet Ring Protection (ERPS) ITU G.8032 to ensure redundancy and switching. Through this protocol we can provide sub-second switchover.

(c)SDH

APCL use SDH network for express and backbone network. This technology also use for guaranteed service like IPLC circuit. We are exploring DWDM for upgrading our backbone network.

Chapter 3

Overview of Data Communication and Networking

Information correspondence alludes to the trading of information between a source and a recipient by means of type of transmission media, for example, a wire link. Information correspondence is said to be neighborhood if imparting gadgets are in a similar building or a comparably limited geological zone. The implications of source and beneficiary are exceptionally straightforward. The gadget that transmits the information is known as source and the gadget that gets the transmitted information is known as collector. Information correspondence goes for the exchange of information and upkeep of the information amid the procedure yet not the genuine age of the data at the source and recipient.

A system is an accumulation of PCs, servers, centralized computers, organize gadgets, peripherals, or different gadgets associated with each other to permit the sharing of information. An astounding case of a system is the Internet, which associates a huge number of individuals everywhere throughout the world. The following is a model picture of a home system with numerous PCs and other system gadgets all associated with one another and the web.

3.1.1 Components or Elements of Data Communication

There are five elements of data communication systems-

a) Message
b) Sending and Receiving Devices
c) Communication Channel
d) Connecting Device
e) Data Transmission Specification

a) Message:

It is the information to be communicated. Popular forms of information include text, pictures, audio, video etc. that are converted into different forms.

b) Sending and Receiving Devices

- Start or acknowledge the transmission of information, directions and data.

- Scratch pad and personal computers, Tablet PCs, mid-range servers and centralized computer PCs would all be able to fill in as sending and getting gadgets.

- Can discuss specifically with another PC, with several PCs on an organization arrange or with a great many PCs on the web.

- A web-empowered hand-held gadget likewise fills in as a sending and accepting gadget. Gives access to the web and email from any area.

c) Communication Channel:

A way through which data is transmitted starting with one place then onto the next is called correspondence channel. It is likewise alluded to as correspondence medium or connection. The wound combine wire, coaxial link, fiber optic link, microwave, satellite and so forth are instances of correspondence stations.

In a correspondence channel, information is transmitted as signs (simple flag). The information transmission is estimated in data transfer capacity. The transmission capacity will be higher if more flags can be transmitted. All things considered, the transfer speed estimates the measure of data that can be transmitted through the media inside the given timeframe

There are two types of communication channel or media. They are:

- Physical or Cable and
- Logical or Broadcast

Physical communication channel or Cable media

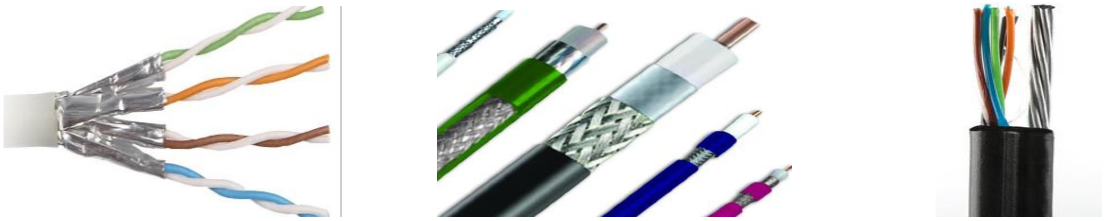
A communication channel or simply channel refers either to a physical transmission medium such as a wire, or to a logical connection over a multiplexed medium such as a radio channel in telecommunications and computer networking. Cable or wire line media use physical wires of cables to transmit data and information.

Useable communication channels are:

- Twisted pair cables
- Coaxial cables
- Fiber optic cables
- Terrestrial stations
- Data Transmission Specification

1)Twisted-pair cable:

Signs are transmitted utilizing sets of freely protected wires that have been physically curved together. Utilized by more established phone systems. System links utilize a RJ-45 jack for four sets of curved match Cable. Here, figure 1.1(a) demonstrates the bent match link.



a) Twisted-pair cable b) Coaxial Cable c) Fiber-optic cable

Figure 3.1.1: Different types of communication channel

2)Coaxial Cable:

Core of the wire is copper. High frequency signals can be carried on a single cable – used for video transmission. Used when twisted pair cabling is not adequate to carry the required amount of data. Figure 1.1(b) shows the coaxial cable.

3)Fiber-optic cable:

Digital signals are sent as light pulses which are translated back into electrical signals. Composed of fine glass strands. Centre core is composed of: Fine glass strand surrounded by glass cladding and protective layer. Glass cladding reflects light back into the core, guiding the light along the wire. Thousands of transmissions can be carried on a single strand. Can transmit signals faster than twisted pair and coaxial cables. Figure 1.1(c) shows the fiber-optic cable.

4)Terrestrial stations:

Information is sent via microwaves from ground based transmitting and receiving stations. Text, sound, and graphics are converted into microwave pulses and transmitted. Microwave stations must be placed every 50 kilometers to receive, amplify, and then pass the signal along. Transfer information at much higher speeds than cabling.

5)Communication Satellites:

It is orbiting around earth and avoids cost of cabling and repeater stations. Minimum of three satellites are needed to provide world-wide communication. Transfer information at much higher speeds than cabling.

Standard Cabling:

Links are the commonest type of transmission media which is utilized to fabricate a system. They are normally produced using copper wire, for example, co-hub and curved match. Fiber-optic links are additionally utilized for quick, expansive limit systems or to associate areas of a system in a substantial building like a school or school. In an Ethernet organize, contorted combine cabling is regularly utilized, and each system point will be associated back to a center point or switch, which thus is associated with the server.Figure demonstrates a standard cabling.

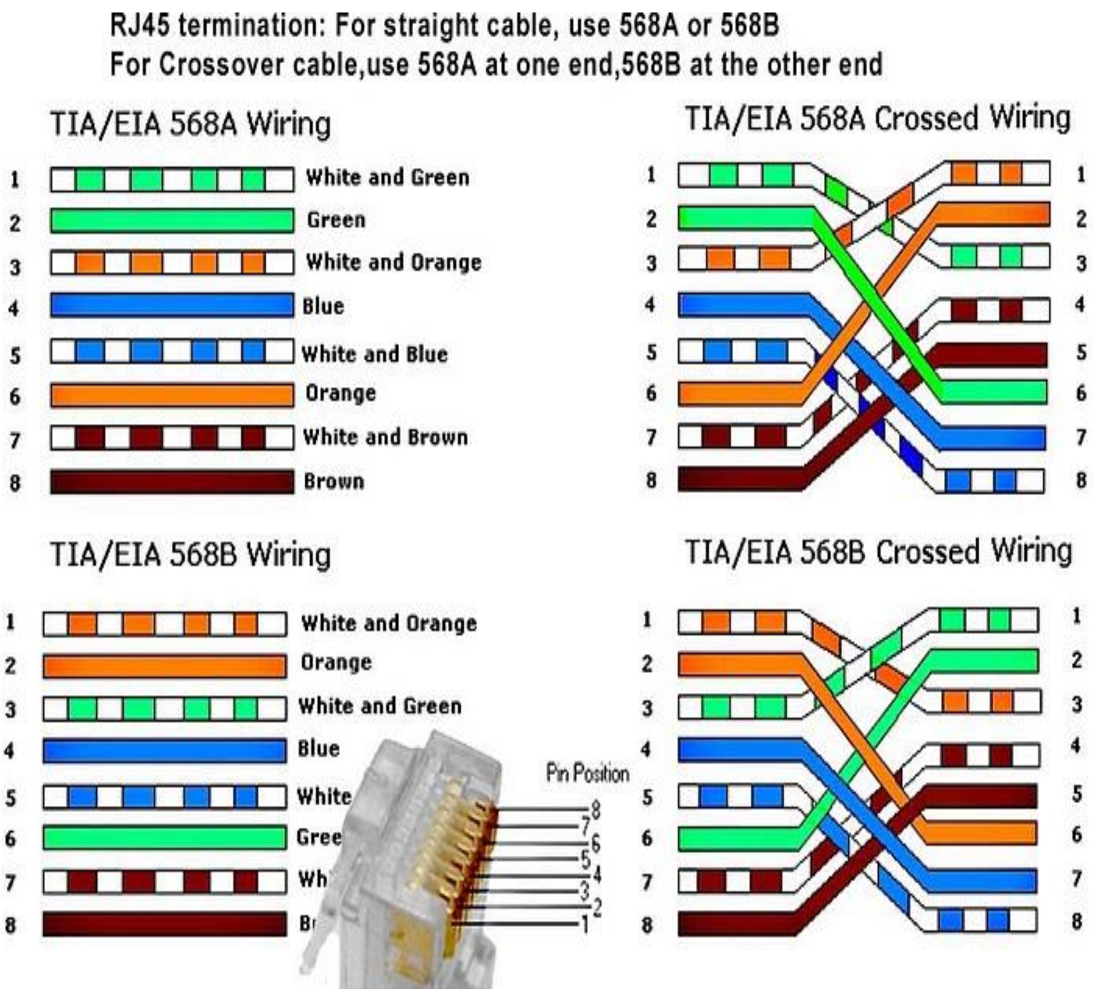


Figure 3.1.2 : Standard Cabling

Logical communication or Broadcast media:

Broadcasting is the distribution of audio or video content to a dispersed audience via any electronic mass communications medium, but typically one using the electromagnetic spectrum (radio waves), in a one-to-many model.

Generally speaking, broadcast advertising is radio, satellite television, wireless computer mice, television, and Internet advertising. The commercials aired on radio and televisions are an essential part of broadcast advertising. The broadcast media like radio and television reaches a wider audience as opposed to the print media.

- **Wireless communication:**

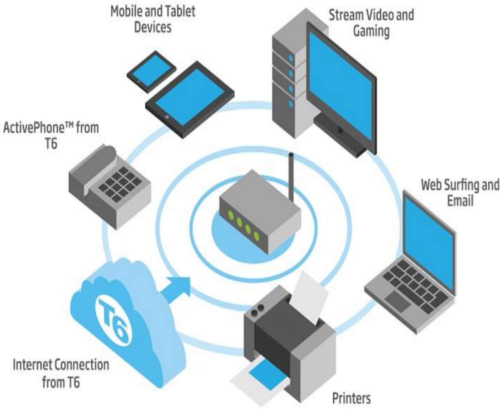
Wireless communication is the transfer of information or power between two or more points that are not connected by an electrical conductor. The most common wireless technologies use radio waves. With radio waves distances can be short, such as a few meters for Bluetooth or as far as millions of kilometers for deep-space radio communications. It encompasses various types of fixed, mobile, and portable applications, including two-way radios, cellular telephones, and personal digital assistants. Figure 1.1(a) shows the wireless communication.

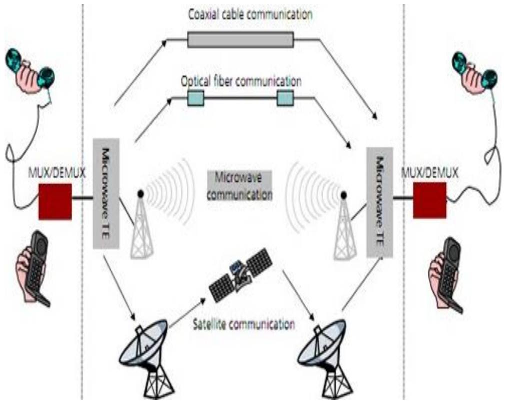
- **Microwave communication**

The transmission of signals by sending microwaves, either directly or via a satellite. The receivers for microwave signals are usually disc-shaped antennae from a foot to a few feet across and are often seen installed in business locations or near private homes. Satellite communications is the use of satellite technology in the field of communications. The services provided by satellite communications are voice and video calling, internet, fax, television and radio channels. Figure 1.1(b) shows the microwave communication.

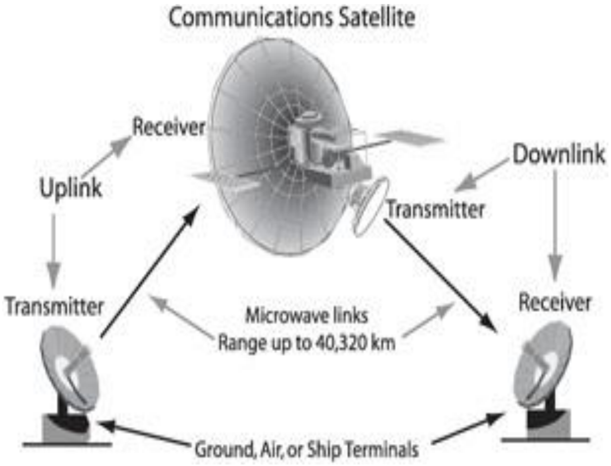
- **Satellite Communication**

Satellite communications can provide communication capabilities spanning long distances and can operate under circumstances or conditions which are inoperable for other forms of communication. Figure 1.1(c) shows the satellite communications.





a)Picture of Wireless Communication b)Microwave Communication



d) Satellite Communication

Figure 3.1.3: Different types of logical communications

e) Connecting Device:

Connecting devices are bridges between the different parts of a document that tie all of the pieces together into one coherent package. Connecting devices show the reader how various sections of information are related, and they help keep the reader o n track with the flow of information.

There are many types of connecting device. They are;

❖ **Networking Switch:**

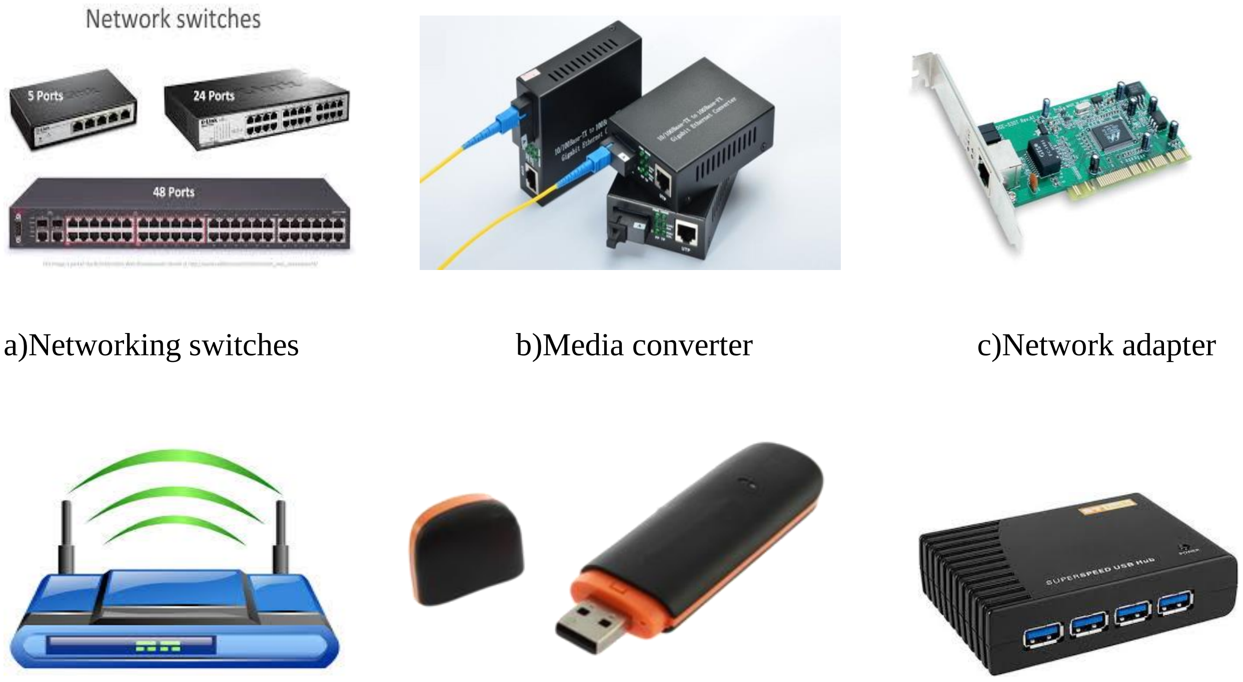
A network switch is a computer networking device that connects devices together on a computer network by using packet switching to receive, process, and forward data to the destination device. Figure1.1 (d)-(a) is shows the networking switch.

❖ **Media Converter:**

A media converter, in the context of network hardware, is a cost-effective and flexible device intended to implement and optimize fiber links in every kind of network. Among media converters, the most often used type is a device that works as a transceiver, Figure1.1 (d)-(b) is shows the media converter.

❖ **Network Adapter:**

A network adapter is the component of a computer’s internal hardware that is used for communicating over a network with another computer. It enables a computer to connect with another computer, server or any networking device over an LAN connection. A network adapter can be used over a wired or wireless network. Figure1.1 (d)-(c) is shows the network adapter.



a)Networking switches b)Media converter c)Network adapter

d)WAP e) Modem f)Networking Hub

Figure 3.1.4: Connecting Devices

❖ **WAP (Wireless Access Point):**

A wireless access point (WAP) is a hardware device or configured node on a local area network (LAN) that allows wireless capable devices and wired networks to connect through a wireless standard, including Wi-Fi or Bluetooth.Figure1.1 (d)-(d) is shows the wireless access point..

- **Modem:**

A modem is a system gadget that both adjusts and demodulates simple transporter signals (called sine waves) for encoding and disentangling advanced data for handling. Figure1.1 (d)- (e) is demonstrates the modem.

- **Networking Hub:**

A system center is a hub that communicates information to each PC or Ethernet-based gadget associated with it. A center point is less advanced than a switch, the last of which can disconnect information transmissions to explicit gadgets. Figure1.1 (d)- (f) is demonstrates the systems administration center point.

e) Data Transmission Specification:

1. Bandwidth: Bandwidth is the capacity of a wired or wireless network communications link to transmit the maximum amount of data from one point to another over a computer network or internet connection in a given amount of time.

2. Data Direction: Communication between any two devices can be

a. Simplex
b. Half-Duplex,
c. Full-Duplex.
a. Simplex:

The simplex transmission is the one that movements in just a single bearing. It very well may be all the clearer on the case of individual talking into receiver and afterward hearing voice from the speaker. Flag goes in just a single course from mouthpiece to speaker. Thusly of transmission can be likewise called unidirectional or one-way transmission.

b. Half-Duplex:

The half-duplex transmission is capable of sending signal in both directions, but in only one direction at a time. Some networks use half-duplex transmission, but it is required to specify this requirement for all the nodes in the network. An example could be police car radio phones allowing one person talk at a time.

c. Full-Duplex:

It allows signal transmission in both directions simultaneously. An example is a telephone IP service. This type of transmission can also be called bidirectional transmission.

3. Protocol:

A protocol is a set of rules and guidelines for communicating data. Rules are defined for each step and process during communication between two or more computers. Networks have to follow these rules to successfully transmit data.

Common TCP/IP protocol used for internet Are-File Transfer protocol (FTP), Secure Shell (SSH), Telnet, Simple Mail Transfer Protocol (SMTP), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Trivial File Transfer Protocol (TFTP), Hyper Text Transfer Protocol (HTTP), Post Office Protocol (POP), Network Time Protocol (NTP), Internet Message Access Protocol (IMAP), Border gateway Protocol (BGP) and so on.

3.2 The major network criteria

The major criteria that a Data Communication Network are:

❖ Performance:

Performance is the defined as the rate of transferring error free data. It is measured by the Response Time. Response Time is the elapsed time between the end of an inquiry and the beginning of a response. Request a file transfer and start the file transfer.

- **Consistency:**

Consistency is the predictability of response time and accuracy of data.

- **Reliability:**

Reliability is the measure of how often a network is useable. MTBF (Mean time between failures) is a measure of the average time a component is expected to operate between failures. Normally provided by the manufacturer. A network failure can be: hardware, data carrying medium and Network Operating System.

- **Recovery:**

Recovery is the Network's ability to return to a prescribed level of operation after a network failure. This level is where the amount of lost data is nonexistent or at a minimum. Recovery is based on having Back-up Files.

- **Security:**

Security is the protection of Hardware, Software and Data from unauthorized access. Restricted physical access to computers, password protection, limiting user privileges and data encryption are common security methods. Anti-Virus monitoring programs to defend against computer viruses are a security measure.

3.3 Types of Computer Network

Computer network can be categorized in several ways that are:

a) Local Area Network (LAN)
b) Metropolitan Area Network (MAN)
c) Wide Area Network (WAN)

(a) Local area network (LAN)

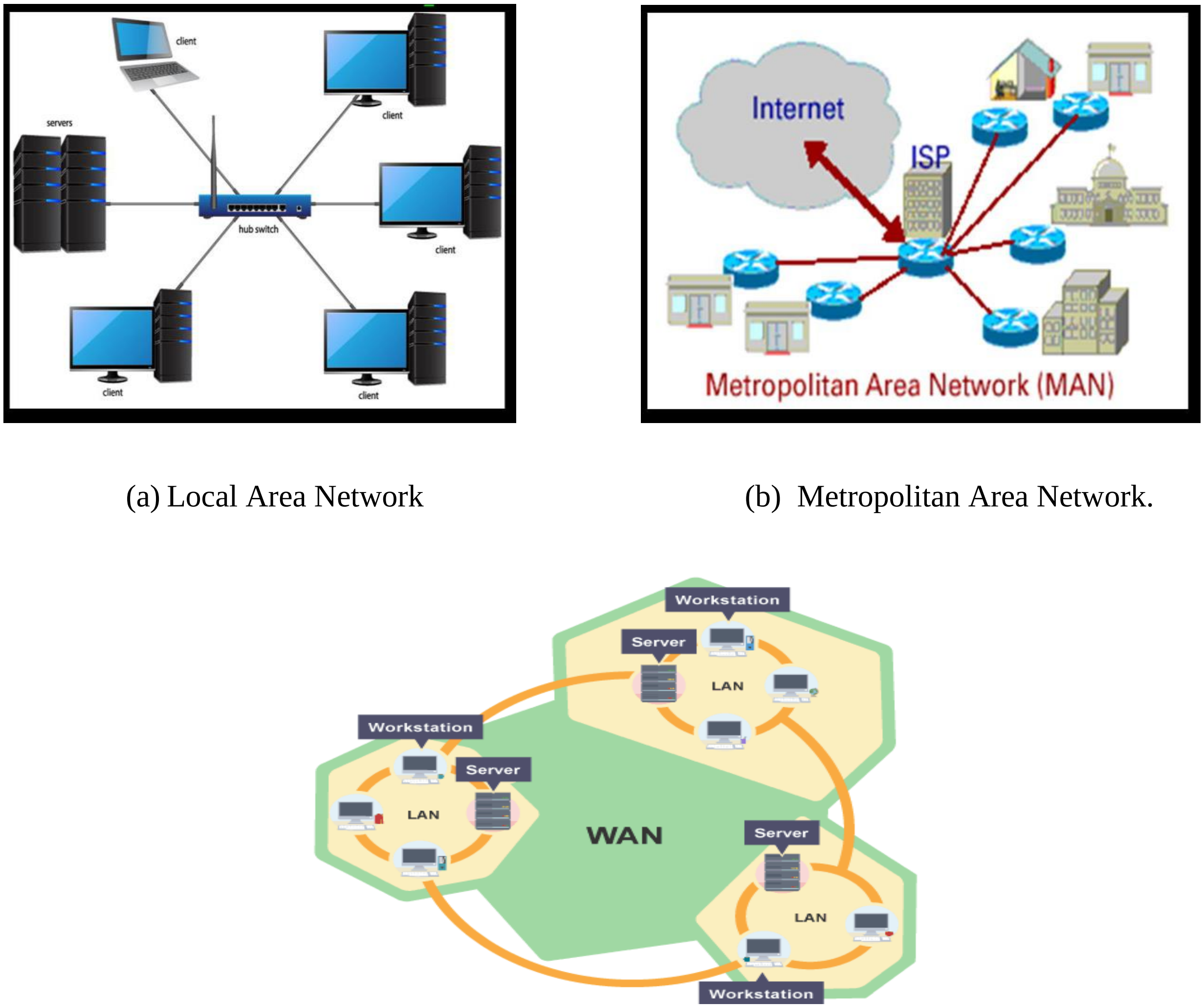
A local area network (LAN) is a group of computers and associated devices that share a common communications line or wireless link to a server. Typically, a LAN encompasses computers and peripherals connected to a server within a distinct geographic area such as an office or a commercial establishment. Computers and other mobile devices use a LAN connection to share resources such printer or network storage. Figure 3.3(a) shows the local area network.

(b) Metropolitan area network (MAN)

A metropolitan area network (MAN) is a computer network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN). The term MAN is applied to the interconnection of networks in a city into a single larger network which may then also offer efficient connection to a wide area network. It is also used to mean the interconnection of several local area networks in a metropolitan area through the use of point-to-point connections between them. Figure 3.3(b) shows the metropolitan area network.

(c) Wide area network (WAN)

A wide area network (WAN)is a geographically distributed private telecommunications network that interconnects multiple local area networks (LANs). In an enterprise, a WAN may consist of connections to a company's headquarters, branch offices, collocation facilities, cloud services and other facilities. Typically, a router or other multifunction device is used to connect a LAN to a WAN. Enterprise WANs allow users to share access to applications, services and other centrally located resources. This eliminates the need to install the same application server, firewall or other resource in multiple locations. Figure 3.3(c) shows the wide area network.



(a) Local Area Network

(b) Metropolitan Area Network.

(c)Wide Area Network

Figure 3.3: Types of computer network

3.4 Network Topology

A topology is a usually schematic description of the arrangement of a network, including its nodes and connecting lines. There are two ways of defining network geometry: the physical topology and the logical (or signal) topology.

There are two ways of defining network geometry: -

- Physical topology and

- Logical (or signal) topology

The physical topology of a network is the actual geometric layout of workstations and how they are actually interconnected with wires and cables. A logical topology is how devices appear connected to the user. The logical topology of a network can be dynamically maintained and reconfigured. The study of network topology recognizes eight basic topologies- point-to-point, bus, star, ring or circular, mesh, tree, hybrid, or daisy chain. Some of the important are discussed below and as shown in the illustration: -

a) Bus Topology

Alternatively referred to as a line topology, a bus topology is a network setup in which each computer and network device are connected to a single cable or backbone. Depending on the type of network card used in each computer of the bus topology, a coaxial cable or a RJ-454 network cable is used to connect computers together.

The following sections contain both the advantages and disadvantages of using a bus topology with your devices. Figure 3.4(a) shows the bus topology.

b) Ring Topology

A ring topology is a network configuration in which device connections create a circular data path. Each networked device is connected to two others, like points on a circle. Together, devices in a ring topology are referred to as a ring network.

In a ring system, bundles of information head out starting with one gadget then onto the next until the point that they achieve their goal. Most ring topologies enable bundles to travel just one way, called a unidirectional ring system. Others allow information to move in either bearing, called bidirectional.

The major disadvantage of a ring topology is that if any individual connection in the ring is broken, the entire network is affected. . Figure 3.4(b) shows the ring topology.

c) Star Topology

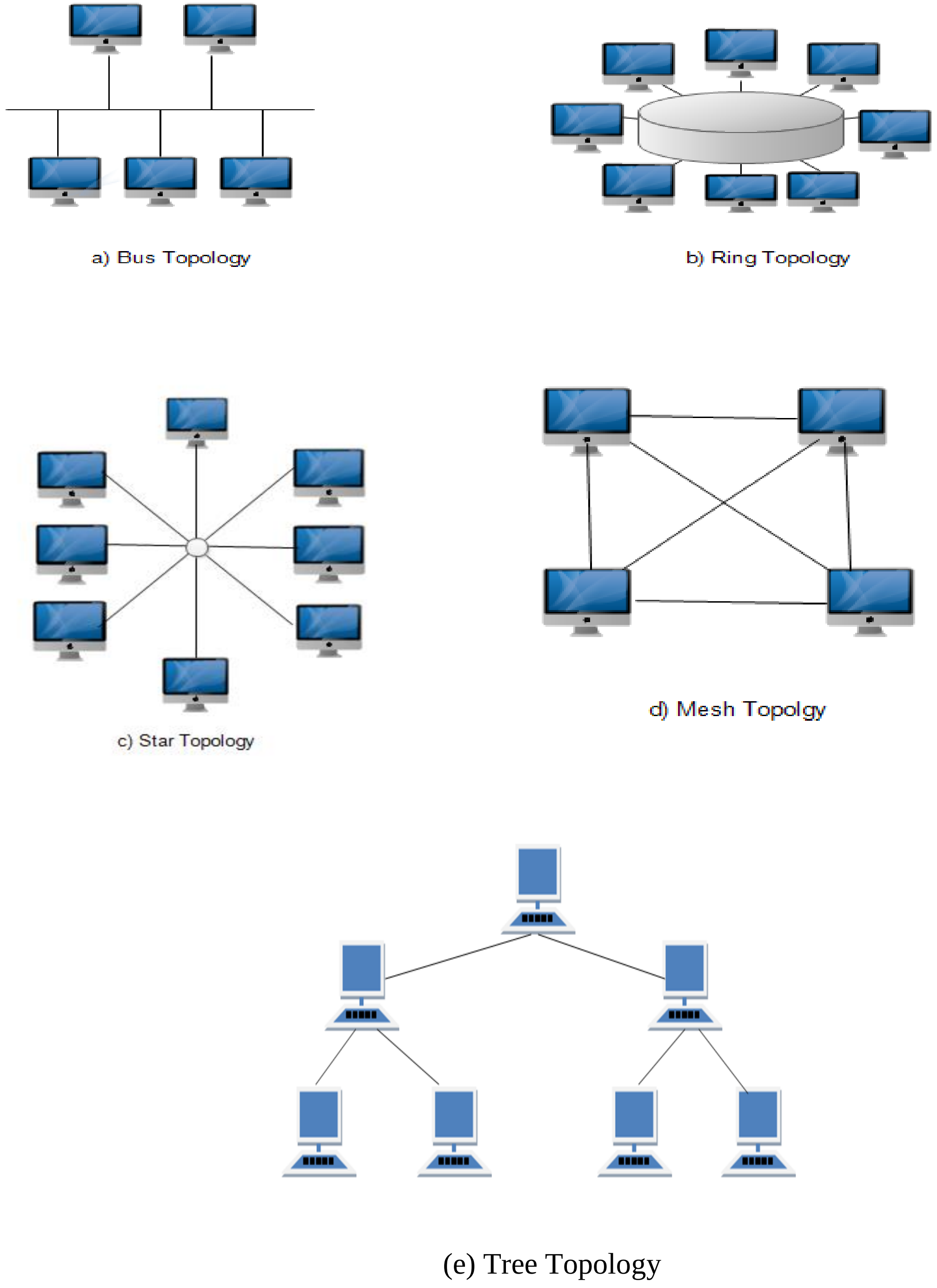
In Star topology, all the components of network are connected to the central device called “hub” which may be a hub, a router or a switch. Unlike Bus topology), where nodes were connected to central cable, here all the workstations are connected to central device with a point-to-point connection. So it can be said that every computer is indirectly connected to every other node by the help of “hub”. Figure 3.4(c) shows the star topology.

d) Mesh Topology

In a mesh network topology, each of the network node, computer and other devices, are interconnected with one another. Every node not only sends its own signals but also relays data from other nodes. In fact, a true mesh topology is the one where every node is connected to every other node in the network. This type of topology is very expensive as there are many redundant connections, thus it is not mostly used in computer networks. It is commonly used in wireless networks. Flooding or routing technique is used in mesh topology.

There are two types of MESH topology and these are

- Partial MESH topology
- Fully MESH topology.
  Figure 3.4(d) shows the mesh topology.



a) Bus Topology

b) Ring Topology

c) Star Topology

d) Mesh Topolgy

(e) Tree Topology

Figure 3.4: Different types of topology

e) Tree Topology

Tree Topology integrates the characteristics of Star and Bus Topology. Prior we perceived how in Physical Star arrange Topology, PCs (hubs) are associated by one another through focal center point. What's more, we additionally found in Bus Topology, work station gadgets are associated by the normal link called Bus. In the wake of understanding these two system designs, we can comprehend tree topology better. In Tree Topology, the quantities of Star systems are associated utilizing Bus. This fundamental link appears to be a principle stem of a tree, and other star organizes as the branches. It is also called Expanded Star Topology. Ethernet protocol is commonly used in this type of topology.Figure 3.4(e) shows the tree topology.

3.5 Network Strategies

There are two types of computer network strategies.

(a) Client-Server Network.

(b) Peer -to-Peer Network

3.5(a) Client-Server Network:

In a customer/server organize, a brought together, extremely incredible PC (server) goes about as a center point in which different PCs or workstations (customers) can associate with. This server is the core of the framework, which oversees and gives assets to any customer that demands them.

Advantages of a client/server network

Resources and data security are controlled through the server. Not restricted to a small number of computers. Server can be accessed anywhere and across multiple platforms.

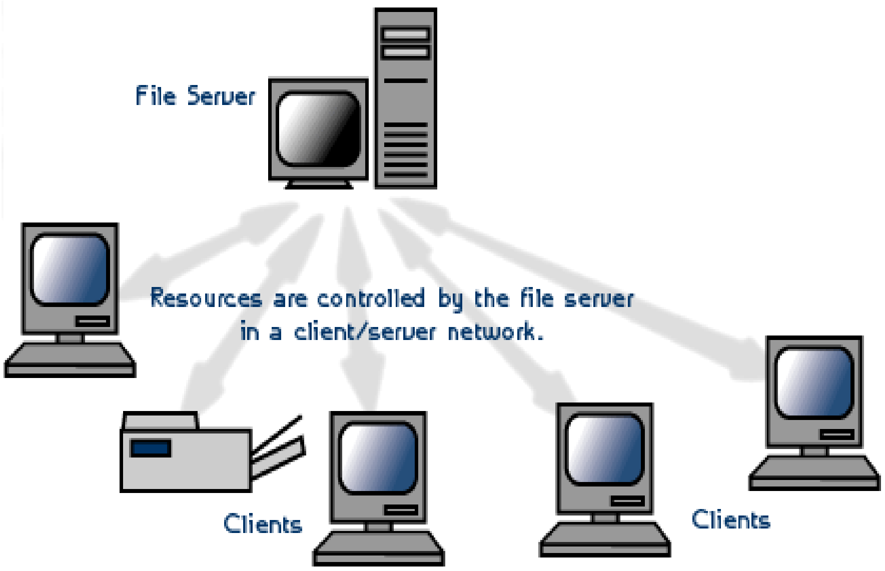

File Server
Resources are controlled by the file server in a client/server network.
Clients
Clients

Figure 3.5(a): Client/Server Network

3.5(b) Peer-to-Peer Network

In a distributed system, errands are allotted to each gadget on the system. Besides, there is no genuine progressive system in this system, all PCs are viewed as equivalent and all have similar capacities to utilize the assets accessible on this system. Rather than having a focal server which would go about as the common drive, every PC that is associated with this system would go about as the server for the documents put away on it.

Advantages of a peer-to-peer network

Does not require a dedicated server which means it's less costly. If one computer stops working, the other computers connected to the network will continue working. Installation and setup is quite painless because of the built-in support in modern operating systems.

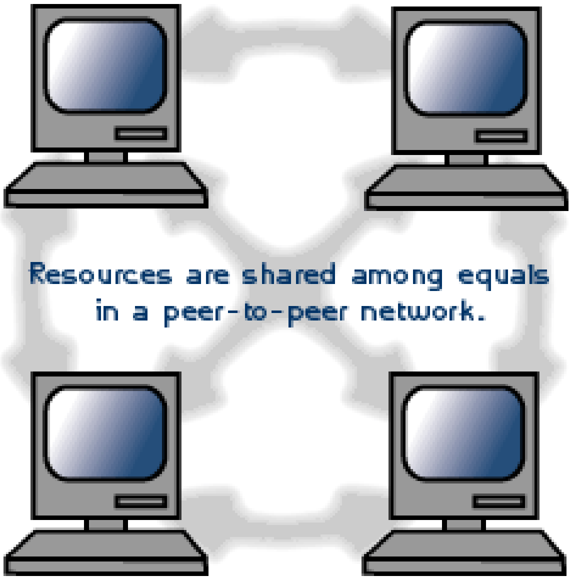


Figure 3.5(b): Peer-to-Peer Network

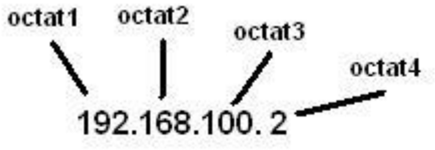
Chapter 4

Overview of IP Addresses

4.1 Importance of IP Addresses

IP address is very important in TCP/IP networking. It’s the address that recognized and understood by computers and networking devices, so that they can communicate with each other. This 32bits IP address is also called IPv4.

IP address contains 4 octets, each octet can be represented by number 0-255 and separated by periods. For example, 192.168.100.2 is an IP address.



4.2 OSI Model

The Open Systems Interconnection (OSI) model defines a networking framework to implement protocols in layers, with control passed from one layer to the next. It is primarily used today as a teaching tool. It conceptually divides computer network architecture into 7 layers in a logical progression. The lower layers deal with electrical signals, chunks of binary data, and routing of these data across networks. Higher levels cover network requests and responses, representation of data and network protocols as seen from a user's point of view.

4.3 The relationship of OSI model and TCP/IP:

TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. Protocols are set of rules which govern every possible communication over a network. The figure 2.2 shows the relationship between the OSI model and TCP/IP.

Table 4.3: the relationship of OSI model and TCP/IP

Layer	OSI Model	PDU	TCP/IP Model	Layer
7	Application		Application	
6	Presentation	Data		5
5	Session			
4	Transport	Segment	Transport	4
3	Network	Packet	Internet	3
2	Data Link	Frame	Link	2
1	Physical	Bits	Physical	1

4.4. IP Address:

An Internet Protocol address (IP address) is a label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing.

It provides the base for all other network and user. Each IP address includes two major parts:

a) **Network ID,**
b) **Host ID.**

a. The Network ID:

A Network ID alludes to a piece of a TCP/IP deliver that is utilized to recognize the subnet that a host might be on. The subnet that the PC is on is dictated by the net cover and IP address of the PC. This subnet address is equivalent to the system ID and is the starting piece of the PCs IP address. At the point when the net veil is setup, it is where probably the most noteworthy bits have a 1's esteem and the rest have estimations of 0. The hugest piece of the net veil with bits set to 1's indicates the system address, and the lower some portion of the location will determine the host address.

b. The Host ID:

Host ID is a specific piece of information which uniquely identifies a computer. Host IDs are used to generate MATLAB license files, which are machine-specific. Most of the time, the host ID is the lowest-enumerated MAC address of the computer. However, there are exceptions to this:

- With an individual license on a Windows machine, the Volume Serial Number of the C: drive can be used as the host ID.
- With network licenses, the IP address can be used as the host ID. This is not recommended, as IP addresses can change due to external factors.

Example:

Binary Format-11000000 10101000 00000011 00011000

Dotted Decimal Format-192.168.3.24

4.5How IP Addresses are Manages

The IP address space is managed globally by the Internet Assigned Numbers Authority (IANA), and by five regional Internet registries (RIR) responsible in their designated territories for assignment to end users and local Internet registries, such as Internet service providers. IPv4 addresses have been distributed by IANA to the RIRs in blocks of approximately 16.8 million addresses each. Each ISP or private network administrator assigns an IP address to each device connected to its network. Such assignments may be on a static (fixed or permanent) or dynamic basis, depending on its software and practices.

4.6IP Version

Two versions of the Internet Protocol (IP) are in use:

- ➢**IP Version 4**
- ➢**IP Version 6**

IPv4 addresses are 32-bit numbers that are typically displayed in dotted decimal notation. A 32-bit address contains two primary parts: the network prefix and the host number.All hosts within a single network share the same network address. Each host also has an address that uniquely identifies it. Depending on the scope of the network and the type of device, the address is either globally or locally unique. Devices that are visible to users outside the network must have a globally unique IP address. Devices that are visible only within the network must have locally unique IP addresses.

IPv6 address is 128-bit numbers and a numerical label that is used to identify a network interface of a computer or a network node participating in anIPv6 computer network.

An IP address serves the purpose of identifying an individual network interface of a host, locating it on the network, and thus permitting the routing of IP packets between hosts. For routing, IP addresses are present in fields of the packet header where they indicate source and destination of the packet.

4.6 Comparison of IPV4 vs IPV6 :

	IPv4	**IPv6**
Address	32 bits (4 bytes) 12:34:56:78	128 bits (16 bytes) 1234:5678:9abc:def0: 1234:5678:9abc:def0
Packet size	576 bytes required, fragmentation optional	1280 bytes required without fragmentation
Packet fragmentation	Routers and sending hosts	Sending hosts only
Packet header	Does not identify packet flow for QoS handling Includes a checksum	Contains Flow Label field that specifies packet flow for QoS handling Does not include a checksum

DNS records	Address (A) records, maps host names Pointer (PTR) records, IN-ADDR.ARPA DNS domain	Address (AAAA) records, maps host names Pointer (PTR) records, IP6.ARPA DNS domain
Address configuration	Manual or via DHCP	Stateless address auto configuration (SLAAC) using Internet Control Message Protocol version 6 (ICMPv6) or DHCPv6
IP to MAC resolution	broadcast ARP	Multicast Neighbor Solicitation
Local subnet group management	Internet Group Management Protocol (IGMP)	Multicast Listener Discovery (MLD)
Multicast	Yes	Yes
IPSec	optional, external	Required

Table 4.6: Comparison of IP version

4.7Classful IP Address

The Internet community originally defined five address classes to accommodate networks of varying sizes. The class of address defines which bits are used for the network ID and which bits are used for the host ID. It also defines the possible number of networks and the number of hosts per network.

IP addresses are split up into several different categories, including Class A, B, C, D (Multicast), and E (Reserved). Address classes are defined, in part, based on the number of bits that make up the network portion of the address, and in turn, on how many are left for the definition of individual host addresses.

- Class A networks have a 1-byte-long network part. That leaves 3 bytes for the rest of the address, called the host part.

- Class B networks have a 2-byte-long network part, leaving 2 bytes for the host portion of the address.
- Class C networks have a 3-byte-long network part, leaving only 1 byte for the host part.
- Class D IP address is reserved for multicast. The four high-order bits in a class D address are always set to binary 1110.
- Class E IP address is an experimental address, which is reserved for future use. The high order bits in a class E address are set to binary 1111.

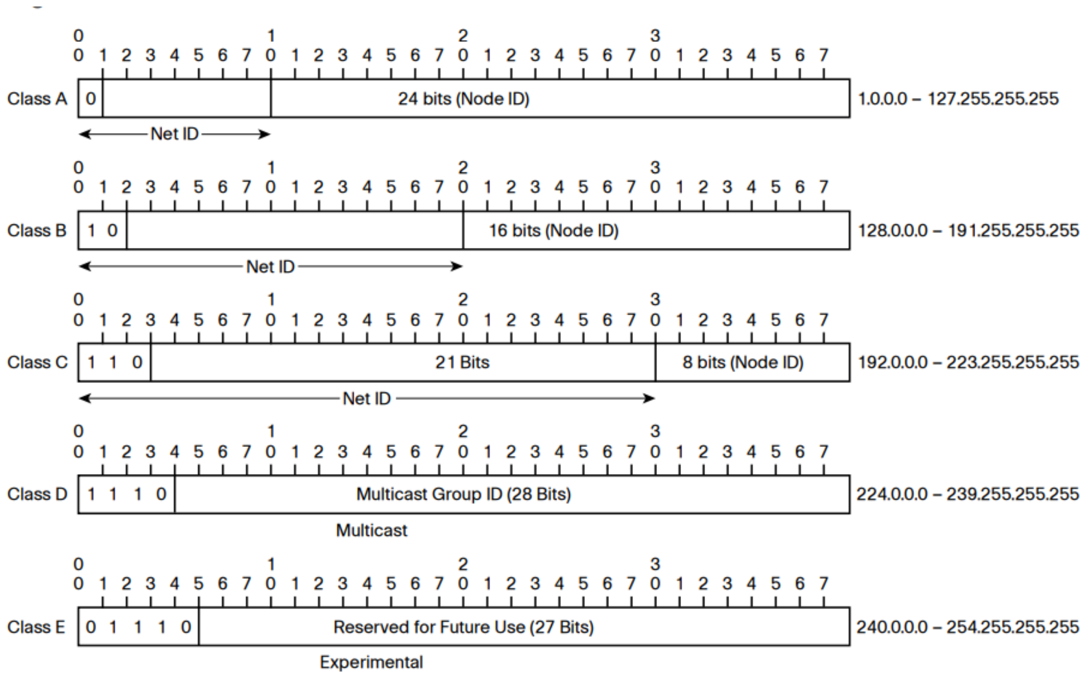


Figure 4.7: Classful IP addresses

4.8Sub netting

Sub netting is the strategy used to partition a single physical network into more than one smaller logical sub-network (subnets). An IP address includes a network segment and a host segment. Subnets are designed by accepting bits from the IP addresses host part and using these bits to assign a number of smaller sub-networks inside the original network. Sub netting allows an organization to add sub-networks without the need to acquire a new network number via the Internet service provider (ISP). It helps to reduce the network traffic and conceals network complexity. Sub netting is essential when a single network number has to be allocated over numerous segments of a local area network (LAN). Subnets were initially designed for solving the shortage of IP addresses over the Internet.

Each IP address consists of a subnet mask. All the class types, such as Class A, Class B and Class C include the subnet mask known as the default subnet mask. The subnet mask is intended for determining the type and number of IP addresses required for a given local network. The firewall or router is called the default gateway.

The default subnet mask is as follows:

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

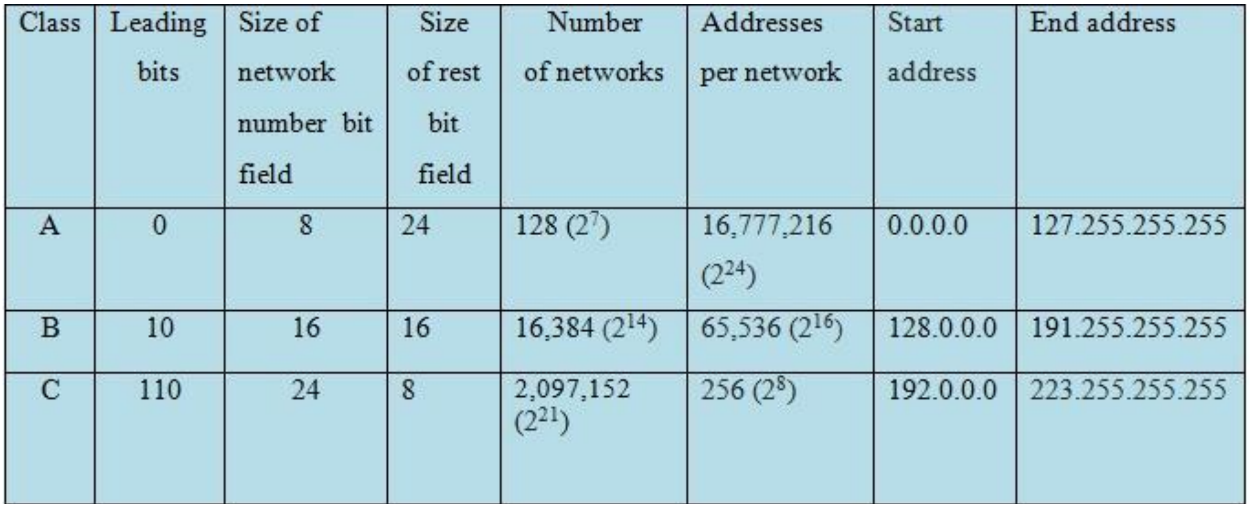
The sub netting process allows the administrator to divide a single Class A, Class B, or Class C network number into smaller portions. The subnets can be submitted again into sub-subnets.

Isolating the system into various subnets gives the accompanying advantages:

- ➢ Reduces the system traffic by diminishing the volume of communicates
- ➢ Helps to outperform the requirements in a neighborhood (LAN), for instance, the most extreme number of allowed has.
- ➢ Enables clients to get to a work arrange from their homes; there is no compelling reason to open the total system.

Class full network design allowed for a larger number of individual network assignments and fine-grained sub network design. The first three bits of the most significant octet of an IP address were defined as the class of the address. Three classes (A, B, and C) were defined for universal uncast addressing. Depending on the class derived, the network identification was based on octet boundary segments of the entire address. Each class used successively additional octets in the network identifier, thus reducing the possible number of hosts in the higher order classes (B and C).

The following table gives an overview of this now obsolete system.



Class	Leading bits	Size of network number bit field	Size of rest bit field	Number of networks	Addresses per network	Start address	End address
A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255

Table 4.8: Classful network architecture.

4.9 Static IP

A static IP address is permanent IP addresses. Static IP is an address which is manually assigned to a particular machine by the administrator or it can even be an IP which is allocated by a Dynamic Host Configuration Protocol(DHCP) server but does not change every time. Static IP address is a permanent number assigned to a computer by an Internet Service Provider (ISP). It is also known as a fixed address.

4.10 Dynamic IP

Dynamic IP address is a temporary IP address. A dynamic IP address is a DHCP server assigned IP address. Dynamic IP address comes with a lease time which is set on the Dynamic Host Configuration Protocol (DHCP) server by the network administrator. This IP changes after the lease time expires or the system reboots or renews its IP. This comes with other requires information of Gateway IP address and DNS IP address.

Chapter 5

ISP network of APCL, Gulshan Link Road Branch

An Internet specialist co-op (ISP), additionally called Internet get to supplier) is a business or association that offers client access to the Internet and related administrations. They give administrations, for example, web get to, web travel, name enlistment and facilitating, dial-up access, rented line get to. The primary target of ISP is to send the web administrations to the doorsteps of individuals and to reinforce the information correspondence. There are two kinds of ISP. They are wired ISP and remote ISP.

5.1 Primary Functions of ISP Network

- Provide a link: Firstly, they provide a link to a company or individual which enables them to access World Wide Web and send Internet e-mail. They are the entities that provide individual and institutional subscribers with access to Internet.

- Facilitating: Secondly, they have destinations or convey an association's site substance to engage diverse associations or clients access to it. For e.g., a person who is excited about moving a webpage will at first get a record with an encouraging pro association and after that will exchange site pages onto his website which is physically arranged on the host's 'server'.

- When the information is stored on the server, the uploaded documents become instantly available to all those with a connection to the Internet.

5.2: Existing Diagram of APCL:

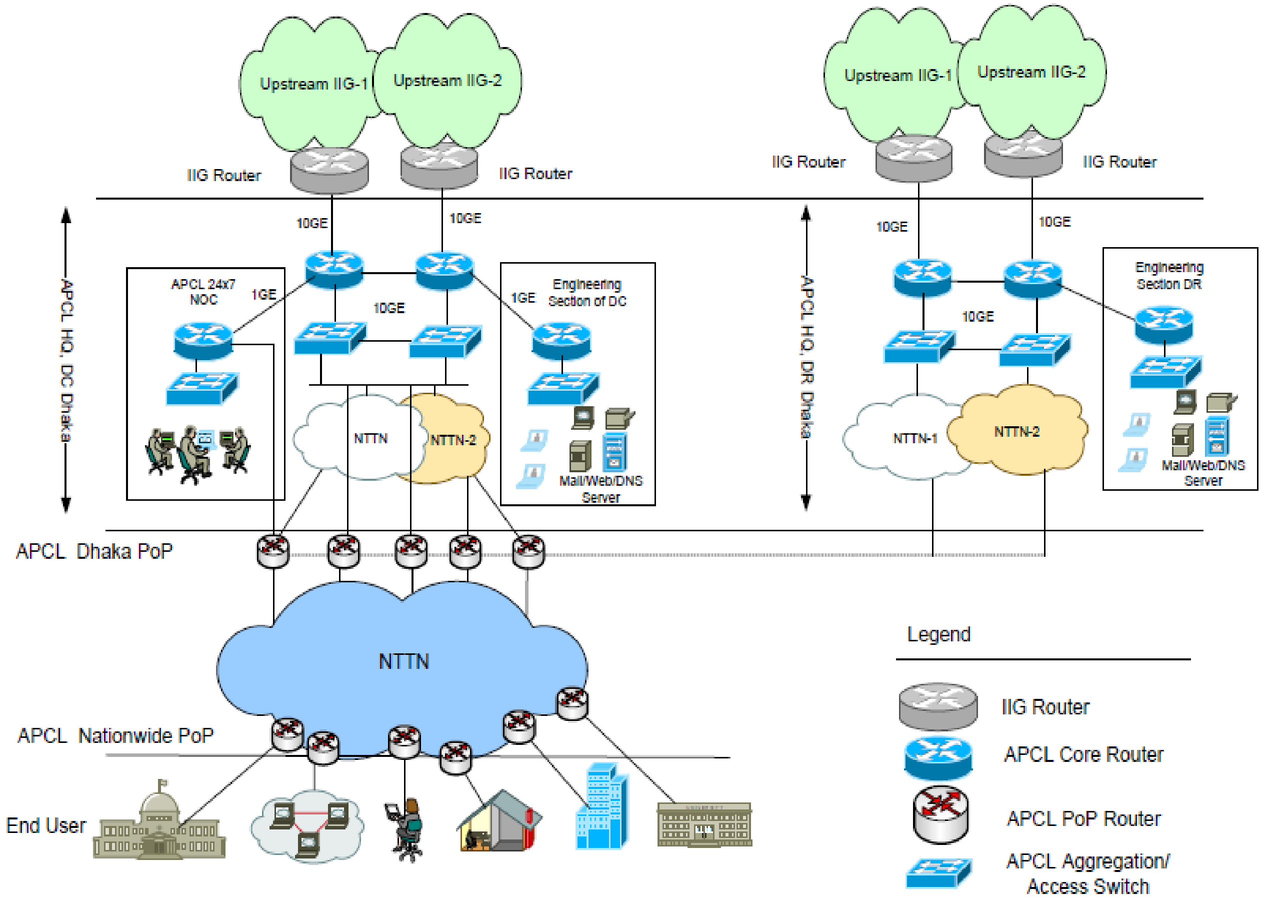


Figure 5.2: The Existing Network of APCL

In figure 5.2, the ISP (Internet Service Provider) of APCL has two (IIG-1 and IIG-2) router. The IIG-1 and IIG-2 router are added with several clouds. IIG-1 router is connected with 100 GBPS bandwidth from IIG-1 cloud and IIG-2 router is connected with 10 GBPS bandwidth from IIG-2 cloud. The Core Router of APCL-1 is added with IIG-1 Router by using Node, the router of APCL-1 is also added with the backup router of APCL and the backup router is connected with switch which added the Pop router of APCL. This switch can communicate with customer’s sector. Again IIG-2 cloud is connected with IIG-2 router by using Core router of APCL and it distributes the data. From back up APCL Core router is joined with a switch (NTTN-2) and DC router. The PoP router of APCL is added with a switch (NTTN-2) and this switch is also added with the consumer router which distributes the data.

Network Operations Center (NOC) in APCL:

APCL has a segment where NOC is included. A network operations center (NOC) is a place from which administrators supervise, monitor and maintain a telecommunications network. Large enterprises with large networks as well as large network service providers typically have a network operations center, a room containing visualizations of the network or networks that are being monitored, workstations at which the detailed status of the network can be seen, and the necessary software to manage the networks. The network operations center is the focal point for network troubleshooting, software distribution and updating, router and domain name management, performance monitoring, and coordination with affiliated networks.

Engineering Sector- Designated Router (DR) in APCL:

A designated router (DR) is the router interface elected among all routers on a particular multi-access network segment, generally assumed to be broadcast multi-access.

Rather than broadcasting LSAs to all their OSPF neighbors, the routing devices send their LSAs to the designated router. Each multi-access network has a designated router, which performs two main functions: Originate network link advertisements on behalf of the network.

Core router:

In APCL, there are two core routers. The core router operates in the internet backbone. APCL core routers are supporting multiple telecommunication interfaces of the highest speed in the core internet and forward IP packets at full speed to all of them. It also supports the routing protocols to all the interfaces of the network. The physical diagram indicates that the branch router is connected to the core routers of the network through the data connectivity provider-1 and 2. The data connectivity providers are the third party physical connection providers that connect the branch router to the core router of APCL.

IIG Router:

APCL is connected with two IIG Router; one is Summit and another is Fiber@ Home. International Internet Gateway (IIG) is connected to the International Internet Traffic through Tata Communications Limited, Bharti Airtel Limited, Singapore Telecommunications Limited, Level 3 Communications Limited, COGENT, NTT and TIS. By using our distinguished International networks our clients have International IP coverage and convergence services throughout North America, Europe and Asia-Pacific. While having the widest PoP presence in cities and all over the country, along with integrated network with global partners, our networks are fully redundant with almost 99.99% uptime. It has already built world class (1+1) infrastructure systems and services for the customers under IIG network.

APCL point of presence (PoP)

An Internet point of presence is an access point to the Internet. It is a physical location that houses servers, routers, MPLS & Ethernet switches also facilitating digital/analog call aggregators. It may be either part of the facilities of a telecommunications provider that the Internet service provider (ISP) rents or a location separate from the telecommunications provider. ISPs typically have multiple PoPs, sometimes numbering in the thousands. PoPs are also located at Internet exchange points and collocation centers.

APCL Aggregation/Access Switch:

An assemblage of the Document or its subordinates with other discrete and free archives or works, in or on a volume of a capacity or dispersion medium, is called a "total" if the copyright coming about because of the gathering isn't utilized to constrain the legitimate privileges of the arrangement's clients past what the individual works allow. At the point when the Document is incorporated into a total, this License does not make a difference to alternate works in the total which are not themselves subsidiary works of the Document. If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

Nationwide Telecommunication Transmission Network (NTTN) of APCL:

Summit and Fiber @ Home are maintaining the NTTN of APCL. They provide high capacity transmission services, internet services and international bandwidth services, through its state-of-the-art fiber optic network with latest available technologies (DWDM, IPMPLS, Metro Ethernet etc.). Aggregating a nationwide network, it has built access to over 33,000 KM network reaching the remotest corners of the country by connecting all the 64 districts, 340 upazillas and more than 3,650 government offices.

5.3: Nationwide Network of APCL:

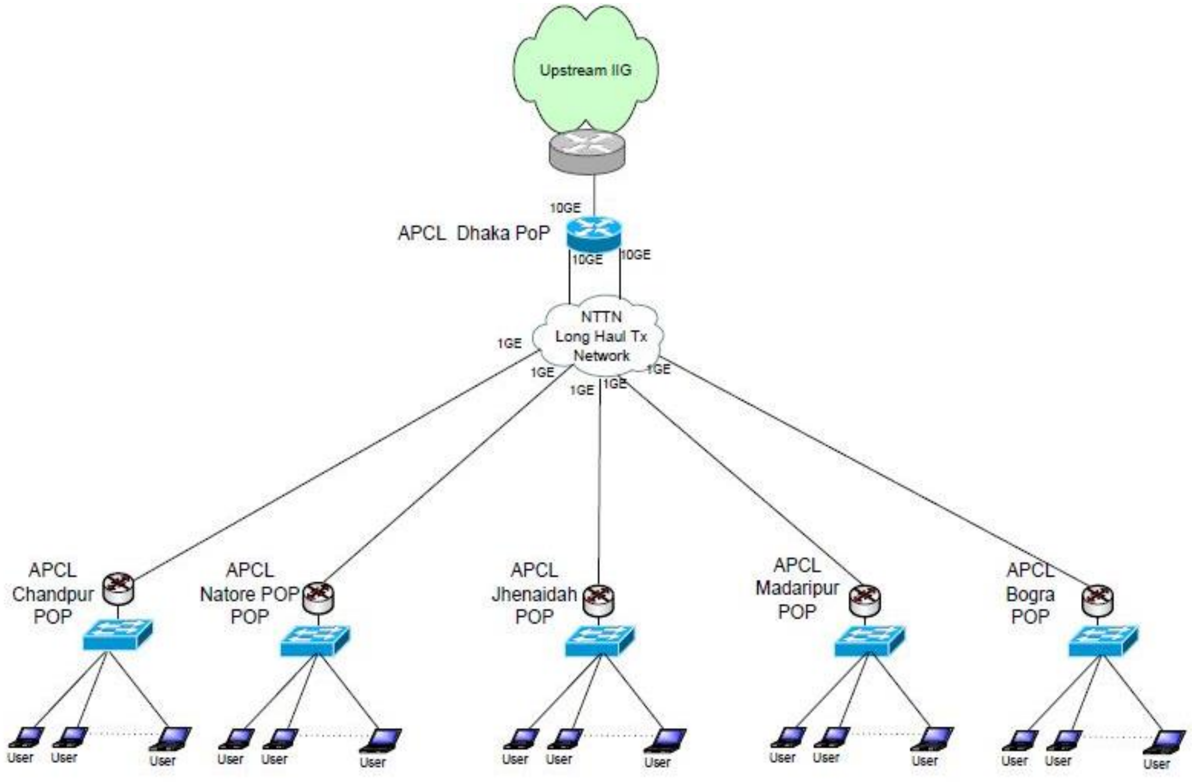


Figure 5.3: The Nationwide network of APCL

The nationwide network of APCL diagram is the map how they provide their network in whole Bangladesh. In figure 5.3, we see that in Dhaka pop is connected an IIG router. In this pop they distribute their network different routers for their local pop. Basically Dhaka pop is connected with Chandpur, Natore, Jhenaidah, Madaripur and Bogra. All network is distributed 10Gbps bandwidth. After connecting all pop they distributed their line another pop and make they also support local users and corporate offices. Dhaka pop distributor easily access their end user easily and support them virtually. All end user connected with a server that server is called ftp server. But end user cannot directly connect Dhaka pop. Because all branch router is the main path for end users. In this map security is not main concern for my company. They don't use here any fairwell because of they just distribute end users but when they distribute corporate office they use firewall and different server to give them security.

5.4 Data Center Infrastructure:

Information of the APCL network infrastructures:

List of Infrastructures	Specifications
Router Model: JUNIPER Router	➢ Quickly introduce new services ➢ More easily deliver customized and personalized services to customers ➢ Scale operations to push IP services closer to customers or to manage network growth when growth forecasts are low or uncertain ➢ Quickly expand service offerings into new sites
Switch **Model:** HUAWEI L2 Switch	➢ Switches increase available network bandwidth ➢ Switches reduce the workload on individual computers ➢ Switches increase network performance ➢ Networks that include switches experience fewer frame collisions because switches create collision domains for each connection.

	➢ Switches connect directly to workstations.
Switch **Model:** HUAWEI L3 Switch	➢ Intelligent packet forwarding (routing) based on Layer 3 information is traditionally the function of routers. ➢ Specialized routing protocols also use Layer 3, enabling routers to "learn" routes between networks. ➢ includes the ability to logically segment a network into two or more Virtual LANs (VLANs)
Switch **Model:** CISCO L2 Switch	➢ The Layer 2 provides direct data transfer between two devices within a LAN. ➢ The switch MAC address table records hardware's MAC addresses ➢ A Layer 2 switch can assign VLANs to specific switch ports, which in turn are in different layer 3 subnets.
Switch Model: CISCO L3 switch	➢ Troubleshooting of L3 issues is simplified compare with L2 ,don't have to care about STP root, FHRP active side, etc ➢ Better segregation of traffic like VRF Late to edge of your network; with this you achieve complete separation of routing tables.

Server Model: LOG Server	➢ Aggregate your logs in a central location: ➢ Perform security checks with SIEM ➢ Work with multiple formats ➢ Perform searches across logs ➢ Meet compliance requirements
Server Model: RADIUS Server	➢ RADIUS should be favored over LDAP ➢ RADIUS is an interesting protocol. ➢ There are free and open source server options on both Linux and Windows. ➢ RADIUS is quite simple. ➢ It's much better than needing to disable them in two places.
Switch Model: OLT Switch	➢ The OLT contains a central processing unit, passive optical network cards, a gateway router and voice gateway. ➢ It can transmit a data signal to users at 1490 nanometers. ➢ That signal can serve up to 128 ONTs at a range of up to 12.5 miles by using optical splitters.
Router Model: MikroTik(CCR)Router	➢ It is the "open minded" advantage, which is good. ➢ MikroTik Router Boards are much cheaper. ➢ The entire networking world is based on Cisco equipment and Cisco protocols.

Router Model: MikroTik(RB)Router	➢ The RB411GL is created for high-end wireless AP, Point-to-Point or CPE OEM applications. ➢ It has Gigabit Ethernet port, so you can take full advantage of 802.11n standard.

5.5 PhysicalNetwork:

APCL maintains some Physical network. They are:

5.5.1Optical Fiber cable:

An optical fiber link, otherwise called a fiber optic link, is a gathering like an electrical link, however containing at least one optical filaments that are utilized to convey light. The optical fiber components are normally independently covered with plastic layers and unshielded turned match (UTP) links are generally utilized in the PC and media communications industry as Ethernet links and phone wires.

There are three types of fiber optic cable commonly used:

(a)Single Mode cable:

Single Mode cables a single stand (most applications use 2 fibers) of glass fiber with a diameter of 8.3 to 10 microns that has one mode of transmission. Single Mode Fiber with a relatively narrow diameter, through which only one mode will propagate typically 1310 or 1550nm. Carries higher bandwidth than multimode fiber, but requires a light source with a narrow spectral width. Synonyms mono-mode optical fiber, single-mode fiber, single-mode optical waveguide, uni-mode fiber.

(b)Multi-Mode cable:

Multi-Mode link has somewhat greater distance across, with a typical breadth in the 50-to-100 micron extend for the light convey part (in the US the most widely recognized size is 62.5um). Most applications in which Multi-mode fiber is utilized, 2 filaments are utilized (WDM isn't ordinarily utilized on multi-mode fiber). POF is a more up to date plastic-based link which guarantees execution like glass link on short runs, however at a lower cost.

(c)Plastic Optical Fiber (POF)

Plastic optical fiber is a type of optical fiber that uses polymathylmethacry late (PMMA) as the core material that allows the transmission of light. POF is often called consumer optical fiber as it is a low-cost optical fiber alternative that is easier to use than glass optical fiber. It sustains a data transfer speed of 2.5GB/s, which isn't as fast as glass optical fiber, but is much faster than traditional copper wire.

5.5.2 UTP Cable:

Unshielded twisted pair (UTP) cables are widely used in the computer and telecommunications industry as Ethernet cables and telephone wires. In an UTP cable, conductors which form a single circuit are twisted around each other in order to cancel out electromagnetic interference (EMI) from external sources. Unshielded means no additional shielding like meshes or aluminum foil, which add bulk, are used.

There are two types of UTP cables. They are:

Category 5 cable:

Category 5 cables, commonly referred to as Cat 5, are a twisted pair cable for computer networks. The cable standard provides performance of up to 100 MHz and is suitable for most varieties of Ethernet over twisted pair. Cat 5 is also used to carry other signals such as telephony and video.

This cable is commonly connected using punch-down blocks and modular connectors. Most Category 5 cables are unshielded, relying on the balanced line twisted pair design and differential signaling for noise rejection.

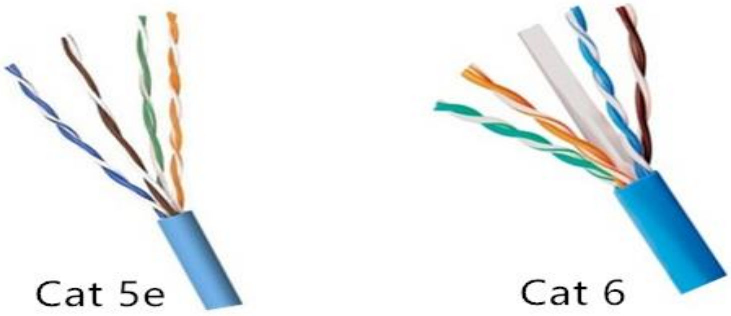


Figure 5.5: Difference type of UTP cable

Category 6 cable:

Classification 6 link, normally alluded to as Cat 6, is an institutionalized contorted combine link for Ethernet and other system physical layers that is in reverse good with the Category 5/5e and Category 3 link models.

Contrasted and Cat 5 and Cat 5e, Cat 6 includes increasingly stringent determinations for crosstalk and framework commotion. The link standard likewise determines execution of up to 250 MHz contrasted with 100 MHz for Cat 5 and Cat 5e.

5.6Routing Protocol:

In internetworking, the way toward moving a parcel of information from source to goal is steering.

Directing is typically performed by a committed gadget called a switch. Directing is a key component of the Internet since it empowers messages to go starting with one PC then onto the next and in the long run achieve the objective machine. Every go-between PC performs steering by going along the message to the following PC. Some portion of this procedure includes investigating a steering decide the best way.

- **BGP**

- **OSPF**

BGP (Border Gateway Protocol): BGP (Border Gateway Protocol) will be convention that oversees how parcels are steered over the web through the trading of directing and achieve capacity data between edge switches. BGP coordinates parcels between self-sufficient frameworks (AS) systems overseen by a solitary endeavor or specialist co-op. Traffic that is directed inside a solitary system AS is alluded to as inner BGP, or I BGP. All the more frequently, BGP is utilized to associate one AS to different self-sufficient frameworks, and it is then alluded to as an outer BGP, or e BGP. BGP settles on best-way choices dependent on current achieve capacity, jump checks and other way qualities. In circumstances where numerous ways are accessible - as inside a noteworthy facilitating office - BGP can be utilized to convey an association's own inclinations as far as what way traffic ought to follow all through its systems. BGP even has an instrument for characterizing discretionary labels, called networks, which can be utilized to control course ad conduct by common understanding among companions.

Open Shortest Path First (OSPF): The OSPF (Open Shortest Path First) protocol is one oaf family of IP Routing protocols, and is an Interior Gateway Protocol (IGP) for the Internet, used to distribute IP routing information throughout a single Autonomous System (AS) in an IP network.

The main advantage of a link state routing protocol like OSPF is that the complete knowledge of topology allows routers to calculate routes that satisfy particular criteria. This can be useful for traffic engineering purposes, where routes can be constrained to meet particular quality of service requirements.

From this database, each router calculates its own routing table using a Shortest Path First (SPF) or Dijkstra algorithm. This routing table contains all the destinations the routing protocol knows about, associated with a next hop IP address and outgoing interface.

- The convention recalculates courses when organize topology changes, utilizing the Dijkstra calculation, and limits the steering convention traffic that it creates.
- It offers help for numerous ways of equivalent expense.

- It gives a staggered chain of command (two-level for OSPF) called "zone directing," so data about the topology inside a characterized zone of the AS is avoided switches outside this territory. This empowers an extra dimension of steering assurance and a decrease in directing convention traffic.
- All protocol exchanges can be authenticated so that only trusted routers can join in the routing exchanges for the AS.

Currently the company is using version 2 of OSPF. The benefits are when OSPF is enabled on an interface and the network address for the interface matches the range of addresses that is specified by the network area command, which is entered in router configuration mode. Alternatively, enabling OSPFv2 explicitly on an interface by using the ip ospf area command, which is entered in interface configuration mode, is possible. This capability simplifies the configuration of unnumbered interfaces with different areas.

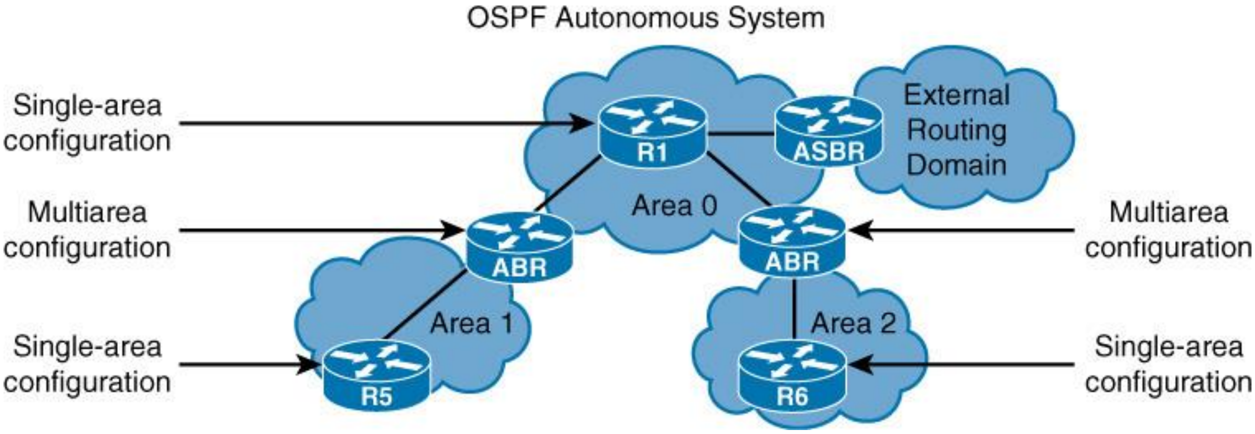


Figure 5.6: Image of Open Shortest Path First (OSPF)

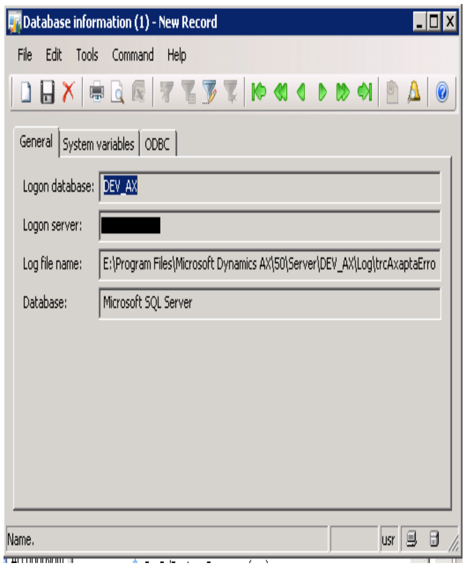
5.7Network Monitoring Tools

- MRTG : The Multi Router Traffic Graphed (MRTG) is free software for monitoring and measuring the traffic load on network links. It allows the user to see traffic load on a network over time in graphical form.

- It was originally developed by Tobias Oinker and Dave Rand to monitor router traffic, but has developed into a tool that can create graphs and statistics for almost anything.

- Dude Server: The Dude is a free application by MikroTik, which can dramatically improve the way you manage your network environment. It will automatically scan all devices within specified subnets, draw and layout a map of your networks, monitor services of your devices and execute actions based on device state changes.

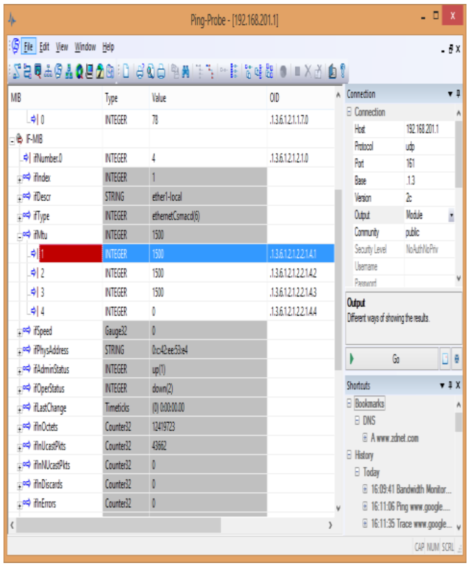
  Not only can you monitor your devices, you can also manage them. Mass upgrade Router OS devices, configure them right from within the Dude interface, run network monitoring tools etc. Figure 5.7(a) shows the dude server



Logon database:	DEV_AX
Logon server:	[redacted]
Log file name:	E:\Program Files\Microsoft Dynamics AX\50\Server\DEV_AX\Log\trcAxaptaErro
Database:	Microsoft SQL Server

Name.

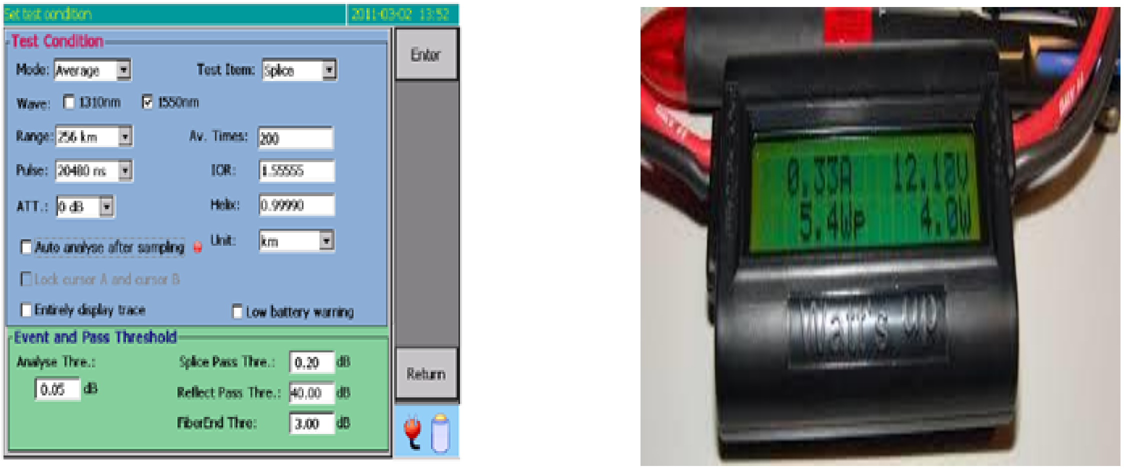
(a) Dude Server


Ping-Probe - [192.168.201.1]
File
Edit
View
Window
Help
Connection
Output
Different ways of showing the results.
Go
Shortcuts
Bookmarks
DNS
A www.zdnet.com
History
Today
16:09:41 Bandwidth Monitor...
16:11:06 Ping www.google....
16:11:35 Trace www.google...
CAP
NUM
SCRL

MIB	Type	Value	OID
0	INTEGER	78	.1.3.6.1.2.1.1.7.0
IF-MIB			
ifNumber.0	INTEGER	4	.1.3.6.1.2.1.2.1.0
ifIndex	INTEGER	1	
ifDescr	STRING	ether1-local	
ifType	INTEGER	ethernetCsmacd(6)	
ifMtu	INTEGER	1500	
1	INTEGER	1500	.1.3.6.1.2.1.2.2.1.4.1
2	INTEGER	1500	.1.3.6.1.2.1.2.2.1.4.2
3	INTEGER	1500	.1.3.6.1.2.1.2.2.1.4.3
4	INTEGER	0	.1.3.6.1.2.1.2.2.1.4.4
ifSpeed	Gauge32	0	
ifPhysAddress	STRING	0:c:42:ee:53:e4	
ifAdminStatus	INTEGER	up(1)	
ifOperStatus	INTEGER	down(2)	
ifLastChange	Timeticks	(0) 0:00:00.00	
ifInOctets	Counter32	12419723	
ifInUcastPkts	Counter32	43662	
ifInNUcastPkts	Counter32	0	
ifInDiscards	Counter32	0	
ifInErrors	Counter32	0	

Connection	
Host	192.168.201.1
Protocol	udp
Port	161
Base	.1.3
Version	2c
Output	Module
Community	public
Security Level	NoAuthNoPriv
Username	
Password	

(b) SNMP



Set test condition 2011-03-02 13:52

Test Condition

Mode: Average ▾ Test Item: Splice ▾

Wave: □ 1310nm ☑ 1550nm

Range: 256 km ▾ Av. Times: 200

Pulse: 20480 ns ▾ IOR: 1.55555

ATT.: 0 dB ▾ Helix: 0.99990

□ Auto analyse after sampling Unit: km ▾

□ Lock cursor A and cursor B

□ Entirely display trace □ Low battery warning

Event and Pass Threshold

Analyse Thre.: 0.05 dB

Splice Pass Thre.: 0.20 dB

Reflect Pass Thre.: 40.00 dB

FiberEnd Thre: 3.00 dB

(c) OTDR

(d) Power Meter

Figure 5.7: Network Monitoring Tools

- SNMP Ping: Utility to check if a specific IP is SNMP enabled. It helps the network engineers to know the availability of a device and also provides basic information like DNS name, system name, location, system type, and system description. Following the SNMP discovery, if required, more details of the node can be retrieved using SNMP Tools like SNMP walker, MIB Browser and SNMP Graph. Figure 5.7(b) shows the SNMP Ping.

- OTDR: An optical time-domain reflectometer (OTDR) is an optoelectronic instrument used to characterize an optical fiber. An OTDR is the optical equivalent of an electronic time domain reflect meter. It injects a series of optical pulses into the fiber under test and extracts, from the same end of the fiber, light that is scattered (Rayleigh backscatter) or reflected back from points along the fiber. Figure 5.7 (c) shows the OTDR.

- Power meter estimates electrical vitality.
- Watt meter estimates the electrical power flowing in any electric circuit.
- Microwave control meter estimates control in a microwave flag.
- Optical power meter estimates control in an optical flag.
- Google Power Meter is an apparatus to follow a family unit's vitality use.

- A cycling power meter estimates the power yield of a bike rider.

A running force meter estimates the power yield of a sprinter. Figure 5.7(d) demonstrates the power meter.

5.8Network Security:

The term network security refers to protecting the digital assets like computer systems, programs, and information from intrusion, destruction, theft, modification, or misuse. Network security can be made up of hardware devices, specialized software, physical security i.e. locked computer rooms, and rules for people to follow.

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Types of network security

- **Access control**

Not every user should have access to our network. To keep out potential attackers, we need to recognize each user and each device. Then we can enforce our security policies. We can block noncompliant endpoint devices or give them only limited access. This process is network access control (NAC).

- **Antivirus and antimalware software**

"Malware," short for "malicious software," includes viruses, worms, Trojans, ransom ware, and spyware. Sometimes malware will infect a network but lie dormant for days or even weeks. The best antimalware programs not only scan for malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage.

- **Application security**

Unfortunately, any application may contain holes, or vulnerabilities, those attackers can use to infiltrate our network. Application security encompasses the hardware, software, and processes you use to close those holes**.**

- **Data Loss Prevention**

Organizations must make sure that their staff does not send sensitive information outside the network. Data loss prevention, or DLP, technologies can stop people from uploading, forwarding, or even printing critical information in an unsafe manner.

- **Firewalls**

Firewalls put up a barrier between your trusted internal network and untrusted outside networks, such as the Internet. They use a set of defined rules to allow or block traffic. A firewall can be hardware, software, or both. Cisco offers unified threat management (UTM) devices and threat-focused next-generation firewalls.

- **Intrusion Prevention Systems**

An intrusion prevention system (IPS) scans network traffic to actively block attacks. Cisco Next-Generation IPS (NGIPS) appliances do this by correlating huge amounts of global threat intelligence to not only block malicious activity but also track the progression of suspect files and malware across the network to prevent the spread of outbreaks and reinjection.

- **Network segmentation**

Software-defined segmentation puts network traffic into different classifications and makes enforcing security policies easier. Ideally, the classifications are based on endpoint identity, not mere IP addresses. We can assign access rights based on role, location, and more so that the right level of access is given to the right people and suspicious devices are contained and remediated.

➢ **VPN**

A virtual private network encrypts the connection from an endpoint to a network, often over the Internet. Typically, a remote-access VPN uses IPsec or Secure Sockets Layer to authenticate the communication between device and network.

➢ **Web security**

A web security solution will control our staff's web use, block web-based threats, and deny access to malicious websites. It will protect our web gateway on site or in the cloud. "Web security" also refers to the steps you take to protect your own website.

5.9 Limitation:

Every organization always moves with some limitations. Like APCL have some limitations. They are:

- The shortage of IPV4 in worldwide.
- Higher transmission rate for data line of NTTN network.
- 15% vat on internet reduced to 5% ,but still 15% on tax is applicable.
- Enduser are reluctant to give vat.
- It has no Facebook Cache Server.
- All Upzila/Thana has no Fiber Optic connectivity.
- Feedback time from Tax lease provider is not uo the mark.

Chapter 6

Upgradation of APCL Network

APCL being one of the leading companies of Bangladesh has all the upgraded facilities. There are most efficient and world class devices and security tools are used.

- Branch network system
- Communication
- Network Infrastructure
- Support system
- Development
- Tracking

The data center is placed right in the middle of the department of ISP. It is well secured with fingerprint sensor. Only authorized personnel have the access of the data center. The entire department has access to their respected information's from the servers. There are also branch servers that can be access from the main branch as well as the branch office where it is located. The co-ordination team manages the hardware required for the ISP division.

6.1 Proposed Upgrades

The purpose of the internship program was to observe the current network precisely and find out any scope to improve the network. During the internship program, there have been some changes made to the network that gave an idea of how to develop and maintain the network. The floor switches were connected to the core switch via copper cables previously. But now the change is made; they are using fiber optic cable with 12 cores. This has made the transaction of network way too faster than the previous one. Also they made an upgrade from EIGR protocol to OSPF.

6.2 The Proposed Network of APCL

The proposed idea is to make better communication and connection between the floors that mostly require fastest IT supports and services. Figure 6.2 shows the changed system that gets the immediate correspondence identified with ISP bolsters. This will decrease the term of pausing and get the data as quickly as time permits. The Backup switch is included this proposed system, to help the center switch. On the off chance that the center switch is down, the reinforcement switch will turn on and work rather than the center switch.

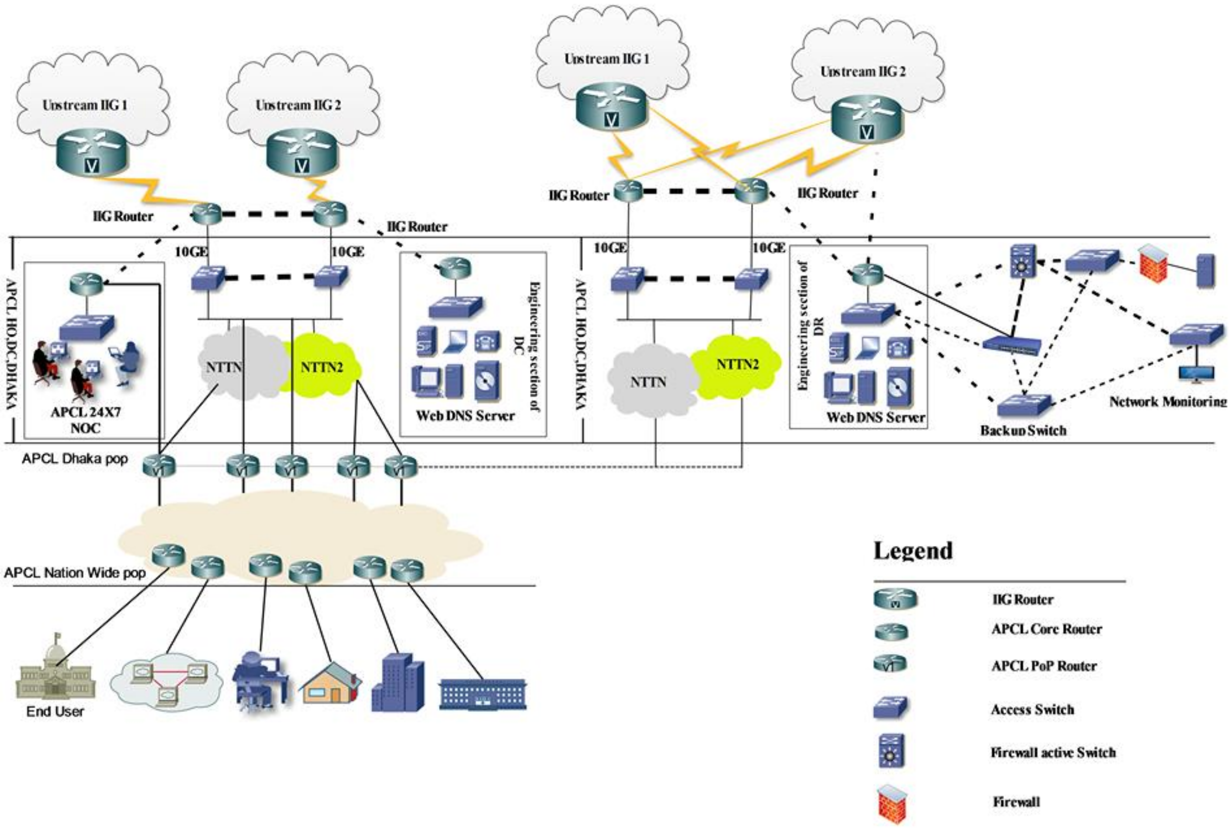


Figure 6.2: The Proposed Network of APCL

Main Process:

Here,

- APCL-Asia Pacific Communication Ltd
- IIG1 (SAMMIT)Core Router
- IIG2 (Fiber @ Home) backup core router
- DESCO-Dhaka Electric Supply Company Limited

In figure 6.2, the ISP (Internet Service Provider) of APCL has two (IIG-1 and IIG-2) router. The IIG-1 and IIG-2 router are added with several clouds. IIG-1 router is connected with 100 GBPS bandwidth from IIG-1 cloud and IIG-2 router is connected with 10 GBPS bandwidth from IIG-2 cloud. The Core Router of APCL-1 is added with IIG-1 Router by using Node, the router of APCL-1 is also added with the backup router of APCL and the backup router is connected with switch which added the Pop router of APCL. This switch can communicate with customer's sector. Again IIG-2 cloud is connected with IIG-2 router by using Core router of APCL and it distributes the data. From back up APCL Core router is joined with a switch (NTTN-2) and DC router. The PoP router of APCL is added with a switch (NTTN-2) and this switch is also added with the consumer router which distributes the data.

On the other side of backup part, there is a cross connection between IIG-1 and IIG-2. Two connections are alternative for each other. From the Engineering sector DR, they can set up a Multilayer switch and three switches can have added with it. On the first switch is used for the consumer and then they can add firewall and a server. By using this firewall, anyone can not access there switch. If the first switch will damage, then the third switch which is backup will support it. They can set up a network monitoring switch. If it will face problem, the third backup switch will support it. Finally, If the third backup switch and multiple switch will damage, on that time the DMZ switch will give them as a backup. Because it is directly connected with the Router.

Functions:

The new architecture is making the connection more communicative and easy accessible. Though this connectivity, the ISP department will be able to help the users faster and efficiently. The users will have direct connectivity so they can get connected any time. All the request will be sent directly to the ISP department to their respected support team. On the other hand, the backup core router will provide maximum support when the main core router is down for any reason. It is a crucial part of this network. If the main core router is down, the whole system will be down as well. To avoid this kind of circumstances, it is very essential to have this backup router.

6.3 File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections.

FTP is a client-server protocol that relies on two communications channels between client and server: a command channel for controlling the conversation and a data channel for transmitting file content. Clients initiate conversations with servers by requesting to download a file. Using FTP, a client can upload, download, delete, rename, move and copy files on a server. A user typically needs to log on to the FTP server, although some servers make some or all of their content available without login, also known as anonymous FTP.

6.4 Backup router communication

To make an uninterrupted bandwidth commucation core router (A) need to connect backup core router (C). Because of APCLcollect their badwidth from two different IIG companies. If any how one router goes down another one router give back at a time. If they make a backup communication for core router (A) to Dhaka pop (B) we provide good service for customer because we reduce data redundency and also reduces data trafic. Corporate line is too much important for supplying uninteruppted services. If coporate router (E) connected with Gazipur pop (F) router we need to worry about the connection loss problem. At once our Gazipur pop switch function as reinforcement switch for corporate switch and coporate switch likewise fill in as a reinforcement switch for Gazipur pop. Mawna branch is associated with Gazipur branch through a switch. However, on the off chance that their construct a correspondence from Gazipur pop switch Mawna branch dodge information repetition and furthermore get reinforcement for continuous correspondence.

6.5 Telnet

Telnet is an underlying TCP / IP protocol for accessing a user command and remote computer. An Administrator or any other user can access other computers through remote Telnet. Remote users on the web, HTTP and FTP protocols Allows to request specific files from the computer, but is not actually logged in as the user of that computer. An administrator is allowed to access specific applications and data by logging on to a computer as a regular user with Telnet. Telnet permits remote access to a person's computer. Although it is not like sitting in front of someone else's computer and using it, it gives the user the ability to access computer data through a text-based interface. Telnet saves time because an administrator can perform any work on his computer often from his computer instead of being physically present on another user's computer. Since it uses plain text so it's very easy to fix problems. Telnet allows for less problems with more information and information transmission. Telnet can be used on any computer from any other place whose is connected directly or indirectly connected with router. Even older systems may be connected to a new computer with different operating system versions.

6.6Benefits of this network:

- Easy and efficient connectivity
- Making the communication easier
- More manageable than the previous one
- Very fast in trouble shooting
- Easier maintain ace process
- Hassel free connectivity
- Backup router provides instant support
- No dead connection

Chapter 7

Design of Upgraded Network of APCL

Cisco Packet Tracer is a powerful network simulator that can be utilized in training for CCNA and CCNP certification exam by allowing students to create networks with an almost unlimited number of devices and to experience troubleshooting without having to buy real Cisco routers or switches. The tool is created by Cisco Systems. The purpose of Packet Tracer is to offer students a tool to learn the principles of networking as well as develop Cisco technology specific skills. However, it is not being used as a replacement for Routers or Switches. The figure 4.1 represents the Cisco Packet Tracer 7.1 version.

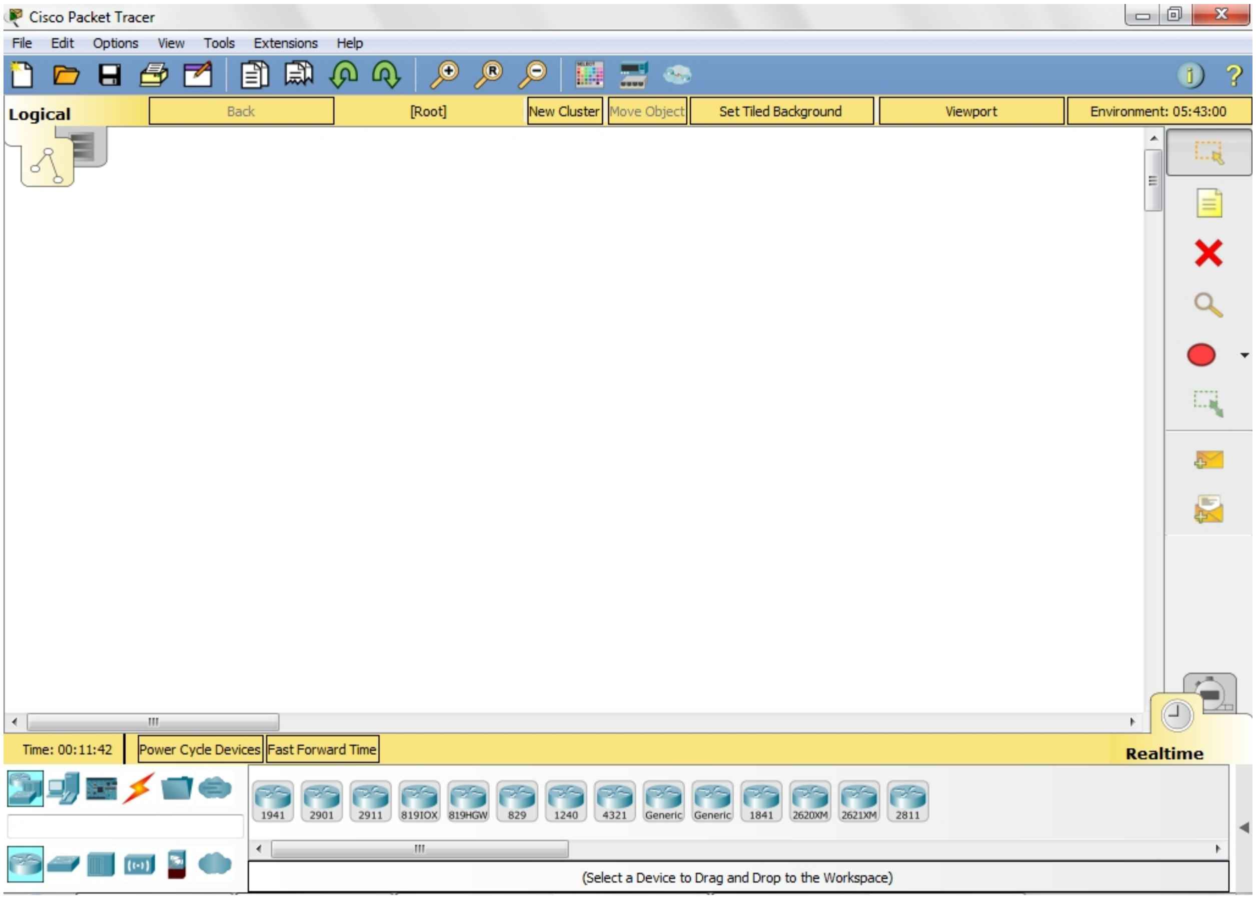


Figure 7.1: The Cisco packet tracer version 7.1

7.2 The Existing network of APCL

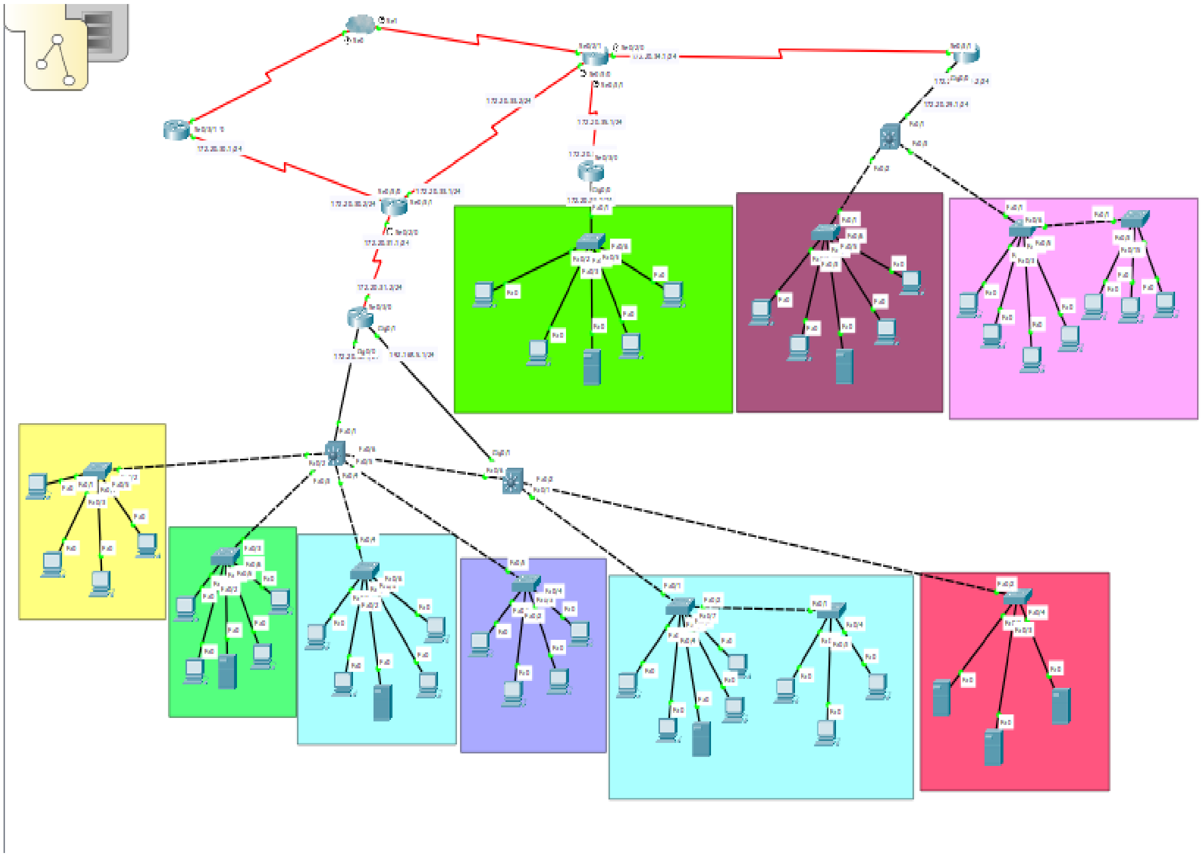


Figure 7.2 The Existing Network of APCL

APCL has a main cloud and the cloud is connected with two IIG (IIG-1 and IIG-2) routers. IIG-1 router is connected with Dhaka Zone. Dhaka zone has a Pop which is known as Dhaka Pop. Dhaka Pop added two multilayer switches and two switches are connected with each other. Here the first multilayer switch is connected with Uttara Branch, Badda , Gulshan and Dhanmondi. On the other side, second multilayer switch is connected with Gazipur and server. Badda, Gulshan and Gazipur has their several server. From the server, anyone can access the data. In the server, which is connected with second multilayer switch there is connection with Uttara and Dhanmondi. In the server, only fixed person or selected person can access the data because these are more secure than others router/ users.

On the other side, the cloud connected with IIG-2 router which works as a backup router and which is directly connected with Bank and Corporate branch. From the Corporate branch, they added a multilayer switch. The switch is consisting of DESCO and Mawna. So they have the backup process and pass their data within short time. If we use a multilayer switch need not access our core router because need to use only backup router which is connected IIG2 cloud. Using multilayer switch, we easily use shortest path for sending data and make communication. Our backup router is not too much busy because in here we don’t use any distribution process for local users.

7.2Configuration Code for Existing Network

7.2.1. Core router configuration

```
Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#in
Router(config)#interface se
Router(config)#interface serial 0/3/0
Router(config-if) #ip add
Router(config-if) #ip address 172.20.30.2 255.255.255.0
Router(config-if) #no shut
Router(config-if) #
%LINK-5-CHANGED: Interface Serial0/3/0, changed state to up
Router(config-if) #exit
Router(config)#in se 0/
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up3/1
Router(config)#in se 0/3/1
Router(config-if) #ip add
Router(config-if) #ip address 172.20.33.2 255.255.255.0
Router(config-if) #no shut
%LINK-5-CHANGED: Interface Serial0/3/1, changed state to down
```

```
Router(config-if) #exit

Router(config)#interface se 0/2/0

Router(config-if) #ip address 172.20.31.1 255.255.255.0

Router(config-if) #no shutdown

%LINK-5-CHANGED: Interface Serial0/2/0, changed state to down

Router(config-if) #exit

Router(config)#router ospf 10

Router(config-router) #network 172.20.30.0 0.0.0.255 area 0

Router(config-router) #network 172.20.30.0 0.0.0.255 area 0

00:05:49: %OSPF-5-ADJCHG: Process 10, Nbr 172.20.30.1 on Serial0/3/0 from LOADING to FULL, Loading Done

Router(config-router) #network 172.20.33.0 0.0.0.255 area 0

Router(config-router) #network 172.20.31.0 0.0.0.255 area 0

Router(config)#enable password 123

Router(config)#line console 0

Router(config)#password 1234

Router(config)#login

Router(config)#username rinty password 12345

Router(config)#local login

Router(config)#end

Router#

%SYS-5-CONFIG_I: Configured from console by console

Router#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Router#
```

7.2.2 Backup Core router configuration

```
Press RETURN to get started!

Router>en

Router#config

Configuring from terminal, memory, or network [terminal]?

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#interface serial 0/3/0

Router(config-if) #ip add

Router(config-if) #ip address 172.20.33.1 255.255.255.0

Router(config-if) #no shut

Router(config-if) #

%LINK-5-CHANGED: Interface Serial0/3/0, changed state to up

exit

Router(config)#interface serial 0/3/1

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up

Router(config-if) #ip address 172.20.35.1 255.255.255.0

Router(config-if) #no shut

%LINK-5-CHANGED: Interface Serial0/3/1, changed state to down

Router(config-if) #exit

Router(config)#interface serial 0/2/0

Router(config-if) #ip address 172.20.34.1 255.255.255.0

Router(config-if) #no shut

%LINK-5-CHANGED: Interface Serial0/2/0, changed state to down

Router(config-if) #exit

Router(config)#router ospf 10

Router(config-router) #network 172.20.33.0 0.0.0.255 area 0

Router(config-router) #network 172.20.35.0 0.0.0.255 area 0
```

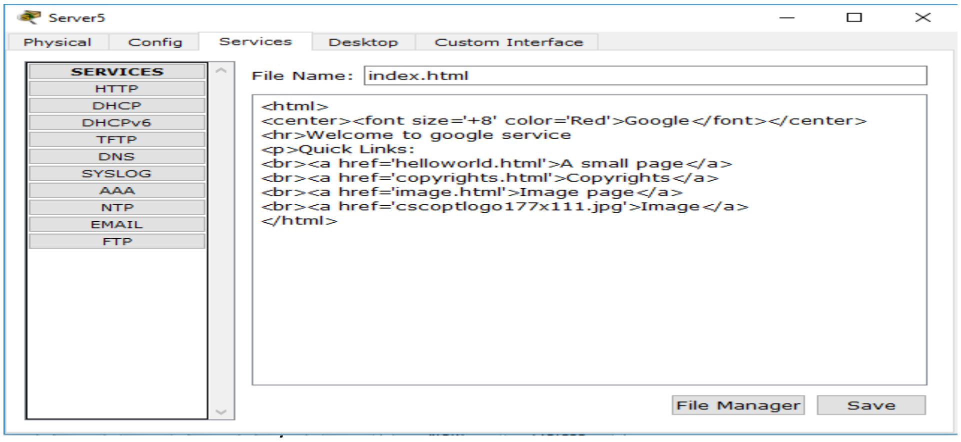
```
00:08:45: %OSPF-5-ADJCHG: Process 10, Nbr 172.20.33.2 on Serial0/3/0 from LOADING to FULL, Loading Done

Router(config-router) #network 172.20.34.0 0.0.0.255 area 0

Router(config-router) #exit

Router(config)#line console 0

Router(config-line) #password 1234

Router(config-line) #login

Router(config-line) #exit

Router(config)#secret password 1234

Router(config)#username rinty pass

Router(config)#username rinty password 12345

Router(config)#line vty 0 4

Router(config-line) #lo

Router(config-line) #log

Router(config-line) #log

Router(config-line) #login local

Router(config-line) #login local

Router(config-line) #end

Router#

%SYS-5-CONFIG_I: Configured from console by console

Router#copy run sta

Destination filename [startup-config]?

Building configuration...

[OK]

Router#
```

7.2.3 Dhaka pop router configuration

```
Continue with configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#in
Router(config)#interface se
Router(config)#interface serial 0/2/0
Router(config-if) #ip address 172.20.31.2 255.255.255.0
Router(config-if) #no shut
%LINK-5-CHANGED: Interface Serial0/2/0, changed state to down
Router(config-if) #exit
Router(config)#interface gigabitEthernet 0/1
Router(config-if) #ip add 192.168.31.1 255.255.255.0
Router(config-if) #no shut
Router(config-if) #
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
Router(config-if) #exit
Router(config)#in gig 0/0
Router(config-if) #ip add
Router(config-if) #ip address 192.168.32.1 255.255.255.0
Router(config-if) #no shut
Router(config-if) #
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
```

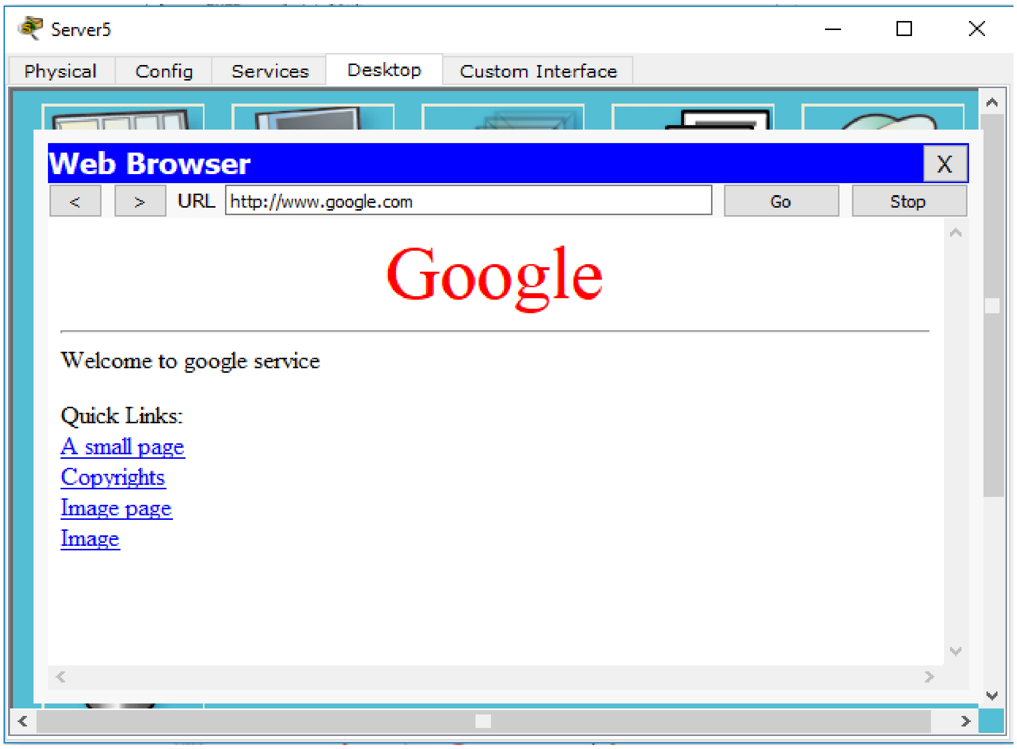
```
Router(config-if) #exit
Router(config)#router ospf 10
Router(config-router) #network 172.20.31.0 0.0.0.255 area 0
Router(config-router) #network 192.168.31.0 0.0.0.255 area 0
Router(config-router) #network 192.168.32.0 0.0.0.255 area 0
Router(config-router) #exit
Router(config)#enable pass 1234
Router(config)#line console 0
Router(config-line) #password 12345
Router(config-line) #login
Router(config-line) #exit
Router(config)#username rinty password 1234
Router(config)#line vty 0 4
Router(config-line) #login local
Router(config-line) #end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#copy run sta
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

7.2.4 Web Server Configuration



File Name: index.html

```
<html>
<center><font size='+8' color='Red'>Google</font></center>
<hr>Welcome to google service
<p>Quick Links:
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscoptlogo177x111.jpg'>Image</a>
</html>
```



URL http://www.google.com

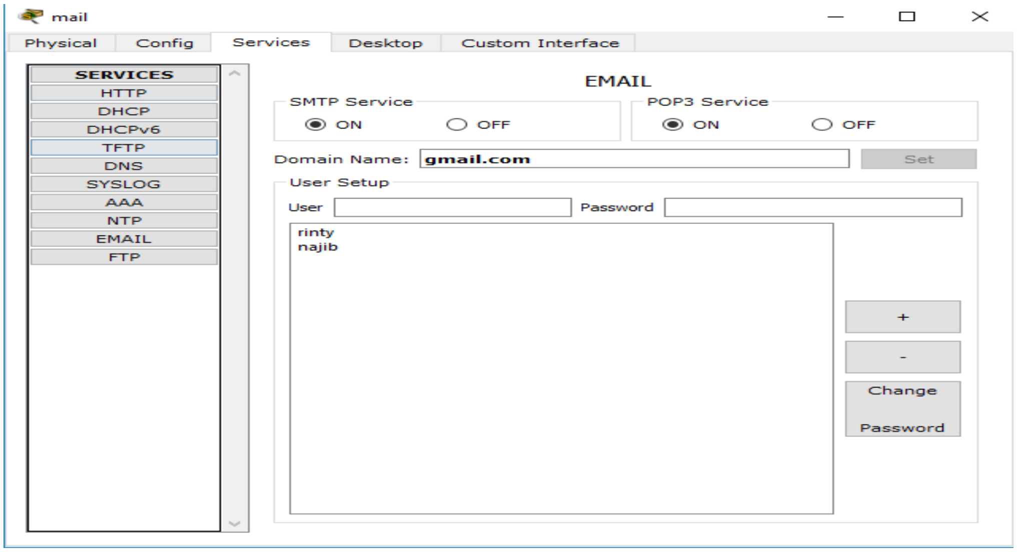
Google

Welcome to google service

Quick Links:
A small page
Copyrights
Image page
Image

Figure 7.2.4 Web server configuration

7.2.5 Mail Server Configuration



EMAIL

SMTP Service ● ON ○ OFF

POP3 Service ● ON ○ OFF

Domain Name: gmail.com

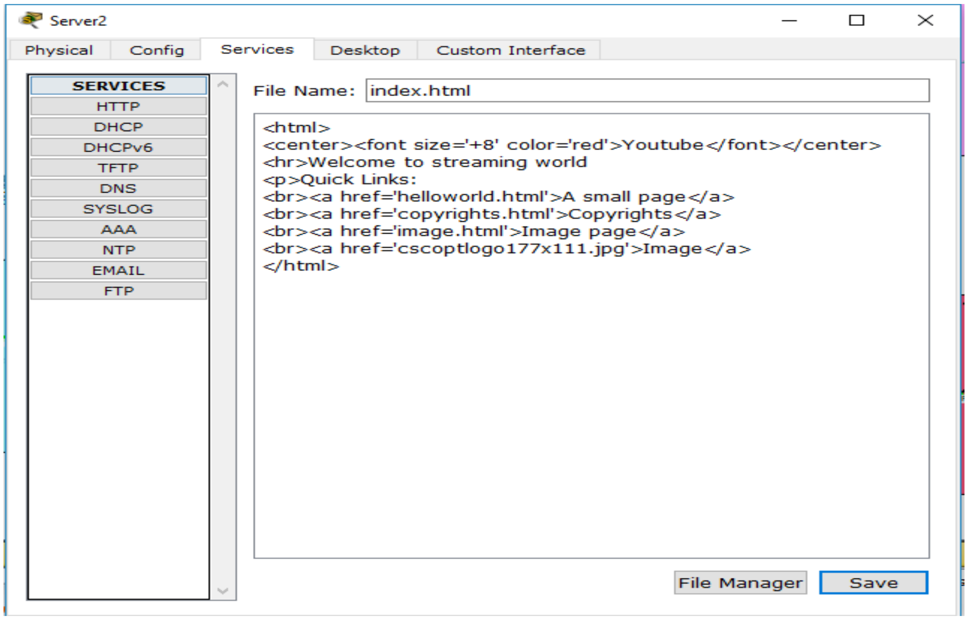
User Setup

User
Password

rinty
najib

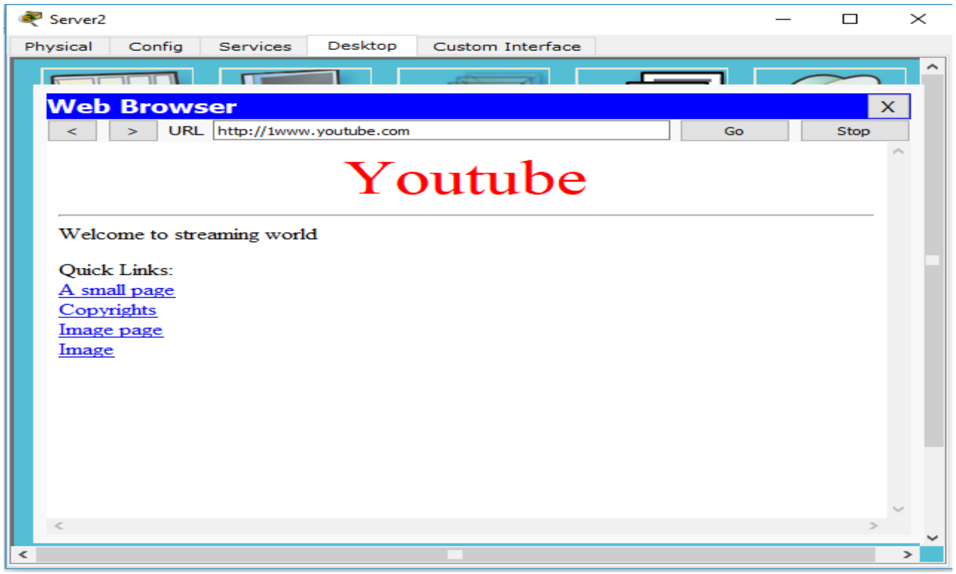
Figure 7.2.5 Mail Server configuration

7.2.6 YouTube Server Configuration



File Name: index.html

```
<html>
<center><font size='+8' color='red'>Youtube</font></center>
<hr>Welcome to streaming world
<p>Quick Links:
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscoptlogo177x111.jpg'>Image</a>
</html>
```



URL http://1www.youtube.com

Youtube

Welcome to streaming world

Quick Links:
A small page
Copyrights
Image page
Image

Figure 7.2.6 YouTube Server setup

7.3 The proposed network

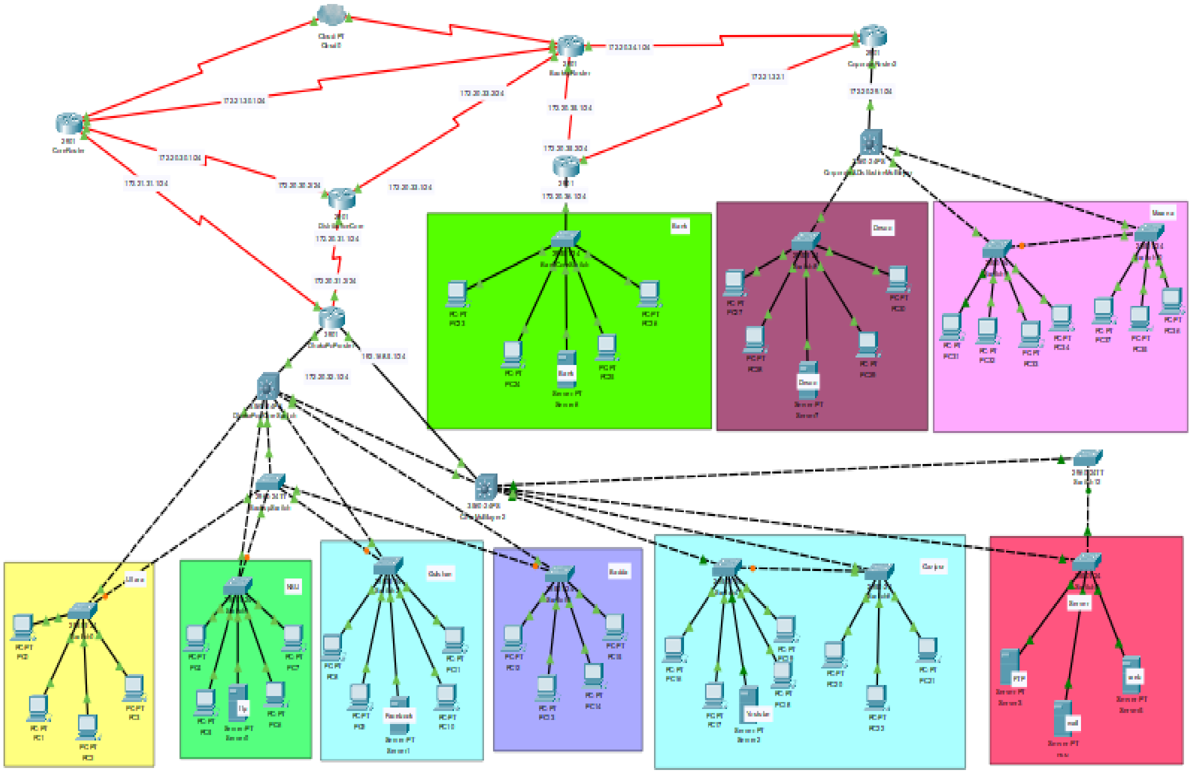


Figure 7.3 The Proposed Network of APCL

Here,

- APCL-Asia Pacific Communication Ltd
- IIG1 (SAMMIT)
- IIG2 (Fiber @ Home)
- DESCO-Dhaka Electric Supply Company Limited

APCL is connected to IIG1 and IIG2 router with their two core router. One core router is used as a main router and all work is process in that router. Another router for distribute data services. Pop core switch is connected with Dhaka pop Uttara, NSU, Gulshan, Badda. ISP is connected with Pop core switch so if any connection will close one ISP can't make any communication with others. So the proposal is if they use a extra switch here its works as a backup switch for support all ISP.

Gazipur ISP is connected with Pop core switch2 which is directly connected with Dhaka PoP router.

In here we have 2 ISP which is distributed two single switch, if we make a communication between two routers it will be supportive for all and work as a backup switch.

They use a single switch for their server it’s too much risky because we need to always our server lives in 24 hours. Without live server we cannot give any service. So the think is if they use a extra switch for their server they can give best service of their clients. If Dhaka pop router will have disconnected from distribution router all ISP will be disconnected from all services, so if Dhaka pop will be connected core router 1 this risk will be less. Because Core router 1 is directly connected with IIG and it is also connected with backup router. Core router 1 is alternatively give support backup router also we use our backup router as corporate router. Because they distribute 2 corporate routers here. One router is connected with bank and another router is connected with DESCO. To make a spontaneous service, they can make a communication between to corporate router, one is backup for another router. From DESCO core switch, they distribute 2 ISP in Mawna. If they make a communication between two switches they ensure provide good services for their client. They appreciate it because the design is helpful for their back services and too much cost efficient. This design not only cost efficient it is also helpful for data redundancy.

7.4 Comparison Between Present Network and Proposed Network:

In 1st network diagram they have only one backup router and our pop router has no any backup line. So when one line will be cut our one zone totally stopped. In these circumstances their client detached from all network activity and they call to inform to solve the problem. But they already solve this problem. In the proposal, distribution router is connected with IIG1 router so if pop router is failed to communicate distribution router IIG1 router directly make communication pop router. So our valuable client will not face any problem. Their backup core router is only connected with IIG2 router. The suggestion is if they create a backup line from IIG1 router to backup core router they make a strong network for APCL. If this proposal they will accept there is no possibility to disconnect from network easily. Here one router is backup router for one another. Also suggested them if they use virtual IP it’s helpful for our security. Virtual IP means our real IP no one can be shown. If no one knows their real IP, they cannot access their router and don’t make fraud requests.

Chapter 8
Conclusion

The ISP network, network infrastructure, communication, support, maintenance, security and development etc. of the existing network is studied thoroughly. The existing network is well formed and up to date. But few limitations were there which was overcome through the proposed plan.

The involvement with APCL as internee has been great. It was a decent affair to meet people with excitement thus supportive nature. The learning opportunity is all around ok to be valued. The system the executives of APCL has such a long way to go from. Their system framework is particularly refreshed with most recent updates. It is a significant accomplishment for me to gain from the framework, it will dependably be a piece of information picking up that will help in future organizations. From the system of APCL, there was such a long way to go. The system of arranging switches, overseeing them was one of the real learning. The exchanging and support of switches are another essential part. Aside from that, figuring out how to plan of a system is an accomplishment. Conquering every one of the restrictions, the report is readied and the result of the proposed system will be helpful for the organization.

References

1. APCL profile: http://www.apclbd.net/about/

2. APCL Internet: http://www.satproviders.com/en/o/APCL-Corporate-Internet

3. APCL mission and vision: https://apclsales.wordpress.com/about/

4. APCL Address: http://www.apclbd.net/about/

5. Network device.URL: http//www.geekinspired.com/networking/network connection- devices/ 6_network_strategies.html

7. OSI Model. URL: https://en.wikipedia.org/wiki/OSI_model

8. TCP/ IP Protocol Suite. URL: https://en.wikipedia.org/wiki/Internet_protocol_suite

9. IP Addressing. URL: https://networklessons.com/ipv6/shortening-ipv6-addresses

10. Comparison of IPv4 and IPv5 URL: https://techdifferences.com/difference-between-ipv4-and-ipv6.html

11. PRTG Network Monitor URL: https://www.paessler.com/manuals/prtg/key_features/

12. Protocol types. URL: http//www.indiastudychannel.com/resources/-Protocols- types.aspx

13. Wireless Communication. URL: https://en.wikipedia.org/wiki/Wireless

14. Computer Networking: https://www.inspiredtechs.com.au/computer-networking/

15. Network Strategies URL: http://www.jhigh.co.uk/Intermediate2/Using%20Information/

16. Category 5 cable URL: https://en.wikipedia.org/wiki/Category_5_cable

17. Category 6 cable URL: https://en.wikipedia.org/wiki/Category_6_cable

Lexicon

- **APCL-**Asia Pacific Communication Ltd
- **LAN-**Local Area Network.
- **MAN-**Metropolitan Area Network.
- **WAN-**Wide Area Network.
- **OSI-**Open Systems Interconnection.
- **TCP/IP-**Transmission Control Protocol and Internet Protocol.
- **IPv4-**Internet Protocol version 4
- **IPv6-**Internet Protocol version 6
- **VPN-**Virtual Private Network
- **AV-**Antivirus