Pearson Higher Nationals in

Computing

Unit 02: Networking

Assignment

ACKNOWLEDGEMENT

We are really grateful because we managed to complete our Network assignment within the time given by our lecturer **Mr. RIFNAS** this assignment cannot be completed without the effort and co-operation from our lecturer. So I sincerely thank our lecturer of Network for the guidance and encouragement in finishing this assignment and also for teaching us in the course. Last but not least, we would like to express our gratitude to our friends and respondents for the support and willingness to spend some times with us to fill in the questionnaires.

Table of Contents

List of Figure

List of Table

LO1 EXAMINE NETWORKING PRINCIPALS AND THEIR PROTOCOLS

What is Network?

A network, in computing, is a group of two or more devices that can communicate. In practice, a network is comprised of a number of different computer systems connected by physical and/or wireless connections.

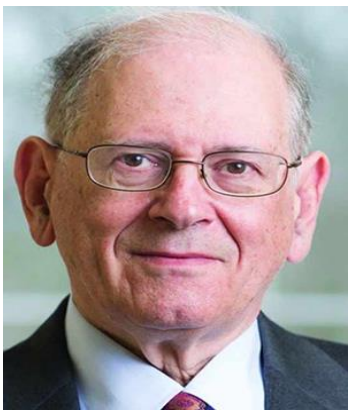
A network is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to one another to allow the sharing of data. An excellent example of a network is the Internet, which connects millions of people all over the world. To the right is an example image of a home network with multiple computers and other network devices all connected.

Figure 1: Network

Introduction to the network

Vinton Cerf and Robert Kahn invented TCP/IP protocol in the 1970s, and in 1972, Ray Tomlinson introduced network email. During the 1980s, the National Science Foundation started to build a nationwide computer network that included its own supercomputers, called NSFNET

Vinton Cerf



Robert Kahn

Ray Tomlinson

Figure 2: Network Introducer's

Advantage and disadvantage for Network:

Table 1: Advantage & disadvantage of network

ADVANTAGE	DISADVANTAGE
• Sharing devices such as printers saves money	• Purchasing the network cabling and file servers can be expensive.
• Site (software) licenses are likely to be cheaper than buying several standalone licenses	• Viruses can spread to other computers throughout a computer network.
• Files can easily be shared between users.	• With risks of network issue

Types of network

Geographical size based type

There are some types of computer networks based on their Geographical size

1. LAN (Local Area Network)
2. MAN (Metropolitan Area Network)
3. WAN (Wilde Area Network)

Local Area Network (LAN)

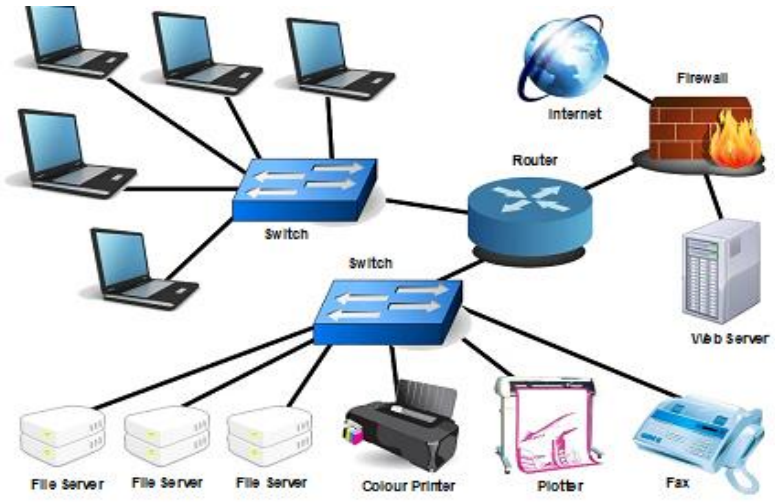


Figure 3: LAN

Table 2: Advantage & Disadvantage of LAN

ADVANTAGE	DISADVANTAGE
• Design and implement is easy	• The use of email within the network can lead to problems of time wasting.
• Costly resources such as printers can be shared by all of the computers.	• long print queues may develop, causing people to have to wait for printed output
• An individual user can load his or her work on any computer on the network.	• Network security can be a problem

Metropolitan Area Network (MAN)

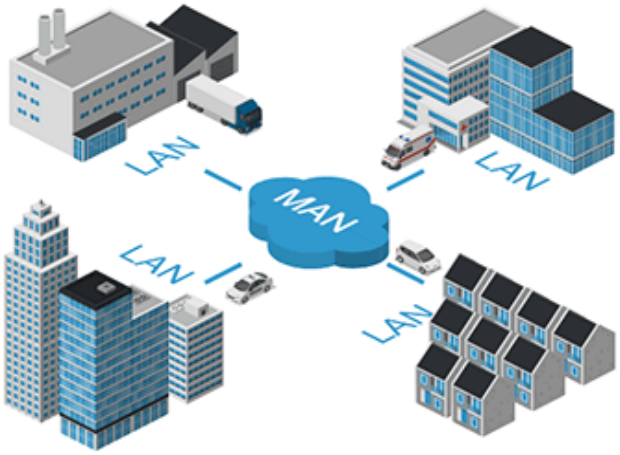


Figure 4: MAN

Table 3: Advantage & Disadvantage of MAN

ADVANTAGE	DISADVANTAGE
• Less expensive	• Difficult to manage
• Sending local emails	• Internet speed difference
• High speed than WAN	• Hackers attack
• Sharing of the internet	• Technical people required to set up
• Conversion from LAN to MAN is easy	• More wires required
• High Security	

Wilde Area Network (WAN)

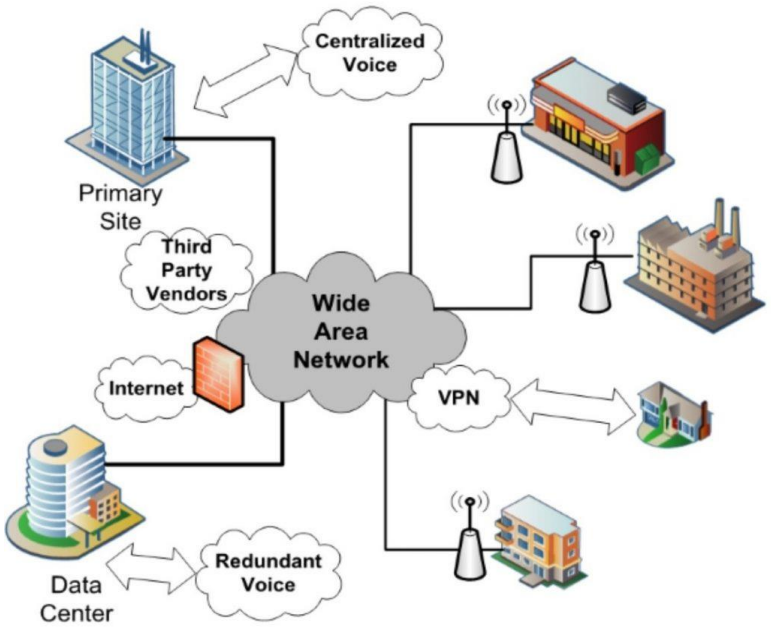


Figure 5: WAN

Wide area network provides long distance transmission of data. The size of the WAN is larger than LAN and MAN. A WAN can cover country, continent or even a whole world. Internet connection is an example of WAN. Other examples of WAN are mobile broadband connections such as 3G, 4G etc.

Table 4: Advantage & Disadvantage of WAN

ADVANTAGE	DISADVANTAGE
• Centralizes IT infrastructure	• High setup costs
• Boosts your privacy	• Security Concerns
• Increases bandwidth	• Maintenance Issues
• Eliminates Need for ISDN	
• Guaranteed uptime	
• Cuts costs, increase profits	

The above are the main types of network. In addition, there are some types of networks are available:

- PAN (Personal Area Network)
- SAN (Storage Area Network)
- EPN (Enterprise Private Network)

Function based type

Networks can also be classified according to their respective functions and structure hierarchy.

Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer.

There are commonly two types:

1. Peer to Peer (P2P)
2. Clint - Server

Peer to Peer

- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.

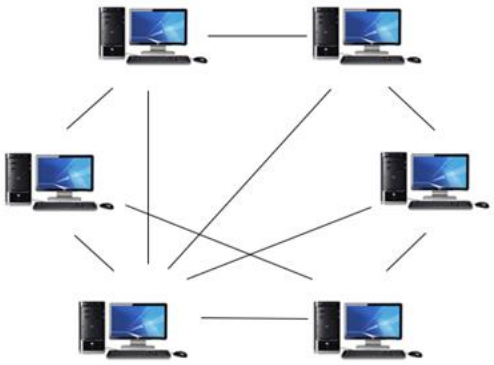


Figure 6: Peer to peer network

Clint - Server

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a server while all other computers in the network are called clients.
- A server performs all the major operations such as security and network management.

Network Standards

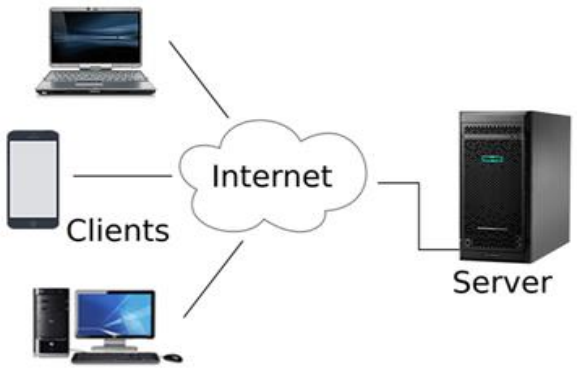


Figure 7: Clint to server

If the different network standards in place today were in print, they would fill volumes upon volumes of text. These network standards serve specific purposes, as defined by the standard itself. For example, there is a standard for you to communicate across the Internet and a different standard for you to talk across the telephone network.

International Telecommunication Union (ITU)

The International Telecommunication Union (ITU) is made up of telecommunication policy makers and regulators, network operators, equipment manufacturers, hardware and software developers, regional standards-making organizations, and financing institutions. The activities, policies, and strategic direction of the ITU are determined and shaped by the industry it serves.

The three sectors of the ITU are Radio communication (ITU-R), Telecommunication Standardization (ITU-T), and Telecommunication Development (ITU-D).

American National Standards Institute (ANSI)

American National Standards Institute (ANSI) serves as administrator and coordinator of the United States private-sector voluntary standardization system. ANSI was founded in 1918 by five engineering societies and three governmental agencies, and is a private, nonprofit membership organization. ANSI ensures each foot-long ruler is accurate in its dimensions, for instance, essentially using a ruler to measure a ruler. ANSI ensures that each inch on the ruler is in fact 1 inch, and that the foot-long ruler is in fact made up of 12 of these inches.

Institute of Electrical and Electronics Engineers (IEEE)

Some of the best-known IEEE standards are as follows:

- IEEE 802.1 (LAN/MAN)
- IEEE 802.3 (Ethernet)
- IEEE 802.5 (Token Ring)
- IEEE 802.11 (Wireless LAN)

What is Network Topology

Network Topology refers to the layout of a network and how different nodes in a network are connected to each other and how they communicate.

Topologies are either **physical** (the physical layout of devices on a network) or **logical** (the way that the signals act on the network media, or the way that the data passes through the network from one device to the next).

Physical topology in computer network.

There are many physical topologies in network.

1. BUS Topology
2. RING Topology
3. STAR Topology
4. MESH Topology
5. TREE Topology
6. HYBRID Topology

Bus Topology

Alternatively referred to as a line topology, a bus topology is a network setup where each computer and network device is connected to a single cable or backbone. Depending on the type of computer network card, a coaxial cable or an RJ-45 network cable is used to connect them together.

The Bus topology transmits data only one direction.

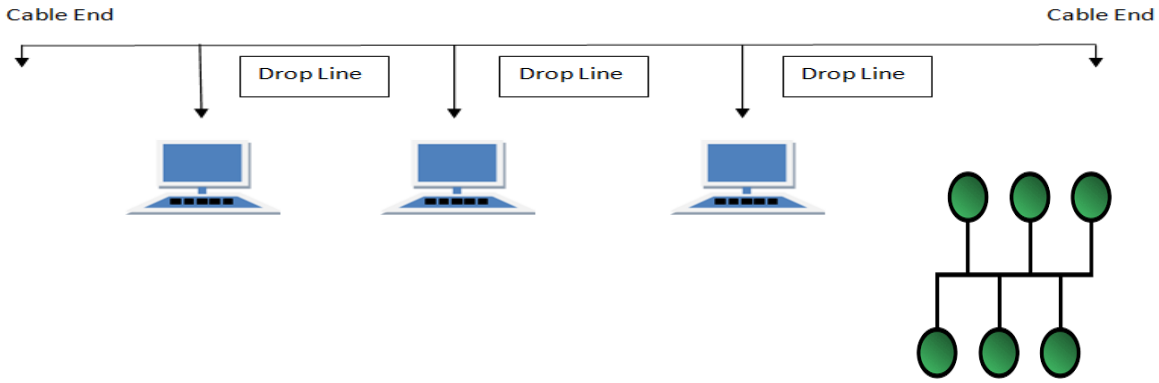


Figure 8: BUS topology & nodes

Table 5: Advantage & disadvantage of Bus topology

ADVANTAGE	DISADVANTAGE
• It is cost effective.	• I Cables fails then whole network fails.
• Cable required is least compared to other network topology.	• If network traffic is heavy or nodes are more the performance of the network decreases.
• Used in small networks.	• Cable has a limited length.
• It is easy to understand.	• It is slower than the ring topology.
• Easy to expand joining two cables together	

Ring Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbors for each device.

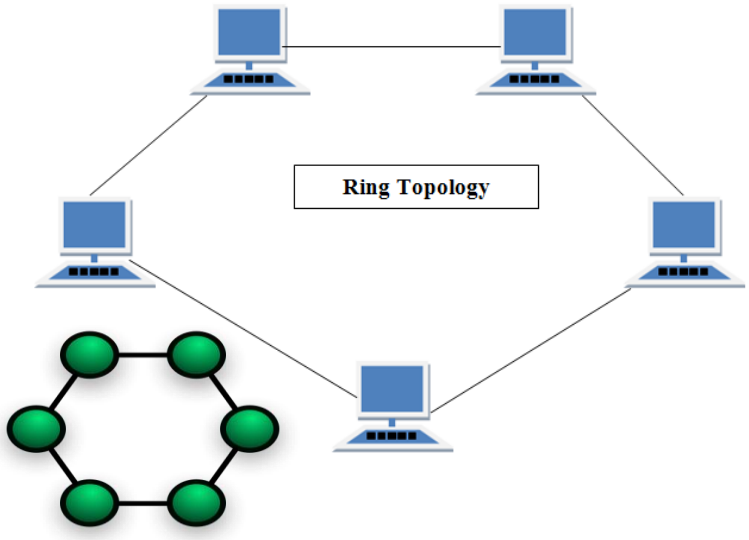


Figure 9: Ring topology & Nodes

Table 6: Advantage & disadvantage of Ring topology

ADVANTAGE	DISADVANTAGE
• Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.	• Failure of one computer disturbs the whole network.
• Cheap to install and expand	• Adding or deleting the computers disturbs the network activity.

Star Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.

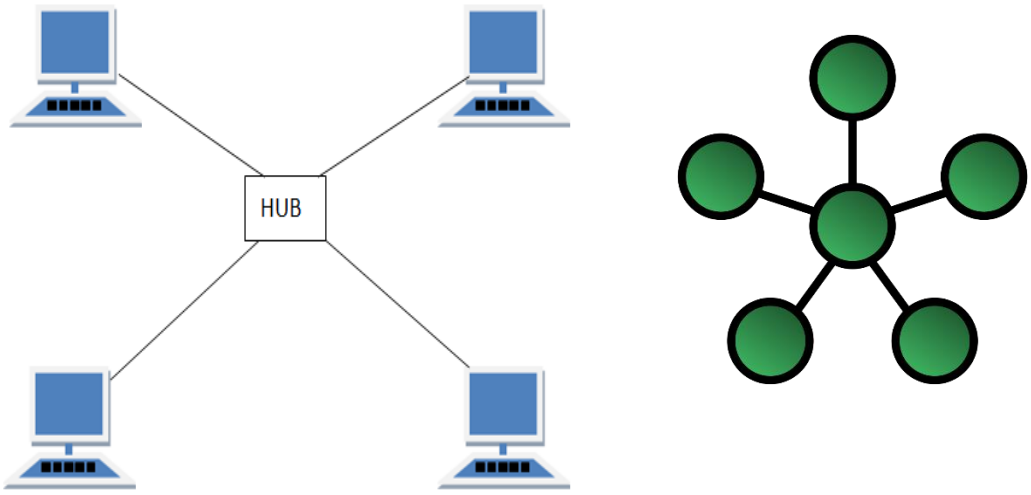


Figure 10: Star topology & nodes

Table 7: Advantage & disadvantage of Star topology

ADVANTAGE	DISADVANTAGE
• Fast performance with few nodes and low network traffic.	• Cost of installation is high.
• Hub can be upgraded easily.	• Expensive to use.

Logical topology in computer network.

The logical topology of a network determines how the hosts communicate across the medium. The two most common types of logical topologies.

1. Broadcast topology
2. Token topology

Broadcast topology

The use of a broadcast topology indicates that each host sends its data to all other hosts on the network medium. There is no order that the stations must follow to use the network.

Token topology

The second logical topology is token passing. In this type of topology, an electronic token is passed sequentially to each host. When a host receives the token, that host can send data on the network. If the host has no data to send, it passes the token to the next host and the process repeats itself. Two examples of networks that use token passing are Token Ring and Fiber Distributed Data Interface (FDDI). A variation of Token Ring and FDDI is Arc net. Arc net is token passing on a bus topology.

Communication and bandwidth requirements.

There is so many ways to **Transmission Modes** the information. from a computer to another computer like human beings. This called as **Communication Mode**.

The method of information transmission mode varies with Directions.

- Simplex Mode
- Half – duplex Mode
- Full – duplex Mode

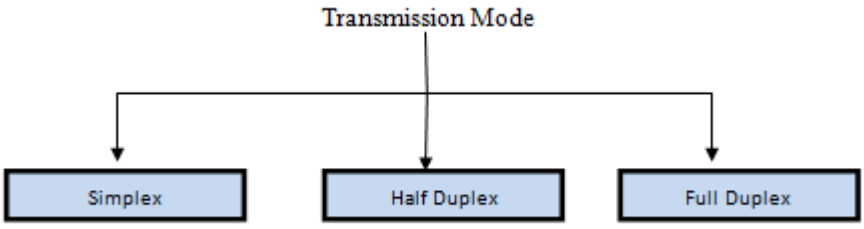


Figure 11: Transmission mode

Simplex mode

In this type of transmission mode, data can be sent only in one direction. communication is unidirectional. We cannot send a message back to the sender.

Examples of simplex Mode are:

- Loudspeakers
- Television broadcasting

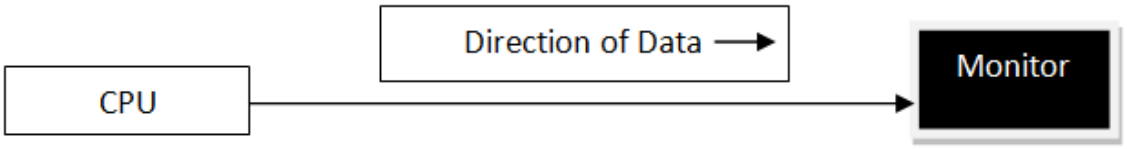


Figure 12: Direction of data in simplex mode

Half duplex mode

Half-duplex data transmission means that data can be transmitted in both directions on a signal carrier, But it only exchanges one message at a time.

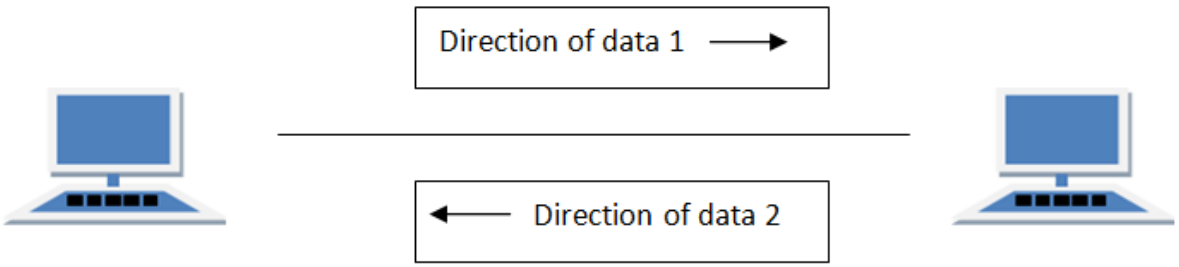


Figure 13: Half duplex mode

Full duplex mode

In full duplex system we can send data in both the directions as it is bidirectional at the same time in other words, data can be sent in both directions simultaneously.

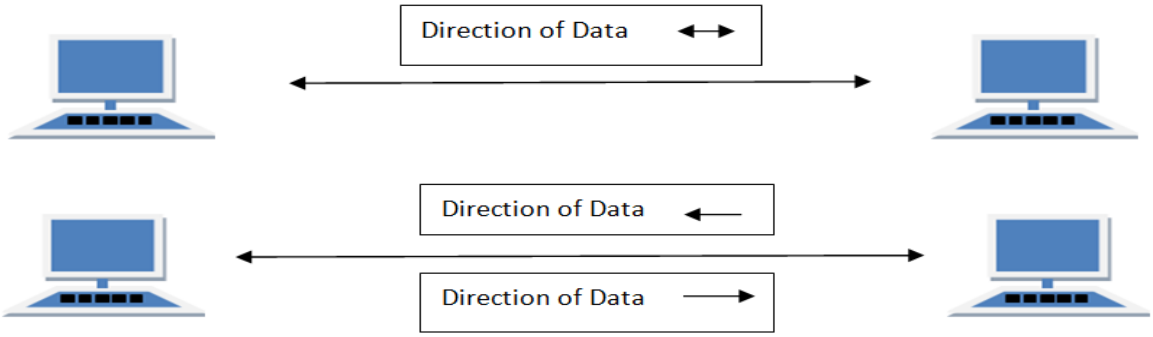


Figure 14: Full duplex mode

Transmission mediums

The way to help to transfer the information is called **Transmission Mediums**.

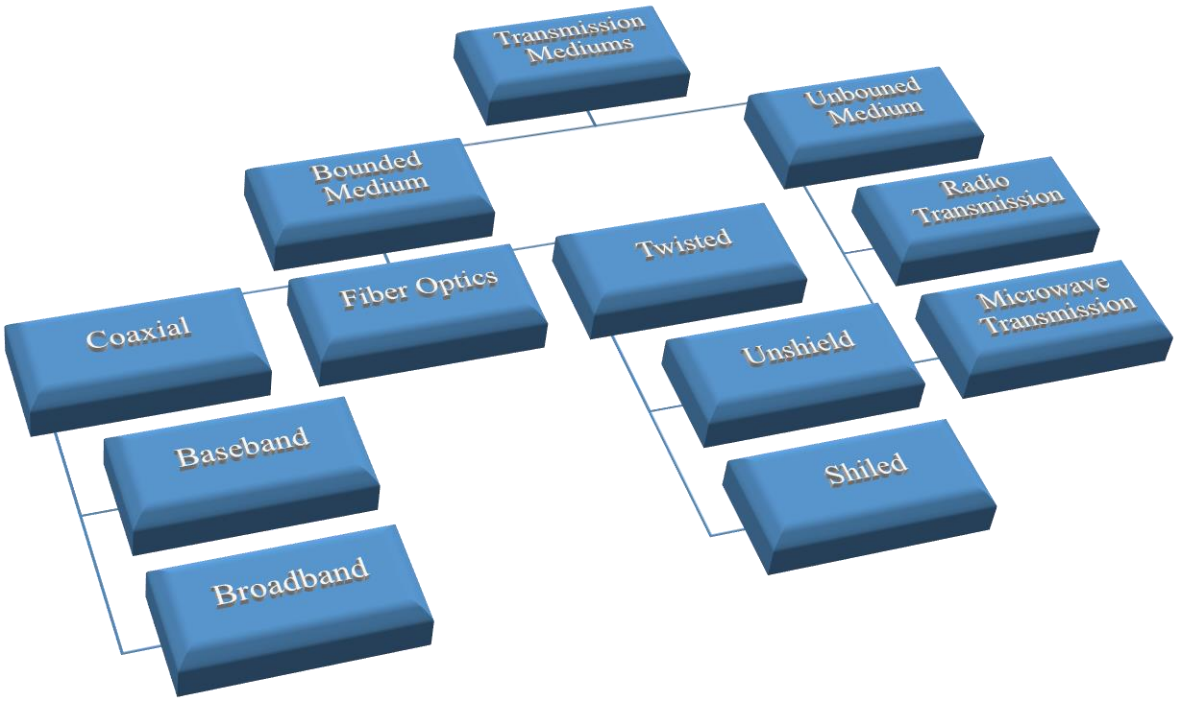


Figure 15: Transmission mediums

Bounded or Guided Transmission Media

Guided media, which are those that provide a conduit from one device to another, include Twisted-Pair Cable, Coaxial Cable, and Fibre-Optic Cable. A signal travelling along any of these media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical Fibre is a cable that accepts and transports signals in the form of light.

Twisted pair Cable

This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network. Some important points:

- Its frequency range is 0 to 3.5 kHz.
- Typical attenuation is 0.2 dB/Km @ 1kHz.
- Typical delay is 50 µs/km.
- Repeater spacing is 2km.

Twisted Pair is of two types:

- Unshielded Twisted Pair (UTP)
- Shielded Twisted Pair (STP)

<u>Unshielded Twisted Pair (UTP)</u>

It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own color plastic insulator. Identification is the reason behind colored plastic insulation.

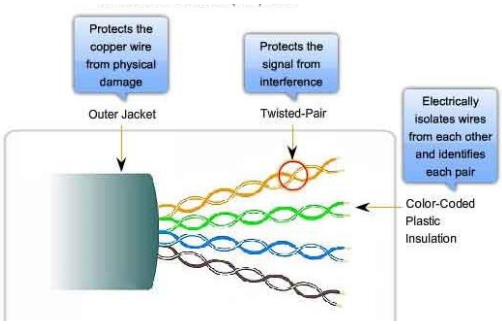


Figure 16: UTP cable

Table 8: Advantage & disadvantage of UTP cable

ADVANTAGE	DISADVANTAGE
• Installation is easy	• Bandwidth is low when compared with Coaxial Cable
• Flexible	• Provides less protection from interference.
• Cheap	
• It has high speed capacity,	
• 100-meter limit	

Shielded Twisted Pair (STP)

Advantages of shielded twisted pair cable

- Easy to install
- Performance is adequate
- Can be used for Analog or Digital transmission
- Increases the signaling rate
- Higher capacity than unshielded twisted pair
- Eliminates crosstalk
- Disadvantages of Shielded Twisted Pair Cable
- Difficult to manufacture
- Heavy

Figure 17: STP cable

Coaxial cable

Coaxial is called by this name because it contains two conductors that are parallel to each other. Copper is used in this as centre conductor which can be a solid wire or a standard one. It is surrounded by PVC installation, a sheath which is encased in an outer conductor of metal foil, braid or both.

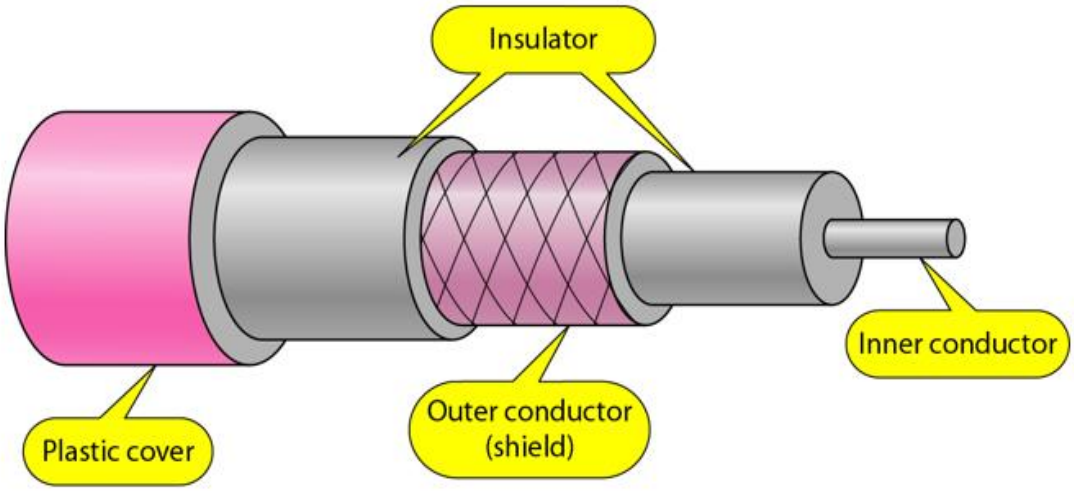


Figure 18: Coaxial cable

Table 9: Coaxial cable standards

Category	Impedance	Use
RG – 59	75 Ω	Cable TV
RG – 58	50 Ω	Thin Ethernet
RG – 11	50 Ω	Thick Ethernet

Coaxial cable connectors

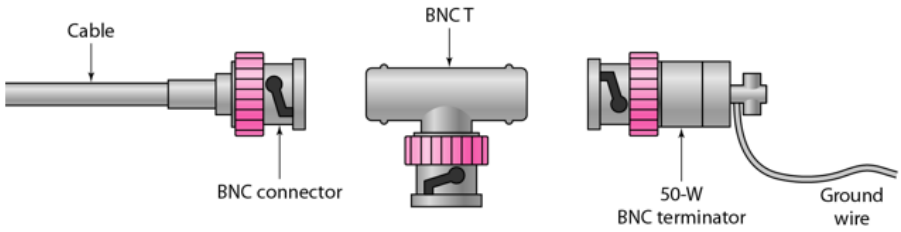


Figure 19: Coaxial cable connecter

Fibre Optic Cable

A Fibre-optic cable is made of glass or plastic and transmits signals in the form of light. For better understanding we first need to explore several aspects of the nature of light. Light travels in a straight line as long as it is mobbing through a single uniform substance. If ray of light travelling through one substance suddenly enters another substance (of a different density), the ray changes direction.

The below figure shows how a ray of light changes direction when going from a denser to a less dense substance.

Internal view of an optical Fibre

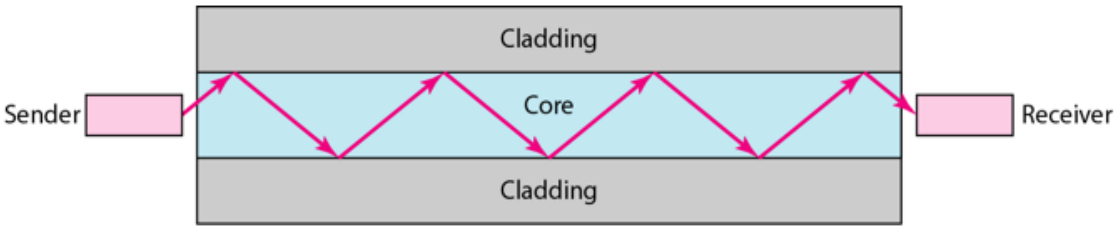


Figure 20: Internal view of fiber optical cable

Fibre sizes for Fibre optic cable

Table 10: Fibre sizes for Fibre optic cable

TYPE	CORE	CLADDING	MODE
50/125	50.0	100	Multi-Mode, Grand Index
62.5/125	62.5	100	Multi-Mode, Grand Index
100/125	100.0	100	Multi-Mode, Grand Index
7/125	7.0	100	Single Mode

Fibre optic cable connectors

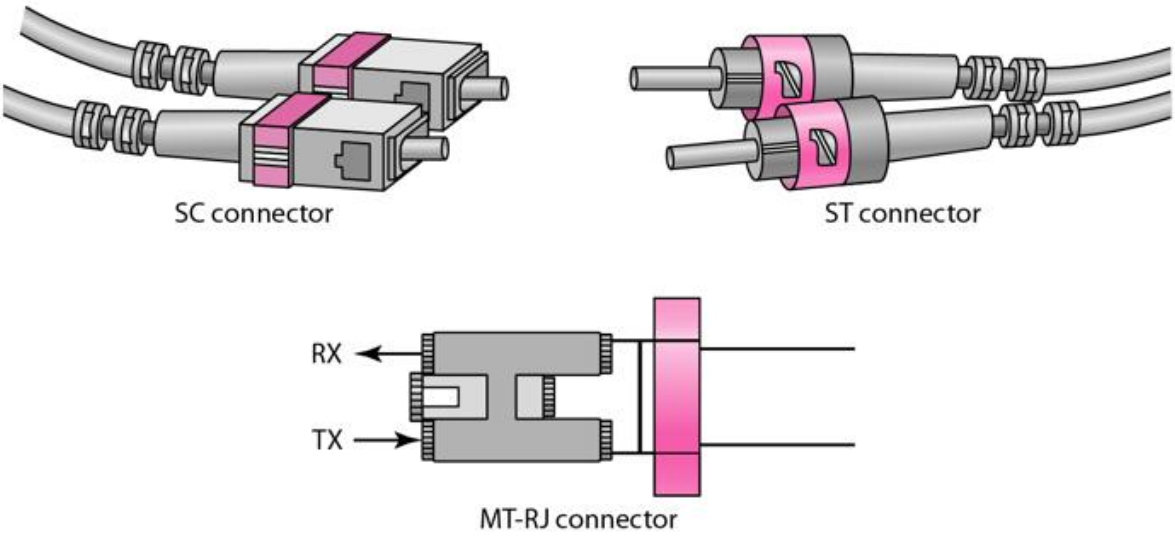


Figure 21: Fiber optic cable connecters

Table 11: Table 15: Advantage & disadvantage of Fibre optic cable

ADVANTAGE	DISADVANTAGE
• Higher bandwidth	• Installation and maintenance
• Less signal attenuation	• Unidirectional light propagation
• Immunity to electromagnetic interference	• High Cost
• Resistance to corrosive materials	• Performance of Fibre Optic Cable
• Light weight	
• Greater immunity to tapping	

Unbounded or unguided transmission media

Unguided medium transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

The below figure shows the part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, used for wireless communication.

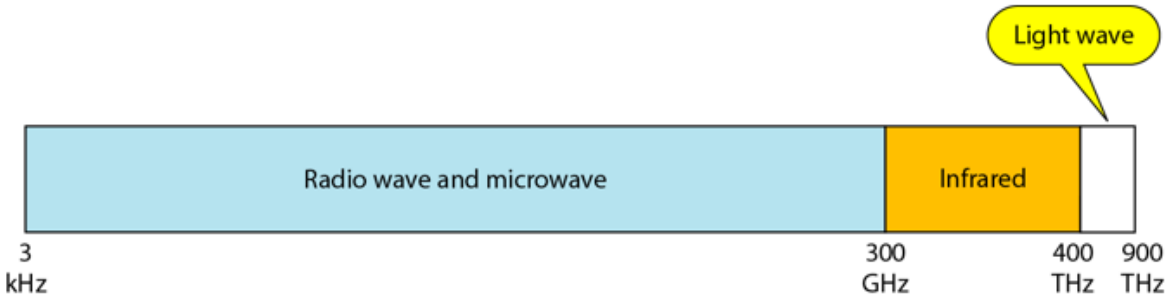


Figure 22: The part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, used for wireless communication.

Unguided signals can travel from the source to the destination in several ways: **Ground propagation, Sky propagation** and **Line-of-sight propagation** as shown in below figure.

Propagation modes

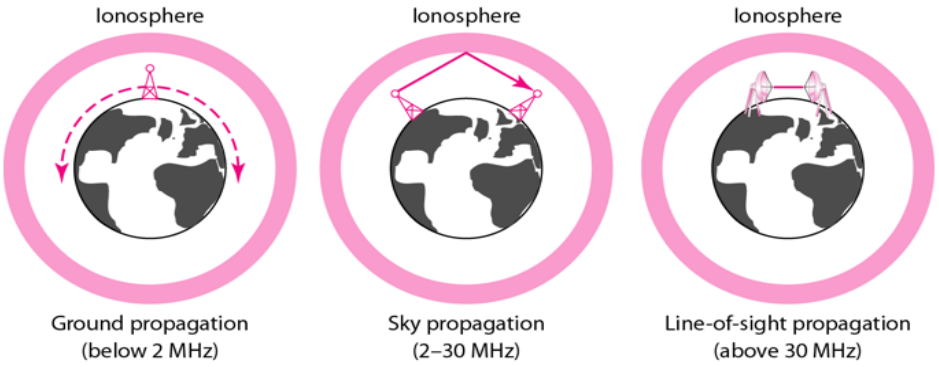


Figure 23: Propagation modes of unbounded transmission medium

We can divide wireless transmission into three broad groups:

1. Radio waves
2. Micro waves
3. Infrared waves

Radio Waves

Electromagnetic waves ranging in frequencies between 3 KHz and 1 GHz are normally called radio waves.

Radio waves are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna send waves that can be received by any receiving antenna. The omnidirectional property has disadvantage, too. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signal suing the same frequency or band.

Figure 24: Omnidirectional antenna for radio waves

Micro Waves

Electromagnetic waves having frequencies between 1 and 300 GHz are called micro waves. Micro waves are unidirectional.

Two types of antennas are used for microwave communications: **Parabolic Dish** and **Horn**.

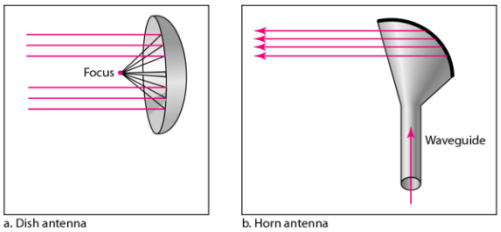


Figure 25: Unidirectional antenna for micro waves

Infrared Waves

Infrared waves, with frequencies from 300 GHz to 400 THz, can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another, a short-range communication system in on room cannot be affected by another system in the next room.

Figure 26: IR Waves

COMMON NETWORK PRINCIPLES.

Government networks form a platform that enables the delivery of digital services. Good network design should create a user experience that the network is transparent, resilient and ubiquitous, with the right balance of quality, speed, security, control and cost.

These principles help designers deliver this experience for their users when designing networks across government. Note that these are principles, not a set of rules that must be arbitrarily followed. Designers can deviate from them where there is good justification.

When we refer to users, we mean government end-users - individuals who consume a service, not those purchasing or provisioning it. The diagram below presents the context for these principles.

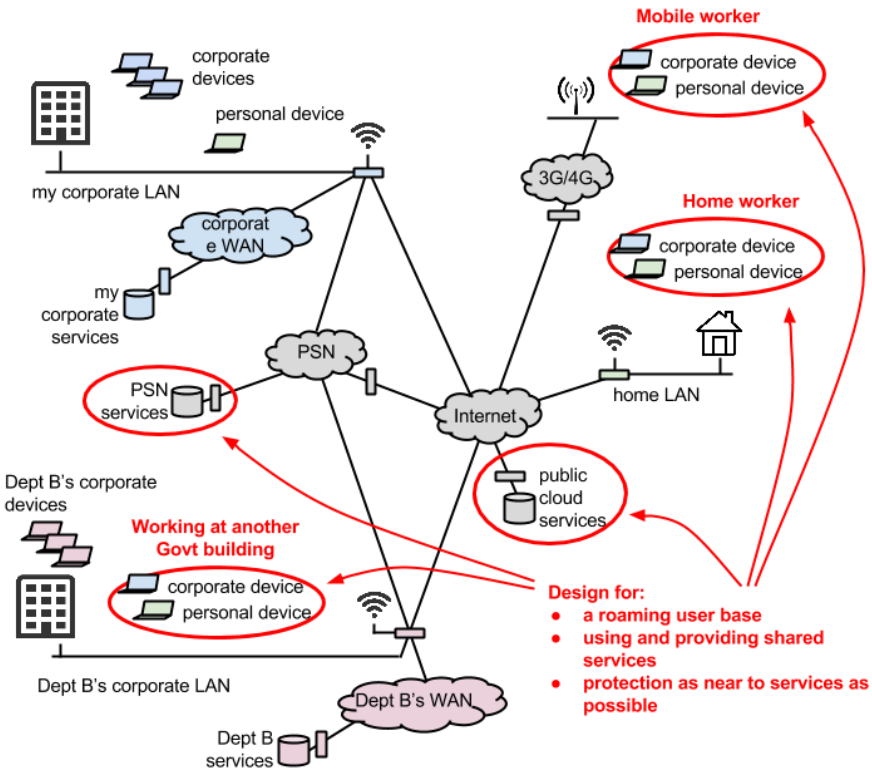


Figure 27: Network principals

Principle 1: Understand the user need

Understand your basic network requirements

Know:

- what business services your users depend on
- what network services they rely on to access them

Document your needs across different networks for:

- bandwidth
- availability
- resilience
- class of service (CoS)
- quality of service (QoS)
- price

Principle 2: Use services to protect your data, don't rely on the network

Know:

- who is managing your networks
- what organizations and jurisdictions have access to your data
- who you are sharing your network with
- whether you have adequate data in transit protection

Principle 3: Design for interworking and flexibility

You should:

- make it easy to change to meet your changing needs
- buy what you need, when you need it
- minimize your own WAN estate - share infrastructure where you can

Publish DNS names

Publish DNS records as widely as possible. This enables the widest range of people find a service and avoids restrictions based on knowledge of its name. Avoid restricting access to DNS records as a security mechanism. Knowledge of a service's domain name or IP address is not the same as being able to access the service.

Network Protocols.

What is a Protocol?

A protocol is a set of rules that governs the communications between computers on a network. In order for two computers to talk to each other, they must be speaking the same language. Many different types of network protocols and standards are required to ensure that your computer (no matter which operating system, network card, or application you are using) can communicate with another computer located on the next desk or half-way around the world. The OSI (Open Systems Interconnection) Reference Model defines seven layers of networking protocols.

There are different protocols on the computer network,

1. HTTP/ HTTPS

   Hyper **T**ext **T**ransfer **P**rotocol / **H**yper **T**ext **T**ransfer **P**rotocol **S**ecured
2. FTP

   File **T**ransfer **P**rotocol
3. SMTP

   Simple **M**ail **T**ransfer **P**rotocol
4. DNS

   Domain **N**ame **S**ystem
5. Telnet
6. TCP

   Transmission **C**ontrol **P**rotocol
7. SPX

   Sequence **P**acket **E**xchange
8. IP

   Internet **P**rotocol
9. IPX

   Internet **P**acket **E**xchange
10. Ethernet

They can be simplified into four layers to help identify some of the protocols with which you should be familiar

Table 12: OSI layers & protocols

OSI Layer	Layer Name	Common Protocols
7	Application Layer	HTTP/HTTPS, FTP, SMTP, DNS, Telnet
6	Presentation Layer	
5	Session Layer	
4	Transport Layer	TCP, SPX
3	Network Layer	IP, IPX
2	Data Link Layer	Ethernet
1	Physical Layer	

Based on these four layers, the media of the Internet helps to communicate

- Ethernet (Physical Layer, Data Link Layer)
- IP, IPX (Network Layer)
- TCP, SPX (Transport Layer)
- HTTP/HTTPS, FTP, SMTP, DNS, Telnet (Application Layer)

Ethernet (Physical/Data Link Layers)

The physical layer of the network focuses on hardware elements, such as cables, repeaters, and network interface cards. By far the most common protocol used at the physical layer is Ethernet. For example, an Ethernet network (such as 10BaseT or 100BaseTX) specifies the type of cables that can be used, the optimal topology (star vs. bus, etc.), the maximum length of cables, etc. (See the Cabling section for more information on Ethernet standards related to the physical layer).

The data link layer of the network addresses the way that data packets are sent from one node to another. Ethernet uses an access method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection). This is a system where each computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit. If some other node is already transmitting on the cable, the computer will wait and try again when the line is clear. Sometimes, two computers attempt to transmit at the same instant.

Table 13: Ethernet Protocol Summary

Protocol	Cable	Speed
Ethernet	Twister Pair, Coaxial & Fibre Optic Cables	10 Mbps
Fast Ethernet	Twister Pair & Fibre Optic Cables	100 Mbps
Gigabit Ethernet	Twister Pair & Fibre Optic Cables	1000 Mbps

IP and IPX (Network Layer)

The network layer is in charge of routing network messages (data) from one computer to another. The common protocols at this layer are IP (which is paired with TCP at the transport layer for Internet network) and IPX (which is paired with SPX at the transport layer for some older Macintosh, Linus, UNIX, Novell and Windows networks). Because of the growth in Internet-based networks, IP/TCP are becoming the leading protocols for most networks.

TCP and SPX (Transport Layer)

The transport layer is concerned with efficient and reliable transportation of the data packets from one network to another. In most cases, a document, e-mail message or other piece of information is not sent as one unit. Instead, it is broken into small data packets,

TCP, paired with IP, is by far the most popular protocol at the transport level. If the IPX protocol is used at the network layer (on networks such as Novell or Microsoft), then it is paired with SPX at the transport layer.

HTTP, FTP, SMTP and DNS (Session/Presentation/Application Layers)

Several protocols overlap the session, presentation, and application layers of networks. There protocols listed below are a few of the more well-known:

- DNS (Domain Name System)
  Translates network address (such as IP addresses) into terms understood by humans (such as Domain Names) and vice-versa
- DHCP (Dynamic Host Configuration Protocol)
  Can automatically assign Internet addresses to computers and user
- FTP (File Transfer Protocol)
  A protocol that is used to transfer and manipulate files on the Internet
- HTTP (Hypertext Transfer Protocol)
  An Internet-based protocol for sending and receiving webpages
- IMAP (Internet Message Access Protocol)
  A protocol for e-mail messages on the Internet
- IRC (Internet Relay Chat)
  A protocol used for Internet chat and other communications
- POP3 (Post Office protocol Version 3)
  A protocol used by e-mail clients to retrieve messages from remote servers
- SMTP (Simple Mail Transfer Protocol)
  A protocol for e-mail messages on the Internet

LO2 EXPLAIN NETWORKING DEVICES AND OPERATIONS

Network Devices

Network devices, or networking hardware, are physical devices that are required for communication and interaction between hardware on a computer network.

Here is the common network device list:

1. Network Interface Card (NIC)
2. Hub
3. Switch
4. Bridge
5. Router
6. Gateway
7. Modem
8. Repeater

Figure 28: Network Device

Network interface card

Network cards also known as Network Interface Cards (NICs) are hardware devices that connect a computer with the network. They are installed on the mother board.

Hub

Hubs connect multiple computer networking devices together. A hub also acts as a repeater in that it amplifies.

Switch

Switches generally have a more intelligent role than hubs. A switch is a multiport device that improves network efficiency. Generally, switches can read the hardware addresses of incoming packets to transmit them to the appropriate destination.

Bridge

Bridges are used to connect two or more hosts or network segments together. The basic role of bridges in network architecture is storing and forwarding frames between the different segments that the bridge connects. They use hardware Media Access Control (MAC) addresses for transferring frames. Bridges can also be used to connect two physical LANs into a larger logical LAN.

Router

Routers help transmit packets to their destinations by charting a path through the sea of interconnected networking devices using different network topologies. Routers are intelligent devices.

Gateway

Gateways normally work at the Transport and Session layers of the OSI model. At the Transport layer and above, there are numerous protocols and standards from different vendors; gateways are used to deal with them. Gateways provide translation between networking technologies such as Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP).

Modem

Modems (modulators-demodulators) are used to transmit digital signals over analog telephone lines. Thus, digital signals are converted by the modem into analog signals of different frequencies and transmitted to a modem at the receiving location. Modems work on both the Physical and Data Link layers.

Repeater

A repeater is an electronic device that amplifies the signal it receives. You can think of repeater as a device which receives a signal and retransmits it at a higher level or higher power so that the signal can cover longer distances, more than 100 meters for standard LAN cables. Repeaters work on the Physical layer.

NETWORK SERVER

A server is a software or hardware device that accepts and responds to requests made over a network. The device that makes the request, and receives a response from the server, is called a client. On the Internet, the term "server" commonly refers to the computer system which receives a request for a web document, and sends the requested information to the client.

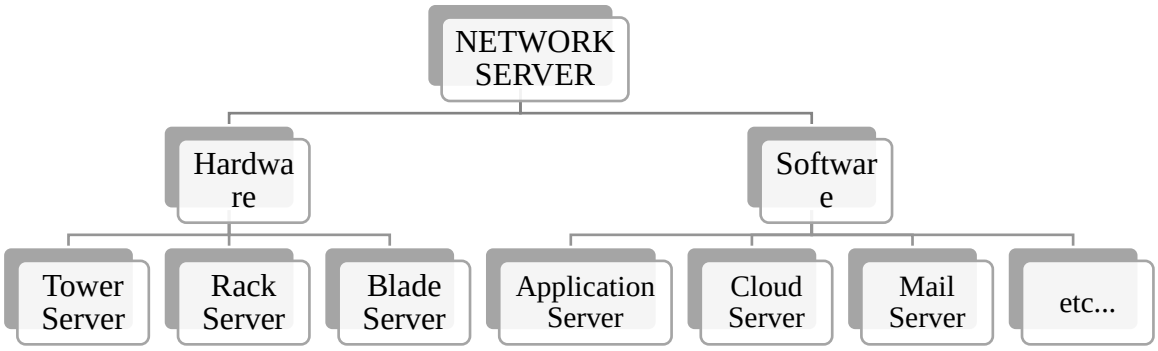


Figure 29: Network server type

Network Server Hardware

1. Tower Server

Figure 30: Tower server

Towers look very similar to desktop PCs. If you are not concerned about space, you can house more drives and more hardware into a single tower. However, if you are looking at future expansion and scalability, space can become a constraint with a tower server.

A tower server is intended for use as a server and is built in an upright standalone cabinet. The cabinet called a tower is similar in dimensions to the cabinet of a tower-style desktop computer.

2. Rack Server

Figure 31: Rack server

Racks are designed to accommodate multiple servers, and are specially constructed to fit into small spaces. They are usually stacked right on top of one other, which makes cooling the devices difficult but is a big plus point when it comes to scalability. Also the stacked model helps in consolidating network resources and minimizing the floor space requirements.

3. Blade Server

Figure 32: Blade server

Although blade servers are similar to rack servers in design, they are thinner, and also cost more than the latter. A blade server is a server chassis which houses multiple thin, modular EC boards, known as server blades. Each blade is actually a server, often dedicated to a single application. The server blades are literally servers on a card that contain processors, memory, integrated network controllers, and other input/output (IO) ports.

Network Server Software

1. Application Server

The application server is a framework, an environment where applications can run, no matter what they are or what functions they perform. An application server can be used to develop and run web-based applications. There are many different types of application servers, including Java, PHP, and .NET Framework application servers.

2. Database Server

A database server is a computer system that provides other computers with services related to accessing and retrieving data from a database. Access to the database server may occur via a "front end" running locally a user's machine (e.g., php My Admin), or "back end" running on the database server itself, accessed by remote shell. After the information in the database is retrieved, it is outputted to the user requesting the data.

3. Application Server

A proxy is a computer server or program that's part of the gateway server or another computer that separates a local network from outside networks. A proxy server will cache all pages accessed through the network allowing users who may want to visit that same page to load it faster and reduce the networks bandwidth. When a page is accessed that is not in the proxy server's cache, the proxy server accesses the page using its own IP address. Then it caches that page and forwards it to the user.

Workstation

A workstation refers to an individual computer, or group of computers, used by a single user to perform work.

If this is how a computer should look to a company. Generally, the system must have good hardware and good software.

It's basically a computer the hardware of this company

- Mother board
- Intel core i3 processor
- Minimum 4GB RAM
- Minimum 1TB Hard disk
- 15-inch Monitor
- and basic relevant hardware’s

It's basically a computer the software of this company

- Operating system
- Office pack
- Player

Network Operating System Software

- Macintosh OS X
- Microsoft Windows Server
- UNIX/Linux

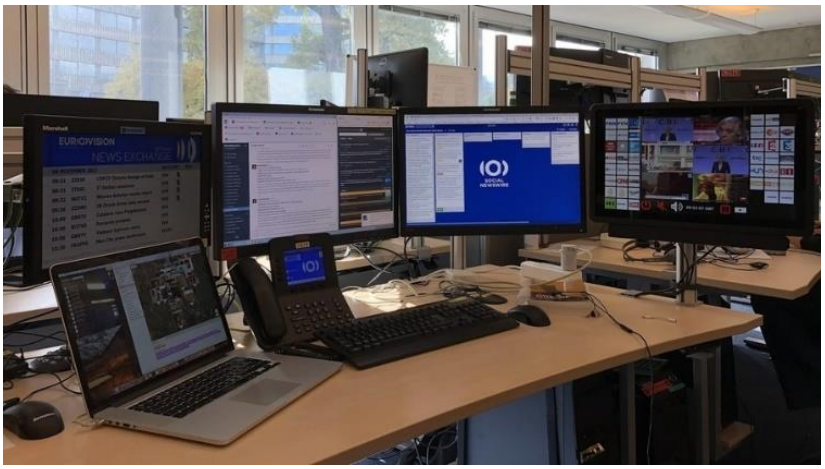


Figure 33: Workstation

Justify the server selection

Generally, the whole companies which are getting services from internet are having the help of servers. Some of the companies buy and operate the servers and some other companies rent and operate the servers. However, the computers which are connected with internet have the help of servers.

As per that, above mentioned XYZ Insurance (pvt) Ltd. is one of the ordinary company since 2015. As I am a Network Engineer, I prefer a suitable network server for this company to bring the company under the control by network.

If are consider the network server hardware, there are three types hardware such as,

1. Tower Server
2. Rack Server
3. Blade Server

We can suggest a suitable network server hardware based on the functions of those hardware's. Accordingly, the complete description of the server hardware is as above

Your company is an ordinary company, there is no more data transfer, every computer in every division head should be observed by. **I prefer that Tower server** is the most suitable server for this ordinary company based on the structure, advantages of disadvantages of this server.

At the same time, Tower server also can be reaped by blade server. But blade server is very costly and most of the company's dos not like to buy and the rent the blade server. As the company is an insurance company, monitoring privacy of each customer is very essential. So that, rent and operate the **blade server is not suitable** for this company.

JUSTIFY THE IDENTIFY THE TOPOLOGY PROTOCOL SELECTION

Generally, the devices in the company must be interconnected. This is because it can be used to communicate with devices using the Network. This will vary depending on the location of the device. Generally, Network engineers have set up many topologies for this.

As per that, above mentioned XYZ Insurance (pvt) Ltd. is one of the ordinary company since 2015. As I am a Network Engineer, I prefer a suitable network topology for this company to bring the company under the control by network.

Although there are many topological systems in common, the topologies suitable for this XYZ Insurance (pvt) Ltd Company.

1. Ring topology
2. Star topology
3. Mesh topology
4. Hybrid Topology

We can suggest a suitable network topology based on the functions of those hardware's. Accordingly, the complete description of the network topology is as above

Other topologies often have many advantages, but they require large amounts of money and area. I recommend Ring Topology as the best topologies for this XYZ Insurance (pvt) Ltd. company based on the above Network topologies.

LO3 DESIGN EFFICIENT NETWORKED SYSTEMS

Step-by-step plan

1. Collect the data according to the user requirements and I arrange some new requirements for the future use
2. Choose the devices, server, and cables for revered equipment for the networking process
3. Select the allocated network area to connect the network using the tree topology system before correct them to assure by drew the system on cisco. Then process it by PC, Switch, Router and configuration
4. After get the feedback from the users and develop them according to their suggestions.

The requirements of Enclave Films is as follows

- Two buildings have organization to be integrated in to a centralized same network. Every user with branch head and all other employees should be given with a separate login with suitable privileges, and client wants high security in system both floors to be equipped with Wi-Fi connections which are limited only to their respective sites.
- The company wants to share some common types of uses an email, a dedicated email server and company needs to manage large amounts of shared documents/file, the file exchange server and also company need to domain server to connect to domain in the network computers. (located in the server room) to share these files

To apprehend these requirements, the consultant will be initiating following procedures

- The networking system will be using the tree topology network designs and all the areas (customer area, general office and managers, reception, accounts, and administration, sever room, workstation area) will be assigned to VLANs of each area. The LAN will abide the IEEE Standards of 802. Local area networking technologies, and also will abide the protocols and rules of OSI reference modeling standards, as well as the TCP/ IP Standard protocols.
- A Server based Anti-virus solution will be provided for all the users for security and a Software firewall will be executed to limit both the internal and the external

threats. A domain server will be planted and the network will design as in the client-server type, providing significant user privileges to certain users of the domain.

- FTP Server, DHCP server and a Backup Server and Mail Server will be assigned to the company.
- Dynamic IP Addresses will be assigned to each required user pool, using the router DHCP Pool Service

Justify the security requirements and quality of services needed for selection of accessories

A Server based Anti-virus solution will be provided for all the users for security and a Software firewall will be executed to limit both the internal and the external threats. A domain server will be planted and the network will design as in the client-server type, every user with branch head and all other employees should be providing significant user privileges to certain users of the domain and client wants high security in system. As companies increase their security requirements and integrated service needs, more intelligent office solutions are required. The Cisco 1841 router provides the opportunity to integrate the functions of separate devices into a single, small, manageable solution remotely. By given that integrated services, as well as high standard density and high performance, the Cisco 1841 delivers security, versatility, scalability and flexibility for multiple SME and SMB applications and a premium customer service supplier.

The Cisco 1841 router easily provide somewhere to set a wide range of network applications, such as secure access to office data, including NAC for virus security, VPN, enterprise-class DSL, IPS support, firewall protection, VLAN routing and serial device focus . The Cisco 1841 router provides customers with the industry's most flexible, secure and adaptable infrastructure to meet business requirements for maximum protection. Allows businesses to securely and transparently extend their networks to any Internet-enabled location using SSL VPN; the Cisco IOS Web VPN supports clientless access to applications such as HTML-based intranet content, e-mail, network file shares, and Citrix and to the

Cisco SSL VPN Client, enabling full network access remotely to virtually any application Hardware-based encryption acceleration downloads encryption to provide improved performance for IP Sec 3DES and AES. With optional VPN integration, NAC Anti-Virus, Cisco IOS-based firewall and IPS support, Cisco offers a robust, scalable and robust

security solution for small and medium-sized businesses and small businesses. High-Performance Processor Supports concurrent deployment of high-performance, secure data services with headroom for future applications Modular Architecture Offers wide variety of LAN and WAN options; network interfaces are field-upgradable to accommodate future technologies Provides many types of slots to add connectivity and services in the future on basis Supports more than 30 modules and interface cards, including existing WAN (WIC) and multiplex (VWIC) interface cards (for data support only on the Cisco 1841 router) and advanced integration modules (AIMs) Most current WIC cards, multiple floppy cards (data only), and advanced integration units (AIM) are compatible with Cisco 1841.

Software Security Implementations

- Threats to the safety and security of any business network come in all shapes and sizes. Strong network security is imperative for any business, as our entire economic infrastructure becomes a more intrinsic part of the Internet and global communications.
- Any company's private, internal network can fall prey to viruses, Trojan Horses, brute force attacks, malware, botnets, Distributed Denial of Service attacks and other malicious software at any time without the right protection.

This quick guide will give you an idea of what you need to protect and secure your business network as well as how to choose the right software to accomplish it.

- Firewalls and Security
- Deploying SSL
- Single Sign-On Options

Firewalls and Security

A firewall can be a valuable component in an overall security strategy. However, firewalls alone do not create security. Firewalls typically provide the first line of defence, intelligently routing requests and filtering out those that do not meet requirements configured into the device (or software). Depending on the sophistication of the firewall product, more or less intelligence can be built into the decision tree affecting whether a packet should pass through the firewall. Having a firewall in place can provide a false sense of security.

Install & configure network services and applications of your choice.

Install and configuration Domain Server

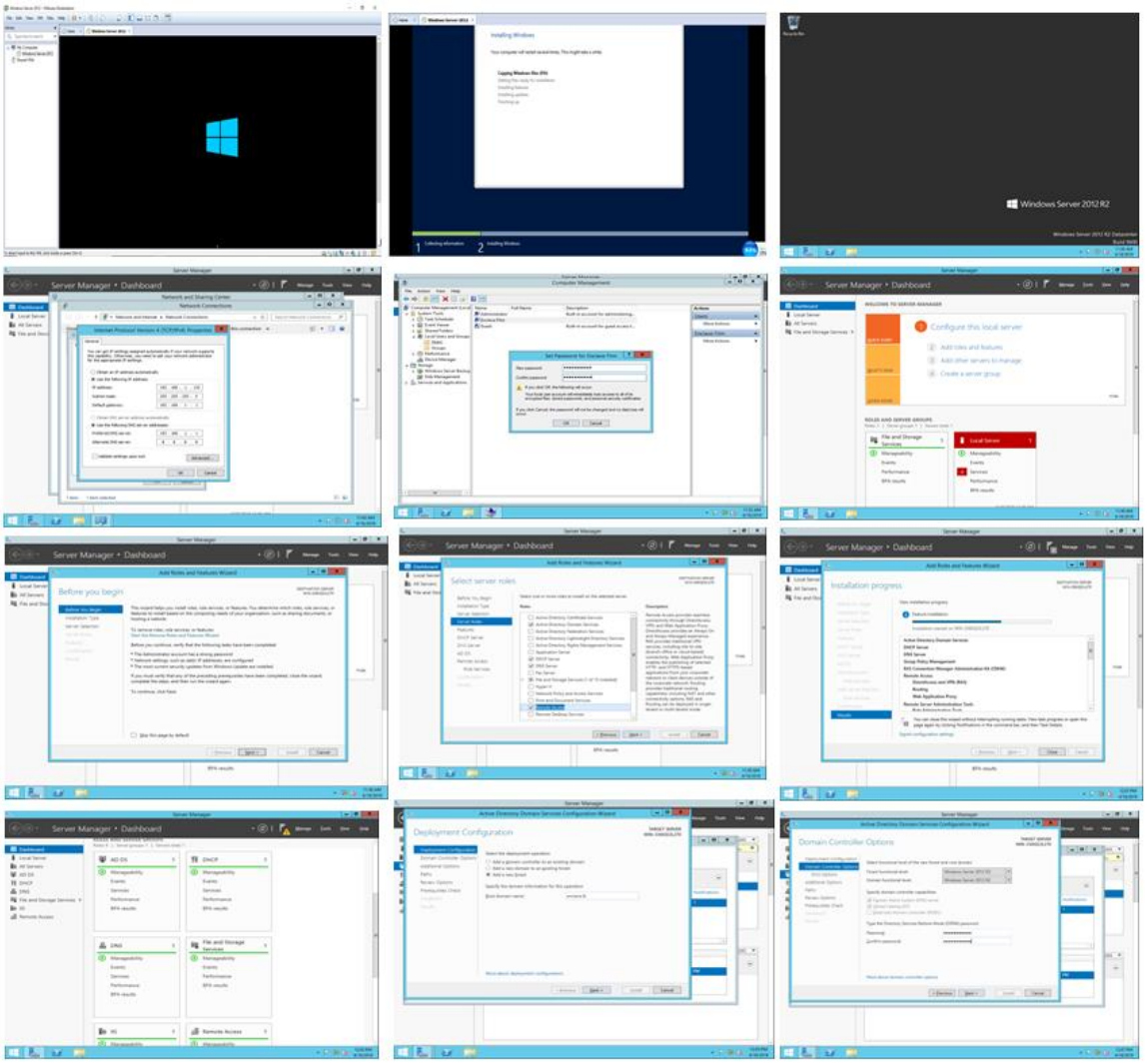


Figure 34:Install and configuration Domain Server

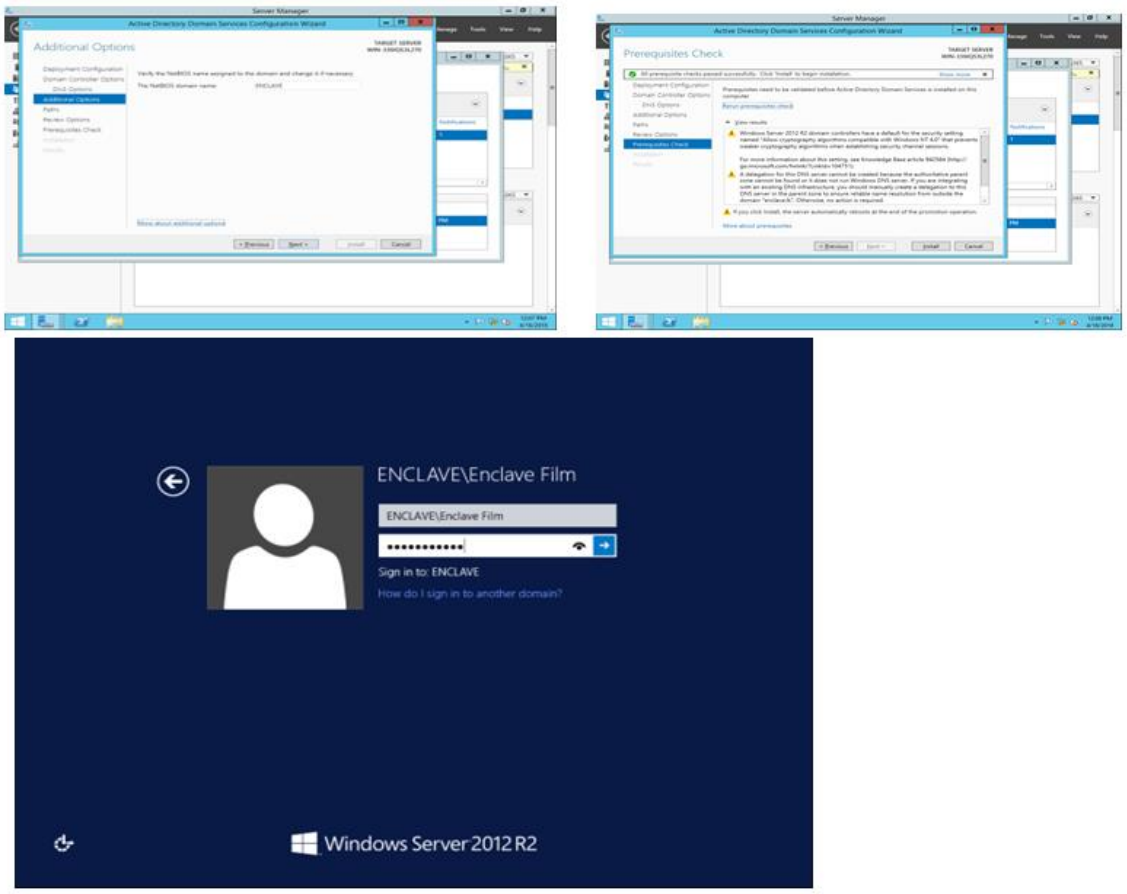


Figure 35: Install and configuration Domain Server

Install Application Software

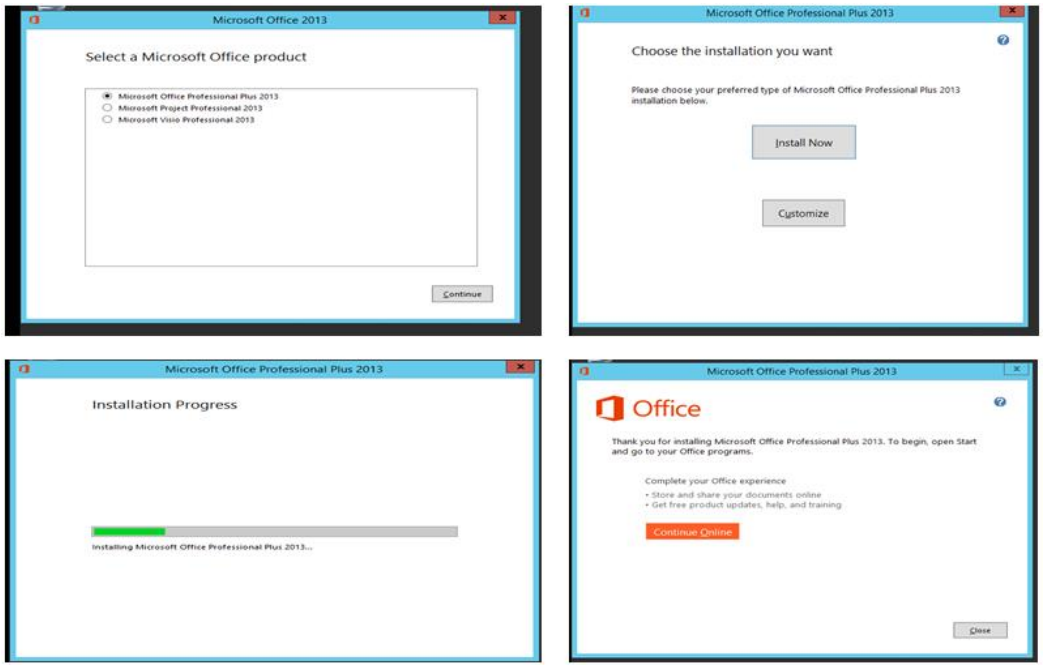


Figure 36: Install Application Software

Conduct a test and evaluate the design to meet the requirements and analyses user feedback

Google form

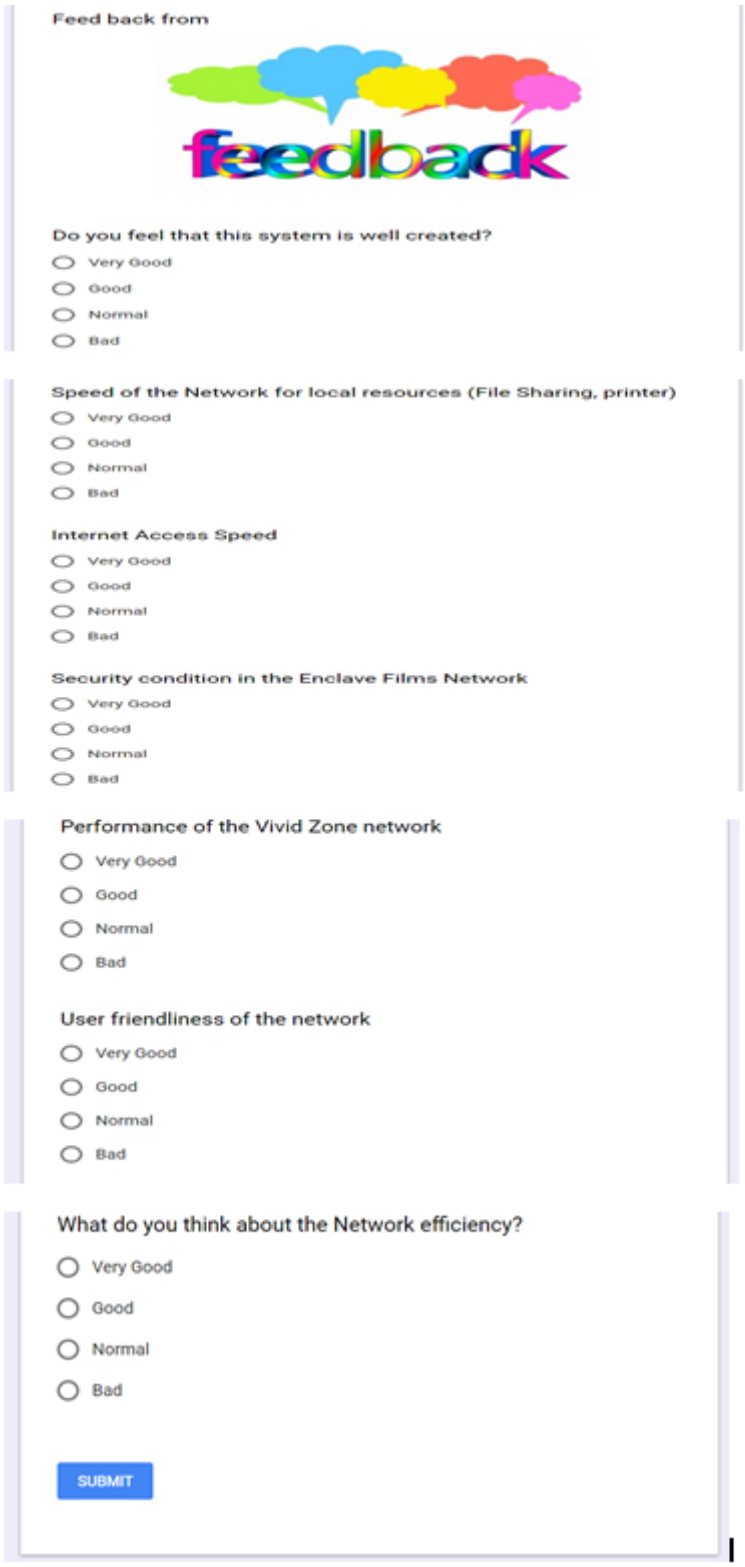


Figure 37: Google form

This from is analysis the Network system, The form is web-based and can be shared with respondents by sending a link, emailing a message, or embedding it into a web page post. User will use the Network system then answers the feedback form questions

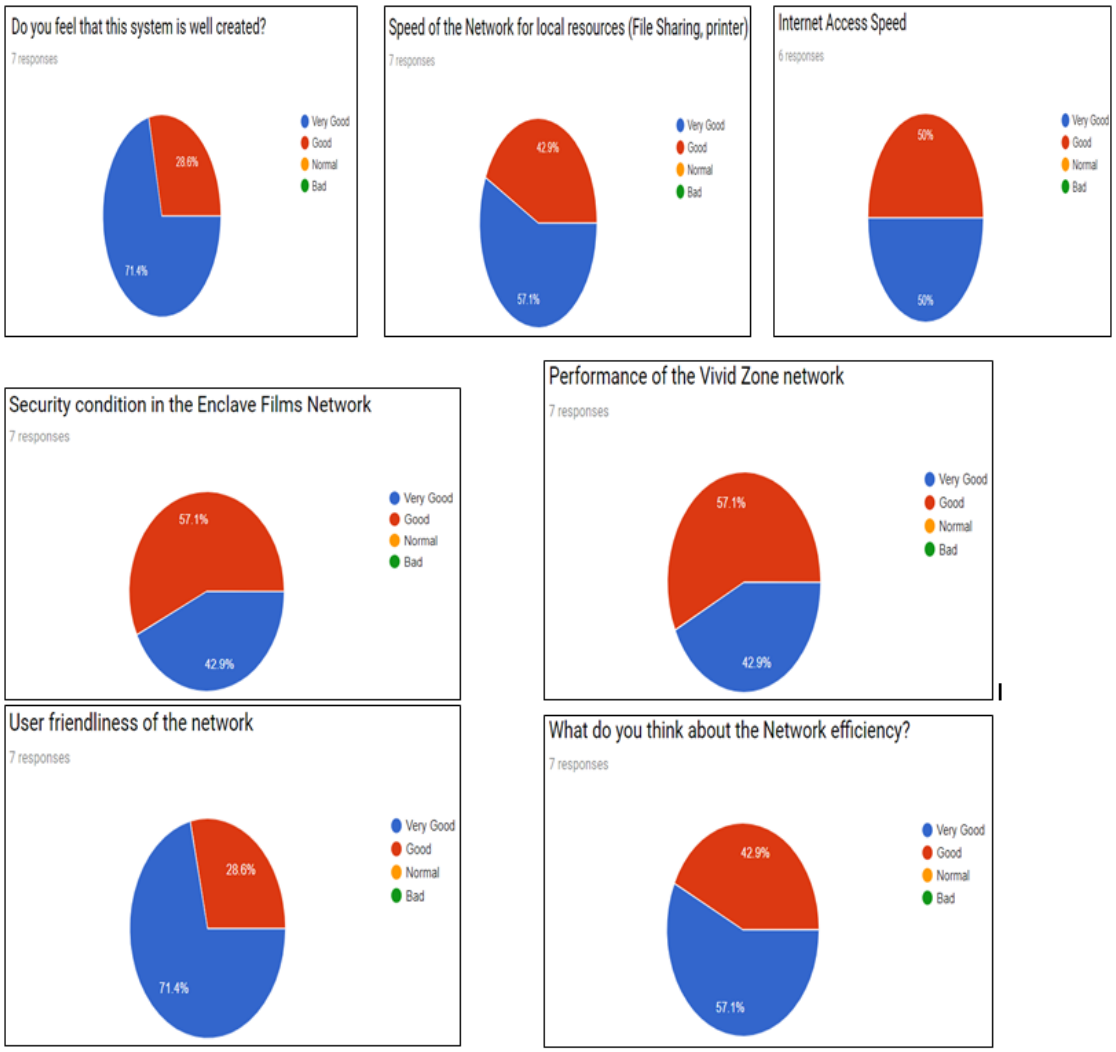


Figure 38: Feedback summery

Around the feedback summery is most customers are satisfied with the network systems provided by the consultant. Some problems with network management and I developed security, Internet access speed in the Enclave Films Network system

Suggest a maintenance schedule to support the networked system.

Computer system for Enclave film Company is the base Information, company ids, documents, important certificates, communications and what not is done on computers. The entire company depends upon the IT department to maintain the systems of the company. Everyone screams at them when they don't. Here's some ways to keep your computer running smoothly into its old age. Will keep your computer from ever having problems, it will at least help prevent them, and make recovery easier when they do occur.

1. **Back up your data**
2. **Clean dust from your computer.**
3. **Organize your installation disks**
4. **Run antivirus and spyware scans regularly.**
5. **Clean up your software.**
6. **Update everything**

Maintenance Schedule

Table 14: Maintenance Schedule

ENCLAVE FILM COMPANY NETWORK				
Services Affected	Occurrence	Start	Duration	Impact to Business
Backup Schedules				
Active Directory	Twice a week	06:00am	3 hours	No Impact in daily activities
Email Server	Once a week	10:00am	30 minutes	No Impact to Business
Database Server	Twice a week	06:00am	3 hours	No Impact to Business
File Server	Once a week	2:00am	4 hours	No Impact to Business

Log Server Review				
Server Access Logs	Monthly	9:00am	30 minutes	No Impact in daily activities
Data Base Transaction Logs	Monthly	10:00am	1 hours	No Impact in daily activities
Firewall Logs	Monthly	11.00am	1 hours	No Impact in daily activities
Update/Testing				
Windows Server Updates	Weekly	10.00PM	3 hours	All Windows servers will need to be restarted after update. This means servers will be down throughout the for 5-10 minutes
Windows Desktop clients Updates	Weekly	11.00PM	1 hour	All Windows desktop clients will need to be restarted after update. This means client computers be down throughout for 5-10 minutes
DNS Server Updates	Monthly	06:00AM	30 minutes	IP addresses will not be mapped while the DNS server is being updated.
Virus Protection Software Updates	Twice a week	06:00AM	1 hour	Individual desktops may run slower while virus update is being performed on it.
Deployment Schedules				
Hardware Deployments	Scheduled/ On Demand	Scheduled/ On Demand	Unknown	Hardware upgrades will take the system being updated down for the time of the upgrade.
server roles	Scheduled/ On Demand	Scheduled/ On Demand	Unknown	Some servers roles need to restart sever. It means server will down for 5-10 minutes

LO4 IMPLEMENT AND DIAGNOSE NETWORKED SYSTEMS

Configuration of Switch Building

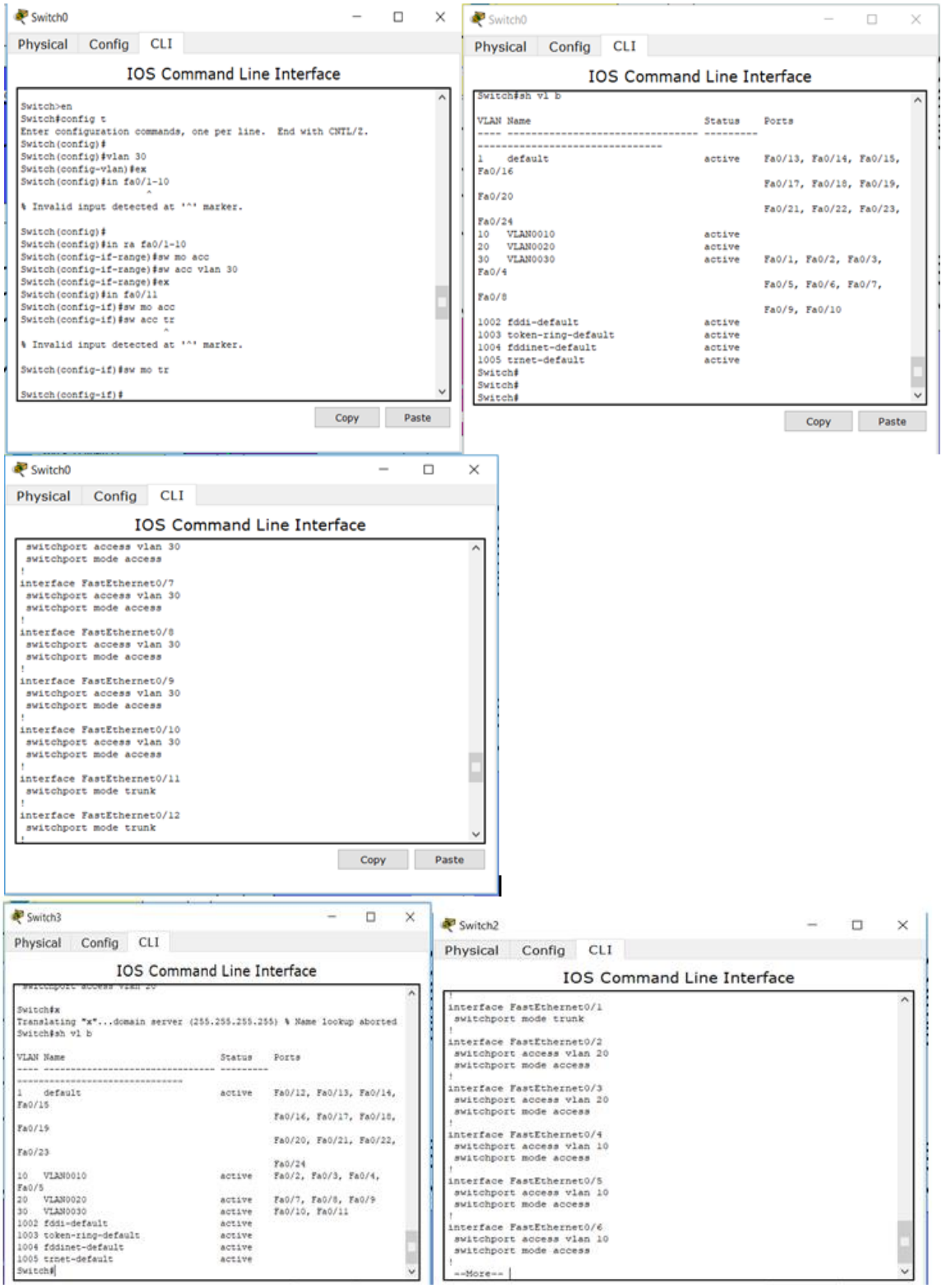


Figure 39: Configuration of Switch Floor 1,2,3

Configuration of Router

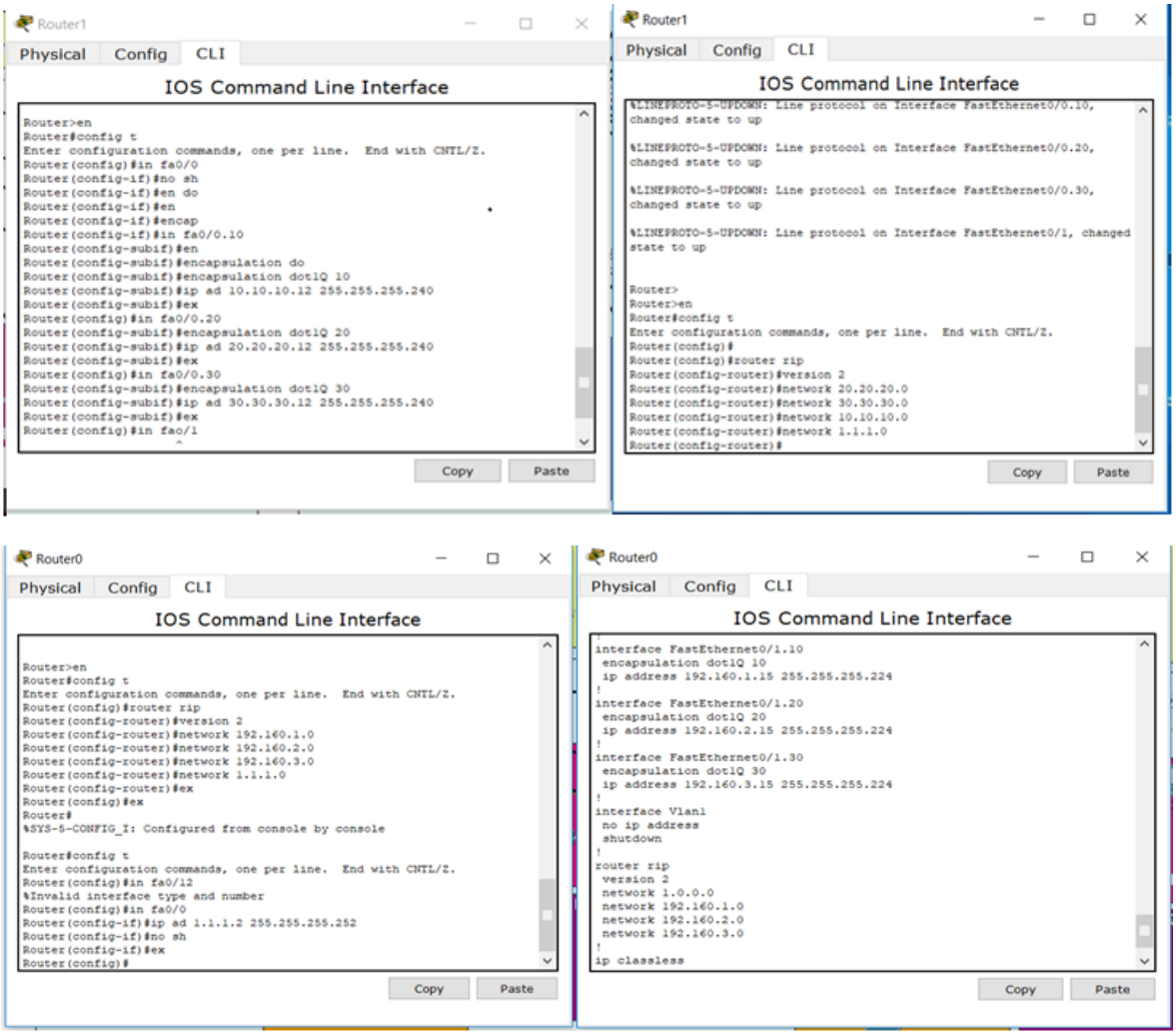


Figure 40: Configuration of Router Floor 1,2,3

Configuration of Wireless Router

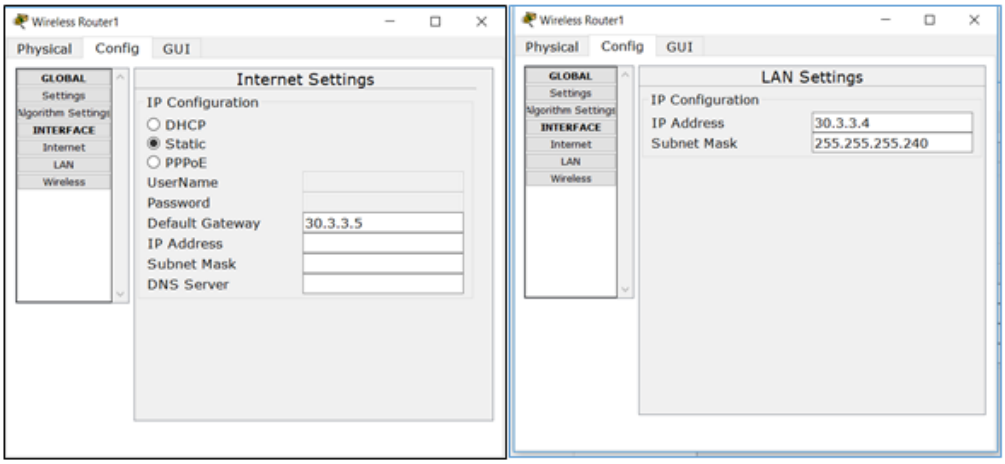


Figure 41: Configuration of Wireless Router

Configuration of laptop, tablet, PC, Printer

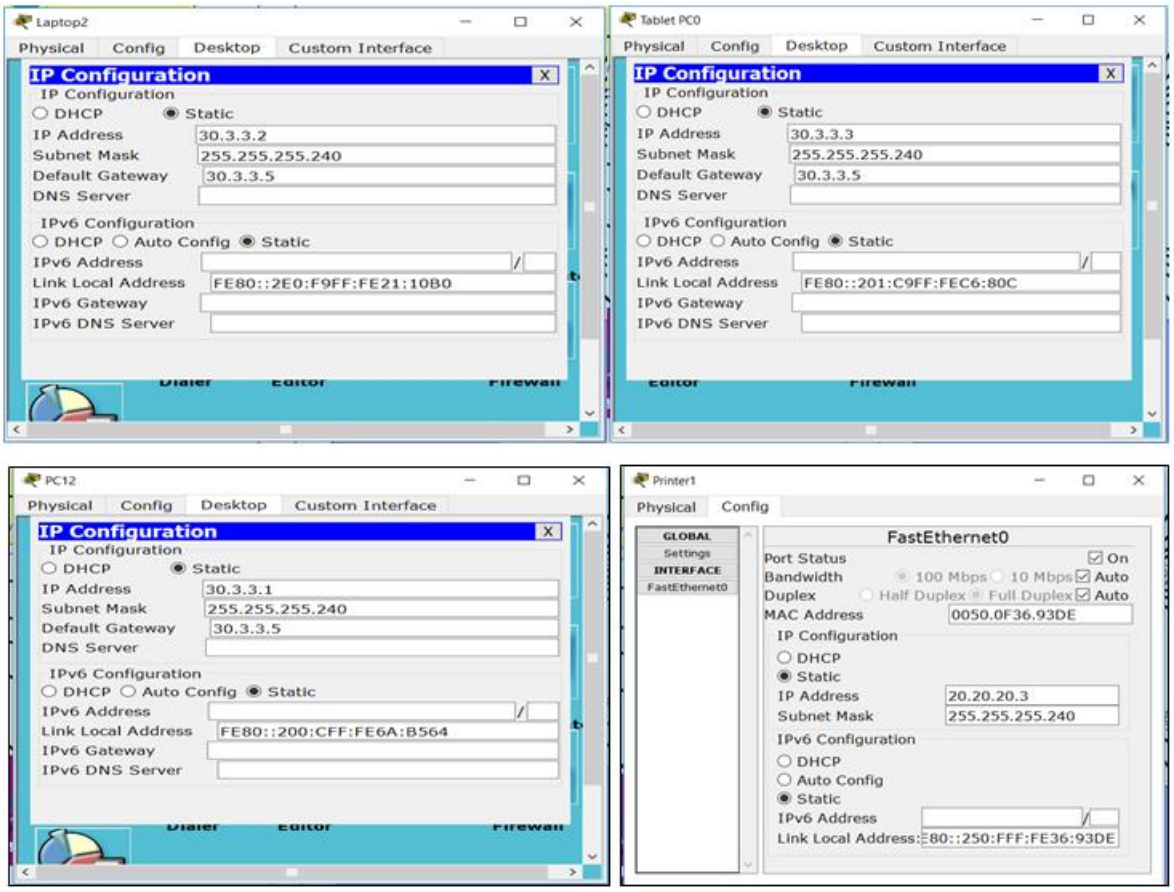


Figure 42: Configuration of laptop, tablet, PC, Printer

Configuration of Server

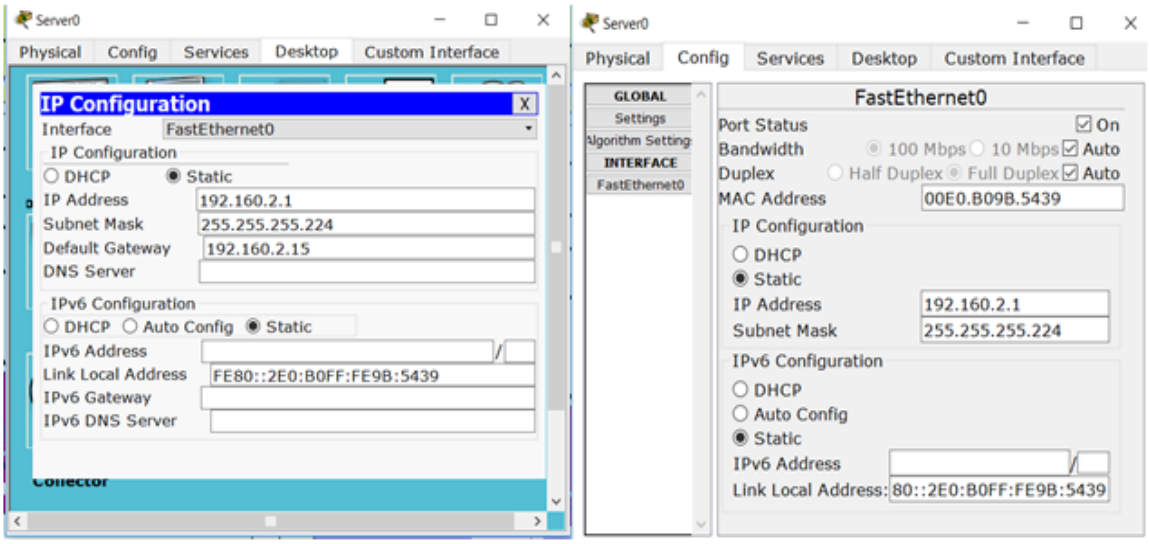


Figure 43: Configuration of Server

Addition of communication devices and network growth

Enclave Film is necessary to update the network reliability, sustainability, availability and scalability of the proposed system. Be able to support device growth, able to support addition of communication devices, able to cope with bandwidth use and trend changes, protocol utilisation, addressing Selection of components: supporting infrastructure needs; supporting connectivity requirements. To improve network quality, the author requirements budding expenditures for this network after six month of implementation. The present network cables are CAT6 Ethernet cable, which will not be necessary for future network. So the author powerfully points to the transition to fiber optic cables, which will maintenance the large bandwidth size

Be able to implement and support networked systems

Devices: installation of communication devices, allocation of addresses, local client configuration, server configuration, server installation

Connectivity: installation of internet work communication medium

Testing: communication; bandwidth

User access: bandwidth, applications, devices

Policy review: bandwidth, resource availability

System monitoring: utilization, bandwidth needs, monitoring user productivity

Maintenance schedule: backups, upgrades, security, auditing

Evaluate work and justify valid conclusions

My network is simple and secure, the devices which I used have suitable for their aspects and essay to handle and control.my system is credibility and safety. I built this system using my whole ideas. I faced some obstacles in some situation. I get the help from my lecturer to solve that problem explained to me during the feedback period, then I thought about the idea of each task style separately, and the whole thing went easily.

I build this system suitable for the Enclave Films Company. I used 2 Router for this system and 5switch also all devices are connected with Vlan and set different IP address according of them. I used network operating systems, different types of connected clients with the server, Created Domain and Child domain, network maintenance plan etc.

I have get the basic server, router and network infrastructure knowledge, I've learn how to draw a Network Diagram (Cisco package) while doing this assignment. I feel it would be better next network system I had used less time to create and develop the network, because I used this system is full and full dependent in my own ideas so I have good expedients in this session.

Requirement of devices, Justification and Improvements to LAN

CAT 6e UTP Patch 10 Meter Network Cable, Ethernet Cable, LAN Cable in RJ45 Connector: https://mmsrilanka.com/cat-6e-network-10m-cable_with_1250.00 proximity 1250.00LKR per 10 meters.

First floor networking devices;
16 port level 3 switch: Edimax 16-Port Fast Ethernet Rack-Mount Switch ES-1016 at proximity LKR 10.250.00, which may be bought at https://mmsrilanka.com/edimax-16-port-switch?search=switch

Reason: 16 port switches is employed because 9 of the ports are used and just in case the amount of clients within the 1st floor increases, the switch doesn't need to get replaced . A level 3 manageable switch thanks to necessity of connecting switches in between and for VLAN configuration.

In the 1st floor, the marketing department is configured to possess a VLAN. The outline states that 10 employees add the marketing division, so as to chop down cost and save time I propose that the batch of 10 is split into 2 and that they add shifts on the computers.

There are 2 networked clients on the reception area so as for the receptionists; a printer has been placed alongside them just in case they have to print invoices, documents, bills etc.

The customer interview area has been purposely decentralized as this area may be a probable area from which threats to the safety of the network can arise from. A home ADSL router has been placed to ensure WiFi.

The wifi router is suggested to be bought from your chosen ISP.

I propose using SLT thanks to their smart plans and high-speed internet. They also provide 5G routers alongside the subscription to their servers.

The GM room has an IP phone hook up with the network just in case the GM has calls with international lines, this might help hamper costs and a probable improvement is implementing IP phones within the calling centres also.

IP phones are often bought alongside services from 3CX at http://fennix.lk/3cx/ a Sri Lankan 3CX provider.

The computer placed within the GM room is additionally networked.

10 Advantages of 3CX Phone System

- Software based: Easy to install & manage
- Inexpensive to buy and expand
- Work from anywhere with iOS & Android clients
- Leverage existing IT infrastructure & Server hardware
- Save on your phone bill with SIP Trunks & Mobile / Remote clients
- Integrated video conferencing using WebRTC
- Better customer service with advanced call queues
- Integrate with CRM & Accounting software
- Standards based – use popular IP Phones, SIP Trunks
- Personal Click2Meet URL

Second floor networking devices;

3x 48 port level 3 rack mountable switches-TP-Link 48-Port 10/100Mbps Rackmount Switch- TL-SF1048 at proximity 28,950.00 LKR per each.

A total of 144 ports are going to be available out of which 121 ports are going to be used, the surplus ports are for the probability of upgradability within the future. there's a complete requirement of a particular 120 clients so this switch is that the idea, it fires at 10~100Mbps and is rack mountable which allows for better usability which you'll patronize https://mmsrilanka.com/. This switch is suggested for little to medium scaled business in Sri Lanka.

The accounting department has been decentralized as requested and contains 3 laptops for every employee networked separately by a 4 port Ethernet hub for any necessity of communication between the laptops. The accounting department has been equipped with laptops in order that locational flexibility is ensured.

Netgear EN104TP 4-Port 10 Mbps Ethernet Hub RJ-45 with Uplink Button are often bought at https://www.amazon.com/Netgear-EN104TP-4-Port-Ethernet Uplink/dp/B00000J4M9 for 14,850 LKR. A possible improvement is that the accounting department is centralized and connected to at least one of the 48 port level 3 switches but be assigned to a VLAN of its own, for extra security purposes, surfing the web are often restricted, activity are often monitored, antimalkware and virus guards like MalwareBytes or AVG are often installed and sensitive information are often rigorously encrypted using AES 256 bit in GCM mode, with a 24 character alphanumeric key that's auto generated.

The video conferencing room has been only equipped with 1 client because the outline doesn't state the precise goal of this room and what functions it performs aside from the apparent video conferencing, this installation is however vague so I propose disconnecting this client from the network if there's no necessity for video conferencing to possess any relationship with the network. For video conferencing across countries, I personally recommend Skype thanks to their backing by Microsoft and their top quality .

Third floor networking devices;

2x 48 port level 3 rack mountable switches-TP-Link 48-Port 10/100Mbps Rackmount Switch- TL-SF1048 at proximity 28,950.00 LKR per each.

Out of the 96 ports available 81 will be used. As per the afore mentioned benefits of using this switch, a particular advantage arises from using this same switch in the 3rd floor as well, as companies allocate discounts when you buy these switches in bulk also if an error occurs be it physical or virtually it will be very easy to troubleshoot.

Server: PowerEdge T630 Server with Intel Xeon E5-2620 v4 2.1GHz and 16GB RDIMM, 2400MT/s, Dual Rank RAM, the server comes with 600GB but I suggest installing additional HDDs or buying a cloud storage from Azure(which has distributors in Sri Lanka). This server can be bought at NEAT technology, call them at +94 115 565 000 and reserve this server at proximity 650,560.00 LKR with 3 years warranty period. It is extremely powerful and can withstand any and all demands in the company. I recommend buying the same server for the Kandy branch as well.

For hardware firewall solutions, I recommend contacting techgates at +94 115 565 500 and arranging for a firewall service, they provide hardware firewalls from KerioControl based in the European region and is one of the most affordable firewalls in Sri Lanka. This service comes with full navigation, control, restriction, user based access control and traffic sharping technologies. They offer deployment in software or hardware level, but as XYZ is an insurance company, it is recommended to have a hardware firewall.

A possible improvement is replacing the firewall with a router that has an integrated firewall with it, this is the ideal solution for high-end networks. The management can discuss and go for a router like this, I could recommend the Cisco 3000 firewall+vpn+routing capability.

For the routers placed in the 3rd floor plan, the logical implementation somewhat ideally shows that it is arranged in an IPsec structure between the Colombo and kandy branch. Arrange for an IPsec service from your ISP and they will provide your Colombo branch and kandy branch 2 routers, the router placed in the middle is not a company router, it is owned by the ISP.

The firewall has been placed after the router and before the server so that any and all traffic to the server is strictly monitored and identified. I suggest using WireShark, which is a packet sniffer that can help analyze all the packets that enter and leave the server. This can be proven to a solid way of monitoring the security of the server.

The server however must be installed with Windows Server 2012, by Microsoft and equipped with the business plan of MalwareBytes to scan for malware, spyware and rootkits regularly.

CONCLUSION

We were assigned by our lecturer to network a corporation.

The lecturer did many helps to conduct this. We encountered the way to network a corporation and therefore the problems that occur. We learned what a network is and the way important it's to Network for a corporation.

We also learned the way to connect computers in Cisco to a network and the way information is transferred. This helped us to know the necessity for Network with the knowledge of our Network. The lecturer encouraged us to seek out many new things on the web for self-serving. This helped us to figure better.

SELF REFLEX

Table 15: Self-reflex

Strength	Weaknesses
Communicate for all members	Speaking English
Problem Solver	Long term planning
Positive thinking	I can’t do anything on work pressure
Smart Working skill	Time management
Self-confidence	
Dedication	

GANTT CHART

TASK	ASSIGNED TO	PROGRESS	START	END
LO 01		100%	3/16/20	4/4/20
LO 02		100%	4/5/20	5/5/20
LO 03		100%	5/6/20	5/31/20
LO 04		100%	6/1/20	6/21/20

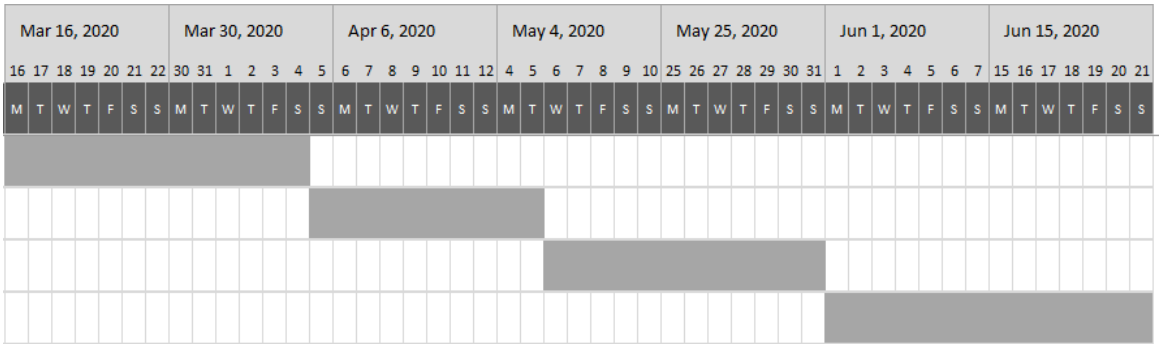


Figure 44: Gantt Chart

REFERENCES

Elizabeth, P. Lauren, C. (2014). Who Invented the Internet? [online], viewed 16 March 2020, Available at: https://www.livescience.com/42604-who-invented-the-internet.html.

Paras, C. (2018). The winner takes all fallacy and the structure of network effects [online], viewed 16 March 2020, Available at: https://invertedpassion.com/the-winner-takes-all-structure-network-effects.

Chaitanya, S. (N/D). Types of Computer Network: LAN, MAN and WAN [online], viewed 18 March 2020, Available at: https://beginnersbook.com/2019/03/types-of-computer-network-lan-man-and-wan .

etutortials.org. (N/D). Network Standards [online], viewed 18 March 2020, Available at: http://etutorials.org/Networking/Lan+switching+first step/Chapter+2.+Network+Models+and+Standards/Network+Standards/

Studyyonight, (N/D). Types of Network Topology [online], viewed 18 March 2020, Available at: https://www.studytonight.com/computer-networks/network-topology-types

Studyyonight, (N/D). Transmission Modes in Computer Networks [online], viewed 18 March 2020, Available at: https://www.studytonight.com/computer-networks/transmission-mode

Studyyonight, (N/D). Bounded Media [online], viewed 20 March 2020, Available at: https://www.studytonight.com/computer-networks/bounded-transmission-media

Studyyonight, (N/D). Unbounded Transmission Media [online], viewed 04 April 2020, Available at: https://www.studytonight.com/computer-networks/unbounded-transmission-media

GOV.UK, (2015). Guidance Network principles [online], viewed 04 April 202, Available at: https://www.gov.uk/government/publications/network-principles/network-principles

Dr.Roy Winkelman, (N/D). Protocol [online], viewed 04 April 2020, Available at: https://fcit.usf.edu/network/chap2/chap2.htm

Certiology, (N/D). Network Device [online], viewed 05 April 2020, Available at: http://www.certiology.com/computing/computer-networking/network-devices.html

Dealna, (2019). Three Types of Server Hardware [online], viewed 13 May 2020, Available at: https://dealna.com/en/Article/Post/1391/Three-Types-of-Server-Hardware

ComputerHope, (2020). Server [online], viewed 13 May 2020, Available at: https://www.computerhope.com/jargon/s/server.htm

wikiHow. (2019). How to Install, Configure, and Test Windows Server 2012 R2, viewed 21 May 2020 [online] Available at: https://www.wikihow.com/Install,-Configure,-and-Test-Windows-Server-2012-R2