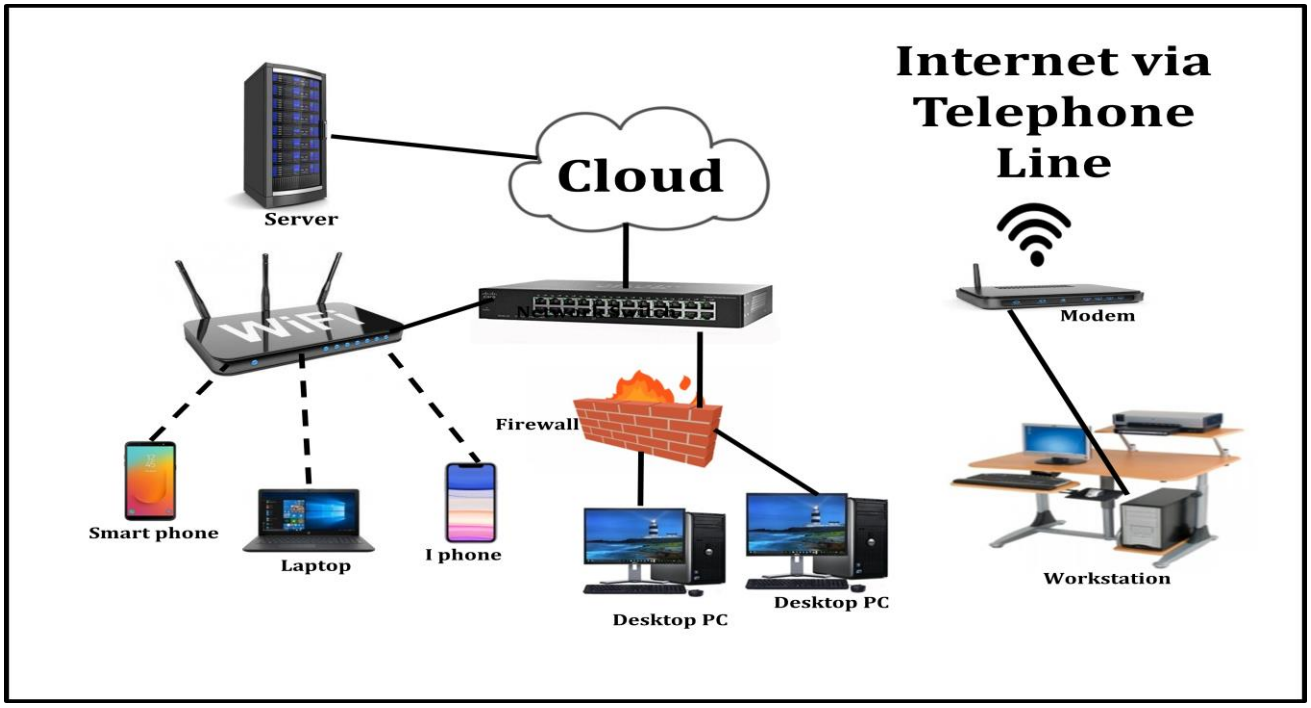
सत्यमेव जयते

GOVERNMENT OF INDIA
CENTRAL PUBLIC WORKS DEPARTMENT
Handbook
on
"Data Connectivity Framework
in
Public Buildings"



CPWD

PUBLISHED UNDER THE AUTHORITY OF
DIRECTOR GENERAL, CPWD, NEW DELHI -110011

Data Networking Framework

“The physical distance has been narrowed down drastically by Data & Communication Networks throughout the world. This is the power of Information &Communication Technology that goes into Networking of Devices, be it collection of computers, servers, mainframes, peripherals, or any other devices connected to one another to allow the sharing of data as well as communication. Internet-an excellent example of Network, connects millions of people around the world.”

Disclaimer

The world of network engineering is very complex and is full of new and ever growing vocabulary. Nevertheless, it is very interesting.The basic concept of networking of computers and other peripherals through the use of cables and other hardware including details of various components of hardware and their basic specifications is guiding in preparing the bill of quantities, forming of conditions and executing the work has been covered here.The technology of this field is changing very fast and it is very difficult to keep up-to date with changes. Hence basic framework only has been provided here which needs to be suitably revised as per the requirement of individual Client/ Department.

VINIT KUMAR JAYASWAL
Director General

सत्यमेव जयते

Central Public Works Department
Nirman Bhawan, New Delhi

FOREWORD

Providing Data Network Connectivity in Public Buildings has become an essential requirement in today's work environment. All public buildings, therefore, require high speed data connectivity with latest features of data security, threat management measures, continuity of data, data monitoring etc.

It is imperative that the entire Networking System is planned prudently. I hope that this Handbook will be very useful in planning of networking systems with appropriate technology.

I acknowledge the efforts of Shri Anant Kumar, ADG(Tech), Shri C.K.Varma, CE CSQ(E) and his team of officers, who have worked tirelessly to bring out this Handbook.

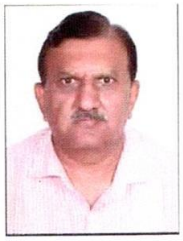
New Delhi,
August, 2020

(Vinit Kumar Jayaswal)

ANANT KUMAR
ADDITIONAL DIRECTOR GENERAL (TECH)

सत्यमेव जयते

Central Public Works Department
Nirman Bhawan, New Delhi



PREFACE

The philosophy of the Department has always been to select the best of the technologies and specifications in all types of works. The same applies to the data connectivity network in Public buildings which is essential infrastructure in present day built environment and needs to be latest, fastest and yet compatible to any latest intervention of this field.

The present document is one step forward, towards fulfillment of above philosophy. It is a very difficult task to come out with generic specifications in this field because of ever evolving technologies and equipments having fastest growing features. Therefore as a first step, this Handbook has been developed to help the tender inviting authority while framing the specifications.

I appreciate the efforts of Sh. C.K.Varma, CE CSQ (E) with the active support of Sh. M.V. Chalapathi Rao, SE TLQA(E) for bringing out this document in such a short time which will substantially help the field units.

New Delhi,
August, 2020

(Anant Kumar)

CHAITANYA KUMAR VARMA
Chief Engineer (E) CSQ

सत्यमेव जयते

Central Public Works Department
Nirman Bhawan, New Delhi

ABOUT THE BOOK

This compilation from Internet is the culmination of the efforts to comprehend the computer networking from a User's/ Building Engineer's perspective. The framework for data connectivity has become an essentiality in every Building in the wake of requirement of fastest mode of information and communication.

New terms are being added to network engineering very frequently apart from technological advancements in wired as well as wireless technologies which have made the subject quite complex besides being very interesting. Considering all this, the subject matter requires requisite elucidation for understanding the basic building blocks and from there to build complex networks and systems to facilitate the infrastructure of smart buildings which are being built now.

This handbook is the first attempt to provide insight into the complexity of Data Network and facilitate in handling Clouds of doubts. All suggestions for improvement may be sent to O/o CE CSQ (E), CPWD, Nirman Bhawan, New Delhi, at delceecsq.cpwd@nic.in & delseetlqa.cpwd@nic.in

(C.K.Varma)
CE CSQ (E)
19/8/2020

CONTENTS

Section 1
Introduction

CPWD is into the construction of buildings for Central Government Departments, Institutions funded by Central Government/State Government either partly or fully or by Central PSUs/State PSUs. As time has progressed, the construction of Smart / Intelligent buildings besides being energy efficient and renewable energy compliant has been expected by most of the organizations. In such buildings, the various Equipments installed for fire safety, energy consumption, video surveillance, building services management etc. communicate with each other, in addition to the occupants of the building. Thus data networking together with dedicated communication network is the need of every modern building.

Data Networking in Offices

Modern Government offices require data communicationfor file transfer, e-mails, e-Governance initiatives, e-office applications, ERP applications etc. over secured network for their effective functioning. In addition, various other systems like Video surveillance, Building Management, voice communication and other systems like access control, lighting control, Video conferencing etc. are also the requirement of modern and intelligent offices. Modern technology has provided thecomprehensivesolution for not only faster data transfer but also integration of all communication systems whether it is voice communication, human- machine or machine to machine communication for the efficient operation and effective maintenance of building services including safe functioning of the building from the point of view of fire, unauthorized entrants etc. So, many systems can be integrated with one network only. This can ease the data and communication infrastructure requirements of the building to a great extent. Many times, the building owner wants to incorporate number of systems for meeting his objectives, but due to paucity of budget/fund, it may not be feasible to include those systems at the time of original construction. In such situations, providing networking framework in the building eases the situation considerably.However, sometimes certain considerations like security restrictions for video surveillance etc. necessitate separate network.In such cases, a separate sub network can be considered with the provision to connect to the mainframe of the network system of the building. Therefore, it is quite reasonable to conceive framework for data networking while planning different services for the building.This framework should however have the flexibility to add any new system requiring data framework within a reasonable time frame.

Network Requirements in other types of buildings

In addition to the normal office buildings, there are other type of buildings like Academic Institutions,Court rooms, Hospitals, Hostels, Barracks, Sports complexes etc. where different activities take place and accordingly requirements of these buildings take a different dimension over and above a normal office building. For instance, in an academic institution, there are many class rooms requiring smart black boards and computing devices for interactive discussions among faculty and students with internet facility. In a hospital there are OPDs, ICUs, Labs, Surgery Rooms etc. requiring integration of all services for the hospital management to review and record. All these facilities necessitate different requirements on the centralized data network and therefore need special focus for enabling these buildings to be intelligent, people friendly and efficient in their core activity.All these specialized activities together with other miscellaneous facilities are possible through proper data framework.

Section 2

General Layout of Data Network
In a Building

Data network in a building can be conceptualized based on various factors. Prominent among them are- Number of occupants in the building, types of business activity,features of building i.e. number of floors, number of people working,type and number of control systems, computing and other peripheral devices, redundancy to avoid disruption of connectivity of data as well as communicationsetc.
Based on a typical high-riseofficebuilding,having different business activities being carried out at different floors, following plan can be considered as a general layout (however, there may be variations possible due to availability of numerous options):

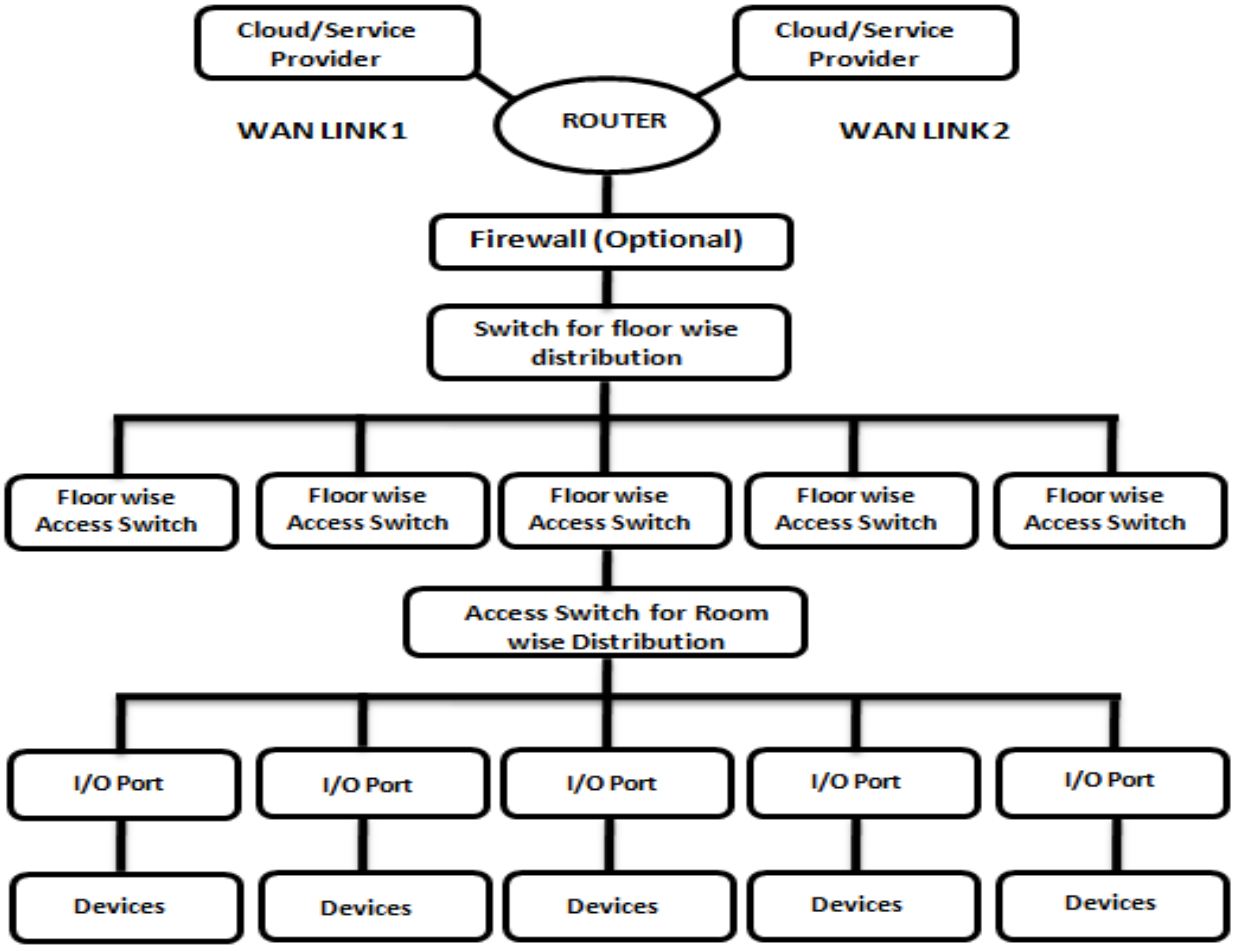


Figure 1: General Scheme of Data Network

The above diagram depicts the schematic arrangement of Network Operating Centre abbreviated as NOC. For the sake of redundancy, two such centers can be conceived in any building at a location convenient for access by the team of network operation and maintenance personnel as well as Equipments; without disturbing the business activities of the work space.
Note:- 1.Firewall can be a part of NOC or it can be provided in the Cloud2.Switching is usually three layered.

The flow of data communication is a two-way process. Network service provider depending upon the agreement between user and himself, provides the data at a speed based on its capability and user's requirement. This data is provided in the user's premises through fiber optic cable over leased telephone lines.

100% redundancy is normally conceived at the time of conceptualizing the NOC to provide continuous flow of data in case of failure of one of the WAN links. The network service provider has arrangements with its Data Centre to provide various services which different clients' demand and through WAN protocol and configuration, NSP provides them to its bulk customers. Within the premises of the customer, data is further transmitted through distribution switches which are in three layers namely Core layer which connects both the NOCs, distribution layer which sends data to various floors and then access layer to various offices in each floor. The computers and other devices in the floors are connected in star formation for direct transmission of data without any loop or other device for fastest communication.

In a Campus (Campus Area Network)

Campus is a collection of buildings and grounds that belong to a given institution, either academic or non-academic. Thus, the scheme of data networking is little different in a campus as compared to a building. In fact, a campus consists of a conglomeration of buildings which are built either adjacent to each other or are separated by a few meters. In such cases, the main networking Equipments are kept in the main building which is normally the Administrative building or block.

The distribution within that building and other buildings is done through CAT6 and fiber optic cable depending upon the separation distance. The distinguishing features of the campus are the networking through a dual ring network connected by optical fiber network besides distribution and access layer in sub buildings. For providing redundancy BGP(Border Gateway Protocol) Multihoming can be used. It is one of the key protocols to seek redundancy in Internet connection. With Multihoming, it provides network optimization while offering redundancy .

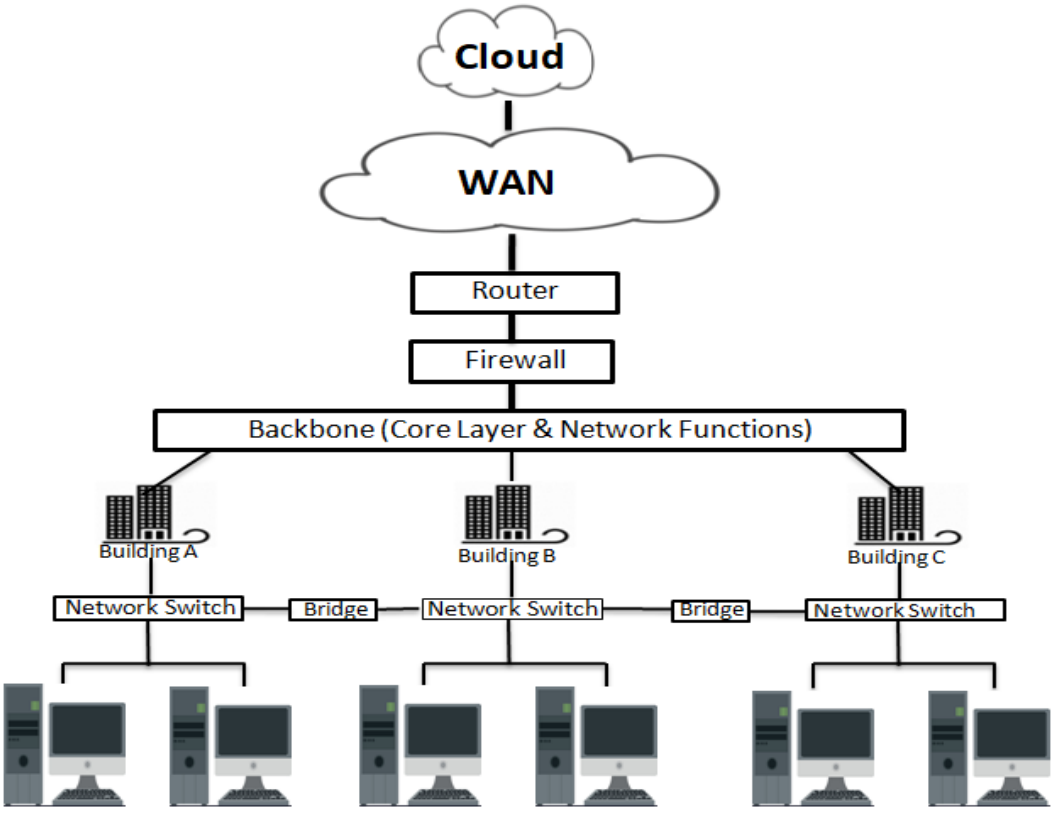


Figure 2: Schematic Diagram of Campus Area Network

Section 3

Elements of Data Network

There are various elements of the data networking framework and a reasonable understanding of them is necessary in the visualizationand implementation of proper framework and solutions.

Network Service Provider –
It is the first link in any networking framework. Network Service Provider denoted by NSP signifies a business organization which provides network access from cloud. For Government Departments/ Ministries, NIC(National Informatics Centre) being the Government entity is usually the first preference. In addition, many private players of repute are also available. It is therefore very essential to have tripartite discussions in the planning stage itself amongst Network provider, Client Department and Planning team of CPWD and then at regular intervals as required.

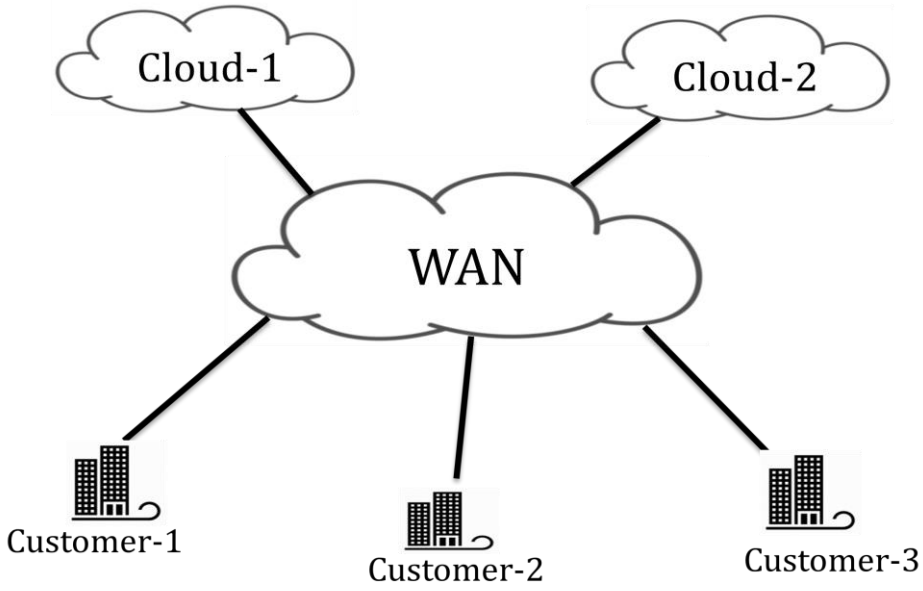


Figure 3 : Infrastructure of Network Service Provider

Network service-
Network service provides data storage and manipulation, presentation, communication or other capabilities which are implemented using a client-server or peer-to-peer architecture based on application layer network protocols.

It includes NTP(Network Time Protocol), DNS(Domain Name System), DHCP(Dynamic Host Configuration protocol), VoIP(Voice Over Internet Protocol), File and Directory, Hardware Sharing, Email, and Website Hostingand deal with the data networks which may comprise of a variety of communication systems allowing computers to exchange data. The connections between different nodes are either established through cable media or wireless media.

Figure 4: Examples of Network services

Cloud –

Storehouse of many resources related to data transmission, this term is generally used to describe data centers available to multiple users over the internet. Large clouds are predominant today and have functions distributed over multiple locations from central servers. Clouds limited to a single organization are called Enterprise clouds and when to many organizations are called Public Clouds.The word cloud is now used for the internet as a metaphor and a standard cloud shape is used to denote storehouse of network resources.

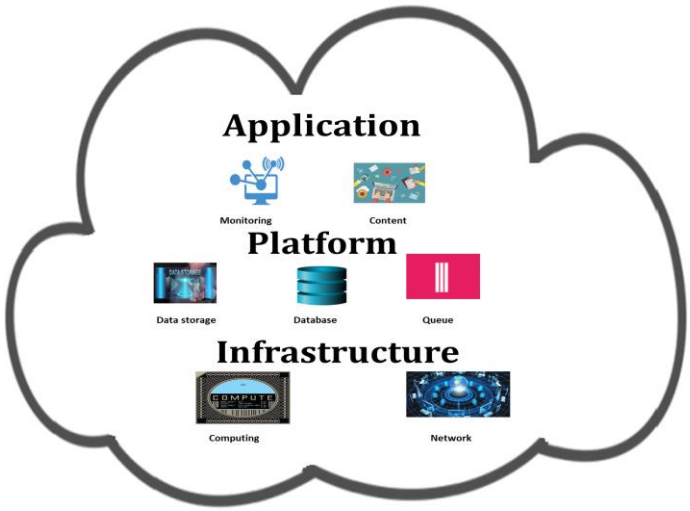


Figure 5 : Cloud

The activities contained inside a cloud can be many. However, broadly there are 3 different types of activities namely: Application, Platform and Infrastructure. The above diagram illustrates few examples of these activities.

This cloud can then be connected to different users through different arrangements like ISPs i.e. Internet Service Providers for general public via either mobile network or through broadband, NSPs i.e. Network Service Providers for bulk institutional users etc.

WANLink

WAN Link is a communication circuit that joins two or more local area networks (LANs) into a wide area network (WAN) through fiber optic cable.It is provided by Network Service Provider to Institutional Client and controlled from the premises where it is physically located.

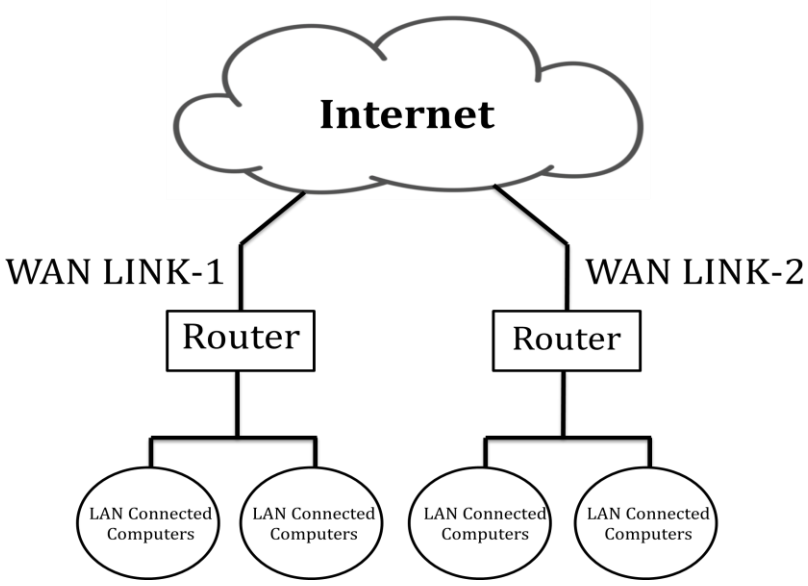


Figure 6: WAN LINKS

The Link or line is connected through fiber optic cable required for transfer of large amount of data. Normally, minimum two links through fibre optic cables are taken which are the leased lines from the telecom company.

WAN- WAN is the Wide Area Network for feeding data over a large network of devices. The network in the context of network service provider covers wide area and hence is called WAN. It normally feeds network to a large group of buildings over a large area.

Router- Routera networking device forwards data packets between different computer networks. Thus, it performs traffic directing functions on Internet. Data sent through the internet, such as a web page or email, is in the form of data packets which are exchanged between different networks through Router.Routersare wired as well as wireless.

Routers can be distinguished based on their operating network. Hence, aRouter in local area network (LAN) of a single organization is called an interior Router while aRouter operating in the Internet backbone is called as exterior router. A router connecting a LAN with the Internet or a wide area network (WAN) is called a border router, or gateway router.

Figure 7 : Router

Firewall – It acts as a protective shield of the network. There are all sorts of spurious data in a network due to multiple entry points. Further hackers also endlessly attempt to misdirect or steal many information.Thus, vulnerability of data network is covered by firewall. But Firewall makes the flow of data slow.

A firewall is therefore a network security system for monitoring and controlling incoming and outgoing network traffic on the basis of predetermined security rules. A firewall establishes a barrier between a trusted internal network anduntrusted external network, such as Internet.

Firewalls are categorized as network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks and run on network hardware. Host-based firewalls on the other hand run on host computers and control network traffic in and out of those machines.

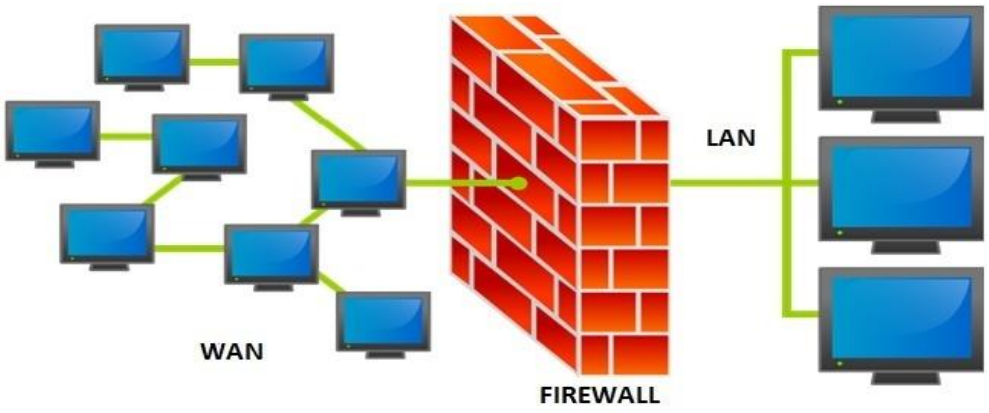


Figure 8: Firewall Concept

LAN

Within the building, various data exchanging devices are inter-connected. This connection within the Office/Ministry/Department is known as LAN or Local Area Network. There are many configurations possible and selection of any configuration depends upon many factors like type of office, redundancy required, secrecy of the data etc. Configurations/topologies define the manner in which network devices are organized.

Seven common LAN topologies exist: bus, ring, dual ring, star, tree, mesh and hybrid. Topologies are driven fundamentally by types of connection:Point-to-Point and a Multi-Point connection.Aconnection is a direct link between two devices. For example, when a computer is attached to a printer, point-to-pointconnectionis created. In networking terms, pointto point connections are associated with modems and PSTN (Public Switched Telephone Network) communications. A multipoint connection on the other hand is a link between three or more devices. Now-a-days, multipoint connections link many network devices in various configurations.

A few configurations of LAN network along with diagrams is given below:

Bus Topology

All nodes are connected to a single cable. The cable to which the nodes are connected is called "Backbone". So if the backbone is broken, entire segment fails. Bus topology is easy to install and does not require much cabling as compared to other alternatives.

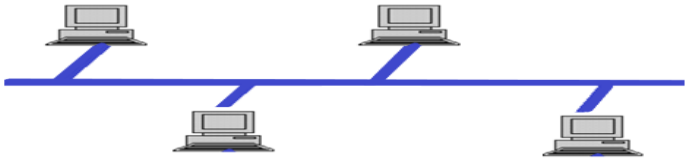


Figure 9 : Bus Topology

Ring Topology

Here, every device has two adjacent devices. As all data travels in the same direction through a ring, failure in any cable or device breaks the loop and entire segment breaks down.

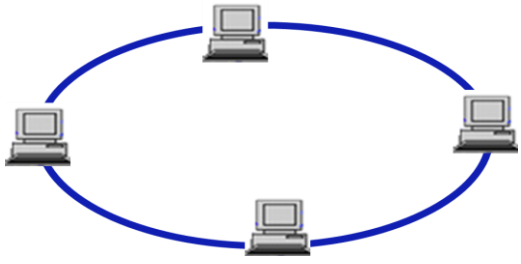


Figure 10: Ring Topology

Dual Ring Topology

It is an improvement of ring topology. In this topology, two concentric rings connect each node on a network instead of one network ring. The secondary ring is used as a backup in case the primary ring fails.

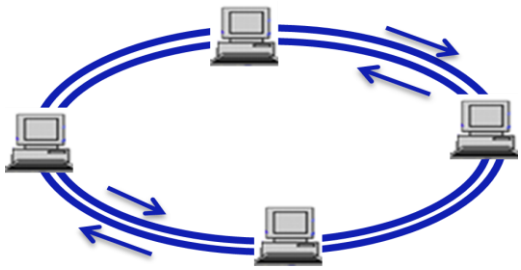


Figure 11: Dual Ring Topology

Star Topology

In this topology, all nodes are individually connected to a central connection point. This configuration consumes more cable than bus topology with the advantage that if one cable fails, only one node is affected.

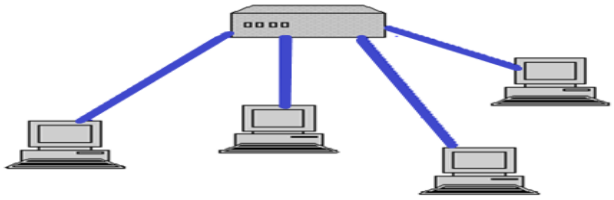


Figure 12 : Star Topology

Tree Topology

A tree topology combines Bus and star topologies.It consists of groups of star-configured workstations connected to a linear bus backbone cable.Tree topologies allow for the expansion of an existing network.

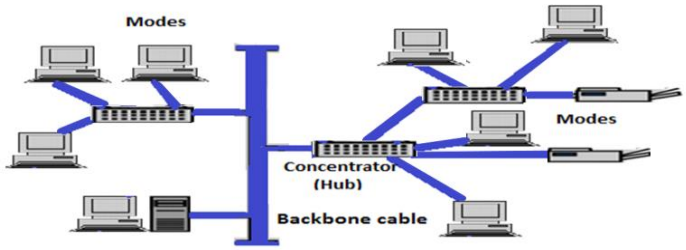


Figure 13 : Tree Topology

Mesh Topology

In mesh topology, infrastructure nodes connect directly, dynamically and non-hierarchically to as many nodes as possible and cooperate with one another to efficiently route data from/to clients.

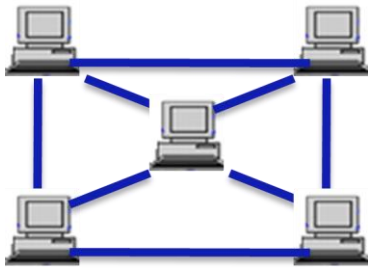


Figure 14 : Mesh Topology

Hybrid Topology

It combines two or more topologies in such a way that the resulting network does not exhibit any of the standard topologies like bus, star, ring etc.A hybrid topology is always produced when two different basic network topologies are connected.

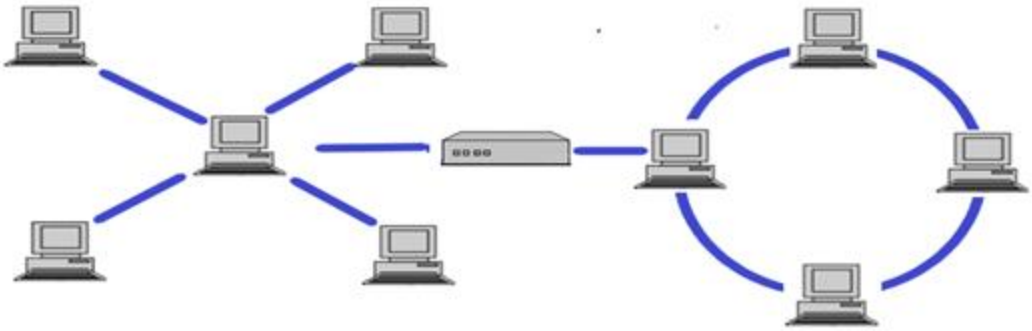


Figure 15 : Hybrid Topology

Table below summarizes features and applications of different topologies/configurations

S.N.	Type of Topology	Features	Applications
1.	Bus	1. All nodes connected to a single cable. 2. Easy to install. 3. Cabling requirement is less. 4. Entire Network breaks down due to fault in cable.	Very small Office Networks.
2.	Ring	1. Devices are connected in ring formation. 2. If one device or cable breaks, entire segment breaks down.	Only used in Small Offices.

3.	Dual Ring	1. Two concentric rings connect each node on a network instead of one network ring. 2. Used as a backup to primary ring.	Where data connectivity requires redundancy in small offices.
4.	Star	1. All devices are connected with the hub/switch in star formation. 2. Cable requirement is more.	Mostly used in all big Offices.
5.	Tree	All devices are connected in tree formation.	When different computers are needed to be connected together and are required to be separated for data breach/security.
6.	Mesh	1. All devices are connected in mesh formation. 2. Every device is connected to every other device.	Useful in small offices.
7.	Hybrid	Devices are connected in different configuration and then these configurations are connected together in series.	Useful when different offices are connected together.

VLAN

It is the abbreviation of Virtual LAN.In this local networking scheme, a group of devices are connected wireless &configured to communicate. This gives a network ecosystemwhere it appears as if they are attached to the same wire, while they are located on a number of different segmentsconstitutingVirtual LAN. The flexibility is the gain point in this configuration, since VLANs are based on logical rather than physical connections.Combining group of devices from both wired & wireless networks(which could be many in number) into a single logical network is a distinct advantage in this type of network scheme.

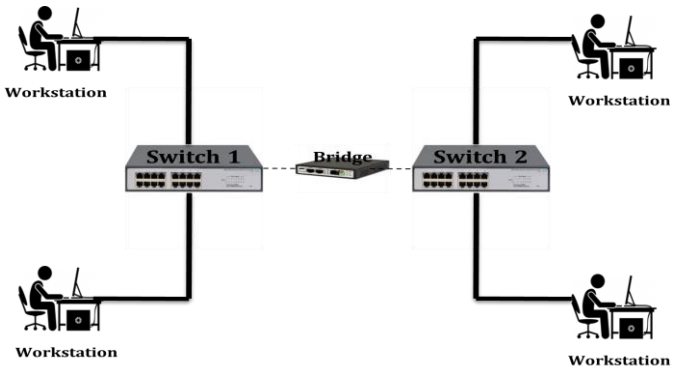


Figure 16 : Concept of VLAN

In the above figure 4 workstations are connected with the help of 2 switches and a bridge. This way all the 4 workstations are connected together by wire as well as by wireless connections.The 2 workstations each are connected by a switch and the 2 switches are connected together with the help of a bridge(also a kind of a switch) wirelessly and thus the networking is established between all the 4 workstations/devices.

WLAN

An acronym for wireless LAN, it is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN). This arrangement is mostly used within a limited area such as a home, school, computer laboratory, campus, or office building.Ituses Radio, Infrared orMicrowave transmission to transmit data from one point to another without cables.

Figure 17: Concept of WLAN

Wireless Access Point

A WAP is also known as a hotspot.It 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. WAPs feature radio transmitters and antennae, which facilitate connectivity between devices and the Internet or a network.

OSI Model

A reference model is a necessity to describe how information flows from a software application in one computer to the software application in another computerthrough a physical medium.OSI Model (Open Systems Interconnection Model) fulfills that need and is a conceptual framework used to describe the functions of a networking system. OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.

OSI Model comprises of seven layers and each layer is conceived to perform a particular network function.Thus this model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task and the task assigned to each layer can be performed independently.Thus each layer is self-contained.

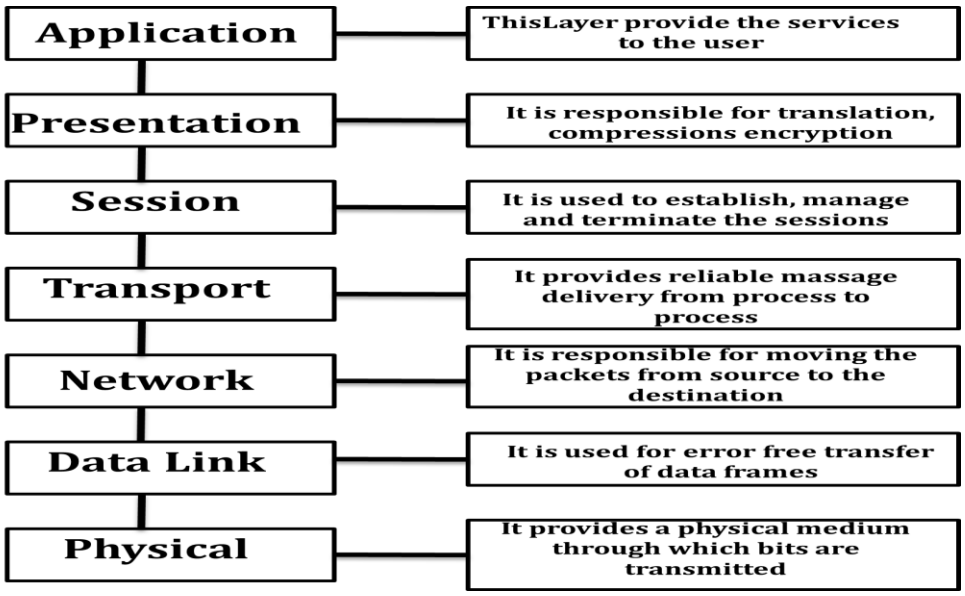


Figure 18 : Layers of OSI Model

The above diagram is self-explanatory in so far as the functions of each layer are concerned. Further, the OSI model is divided into two layers: upper layers and lower layers.The upper layer mainly deals with the application related issuesand are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications.

The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

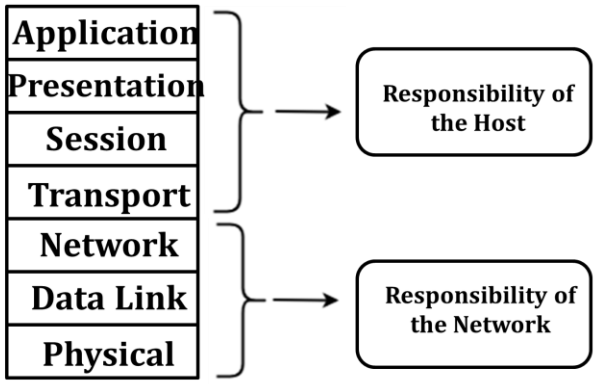


Figure 19: Responsibilities of different layers of OSI Model

The above diagram illustrates the division of layers into upper and lower layers and their assigned responsibilities.

Though OSI Model was elaborate but cumbersome, hence a concise version was required. Hence, TCP/IP Model fulfils this requirement.

TCP/IP Model

It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model and contains four layers, unlike seven layers in OSI Model.This model is used by the majority of internets because it encompasses a number of different protocols for different purpose and needs.

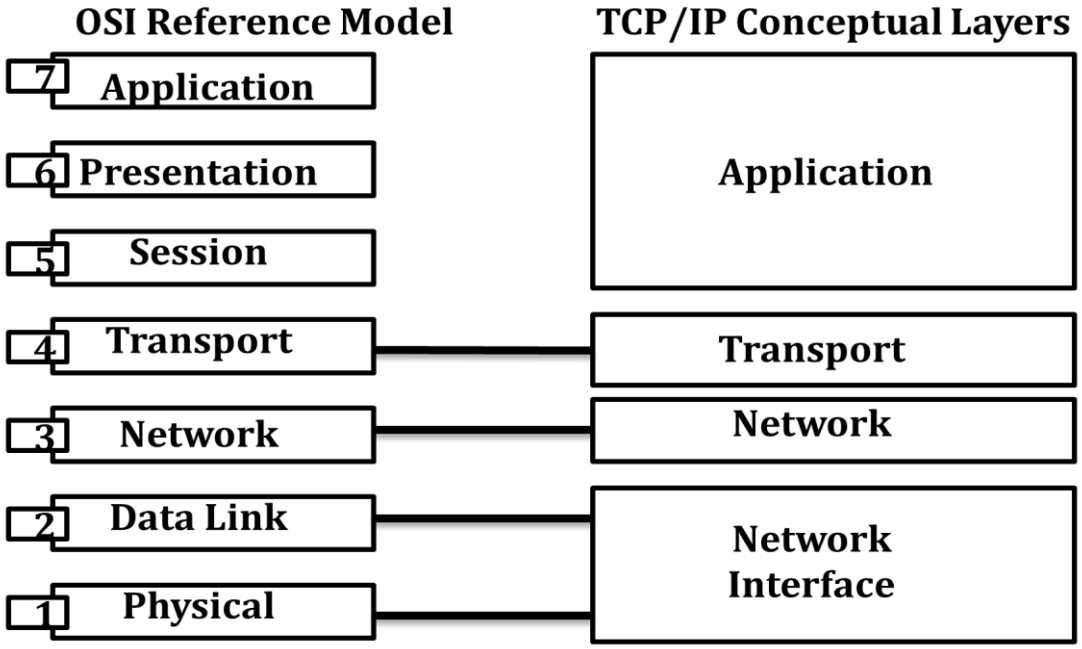


Figure 20: Comparison of TCP/IP Model with OSI Model

Common protocols of TCP/IP include the following:

a) HTTP (Hyper Text Transfer Protocol) for handling the communication between a web server and a web browser.

b) HTTPS (Secure HTTP) for handling secure communication between a web server and a web browser.

c) FTP (File Transfer Protocol) for handling transmission of files between computers.

Layers of Switching at User's Premises

Normally, there are three layers of switching for distribution of data namely core layer, distribution layer and access layer.

Core layer

The core layer consists of high-speed Switches and Routers for optimization of performance. Located at the core layer of enterprise network, a core layer switch functions as a backbone switch for LAN access and centralizes multiple aggregation devices to the core. Thus, core layer is a high-speed backbone that is designed to switch packets of information as fast as possible to optimize communication within the network. The Core layer connects all Distribution layer devices and switches and routes large amounts of trafficreliably as well as quickly.

Distribution Layer

The distribution layer is the smart layer in the three-layer model of internetworking. Routing, filtering, and QoS(Quality of Service) policies are managed at this layer. This layer is also called the Workgroup layer.The distribution layer thus aggregates the data received from the access layer switches before it is transmitted to the core layer for routing to its final destination. Distribution layer is the boundary between the Layer 2 domains and the Layer 3 routed network.

Access Layer

The Access layer is the level where host computers are connected to the network. The Distribution layer acts as an aggregation point for all the Access layer devices. The Core layer connects all Distribution layer devices and reliably and quickly switches and routes large amounts of traffic.

The Figure below depicts the functionality of different switching layers:

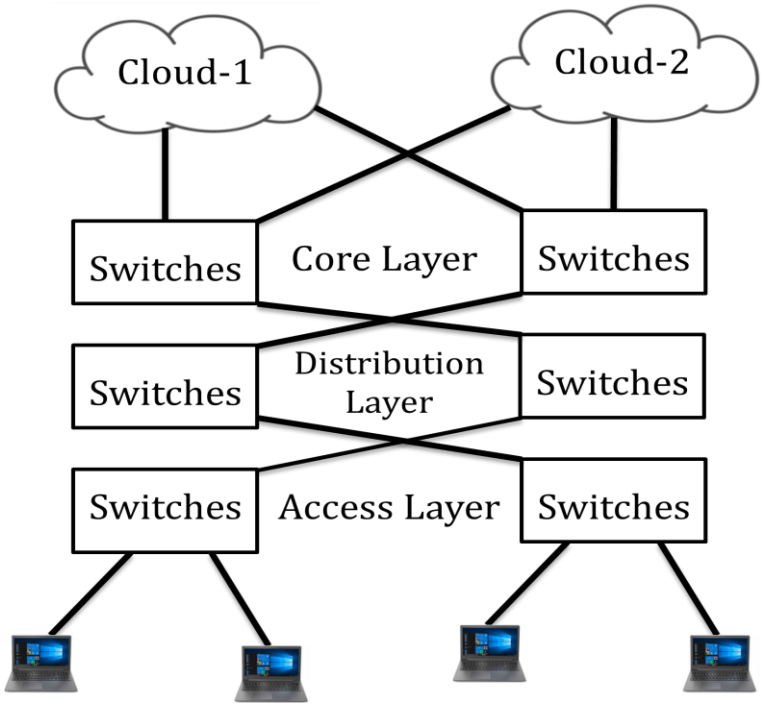


Figure 21 : Layer of Network Switching

Network Switch

It is a multiport network link that uses MAC (Media Access Control) address to forward data at the data link layer (layer 2) of the OSI model.

Figure 22: Network Switch with Cable Connections

Core Switch

It is a high capacity switch.It serves as the gateway to a wide area network (WAN) or the Internet. Generally positioned within the backbone or physical core of a network, it provides the final summation point for the network.

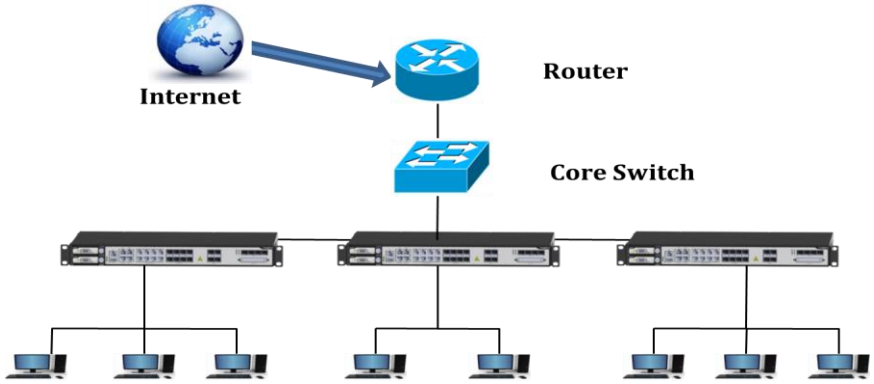


Figure 23 : Core Switch Connections

Distribution Switch

It uplinks core switch and downlinks access/edge switch. Acting as an aggregation switch to bridge between core layer switch and access layer switch, it collects data from all the access switches and forwards to the core layer switches.

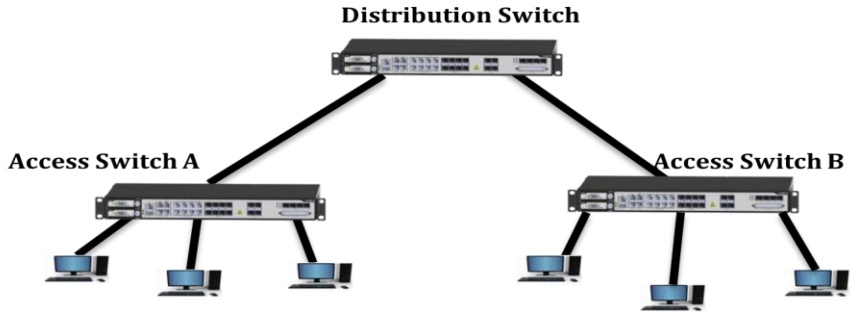


Figure 24 : Distribution Switch Connections

Access Switch/Edge Switch-

Function of this switch is to provide network access to the users.Access layer switches connect to distribution layer switches to perform network foundation functions such as routing, quality of service (QoS) and security.

Figure 25Access Switch/Edge Switch

Network Cables-

Used for connecting one network device to other networking devices. Different types of network cables such as coaxial cable, twisted pair cables and optical fiber cableare invariably used depending on the network's topology and distance between devices.

For short distancesin offices up-to 100 meters,twisted pair cables are used.For distances beyond this, optical fiber cable is the automatic choice.

Co-axial cable

It is a type of electrical cable consisting of an inner conductor surrounded by a concentric conducting shield separated by dielectric. Many coaxial cables also have a protective outer sheath or jacket. Itis also used within a buildingbut primarily used for cable TV. It transmits radio frequency signals and is used in all forms of transmission of entertainment data.

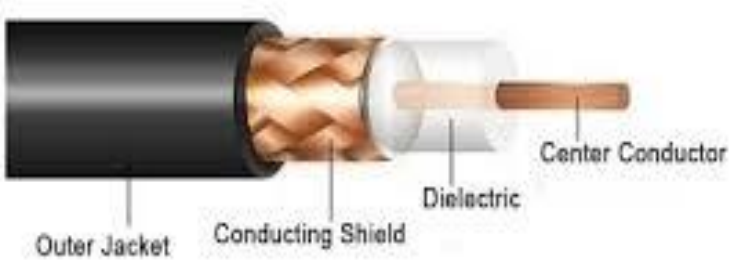


Figure 26: Coaxial Cable

Unshielded Twisted Pair (UTP) Cable-

In this type of cabling, two conductors of a single circuit are twisted together for improving electromagnetic compatibility. It consists of two separate insulated copper wires twisted together and run in parallel,one for transmission of data and the other for ground reference purpose. The copper wires are of typical diameter of 1 mm. Since all transmissions are prone to noise,

interferences and cross talks,so due to twisting, some part of the noise signal is in the direction of data signals while the others are in opposite direction thuscancelingeach other out and data gets rid of unwanted noise signals. These are generally used within a building for providing connection in telephone, DSL(Digital Subscriber Line) and LAN lines.

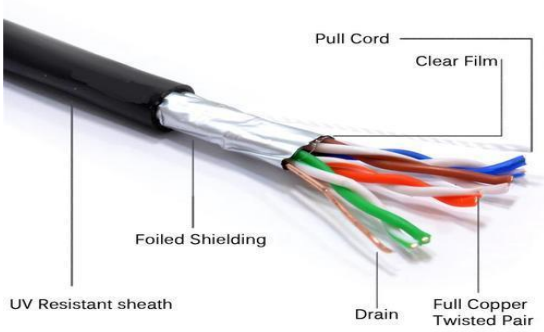


Figure 27:UTP Cable

UTP cables come in different categories and accordingly categorized as Cat 1 to Cat 7 cables. Cat 8 cables are the latest entrant into this segment. There are eight wires grouped in four pairs, each composed of a solid-colored wire and a stripped wire.Each wire is twisted a certain number of times to minimize interferences with the other pairs. A higher number of twists per inch results in a higher data transmission.

TIA/EIA-568A stipulates the commercial cabling standards for LAN installations and is the standard most commonly used in LAN cabling environments.

In the UTP segment, Cat 1 cable was introduced in 1985.Being an unshielded twisted pair (UTP), it consisted of two insulated copper wires twisted around each other to eliminate crosstalk. Being of low cost and easy in installation made it popular for connecting home and business computers to a telephone companies' equipment. UTP cable is more susceptible to radio and magnetic interference than shielded cables. Typically used for telephone wiring, its data rate is 1 Mbps. CAT 1 is typically used for telephone wire.This type is not capable of supporting computer network traffic and is not twisted. CAT1is also used by telecom companies providing ISDN and PSTN services.

An improvement, Cat 2 was released shortly thereafter with a data rate of 4 Mbps.CAT2 is used mostly for token ring networks, supporting speeds up to 4 Mbps.

Category 3 reached its peak in the early 1990s and featured a data rate of 10 Mbps with a bandwidth of 16 megahertz (MHz). Category 3 and its successors are made up of four pairs of twisted wires, allowing the simultaneous transmission of voice, data and video over a single cable.Category4 cable was an upgrade to Cat 2 and was primarily used for Token Ring networks. It was also used in what are now antiquated telephone and data networks. The transmission speed for Cat 4 is 16 Mbps.

Category 5 was introduced in 1995 and is the successor to Cat 3. This was the first cable to be dual-rated at 10/100 Mbps with a bandwidth of 100 MHz It can distribute video and telephone signals at distances of 100 meters, or 328 feet.CAT5 wire has more twists per inch and is suitable upto the speed requirements of 100 Mbps. It is used for Ethernet, Fast Ethernet and Token Ring Networks.

Category 5e is an enhanced version of Cat 5 and can support speeds up to 1 Gbps over a distance of 55 meters, or 180 feet, with a bandwidth of 100 MHz This was accomplished by increasing the number of twists, making the cable much more resistant to crosstalk. After its introduction in 2001, it quickly became the cable of choice for new and retrofit installations.CAT5e has replaced more used Cat 5 cable due to its superior speed which is upto 1Gbps and provides improved cross talk specification.

Category 6 raised the bandwidth of a UTP cable to 250 MHz at a speed of 1 Gbps over 55 meters. Cat 6 is also available in a shielded version.Category6a was introduced in 2008 and supports speeds up to 10 Gbps at a bandwidth of 500 Mhz. CAT 6 wire is similar to CAT 5e but contains a physical separator between four pairs to further reduce electromagnetic interference. Today most new installations use CAT 6. However, the limitation is thatall cabling componentslike jacks, patch panels, patch cords etc. should be CAT6 certified and extra precaution must be taken for proper termination of cable ends.Cat6a is only available as a fully shielded cable.

Category 7 came out in 2010 and still has a speed of 10 Gbps, but it has an increased bandwidth of 600 MHz This was accomplished by adding more shielding.Category 7a, introduced in 2013, maintains the 10 Gbps speed while increasing the bandwidth to 1.2 GHz.CAT7 cable supports speeds of 10Gbps at lengths of up to 100 meters. To achieve this, the cable features four individually shielded pairs plus an additional cable shield to protect the signals from crosstalk and electromagnetic interference (EMI).Due to the extremely high data rates, all components used throughout the installation of a CAT7 cabling infrastructure must be CAT7 certified. This includes patch panels, patch cords, jacks and RJ-45 connectors. Failing to use CAT7 certified components will result in the overall performance degradation and failure of any CAT7 certification tests (e.g. using a Cable Analyzer) since CAT7 performance standards are most likely not to be met. Today, CAT7 is usually used in DataCenters for backbone connections between servers, network switches and storage devices.

The newer Cat cables are shielded, making them more expensive and harder to install and terminate. They also require different connectors than their predecessors. I am seeing projects that may be over specified. Many computers have an Ethernet card that is only good for 100 Mbps, which can be handled with a Cat 5e instead of higher rated cables. This may be a good alternative to suggest to your customers. Category8 was developed primarily to help data centers increase bandwidth and network speeds. It has a speed of 40 Gbps and a bandwidth of 2 GHz over a maximum of 30 meters, or 98 feet.

Optical fiber cable

It is used for long distances or for applications requiring high bandwidth or electrical isolation. Also known as Fiber optic cable, it is an assembly containing one or more optical fiber which carries light. It contains strands of glass fiber inside an insulated casing designed for long distance, high performance data networking.The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. In comparison to wired cables, fiber optic cables provide higher bandwidth and

transmit data over long distances.

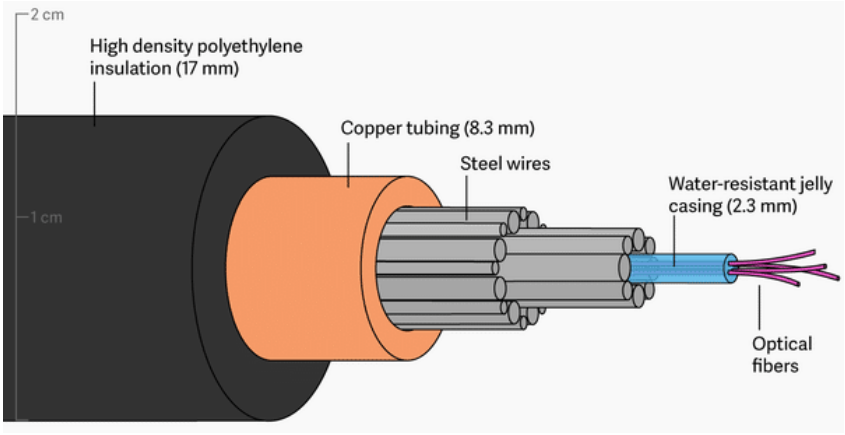


Figure 28: Fiber Optic Cable

Three types of fiber optic cables commonly used are Single Mode, Multi-Mode and Plastic optical Fiber(POF). The infrared light propagates through the fiber with much lesser attenuation hence it is advantageous compared to an electrical cable.

Different types of cableare used for different applications, for example, long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Further, depending upon the uses,Fiber optic cable is of following types:

1. Duct type single sheathed
2. Under water steel wire armored
3. Central Tube Armored single sheathed
4. Central Tube Armored double sheathed
5. Central Tube Unarmored
6. Aerial Type
7. Tight Tube Non-Metallic

I/O Port

An I/O port is a socket on a computer/ Network device for plugging a cable . The port connects the CPU(Central Processing Unit) to a peripheral device via a hardware interface or to the network via a network interface. It also acts as an interface between computer and external devices.

Figure 29: I/O Port

In the above figure, different types of ports like LAN port, HDMI port, VGA port, Serial port are shown for connecting cables according to the application.

Connector

A connector is a device which is connected to both the ends of the cable so that it is securely connected to the computer at one end and networking devices on the other hand.

There are different types of connectors as per the use.

Fiber LC (Local Connector)

These connectors are used for single-mode and multimode fiber-optic cables andoffer extremely precise positioning of the fiber-optic cable with respect to the transmitter's optical source emitter and the receiver's optical detector.

Figure 30: Fiber Local Connector

SC(Standard Connector) — This connector is square, like an LC, but is approximately twice the size. It also holds into place using a push/pull mating mechanism.

Figure 31: SC Connector

ST(Straight Tip) Connector — This is a round connector that uses a bayonet-style mechanism and has to be twisted into place. It is about the same size as the SC connector.

Figure 32: ST Connector

MT-RJ (Mechanical Transfer Registered Jack)connectors are used with single-mode and multimode fiber-optic cables. The **MT-RJ** connectors are constructed with a plastic housing and provide accurate alignment via their metal guide pins and plastic ferrules.

Figure 33: MT-RJ Connectors

RJ(Registered Jack) Connector

It is a standardized telecommunication network interface for connecting voice and data equipment to a service provided by local exchange carrier or long-distancecarrier.It is also used for connecting computers to Ethernet based LAN.
RJ45 is an 8P8C modular connector. 8P8C = 8 position, 8 contact.The "45" simply refers to the number of the interface standard. It looks similar to a telephone jack, but is slightly wider with the advantage that it is easy to install, very reliable and suitable for 100 Mbps speed.

Figure 34 : RJ-45 Connectors

USB(Universal Serial Bus)

It is designed to replace serial and parallel ports. A single USB port can be used to connect up to 127 peripheral devices, such as mouse, modems, keyboards, digital camera's incoming port, printers, scanners, MP3 players etc. It also supports Plug-and-Play installation and hot plugging.

Gang Box for data outlet

For taking internet and other services from the access switch provided on each floor, Gang boxes of different configuration are provided on the wall of cabins/workstations. These are grouted on

the wall at a suitable location as decided by the user department/architect. The incoming connections to the gang box are given through Cat 5/6 cable depending upon the speed of data transmission.

Figure 35 : Gang Box and its components

Section 4

Space and Other Functional Requirements of Network Control Centre

Assessing the space requirement of Network control center is the first priority of the architectural in charge of the project. Normally two centralized and easily accessible spaces should be allocated to the networking center. The size of the room and inside facilities to be provided should be clearly worked out after thorough discussions with the networking agency and drawing the layout of the machines and operating staff. Normally, the machine room is separate from network monitoring room which is manned by operating staff and are provided side by side ideally. The machine room has a different requirement than the monitoring room. It has a raised floor for accommodating the cables to be connected to the Equipments and has electrostatic and ventilation features. Various Equipments are housed in a rack which needs to be properly ventilated to remove the heat generated by the Equipments. There can be a number of racks depending upon the type and number of Equipments. The dimensions of the room are dependent upon the layout of the main Equipments and future expansion including proper space for working on all sides of the communication Racks.

A suggestive layout in which equipment room and monitoring center are shown separatelyis given below. However, these can be together also if requirement so demands:

Figure 36: Network Operating Centre

Besides proper layout, there are other functional requirements of the NOC.

1. Lighting
2. Airconditioning &Ventilation Requirements
3. Power Requirements i/c UPS back up
4. Electrostatic Flooring i/c Earthing Requirements
5. Fire Safety i/c Fire Alarm, VESDA, Fire suppression System

6. Rodent repellant system
7. Water leakage detection system

All the above requirements should be discussed thoroughly with the equipment supplier and network vendor before providing them.However broad parameters are given below for the sake of general guidance.

1. Lighting- The lighting of the equipment room should be bright enough to be able to see various connecting wires clearly by the technician for repairing or other activities related to maintenance after erection. However, the lighting should be equipped with occupancy detectors so as to switch off the lights automatically when no operating personnel is present in order to save wastage of electricity.

2. Air-conditioning & Ventilation Requirement- The air conditioning to be provided for this room is for machines andnot comfort air conditioning.Accordingly precision air conditioning is provided. The parameters of inside conditions i.e. temperature and humidity should be decided mainly on the recommendations of equipment manufacturers. However, as a general guideline temperature of 18^0C and RH of 50 % can be considered for equipment room.Lesser humidity will result in the buildup of static electricity on the systems while more humiditywill lead to corrosion which will start damaging equipmentslowly resulting in permanent equipment failures. Redundancy of one air conditioning unit should be provided as the Equipments remain in24X7 operation. Ventilation as per NBC 2016 should be provided.

3. Power Requirements i/c UPS back up- Power requirements should also be worked out with sufficient redundancy. The UPS system with proper battery back-up should be provided. The number of hours battery backup depends upon the power situation of the place. Generally, 4 hours battery back-up is considered sufficient where power availability is good and power outage is minimum.

4. Electrostatic Flooring i/c Earthing Requirements- This should be given due consideration as per the advice of Equipment manufacturers.

5. Fire Safety i/c Fire Alarm, VESDA, Fire suppression System- Fire safety requirements should be considered carefully and should be adequate. Smoke detector, Very Early Smoke Detection and Alarm system(VESDA) can be considered for fire detection. The fire fighting system should be gas based confined to Equipments room and no water sprinklers should be provided.

6. Rodent repellant System- It is necessary to provide this system in order to repel the rats etc. for protection against cable cutting and thus avoiding downtime of the system.
7. Water leakage detection system- There could be water due to sweating by Air conditioning. This should be detected so as to provide remedial action. Therefore, water leakage detection systems is necessary.

Section 5

Selection Parameters of Network Components

This section deals with selection parameters required for network elements.

Wired Router
Wired routers give fast speeds and works well in case of fiber optic connected internet.Following are some of the parameters of selection of router:

- Speed of the data
- Number of devices to be connected
- Number of WAN Ports
- Router with or without built in firewall
- VPN access.
- Configuration:It should either be fixed or modular.
- Size of the rack for mounting. For example, 19 inch Rack mountable.
- Ethernet Ports on the router should support LAN and WAN protocols.
- Minimum Memory requirements 2GB RAM and 2GB internal flash, for smooth functioning /operation.
- The router should support protocols both existingas well as upcoming ones.
- The Router should be IPv6 ready and certified as per applicable Standards.

Note:- The above are indicative parameters and not exhaustive. NIT Authority may decide for inclusion of more parameters depending upon the requirement of client.

Network Switches
Following parameters are required to be specified:

- Physical Configuration is one of the necessary criteria and accordingly network switches can be either Fixed, Stackableor Modular.In a fixed configuration, number of ports are fixed and are not expandable while in a stackable configuration, number of switches are connected together to increase the expandability.Wherever stacking is required, minimum requirements of stacking should be specified.Modular configuration provides flexibility to address changing networks by adding expansion modules into the switches.
- Number of devices to be connected
- It should supportPoE (Power over Ethernet) and routing protocols.
- The switches should have non-blocking performance with minimum 1GB RAM and 1GB internal flash memory.
- It should support automation like ZTP (Zero Touch Provisioning) and scripting like Python.
- The Switch should support L2 functionalities/ Connectivity. L2 functionality is the most fundamental form of network connectivity needed for virtual machines and is the connectivity to a physical or virtual switch.
- The switch should be IPv6 ready and certified as per applicable Standards.

Note:- The above are indicative parameters and not exhaustive. NIT Authority may decide for inclusion of more parameters depending upon the requirement of client.

Firewall

Following are some of the parameters of the firewall.

- The Firewall should be purpose appliance. It means it is made to optimize for a set of purposes.
- It should not use any proprietary ASIC (Application Specific Integrated Circuit). This indicates that the electronic circuitary used is of generic design and features.
- The Firewall should support UTM(Unified Threat Management) features like Intrusion prevention, Antivirus, Antispam and URL(Uniform Resource Locator) filtering.
- The Firewall should be IPv6 ready and certified as per applicable Standards.

Note:- The above are indicative parameters and not exhaustive. NIT Authority may decide for inclusion of more parameters depending upon the requirement of client.

Cable

Fiber Optic Cable

There are two types of specifications for Fiber Optic Cable:

1. **Optical Specifications**

    - Attenuation
    - Chromatic Dispersion
    - Core/Cladding Concentricity Error
    - Cladding Non- Circularity
    - Cut Off Wavelength
    - Zero Dispersion Wavelength

2. **Mechanical Specifications**

    - Core Diameter
    - Cladding Diameter
    - Coating diameter
    - Installation Temperature

Cable is selected based on the distance between the two networking Equipments. If the distance is more than 100 meters, then this cable is chosen. For distance between 100 meters to 2 KMs, Multimode Fiber optic cable is chosen and beyond that single mode cable is selected. Following Table provides an overview of Fiber cable selection i/c connector type as per application.

Fiber Type	No. of Fibers	Typical Applications	Connector or Type	Connector Image
Single mode /Multimode	1	LANs	ST	
Single mode /Multimode	1	Data/Tele-communications	FC	
Single mode /Multimode	1	CATV, Test Equipment	SC	
Single mode /Multimode	1	Gigabit Ethernet, Video Multimedia	LC	
Single mode /Multimode	2	Gigabit Ethernet, Asynchronous Transmission Mode (ATM)	MT-RJ	

CAT Cables

Following Table gives Overview of Data Rate and application of different CAT cables:

UTP Category	Data Rate	Max. length up to which used	Cable Type	Application
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Upto 10Mbps	100m	Twisted Pair	Token Ring & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Upto 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, GigabitEthernet

CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10g Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10g Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10g Ethernet (100 meters)

Connector Specifications

These include physical construction, wiringand signal semantics. Accordingly, different connectors are specified. For example, Registered Jacks are primarily named by letters RJfollowed by two digits that express type.Additional letter suffixes minor variations. Selection of connector is based on application,cable type and I/O Port.

Rack/Cabinet Specifications

There are three types of rack/cabinetfor housing various electronic switches and systems used in networking:

1. Solid-walled cabinets with a roof fan tray (for bottom to top cooling)
2. Standard open rack
3. Standard perforated cabinet.

Rack Size

The rack unit size is based on a standard rack specification as defined in EIA-310 where EIA stands for Electronic Industries Alliance. The standard was adopted worldwide as IEC 60297 Mechanical structures for electronic equipment. It defines the sizes for rack.

Generally, width of the Rack is defined in terms of inches while its height is defined in multiples of 1U or 1RU which isRU(rack unit) and is defined as 1 3⁄4 inches (44.45 mm). However,a front panel or filler panel in a rack is not an exact multiple of this height to allow space between adjacent rack-mounted components.A panel is 1⁄32 inch (0.03125 in or 0.794 mm) less in height than the full number of rack units would imply. Thus, a 1U front panel would be 123⁄32 inch (1.71875 in or 43.66 mm) tall. If n is number of rack units, the ideal formula for panel height is h = (1.75n − 0.031) for calculating in inches, and h = (44.45n − 0.794) for calculating in millimeters. Normally the height of a Rack used in network/server room is 7 feet but it can be more depending upon the ceiling height of the room and requirement.

Normal width of the front side of the Rack is 19 inch(which isa standardized frame or enclosure for mounting multiple electronic equipment modules) or 23 inch which includes the edges or "ears" that protrude from each side of the equipment, allowing the module to be fastened to the rack frame with screws.

The Rack is having four sides to accommodate switches and other Equipments which have sufficient depth. So, four post Racks are used to accommodate network switches and other Equipments.

Four-post EIA cabinets (perforated or solid-walled)

It must meet the following requirements:

The minimum spacing for the bend radius for fiber-optic cables should have the front-mounting rails of the cabinet offset from the front door by a minimum of 3 inches (7.6 cm).The distance between the outside face of the front mounting rail and the outside face of the back mounting rail should be 23.0 to 30.0 inches (58.4 to 76.2 cm) to allow for rear-bracket installation.

Common uses include computer servers, telecommunications equipment and networking hardware, audiovisual production and scientific equipment.

Requirements Specific to Standard Open Racks

If the chassis is mounted in an open rack (no side panels or doors), the minimum vertical rack space per chassis must be two rack units (RUs), equal to 3.5 inches (8.8 cm) and the distance between the chassis air vents and any walls should be 2.5 inches (6.4 cm).

Requirements Specific to Perforated Cabinets

A perforated cabinet has perforations in its front and rear doors and side walls.

The front and rear doors must have at least a 60 percent open area perforation pattern, with at least 15 square inches (96.8 square cm) of open area per rack unit of door height.The roof should be perforated with at least a 20 percent open area.The cabinet floor should be open or perforated to enhance cooling.

Section 6
System Engineering

The system engineering or engineering management is to focus on designing the system, integrating it with the other disciplines of engineering and maintaining it over the complete life cycle.

Designing the system

When designing a networking system, it is important to select the proper hardware to meet current network requirements, as well as allow for future growth. Within an enterprise network, both switches and routers play a critical role. This selection is a very complex task due to ever-growing scope of network services along with the faster up gradation of technology. It also requires an in-depth analysis of user's requirements vis-a-vis the available technology.

For designing the system, it should be segregated into two parts namely Active components and Passive Components. However, the most challenging part is design of Active Components because of the maximum impact of technology up-gradation.The active components constituteall networking Equipments like Routers, Core Layer including Distributors, Network Switches, Firewall etc. All these are mounted on a Standard Rack while Patch panel, Scanner for monitoring patch panel, Cable Manager etc. are mounted on Passive Rack. The Active and Passive Racks are connected together through cabling and Equipments inside the Active and Passive Racks are also joined together by suitable cabling and jumpers.

For appropriate design of the active system, first of all, commensurate with the requirement of client,all available technologies should be studied first.The most appropriate technology should be selected then based on the available inputs.

For data connectivity in a building to be constructed, functionality requirements, type and speed of data flow, number of floors, floor-wise connectivity matrix, level of data security, redundancy requirements, voice communication facility over data network, bandwidth requirement, attenuation of signals etc. are some of the prime design factors. Based on these factors, designing of data networking is undertaken.

Functional Requirements of the NOC

Supervision, Management and monitoring of the Network, Databases, firewalls, connecting devices etc. are the functional requirements of NOC. Some of the key network operation activities are:

1. Network Monitoring- It is a critical IT process where all networking components like routers, switches, firewalls, servers etc. are monitored continuously to maintain and evaluate their continuous availability.One important aspect of network monitoring is its proactiveness which identifies issues at the initial stage itself to prevent network downtime or failures.

2. Incident Management- It includes Threat Analysis & Intrusion Prevention Systemwhich calls for actual response to incidence threats, their analysis and preventionfor the safety of data networks. Thus, identification, analysis and correction of hazards including prevention are the main activities of Incident Management.

3. Network Performance- NetworkOptimization and Quality Reporting are parts of Network Performance. The process of visualizing, monitoring, optimizing, troubleshooting and reporting on the service quality of network as experienced by usersare important functions and include a set of best practices to improve network performance. A variety of tools and techniques can be used to achieve it like global load balancing, minimize latency, packet loss monitoring and bandwidth management etc.

4. Patch Management- Here system patches are monitored and a decision is taken whether these are needed or not. In case these are needed; they are installed and implemented smoothly. Patch management fixes vulnerabilities on the software and applications which are susceptible to cyber attacks. It also ensures software and applications are kept up-to-date and run smoothly, supporting system uptime.

5. Back-up and Storage-Data back-up is necessary to restore the originaldata after a data loss. There are different types of data storage devices used for keeping data back-up.Sometimes, this function is done in NOC and sometimes in Cloud.

6. Firewall Management- Firewall, a network security system monitors and controls incoming and outgoing network traffic based on pre-decided security rules.

Architecture of NOC

Based on the above functional requirements, architecture of NOC isdecided.Three layer architecture consisting of Core Layer, Distribution Layer and Access Layer are provided. Firewall and allied services with redundancy at each level, to keep network uptime 99.999% is considered. The redundancy is maintained by keeping the switches in High availability mode.

One of the various typical schemes of Network services is described below for the sake of understanding the scheme of networking .

Active Rack

The WAN Link which is provided by fiber optic cable from network service provider comes to the NOC room and connects to the Router. The core switch, distribution switch apart from various systems like network monitoring, Network optimization, performance monitoring etc. are also housed here.For Firewall Management, separate equipment is placed on the active rack with suitable connections. Scanner required for monitoring network components and other functions is also provided in the Active Rack.

Figure 37: View of Active Rack

Passive Rack
It contains all the connections brought from the Access Switches which are provided at each floor. These cables are terminated into Patch Panel.Patch Panel and Cable Manager can also be the part of active Rack.

Patch Panel
It is a requirement of big networks.It acts as a passive networking hub that bunches multiple ports together connecting incoming and outgoing lines and facilitates in providing proper connections between server and network switch and from network switch to computers and other devices.

Figure 38:12 port Patch Panel with Outgoing connections

Cable Manager
It manages the electrical or optical cable in the rack for ease of termination and installation.

Figure 39:Cable Manager

In addition, Floor Racks should also be designed along with Gang boxes and cable laying upto the end point.

Thus, based on the functional requirements of data and communication Network, the line diagram and BOQ is envisaged.

Integrating the System

Next step is to integrate the system with the building design/services layout so as to have the best coordination among various agencies. Normally, fiber optic cable is used for long distance travelling of the data. So, from the NSP/Data Center, connectivity is through optic fiber cable with enough redundancy to avoid any disruption of services.For cabling, suitable ducts, conduiting inside the wall and above false ceiling and Gang boxes are provided which should be well integrated with the building layout. These should not interfere with other services and should be planned accordingly.

Maintaining the system

Maintenance is the key requirement of any asset.It is required to be carried out throughout the life cycle of the building because number of people working in a building change besides changes of layout in various spaces and other changes required on account of changed circumstances etc. A proper maintenance with the objective to reduce the downtime dictates that there should be enough redundancy in the system and availability of those spare parts which are frequently needed.Redundancy in the system minimizes the requirements of breakdown maintenance. Faults in the main Equipments also necessitate upkeep and maintenance. Recording of Fault types and their analysiscan help in reduction of downtime.

Section 7

Standardsfor data networks

Networking Standards define the rules of communication among networked devices by making possible for different manufacturers' network components to work together.

IEEE 802

It is a family of IEEE(Institute of Electrical and Electronics Engineers) standards dealing with local area networks .The number "802" has no particular significance.It was simply the next available number IEEE could assign.The services and protocols specified in IEEE 802 map to the lower two layers (Data Link and Physical) of the seven-layer Open Systems Interconnection (OSI) networking reference model.

Following table provides an overview of the various IEEE standards:

Name	Description	Status
IEEE 802.1	Higher Layer LAN Protocols Working Group	Active
IEEE 802.3	Ethernet	Active
IEEE 802.11	Wireless LAN (WLAN) & Mesh (Wi-Fi certification)	Active
IEEE 802.13	Unused	reserved for Fast Ethernet development
IEEE 802.15	Wireless PAN	Active

Standard for Rack

EIA-310 where EIA stands for Electronic Industries Alliance. The standard was adopted worldwide as IEC 60297 Mechanical structures for electronic equipment. It defines the sizes for rack.

Standard for Fiber Optic Cable

IEC 60793 defines parameters of Optical Fiber cables and optical fibers. IEC 60793-2-10 is applicable to multimode optical fiber type while IEC 60793-2-50 is applicable to single-mode 9/125 optical fiber types B1.

Standard for Cat 5e and 6 cables

TIA/EIA cable standards have been developed by the Telecommunications Industry Association (TIA) and Electronic Industries Alliance (EIA).

TIA/EIA-568 establishes widely employed telecommunications cable standards that support interoperability.

Part of the 568 standards for Cat5e cable and other twisted-pair cabling is the 568A and 568B wiring schemes which specify pin and pair assignments. The schemes define the process of UTP cable terminations. Each wiring pair corresponds to an assigned color during terminations, as in pair 3 to the green on a patch panel or jack. Cat5e cable is connected using the 8P8C modular connectors with terminations in a T568A or T568B scheme.

The 568B standard sets minimum requirements for various categories of cabling, such as Cat5e with performance up to 100 MHz, Fast Ethernet, and Gigabit Ethernet. The TIA/EIA requirements for Category 5e cable are higher than those of basic Cat5. Category 6 and 6a cables deliver performance up to 250 MHz, Fast Ethernet, Gigabit Ethernet and 10-Gigabit Ethernet.

Section 8

Glossary

A

ASIC- Application specific Integrated Circuitis an integrated circuit (IC) chip customized for a specific use, rather than intended for general-purpose use.

B

Border Gateway Protocol (BGP)-is one of the key protocols used to achieve Internet connection redundancy.

Bridge- a computer networking device that creates a single aggregate network from multiple communication networks or network segments. This function is called network bridging. Bridging is distinct from routing.

C

Cable-Networking hardware used to connect one network device to other network devices or to connect two or more computers to share printers.

Connector-a device that terminates a segment of cabling or provides a point of entry for networking devices such as computers, hubs, and routers.

Content-any information that is available for retrieval by the user, including Web pages, images, music, audio, white papers, driver and software downloads as well as training, educational and reference materials.

Computing-any activity that uses computers to manage, process, and communicate information. It includes development of both hardware and software. Computing is a critical, integral component of modern industrial technology.

Cyber Security- It is the protection of computer system or networks from the theft or damage to their hardware, software, electronic data or misdirection of any of their services.

D

Data- Distinct pieces of information formatted in a special way.

Database- Organized Collection of information for easy access, management and updation.

Data Link Layer-The data link layer, or layer 2, is the second layer of the seven-layer OSI model of computer networking. This layer is the protocol layer that transfers data between adjacent network nodes in a wide area network or between nodes on the same local area network segment.

Device- An object used for a particular purpose.

DHCP - It is a network management protocol used on Internet Protocol networks. The elongated form of DHCP is Dynamic Host Configuration Protocol. It automatically provides and assigns IP addresses ,default gateways and other network parameters to client devices.

DNS- Domain Name System is full form of DNS and is known as phonebook of the Internet.

DSL- DSL. Stands for "Digital Subscriber Line." DSL is a communications medium used to transfer digital signals over standard telephone lines.

E

Electrostatic flooring- It protects electronics from damage caused by static electricity, which accumulates as people walk.

Ethernet- A system for connecting number of computer systems to form a Local Area Network with protocols to control passing of information and to avoid simultaneous transmission by two or more systems.

EPABX- A multiline business telephone system.

F

Fiber Optic-A flexible, transparent fiber made by drawing glass or plastic to a diameter slightly thicker than that of a human hair.

File and Directory-A file is a collection of data that is stored on disk and can be manipulated as a single unit by its name while a directory is a file that acts as a folder for other files.

Firewall-a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

G

Gateway- a piece of networking hardware used in telecommunications for telecommunications networks that allows data to flow from one discrete network to another.
Gigabit - A gigabit is very similar to a gigabyte, since they both represent a unit of measurement for digital storage space. One gigabit is equal to 1,000,000,000 bits. The symbol of a gigabit is G. However, a bit is eight times smaller than a byte, which means a gigabit is eight times smaller than a gigabyte.

H

Hacking-Exploring methods for breaching defenses and exploiting weaknesses in a computer system or network.

Hardware-It refers to the physical elements of a computer/Network.It provides support for major functions such as input, processing (internal storage, computation and control), output, secondary storage (for data and programs), and communication.

I

Internet- It is a computer network on the global level. The purpose is to provide a variety of information and communication facilities. This is obtained through interconnected networks using standardized communication protocols.

Internet Protocol- The Internet Protocol abbreviated as IP is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.

IPv4- It is the fourth version in the development of Internet Protocol. It is being used now. IPv6- It is the most recent version of Internet Protocol providing an identification and location system for computers on networks. It also routes traffic across the Internet.

J

Jack-An Ethernet port also called a jack or socket.Itis an opening on computer network equipment that Ethernet cables plug into. The purpose is to connect wired network hardware in an Ethernet

LAN, metropolitan area network (MAN), or wide area network (WAN).

Jumper- A short length of conductor used to close, open or bypass part of an electronic circuit. They are typically used to set up or configure printed circuit boards, such as the motherboards of computers. The process of setting a jumper is often called strapping.

L

Leased line- A leased line is a private telecommunications circuit between two or more locations provided according to a commercial contract. Typically, leased lines are used by businesses to connect geographically distant offices.

M

MAC Address-. It is media access control address and is a unique identifier assigned to a network interface controller for use as a network address in communication within a network segment.

Mainframe-computers used primarily by large organizations for critical applications; bulk data processing, such as census, industry and consumer statistics, and enterprise resource planning; and transaction processing.

Modem- A linguistic blend of "modulator-demodulator"Monitoring. It is a hardware device that converts data into a format suitable for a transmission medium so that it can be transmitted from one computer to another (historically along telephonewires).

Multihoming- When a network is connected to two different ISPs, it is called multihoming. Multihoming provides redundancy and network optimization.

Multimedia- A content that uses a combination of different content forms such as text, audio, images, animations, video and interactive content. Multimedia contrasts with media that use only rudimentary computer displays such as text-only or traditional forms of printed or hand-produced material.

N

Network-a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to one another to allow the sharing of data. An example of a network is the Internet, which connects millions of people all over the world.

Network Layer- It provides the functional and procedural means of transferring variable length data sequences (called packets) from one node to another.

Network switch-It is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device.

NTP(Network Time Protocol)-for clock synchronization between computer systems over packet-switched, variable-latency data networks , this networking protocol is used.It is one of the oldest internet protocol still in use today.

O

OSI Model-Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.

P

Patch Cord- A patch cord, patch cable or patch lead is an electrical or optical cable used to connect one electronic or optical device to another for signal routing. Devices of different types are connected with patch cords.

Patch Panel-A device or unit featuring a number of jacks, usually of the same or similar type, for the use of connecting and routing circuits for monitoring, interconnecting, and testing circuits in a convenient, flexible manner.

Peripheral-A peripheral or peripheral device is ancillary device used to put information into and get information out of the computer.

Port- is a communication endpoint.

Protocol- A set of rules or procedures for transmitting data between electronic devices such as computers.

Python- It is a programming language and used as a scripting language for web application.

Q

Queue- A linear structure which follows a particular order in which the operations are performed. The order is First In First Out (FIFO). A good example of a queue is any queue of consumers for a resource where the consumer that came first is served first.

R

Rack-is a metal frame chassis that holds, stacks, organizes, secures and protects various computer network and server hardware devices. The term "network" refers to the rack being used to house network hardware like routers, switches, access points, and modems

Router-The main purpose of a router is to connect multiple networks and forward packets destined either for its own networks or other networks. A router is considered a layer-3 device because its primary forwarding decision is based on the information in the layer-3 IP packet, specifically the destination IP address.

S

Server- A server is a computer that provides data to other computers.

STP-a type of copper telephone wiring in which each of the two copper wires that are twisted together are coated with an insulating coating that functions as a ground for the wires. ... STP cabling often is used in Ethernet networks, especially fast data rate Ethernets.

T

Telecommunication-Exchange of signs, signals, messages, words, writings, images and sounds or information of any nature by wire, radio, optical or other electromagnetic systems. Telecommunication occurs when the exchange of information between communication participants includes the use of technology.

U

URL- It is abbreviated form of Universe Resource Locator which is also known as web address.

UTM(Unified Threat Management)- It is a combined approach to information security where a single hardware or software installation provides multiple security functions in contrast to the traditional method of having point solutions for each security function.

UTP-Unshielded twisted pair (UTP) is a ubiquitous type of copper cabling used in telephone wiring and local area networks (LANs).

V

VoIP- It is an acronym for Voice over IP. It is the transmission of voice and multimedia content over Internet Protocol Networks. This term is also used for IP telephony.

VPN-virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks

W

Wireless Communication- a method of transmitting information from one point to other, without using any connection like wires, cables or any physical medium.

Z

ZTP-Short form of Zero touch provisioning, it is designed to provide the intelligence needed to allow the switch to boot with minimal disruption to the network. It is the feature of a network switch that allows the devices to be provisioned and configured automatically, eliminating most of the manual labor involved with adding them to a network.

References

https://www.google.com/search?q=networking etc.