# Installation of Surveillance Cameras in Katara Park

## A Project Report

Submitted in Partial Fulfillment of the Requirements for the Award of the Degree of

## Bachelor of Technology

*In*

**Computer Science & Engineering**

*Submitted by*

**Shefali Mohapatro**

Roll no. 1606022

*Under the Supervision of*

**Dr. M. T.U Haider**

Associate Professor

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**

NATIONAL INSTITUTE OF TECHNOLOGY PATNA

PATNA- 800005

June 2020


**NATIONAL INSTITUTE OF TECHNOLOGY PATNA**

(An Institute under Ministry Of HRD, Govt. of India)

ASHOK RAJPATH, PATNA-800005 (BIHAR)

# Certificate

This is to certify that this is a bonafide record of the project entitled "**Installation of Surveillance Cameras in Katara Park**". It is presented Shefali Mohapatro Roll no. 1606022 during their 8th Semester Major Project under the supervision of Dr. M. T.U Haider in partial fulfillment of the requirements of the degree of Bachelor of Technology in Computer Science and Engineering.

**Dr. M. T.U Haider**
Associate Professor
CSE Department
NIT Patna

**Dr. J.P. Singh**
Head of Department
CSE Department
NIT Patna

# Declaration

I hereby declare that the project work entitled " **Installation of Surveillance Cameras in Katara Park**" is an authentic record of my work carried out at National Institute of Technology Patna as a requirement for Major Project in 8th Semester for the award of degree of Bachelor of Technology in Computer Science and Engineering at National Institute of Technology Patna, under the supervision of Dr. M. T.U Haider, Associate Professor, Department of Computer Science and Engineering, National Institute of Technology Patna. I affirm that this work has bot been submitted anywhere for considerable.

Signature

Shefali Mohapatro
1606022

Place: Patna

# Acknowledgement

I would like to acknowledge those who pitched in to push this project over the finish line. I am deeply indebted to **Dr. M. T.U Haider,** for his kind supervision and guidance. He has helped us a lot by giving his precious time in upbringing the project report. I also extend my gratitude to all my colleagues and all the professors of Computer Science & Engineering Department.

I express my sincere thanks to **Dr. J. P. Singh,** Head of Department, Computer Science& Engineering Department, for making every possible arrangement for helping us complete the Major Project.

I am thankful to **Prof. Pradip Kumar Jain,** Director, NIT Patna for providing the student with a friendly environment, Wi-Fi facility and well-maintained Library in the institute.

Signature
Shefali Mohapatro
1606022

INFORMATICA
QATAR

انفـــــورماتيكـا
قطر

Reference No.: IQ/HRA/HRD/EXT/2020-0085

**CERTIFICATION FOR INTERNSHIP**

This is to certify that Miss Shefali Mohapatro, holder of Indian Passport No. R8245111, held the position of Networking Engineer Intern from 10 January up to 10 May 2020.

This certification is being issued upon the request of Miss Shefali for whatever legal purposes it may serve her.

Issued this 27th day of May 2020 at Doha, Qatar.

Certified by:

Wisam Costandi
Managing Director

TEL. +974.4431.3597
FAX. +974.4431.7760
P.O.Box 23604 - DOHA - QATAR

هاتف +٩٧٤٤٤٣١٣٥٩٧
فاكس +٩٧٤٤٤٣١٧٧٦٠
ص.ب ٢٣٦٠٤ الدوحة - قطر

# Contents

# ABSTRACT

During the course of my internship from 10th January 2020 to 10th May May 2020 at Informatica Qatar, I was a part of the networking team of the company. The main and the base work were done by us.

Dealing with the client needs accordingly creating the whole layout virtually before doing it manually.connecting the whole devices as per required and making them work efficiently. Uniquely providing each device with a unique IP address.

The configuration of the layout was first virtually done in Cisco packet tracer.Then the later steps were proceeded.

# ABOUT INFORMATICA QATAR

Informatica Qatar(iQTM) is a technology Solutions, Device Provider and IT consulting Firm that offers innovative and high quality systems integration solutions.

Standing on a solid ground of consumer market experience, they adopt a well defined channel strategy empowered by our premium channel partners base and well tuned retail engine.

With their extensive experience in big four consulting firms and Start-Ups, they have a wealth knowledge from Silicon Valley and an insight into the latest technologies and business processes.

They have various partnership with various companies.

# CHAPTER 1

# INTRODUCTION

## 1.1. Basic Networking Knowledge

**Hub:**

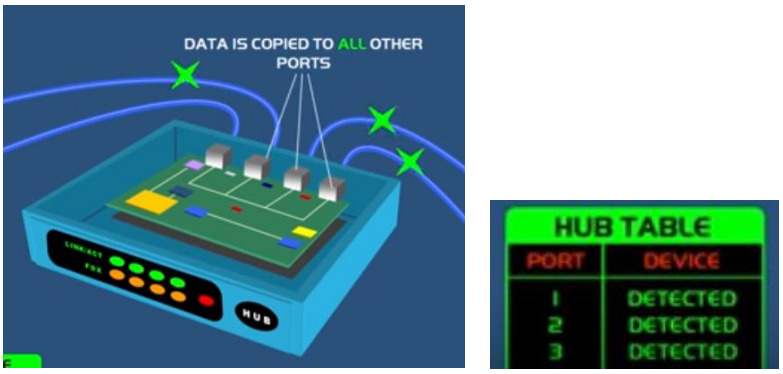



**Figure 1.1. HUB [3]**

The purpose of hub is to connect all your network devices together on an internal network.
Doesn't filter any data or has any intelligence where the data is supposed to be sent.
It only knows when a device is connected to one of its port, and broadcasts to all other connected devices.
Traffic in network, and wastes bandwidth.

**Switch:**

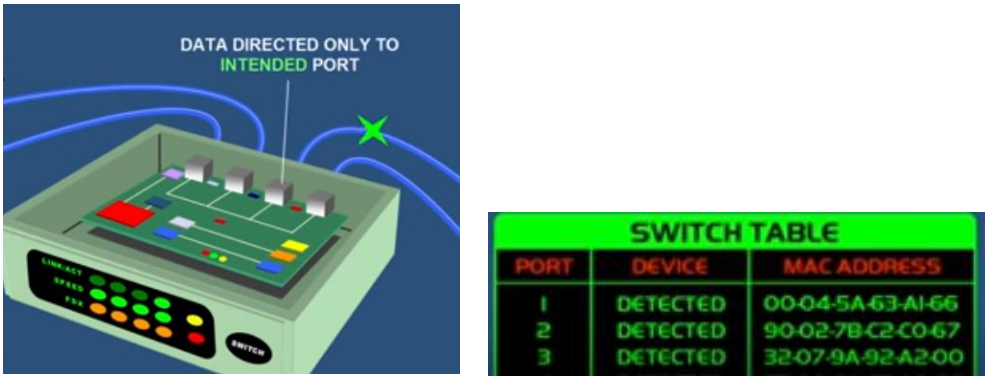



**Figure 1.2. SWITCH [3]**

Switch is intelligent which can learn the physical addresses of the devices that are connected to it and it stores its physical address(MAC address).
When data packet send, its only directed to the intended destination port.

**HUBS & SWITCHES** are used to exchange data within local area network, not used to exchange data outside their own network.
To exchange data outside their own network a device needs to be able to read the ip addresses

**Router:**

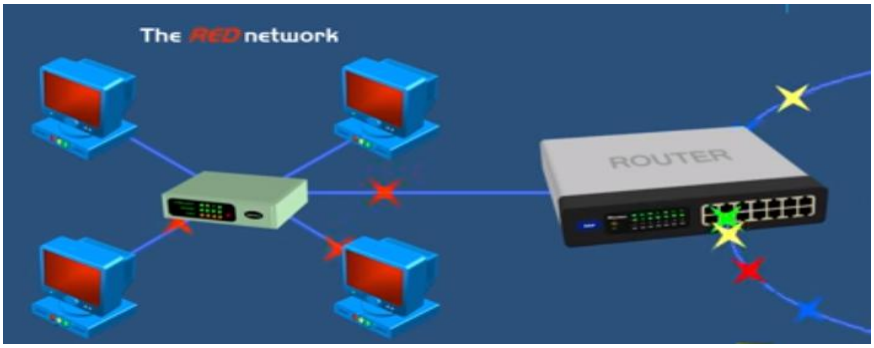



**Figure 1.3. ROUTER [3]**

Routes data from one network to another based on their ip address.
Is the gateway of the network

## 1.1.1. OSI( Open System Interconnection Model)

How data is transferred from one computer to another?
Systems with different architecture how is data being transferred?

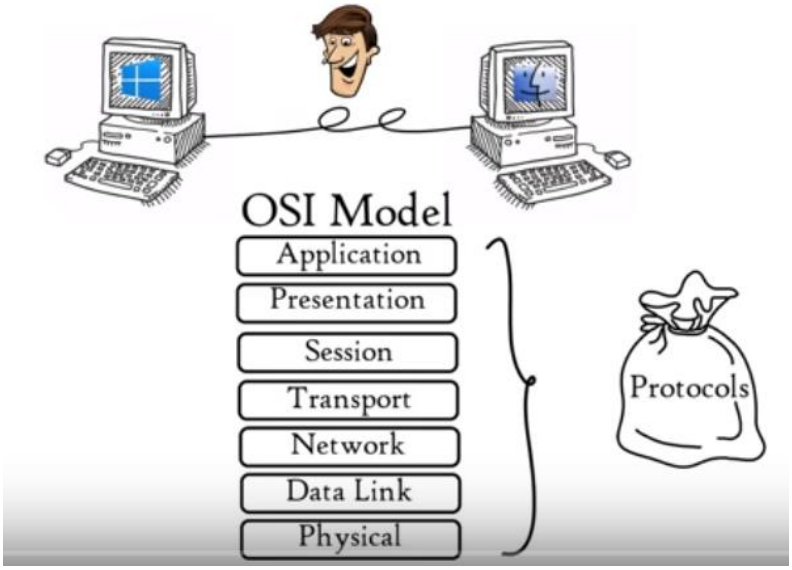



**Figure 1.4. OSI MODEL [3]**

**Application Layer:**

Provide services to Network applications.
Uses protocols that is used by chrome, Firefox, etc to work correctly in network.


**Figure 1.5. Application Layer [3]**

**Presentation Layer:**

Receives data from the application layer, in form of character and numbers.
Presentation layer converts these characters and numbers to machine understandable binary numbers.
Then the converted binary numbers are compressed and it can be lossy or lossless(Data transfer is faster).
Then they are being encrypted for further use.

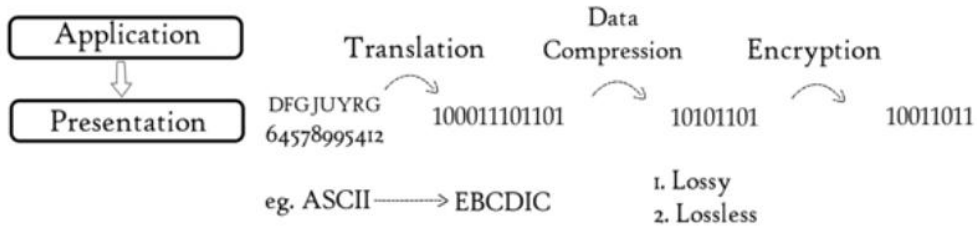



**Figure 1.6. Presentation Layer [3]**

**Session Layer:**

Setting up and managing connections enabling sending and receiving of data.
Has API's for managing.

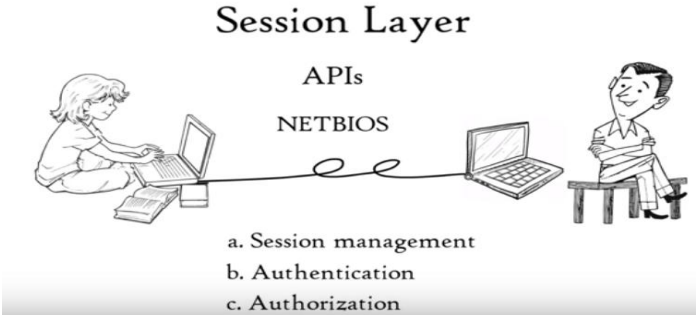



**Figure 1.7. Session Layer [3]**

**Transport Layer:**

Controls the reliability of communication through SEGMENTATION, FLOW CONTROL & ERROR CONTROL.

Segmentation:

The data received is divided into small units named as segments, each segment contains sequence no. And destination port no.
Port no. to correctly direct to the given application.

Sequence no. to reassemble the sequence in the correct order.

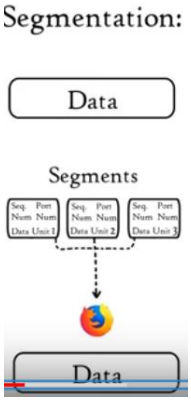



**Figure 1.8. Transport Layer [3]**

Flow Control:

Controls the amount of data to be transmitted. So that no data gets lost

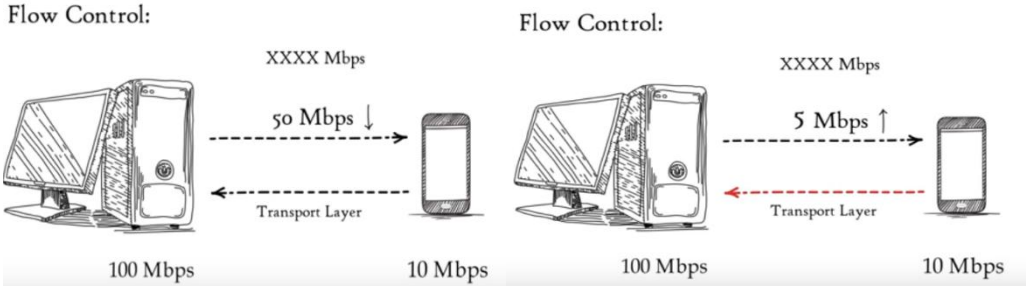



**Figure 1.8. Transport layer -> Flow Control [3]**

Error Control:

If some data doesn't arrive the destination, Automatic Request Repeat schemes are used to resend the data.

A group of bits known as checksum is added to each segment, to check the received corrupted Signal.

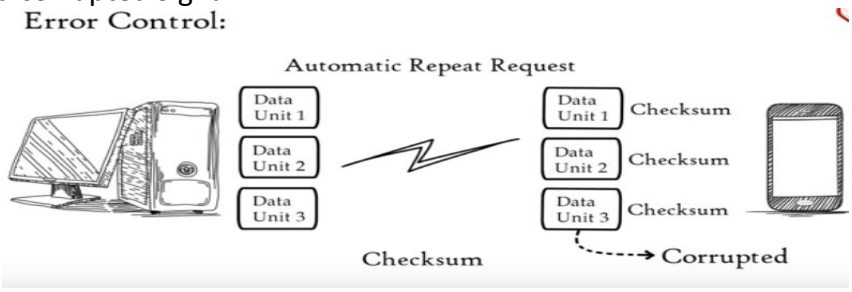



**Figure 1.9. Transport layer -> Error Control [3]**

Transport layer has 2 protocols

1. TCP (Transmission Control Protocol)
   Connection Oriented transmission
   Lost data is re-transmitted as it sends a feedback.
   Eg. Email, www
2. UDP (User Datagram Protocol)
   Connectionless Transmission.
   Faster than TCP, as no feedback is provided.
   Eg. Movies, Songs, Games

**Network Layer:**

Transport layer sends the data segments to the network layer, network layers works for the transmission of the data segments from one computer to another in different network.

Data units are known as packets.

This is the layer where Routers reside.

Logical Addressing:

IPV4, IPV6

Every computer in network,has an unique IP address. Network layer assign senders and receivers

IP address to each segment to form an packet.

To ensure that each packet reaches the correct destination.

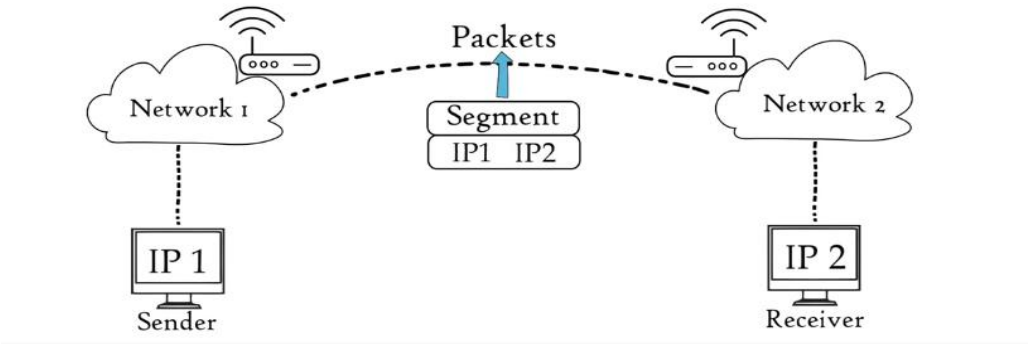



**Figure 1.10. Network Layer [3]**

Routing:

Is a method to move data packets from source to destination.

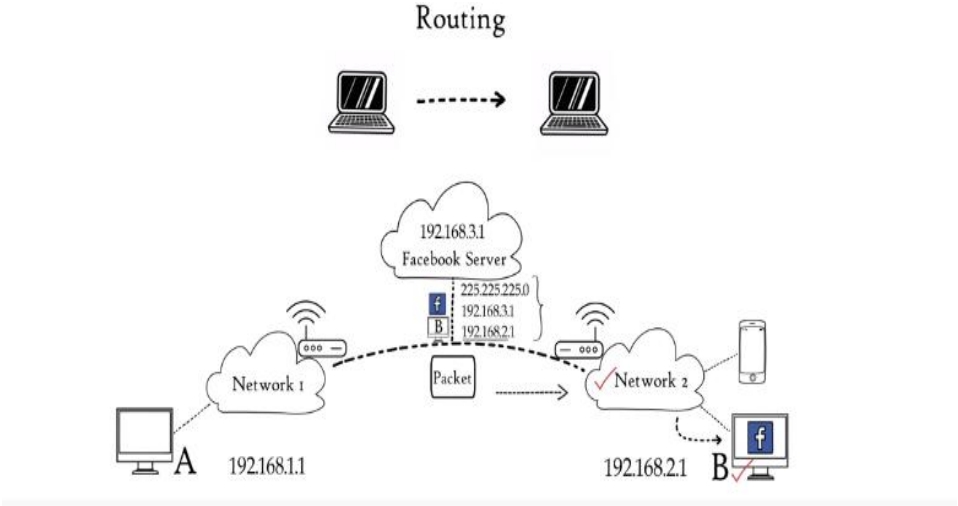



**Figure 1.11. Network Layer -> Routing [3]**

Path Determination:

A computer can be connected to an internet server in a number of ways, choosing the best possible path for the delivery of packets from sender to receiver.

Eg. OSPF, BGP

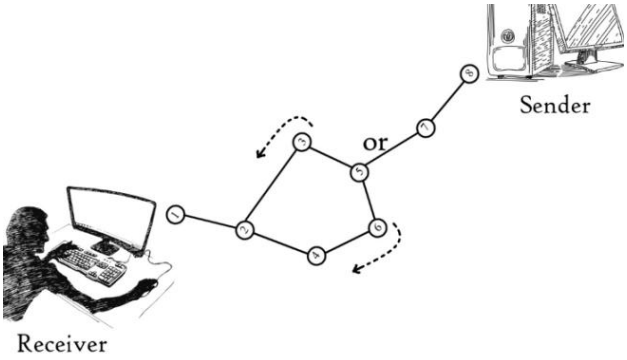



**Figure 1.12. Network Layer -> Path Determination [3]**

**Data Link Layer:**

Physical addressing is done at data link layer where MAC address(embedded in NIC) of the sender and receiver is also included to the data packet to form a frame.

The data packet consists of IP addresses of both he sender and receiver.

Control how data is placed received from media.

Eg. Media access control, Error Detection

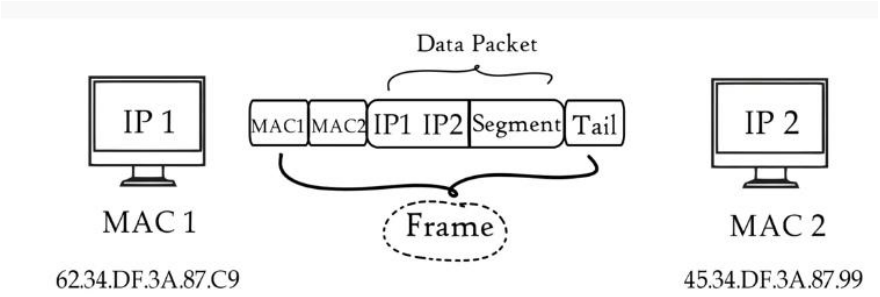



**Figure 1.13. Data Link Layer [3]**

Access to Media:

Done by framing in the whole network connection it decides which data to be transmitted to which device.

The data packets is being framed continuously due to different devices being connected to it.

In this process, encryption and decryption is ongoing.

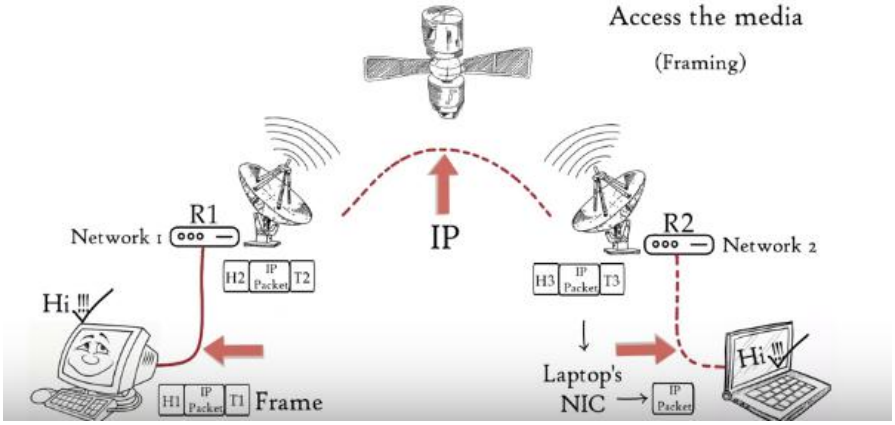



**Figure 1.14. Data Link Layer -> Access to Media [3]**

Control how data is placed received from media:

Number of devices connected to a same media, if the devices sends message during the same time, garbage is being sent to the receiver, which is not understandable
Checks the medium, when free allows data transmission.

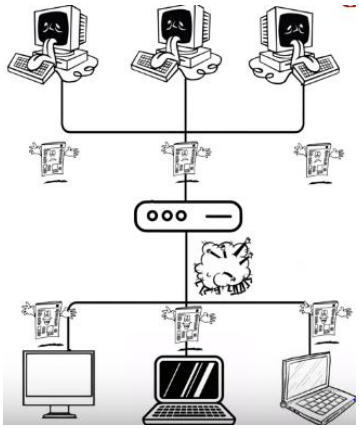


**Figure 1.15. Data Link Layer -> allows free data to transmit [3]**

**Physical Layer:**

The data received by the data link layer is in a sequence of binary 0s 1s, physical layer converts it into a signal electrical signal(copper), light signal(optical fiber), etc.
Signal depends upon the media it transfers through.
The same reverse process occurs, and using the application layers protocols the data is received.

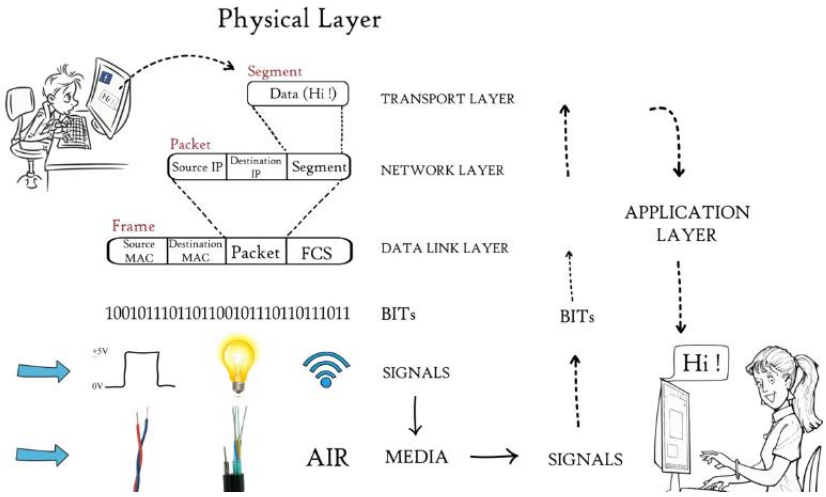



**Figure 1.16. Physical Layer [3]**

## 1.1.2. TCP/IP(Transmission Control Protocol/Internet protocol)

4 layer architecture
Used in current internet architecture

But OSI is 7 layer architecture

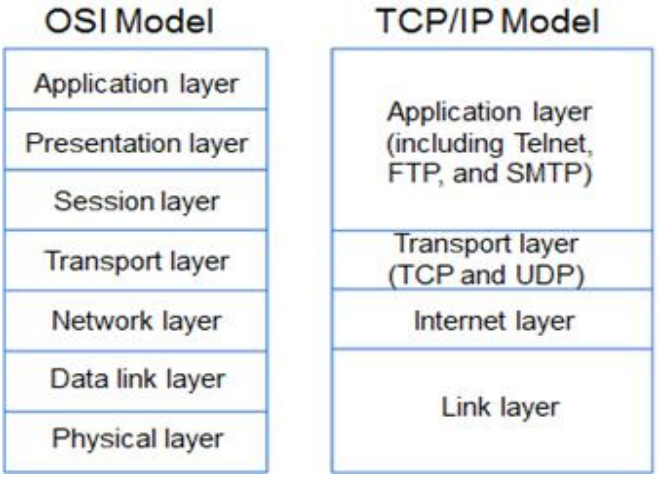



**Figure 1.17. TCP & OSI model relation [9]**

Its the same as OSI model

The 1st layer Application Layer of TCP/IP includes Application layer, Presentation Layer, Session layer of the OSI model.

The 2nd layer Transport Layer of TCP/IP is the same as OSI model.

The 3rd layer Internet Layer of TCP/IP is the same as OSI model.

The 4th layer layer of TCP/IP included Data link layer and Physical Layer of the OSI model.

**Difference between TCP/IP & OSI models**

| TCP/IP | OSI |
|---|---|
| Has 4 layers architecture. | Has 7 layer architecture. |
| Is a client-server model used for transmission of data over the internet. | It is a theoretical model which is used for computing system. |
| Protocol Dependent. | Protocol Independent. |
| More reliable. | Less reliable. |
| Implementation of OSI model. | Reference model. |
| Supports only connectionless communication in the network layer. | Supports only connectionless and connection oriented communication in the network layer. |
| Protocols were developed first and then the model was developed. | Model was developed before the development of protocols |

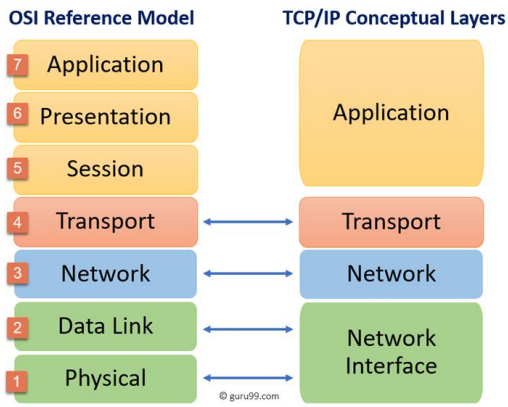



**Figure 1.18. TCP & OSI model relation [9]**

## PROTOCOLS of the Layers

### Application Layer:

**FTP(File Transfer Protocol):**

Standard protocol that is used to transfer files between computer and servers over a network

It is a mechanism provided by TCP/IP for copying a file from one host to another.

It establishes 2 connections Data Transfer(Open & close for each file transfer) & Control

Information(remains connected throughout the session).

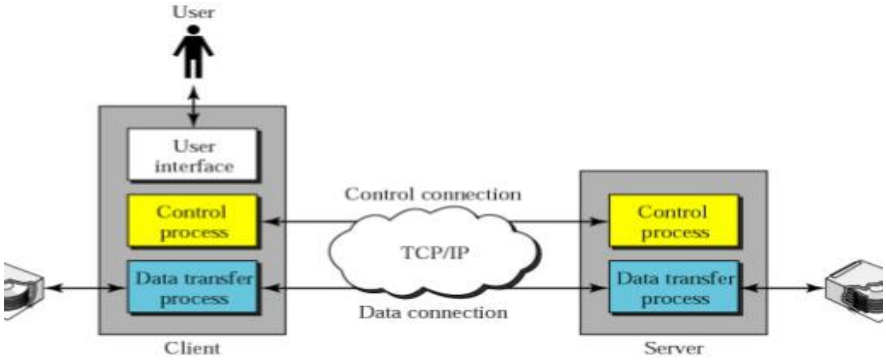



**Figure 1.19. FTP [3]**

User interface interacts with the user.

Control Process, control connection is established.

Then the Data Transfer connection is established. It is connected to the disk as the data is stored in the disk.

It has 2 types of connection.

1. Communication over control connection
   Established due to NVT ASCII
2. Communication over data connection.
   Along with the data File type, data structure and transmission mode[stream mode, block
   mode,compressed mode].

**SMTP(Short Message Transfer Protocol):**

Is a protocol that defines MTA client & Server in the internet.

SMTP is used from senders agent to receivers mail server[used for pushing the message].

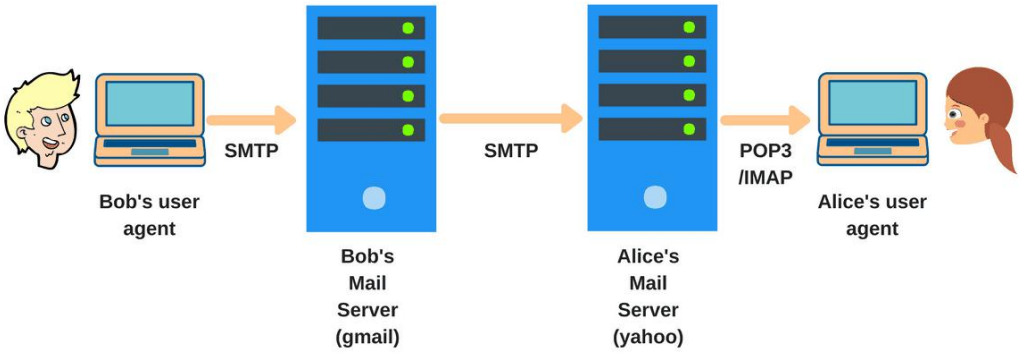



**Figure 1.20. SMTP [3]**

From receivers mail server to receivers agent POP3 or IMAP protocols are used[used for pulling the message].

SMTP uses commands and responses to transfer message between an MTA client and MTA
server.

| POP3 | IMAP |
|---|---|
| Post Office Protocol Version 3 | Internet Mail Access Protocol Version |
| Only allows downloading messages from your inbox to your local computer. | Much more advanced ad allows users to see all the folders on the mail server |
| Can only be accessed from a single device at a time. | Messages can be accessed from multiple devices. |
| User cannot arrange the mails in the mailbox of the mail server. | The user can organize the emails directly in the mail server. |
| The user cannot rename, create, delete emails on the mail server. | The user can create, delete or rename emails directly on the mail server. |
| Cannot search the content of the mail before downloading to the local system. | A user can search the content of mail for specific string before downloading. |
| All messages are downloaded at once. | Message header can be viewed before downloading. |

MIME(Multipurpose Internet Mail Extensions):

It is supplementary Protocol that allows non-ASCII data to be sent through email.

Travels the data in NVT 7-bit ASCII format.

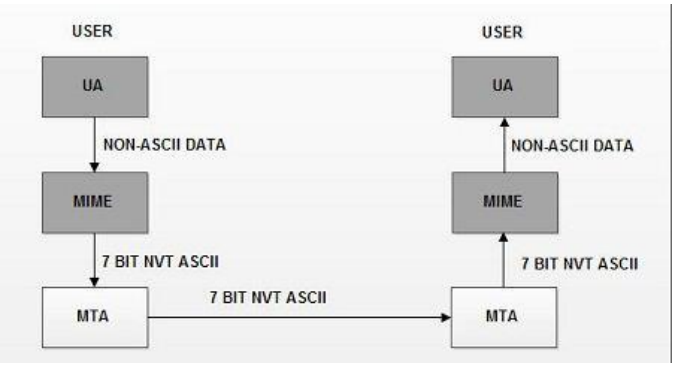



**Figure 1.21. MIME [10]**

Mime header is added to the original email header section

**DNS(Domain Name System):**

Is used to map an alias address to the IP address.

Previously it was easy to access the IP address, Give the alias(website) name and the Table of stored records returned the IP address of that alias.

As the number of websites increased to maintain the records within a single table became impossible.

The idea opted was to divide this huge amount of information into smaller parts and store each part on different computer. Now when the hosts needs the mapping it can contact the closest computer holding the information. This is the DNS method.

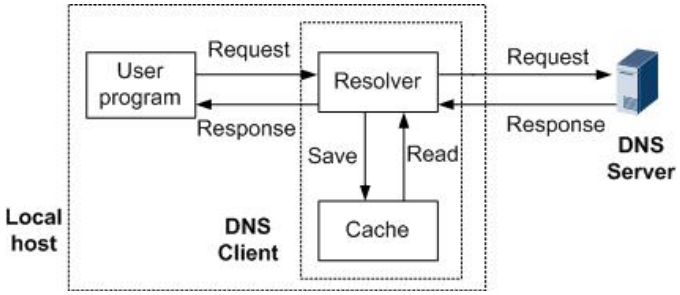



**Figure 1.22. DNS [10]**

Names must be unique because addresses are unique. A namespace maps each address to unique name.

Hierarchical Namespace:

In this name is made of several parts. In authority to assign & control namespace can be decentralized.

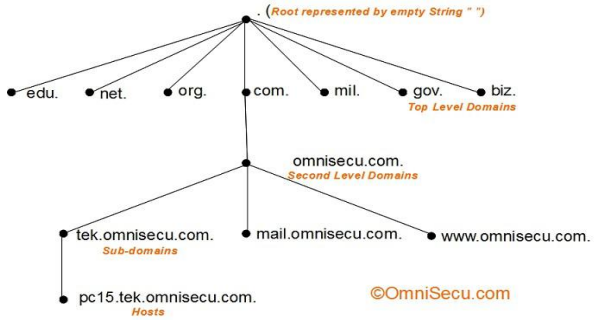



**Figure 1.23. DNS namespace [11]**

**HTTP(Hypertext Transfer Protocol)/HTTPs:**

Follows the standard client/ server.

Eg. Web browser that we are using(Google) is the client to http, the web applications like youtube, gmail are the servers.

Its a stateless protocol. Means any transaction made is independent.

This is used for transferring data from web server to a browser to view web pages.

## Transport Layer:

**UDP:**

User Datagram Protocol.

It is the simplest protocol that involves minimum amount of communication mechanism.

It is connectionless, unreliable transport protocol.

It is process to process communication(done with the help of port numbers).

Has no flow control mechanism.

Has no error control mechanism.

**TCP:**

Transmission Control Protocol.

Process to process communication due to port numbers.

Has flow control mechanism.

Has error control mechanism.

Has numbering system(keep track of the segments that are

received/transmitted).

Three-way-handshaking is a method for establishing connection.

| TCP | UDP |
|---|---|
| Connection Oriented | Connectionless |
| Full-Featured, Reliable Data Transfer | Simple, High Speed, Low functionality |
| Reliable(ack is sent) | Not Reliable |
| Data lost. Retransmission | No retransmission |
| Stream based data is sent | Message based data is sent |
| Sliding window protocol | No flow control |
| Error checking and recovery | Simple error checking but no recovery |
| Rearrange packets in order | No inherent order |

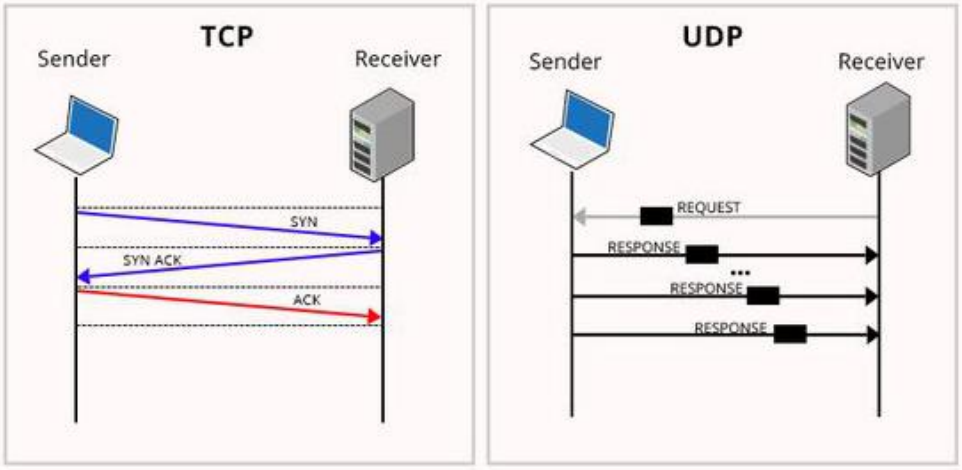



**Figure 1.24. TCP & UDP data transmission**

**Congestion Control And Quality of Services:**

**Quality of service**s: try to create appropriate environment for the traffic.

Reliability- lack of reliability means losing ack, etc

Delay- source to destination delay

Jitter- variation in delay

Bandwidth- different applications require different applications

Techniques to improve quality of services:

1. <u>FIFO Queuing-</u>

packets are served in the same order as they arrive in the queue.

If the queue is full, the packets are being discarded.

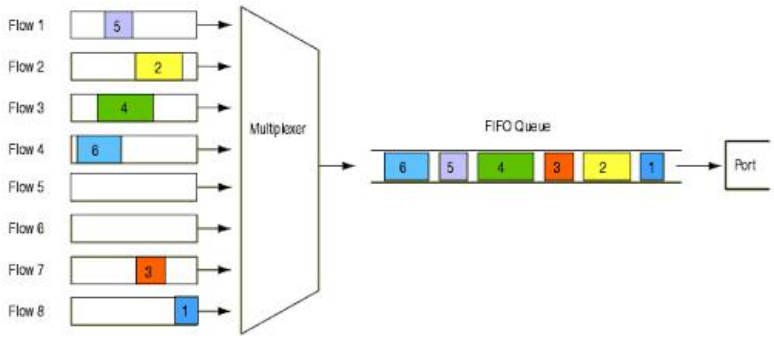



**Figure 1.25. FIFO Queuing [6]**

2. Priority Queuing-

Classifier is used to differentiate the priority and place it accordingly in the queue.

If the queue is full, the packets are being discarded.

Priority queue suffers from starvation.

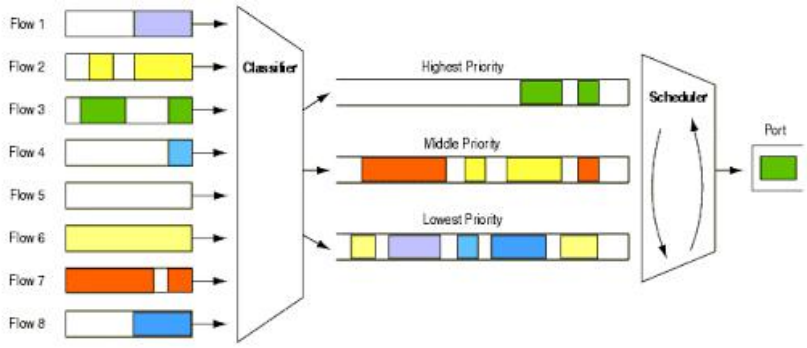



**Figure 1.26. Priority Queuing [6]**

3. Weighted Fair Queuing-

Queues are weighted based on the priority of the Queue.

If the queue is full, the packets are being discarded.

The link decides the number of packets equal to the weight are selected and departed

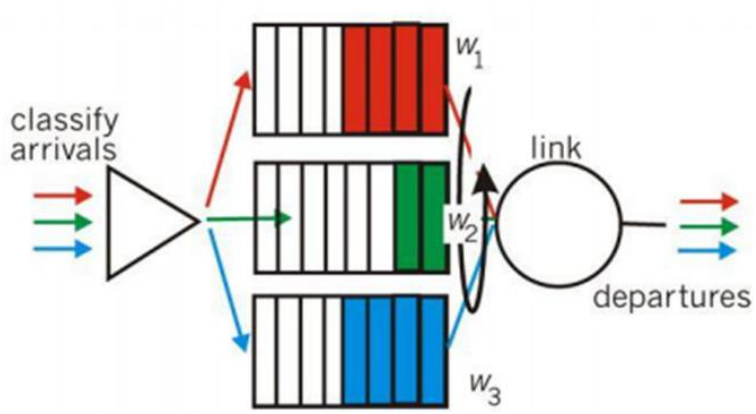



**Figure 1.27. Weighted Queuing [6]**

**Congestion Control**: avoiding the traffic congestion.

Congestion can occurs if the load on the network is greater than the capacity of the network.

Traffic:

Peak data rate: maximum data rate of traffic.

Average data rate: amount of data / total time

Maximum burst size: maximum length of time the traffic is generated at peak rate.

Network performance:

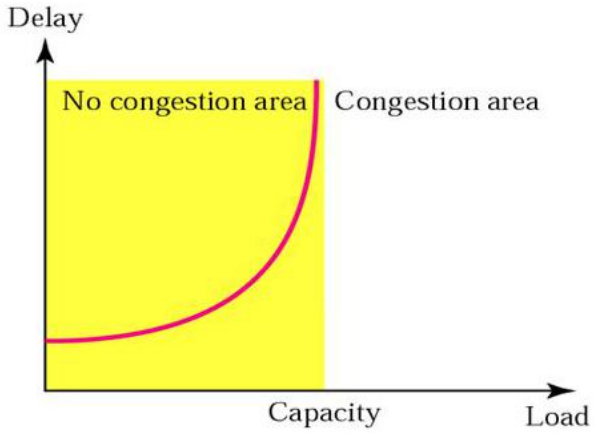



**Figure 1.28. Delay vs Capacity network performance [8]**

Load minimum delay minimum
Load keeps increasing till the capacity,if load keeps increasing beyond capacity the delay becomes infinite.

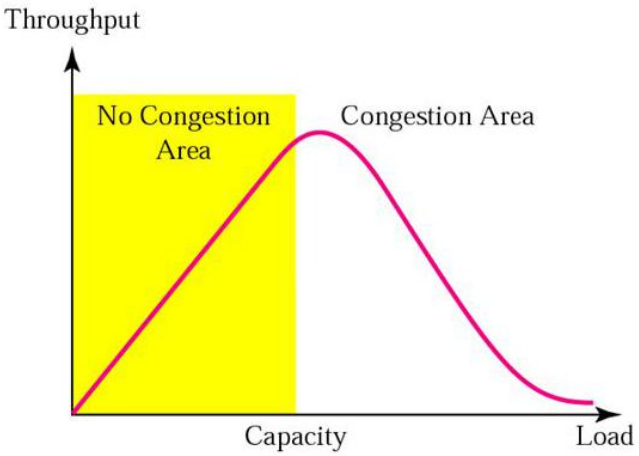



**Figure 1.29. Throughput vs Capacity network performance [8]**

Throughput as a function of load
Number of packets passing through unit time sharp increase in throughput till the capacity is reached, if the load keeps increasing beyond the capacity there is sharp decrease in throughput

Traffic Shaping: is a mechanism to control the amount and the rate of the traffic sent to the network. Approach of congestion management is called Traffic shaping. Traffic shaping helps to regulate rate of data transmission and reduces congestion.

There are of 2 types

1. Leaky Bucket:
   Suppose we have a bucket in which we are pouring water in a random order but we have to get water in a fixed rate, for this we will make a hole at the bottom of the bucket. It will ensure that water coming out is in a some fixed

rate, and also if bucket will full we will stop pouring in it.
The input rate can vary, but the output rate remains constant.
Bursty chunks are stored in the bucket and sent out at an average rate.

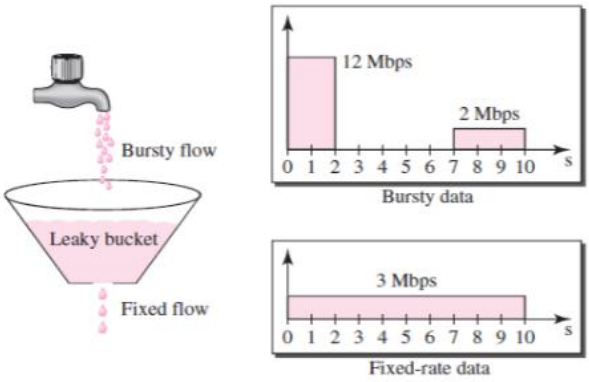



**Figure 1.30. Leaky Bucket [4]**

2. Token Bucket**:**
   A token is added to the bucket at every time t from the host and discarded for every packet transmitted. The bucket can hold specific number of tokens As the packets that needs to be processed are queued up in a queue, and when a token is removed a pack can be processed and then departed, a new token is added into the bucket.

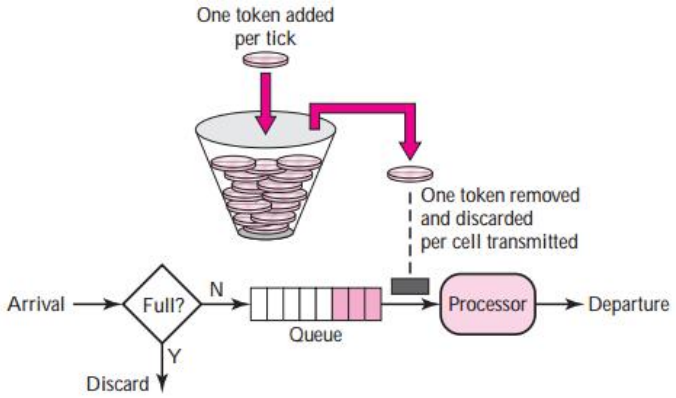



**Figure 1.31.Token Bucket [4]**

| Leaky Bucket | Token Bucket |
|---|---|
| When the host has to send a packet , packet is thrown in bucket. | In this leaky bucket holds tokens generated at regular intervals of time. |
| Bucket leaks at constant rate | Bucket has maximum capacity. |
| Bursty traffic is converted into uniform traffic by leaky bucket | If there is a ready packet , a token is removed from Bucket and packet is send. |
| In practice bucket is a finite queue outputs at finite rate | If there is a no token in bucket, packet can not be send. |

## Network Layer:

### Logical Addressing:

IPV4-

The IPv4 address is a 32-bit number that uniquely identifies a network interface on a machine.
An IPv4 address is typically written in decimal digits, formatted as four 8-bit fields separated by periods
Each 8-bit field represents a byte of the IPv4 address.

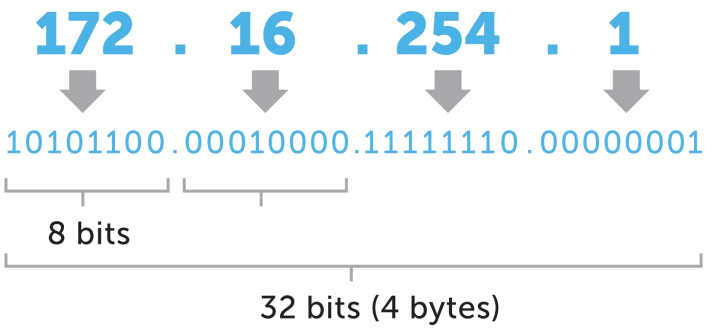



**Figure 1.32. IPV4 [3]**

IPV6-

IPv6 came into existence in 1998 with the sole purpose of taking over and replace IPv4 protocol one day.

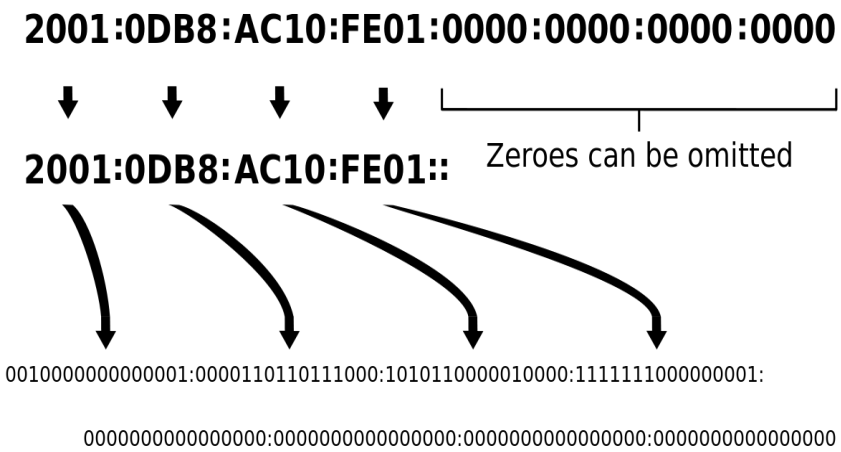



**Figure 1.33. IPV6 [3]**

| IPV4 | IPV6 |
|---|---|
| IPv4 is a 32-Bit IP Address. | IPv6 is 128 Bit IP Address. |
| IPv4 is a numeric address, and its binary bits are separated by a dot (.) Eg. 12.244.233.165 | IPv6 is an alphanumeric address whose binary bits are separated by a colon (:). It also contains hexadecimal. Eg. 2001:0db8:0000:0000:0000:ff00:0042:7879 |
| Has checksum fields | Does not have checksum fields |
| IPv4 offers five different classes of IP Address. Class A to E | IPv6 allows storing an unlimited number of IP Address |
| IPv4 has header of 20-60 bytes. | IPv6 has header of 40 bytes fixed |
| In IPv4 Encryption and Authentication facility not provided | In IPv6 Encryption and Authentication are provided |
| Security feature is dependent on application | IPSEC is inbuilt security feature in the IPv6 protocol |

**Transition from one version to another:**

1. Dual Stack Routers-

   A server with both IPv4 and IPv6 address configured can communicate with all hosts of IPv4 and IPv6 via dual stack router (DSR).

   The dual stack router (DSR) gives the path for all the hosts to communicate with server without changing their IP addresses.

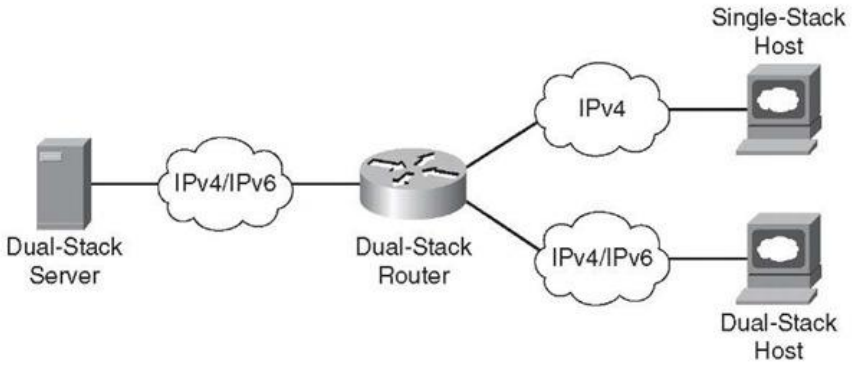



**Figure 1.34. Dual Stack Routers [4]**

2. Tunneling-

   Tunneling is used as a medium to communicate the transit network with the different IP versions.

   Encapsulate one version of IP in another so the packets can be sent over a backbone that does not support the encapsulated IP version.

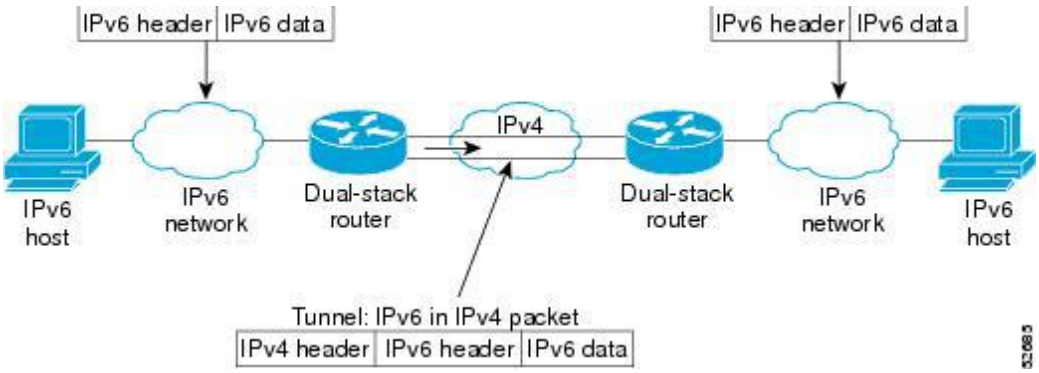



**Figure 1.35. Tunneling [4]**

3. NAT protocol translation-

   By the help of NAT Protocol Translation technique, the IPv4 and IPv6 networks can also communicate with each other which do not understand the address of different IP version.

   We use NAT-PT device which remove the header of first (sender) IP version address and add the second (receiver) IP version address so that the receiver IP version address understand that the request is send by the same IP version, and its vice-versa is also possible.

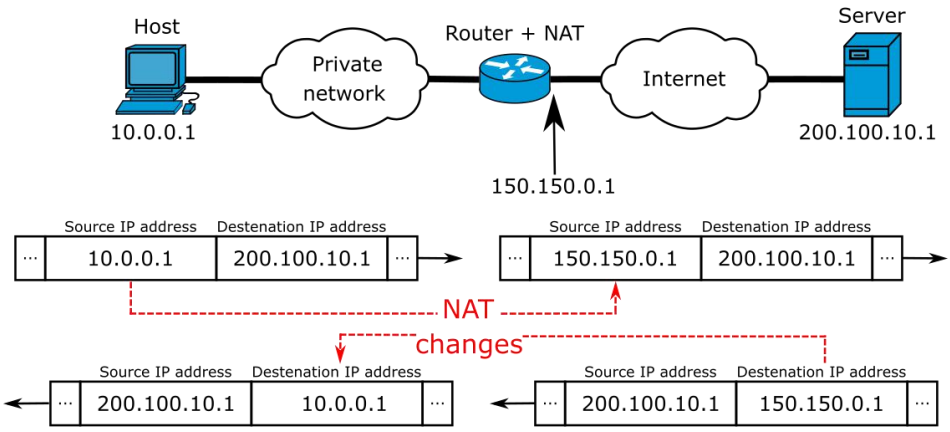



**Figure 1.36. NAT [4]**

**Sub-netting:**

Is a logical subdivision of an IP network.

The process of dividing a network into two or more networks is called sub netting

Help relieve network congestion.

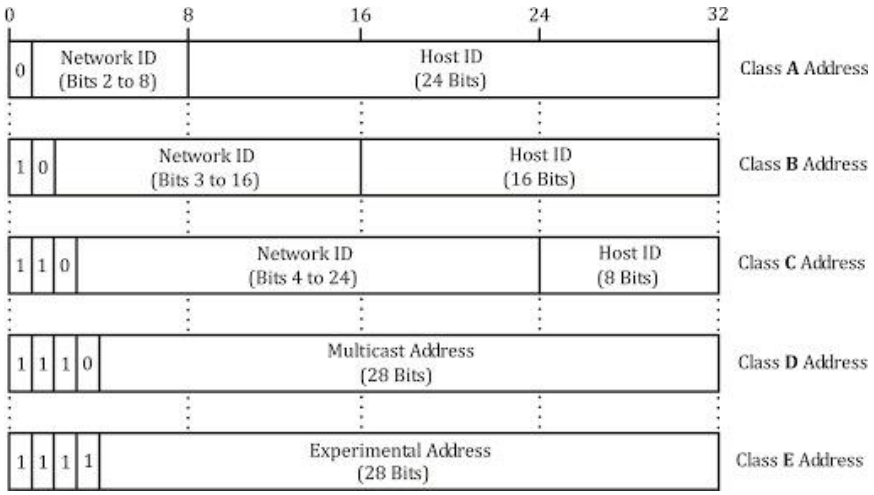



**Figure 1.37. This is the network class [1]**

So accordingly we can find which class, the number of hosts, network address, broadcast address etc

**Internet Protocol:**

**ARP-Address Resolution Protocol.**

Systems keep an ARP look-up table where they store information about what IP Addresses are associated with what MAC addresses. When trying to send a packet to an IP address, the system will first consult this table to see if it already knows the MAC address.

So basically System A has logical address of System B but it requires the physical address, it broadcasts the request signal, when the system B receives the request it uni-casts the reply along with the physical address to System A.

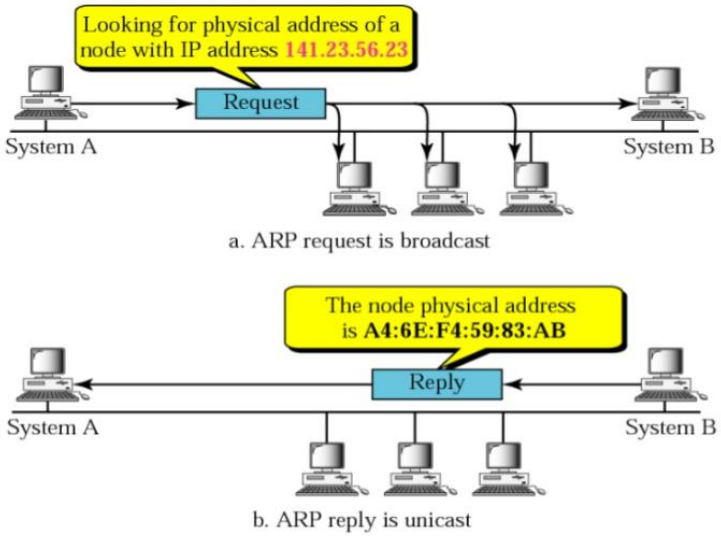



**Figure 1.38. ARP [1]**

**RARP-The Reverse Address Resolution Protocol.**

System A has the physical address of System B but requires the logical address, it broadcasts the request signal, when the system B receives the request it uni-casts the reply along with the physical address to System A.

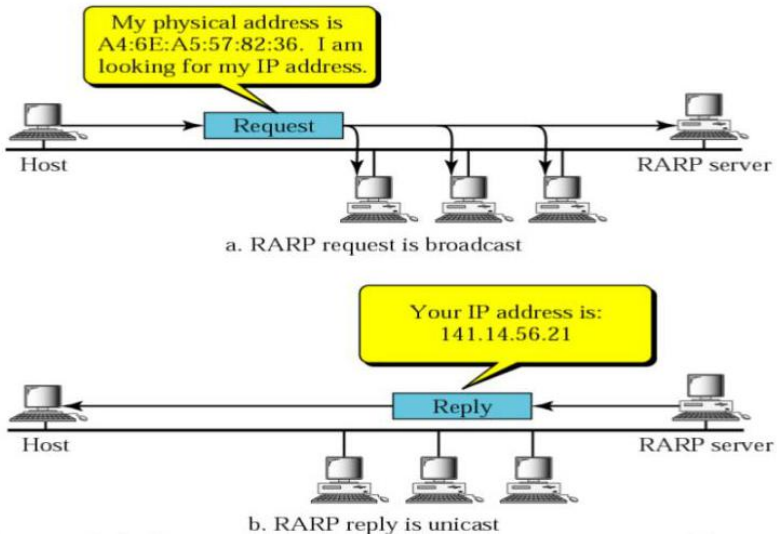



**Figure 1.39. RARP [1]**

**ICMP- Internet Control Message Protocol**

Error Reporting messages, it reports the message to the original source. ICMP doesnt corrrect the errors.

Source quench message**:** This message informs the source that a datagram has been discarded due to congestion

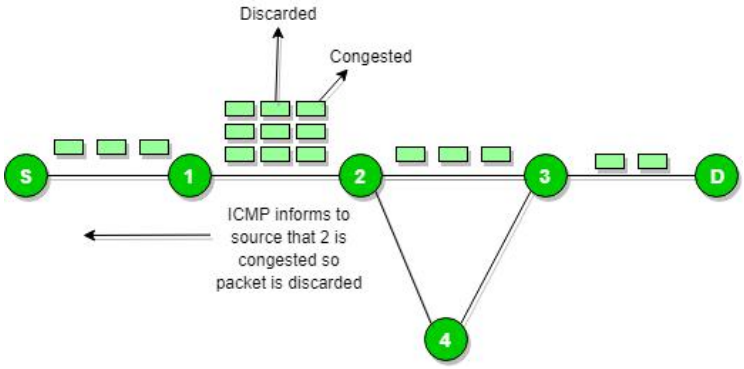



**Figure 1.40. Source Quench [2]**

Parameter problem**:** If a router / host discovers an ambiguity or missing field In the datagram
It discards the datagram and sends the error message to the source.
Code-0, Error / ambiguity in the header field
Code-1, Required part of the option is missing

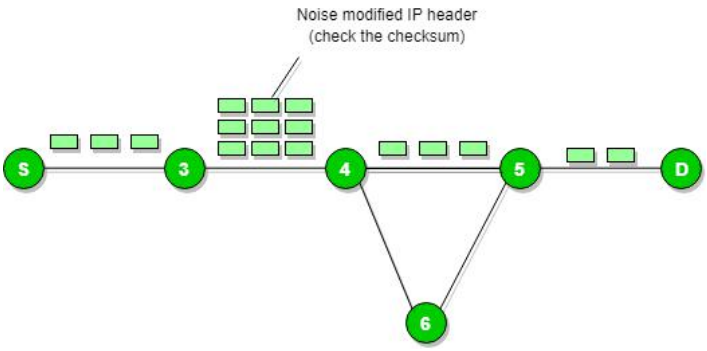



**Figure 1.41. Parameter problem [2]**

Time exceeded message**:**
Code-0, When a router has a datagram with TTL value to 0, it discards and sends time exceeded message to the source
Code-1, When the final destination doesnt receive all fragments in a set time, it discards the received fragments and sends time exceeded message to the source.

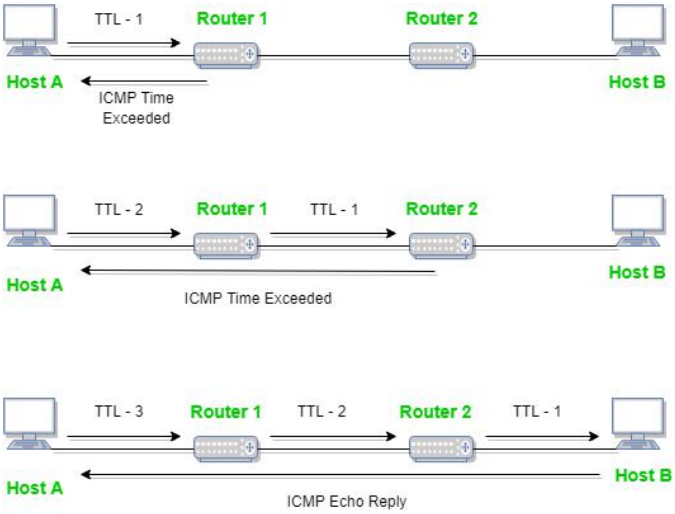



**Figure 1.42. Time Exceeded Message [2]**

Destination unreachable**:** Whenever a router to the destination is not found, datagram is discarded and the router/host sends Destination unreachable message to the source.

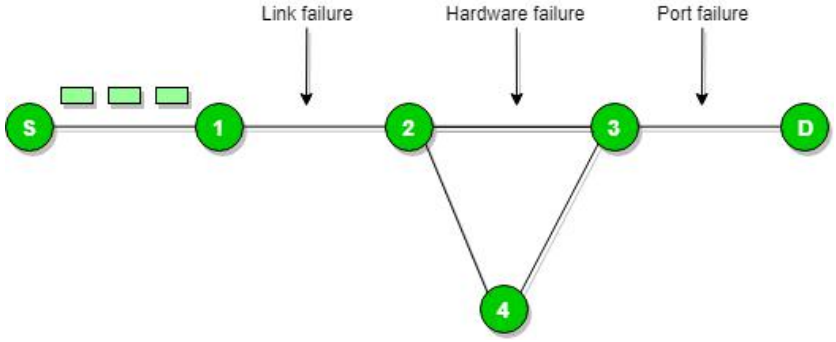



**Figure 1.43. destination Unreachable [2]**

Redirected message: Redirect requests data packets be sent on an alternate route. The message informs to a host to update its routing information

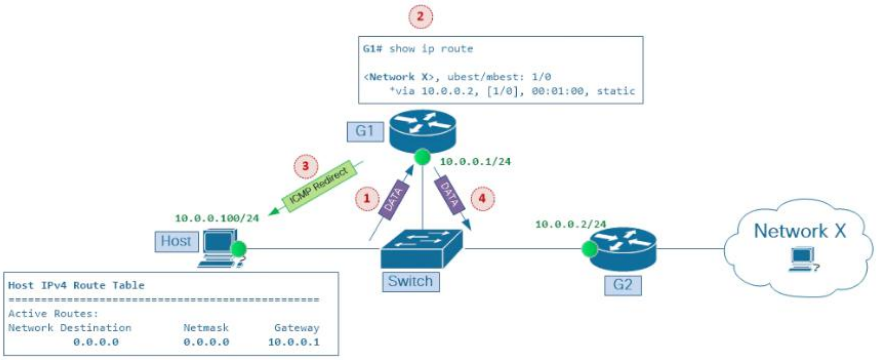



**Figure 1.44. Redirected Message [2]**

Query message, it is used to diagnose some network problems

Echo Request & Reply**:** This is designed to determine whether 2 systems can communicate with each other.
Timestamp Request & Reply**:** Two machines use the messages to determine the round trip needed for an IP data-gram to travel between them.
Address mask request and reply**:** Used to determine the subnet mask used on the Network.
Router solicitation or advertisement**:** Enable a node on a link to discover the routers on the same link.

## Data Link Layer

**Error Control:** This is used for Error Detection and Correction.
Single -Bit Error in which just a bit in the data unit has changed.
Burst Error in which more than 2 bits in the data unit has changed.

1. Parity checking- In this an extra bit needs to be added to each word before transmission. This is for error detection.
   Even parity, number of 1's in the given word including the parity should be even.

Odd parity, number of 1's in the given word including the parity should be odd.
Only applicable for single bit data error.

| | | |
|---|---|---|
| 1.1011010 | = | 10110100 |
| 2.1110111 | = | 11101110 |
| 3.1001001 | = | 10010011 |
| 4.0010000 | = | 00100001 |
| 5.1010101 | = | 10101010 |

**Figure 1.45. Parity Checking (Single Bit) [2]**

For more error we can use Two Dimension Parity checker.
It detects up to 3 bit error
In this the data are arranged in rows and columns manner.
First note down each rows parity , then each columns parity. Then the whole table is sent to the receiver, while checking if the bits have errors the intersection will provide the error

Sent Frame

| | | | | |
|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 | 0 |
| 1 | 0 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 |

Received Frame w/ 1 error

| | | | | |
|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 1 |
| 0 | 0 | 1 | 0 | 0 |
| 1 | 0 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 |

**Figure 1.46. Parity Checking 2D [2]**

2. CRC- In this each word is added to the previous word and checksum is calculated, then checksum is transmitted along with the data.
The original and the CRC is required to first XOR them, the checksum Generated needed to be included in the original data and then again XOR them. The CRC is known from the coefficient of the polynomial

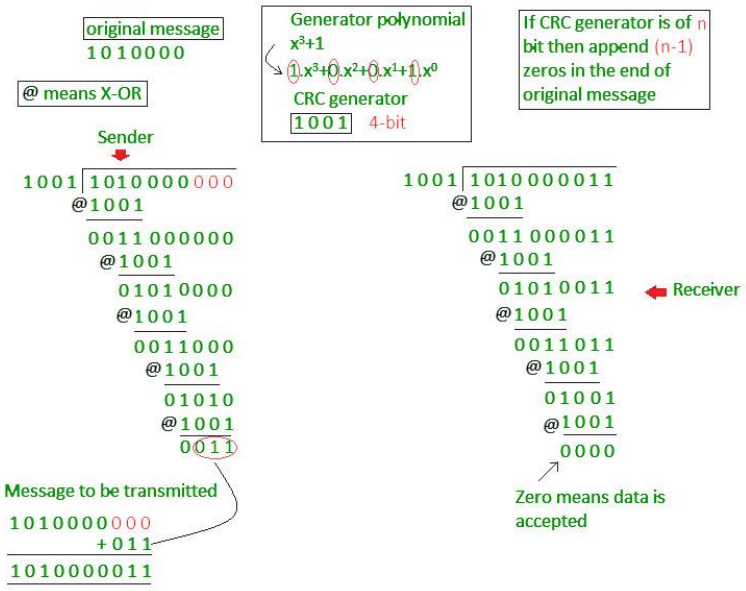



**Figure 1.47. CRC [2]**

3. Hamming Code- This is a set of error-correction codes that can be used to detect and correct the errors that can occur when the data is moved or stored from the sender to the receiver.

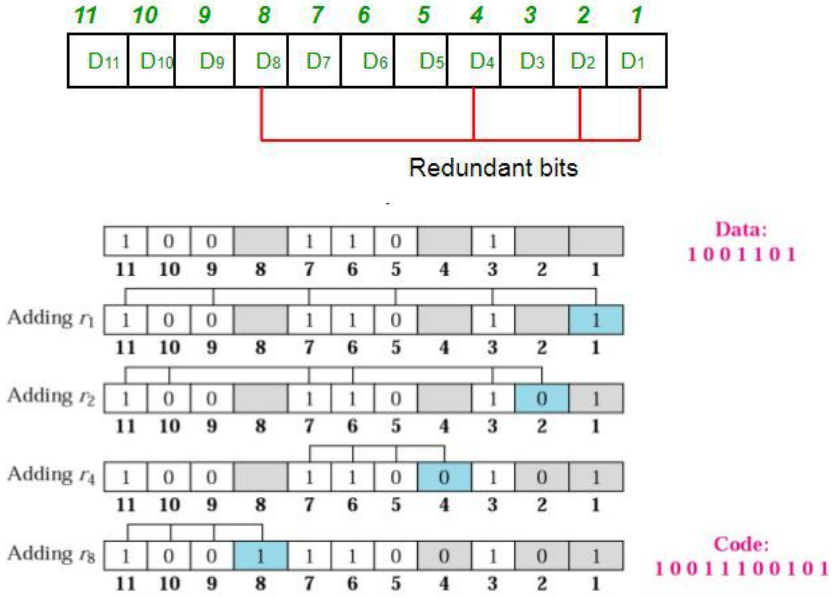



**Figure 1.48. Hamming Code [2]**

1,2,4,8 are the parity bits
P1:1,3,5,7,9,11
P2:2,3,6,7,10,11
P3:3,4,5,9,10,11
P4:4,5,6,7
We have to find the even parity and place the bit 0,1 accordingly.
Using these data we are able to find the parity bits.

## Physical Layer:

### Topology:

1. Star- Each device in the network I connected t a central device called hub, no direct communication.
   If a device needs to communicate, first the data needs to be send to hub then hub transmits to the designated device.

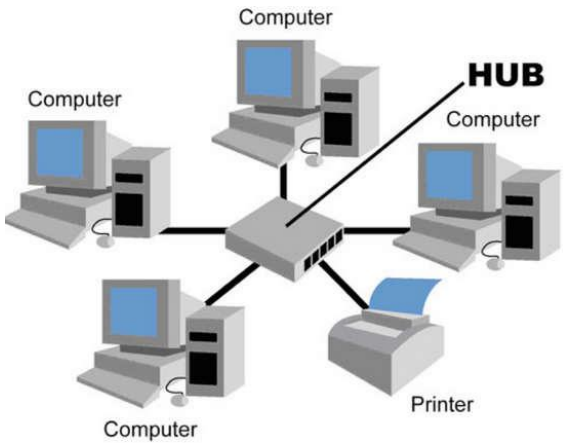



**Figure 1.49. Star topology [7]**

2. Bus- There is a cable and all the devices are connected to the main cable. Data is transmitted through the main cable, thee is a limit of drop lines ans the distance a main cable can have.

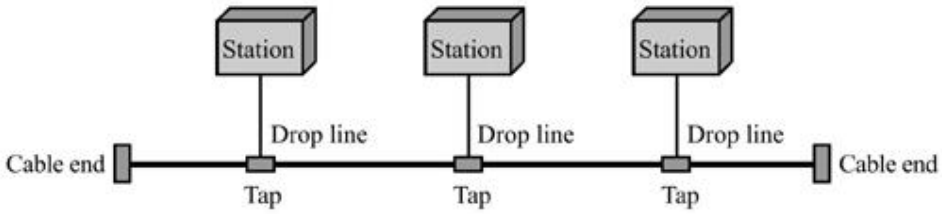



**Figure 1.50. Bus Topology [7]**

3. Mesh- Each device is connected to every other device on the network through a dedicated point-to-point link.
If n devices in the network, each device shoul be connected to n-1 devices, total number of links possible will be n(n-1)/2.

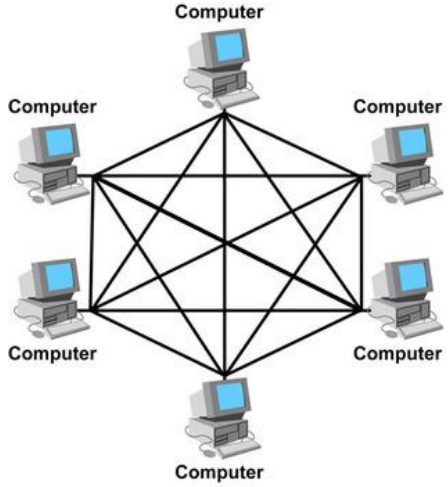



**Figure 1.51. Mesh Topology [7]**

4. Ring- Each devices connected with the two devices on either side of it. Data is sent in one direction.
Each device in ring topology has a repeater, if the received data is intended for other device then repeater forwards this data until the intended device receives it.

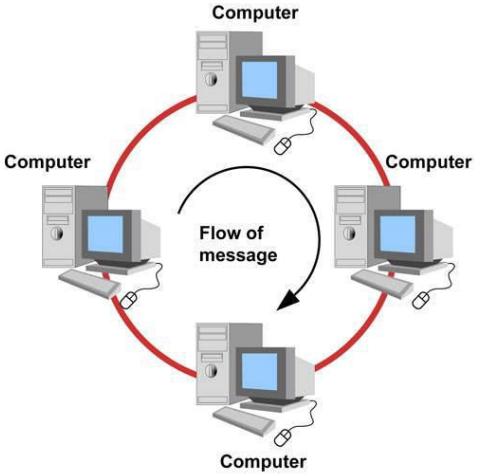



**Figure 1.52. Ring Topology [7]**

5. Hybrid- A combination of two or more topology is known as hybrid topology.
   For example a combination of star and mesh topology is known as hybrid topology.

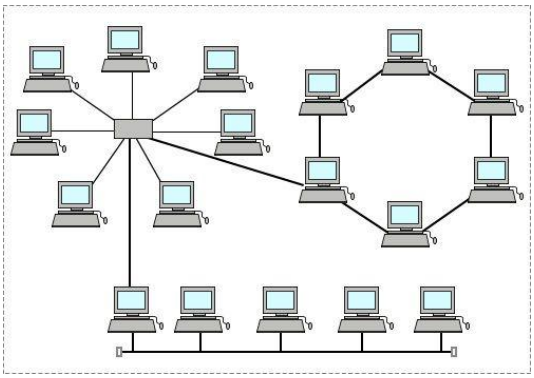


**Figure 1.53. Hybrid Topology [7]**

**Transmission mode:**

1. Simplex Mode- Data can be sent only in one direction.
   Message cannot be send back to the sender.
   No response back.
   Eg. Loudspeakers.

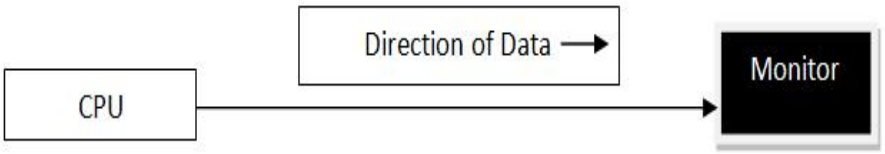



**Figure 1.54.Simplex Mode [4]**

2. Half duplex mode- Data can be transmitted in both the directions on a single carrier, but not at the same time.
   Eg. Walkie-talkie.

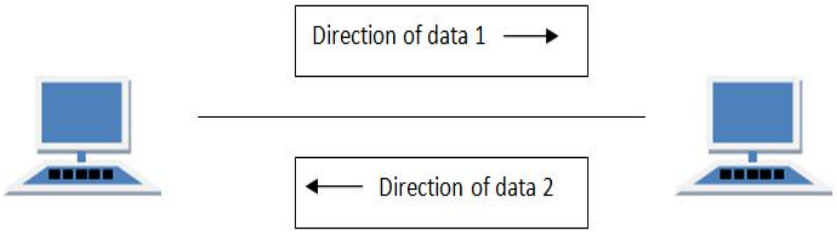



**Figure 1.55.Half Duplex Mode [4]**

3. Full duplex mode- 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.

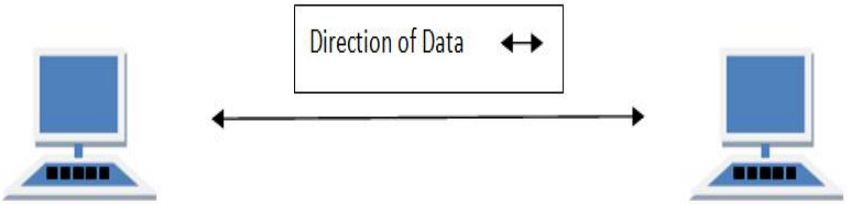



**Figure 1.56.Full Duplex Mode [4]**

# CHAPTER 2

# ASSIGNMENT

Was given an assignment to know about few different type of cables in networking along with its connector.
Coaxial Cables
Twisted Pair Cables
Fiber Optic Cables

1. CABLES

    1.1. Coaxial Cable

    1.2. Twisted pair Cable
    STP(Shielded Twisted Pair)
    UTP(Unshielded Twisted Pair)

    1.3. Fiber Optic Cable
    Multi-Mode Fiber
    Single-Mode Fiber

2. CONNECTOR

    2.1. Coaxial Cable
    BNC Cable connector
    BNC Barrel Connector
    BNC T Connector
    BNC Terminator

    2.2. Twisted pair Cable
    RJ 11 (Registered Jack)
    RJ 45

    2.3. Fiber Optic Cable
    SC
    ST

## COAXIAL CABLE

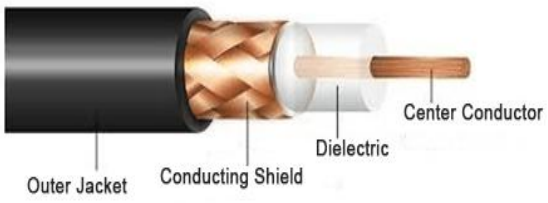



**Figure 2.1. Coaxial Cable [1]**

- Coaxial cable is a type of copper cable specially built with a metal shield and other components engineered to block signal interference.
- At the center of the cable is the copper core which actually carried the electrical signal.

**Figure 2.2. BNC Cable Connector [1]**

**BNC Cable Connector**

- BNC connectors are used with miniature to subminiature coaxial cable in radio, television, and other radio-frequency electronic equipment, test instruments, and video signals.
- Type of connector used with coaxial cables such as the RG-58 A/U cable used with the 10Base-2 Ethernet system.
- The basic BNC connector is a male type mounted at each end of a cable.

**Figure 2.3. BNC Barrel Connector [1]**

**BNC Barrel Connector**

- A BNC barrel connector allows connecting two cables together.
- The BNC (Bayonet Neill–Concelman) connector is a miniature quick connect / disconnect radio frequency connector used for coaxial cable.

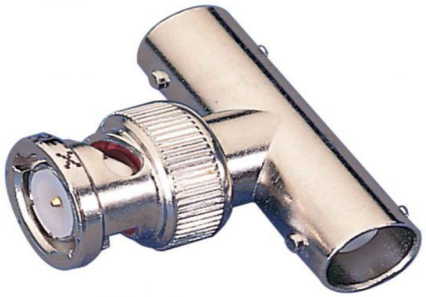


**Figure 2.4. BNC T Connector [1]**

**BNC T Connector**

- BNC T-connectors (used with the 10Base-2 system) are female devices for connecting two cables to a network interface card (NIC).
- A BNC barrel connector allows connecting two cables together.

Figure 2.5. BNC Terminator [1]

**BNC Terminator**

- The BNC T is required to connect a BNC Terminator to the end of a cable that connects to a BNC input.
- By providing the necessary termination, degradation of the signal carried by the BNC cable is minimized.

## TWISTED PAIR CABLE

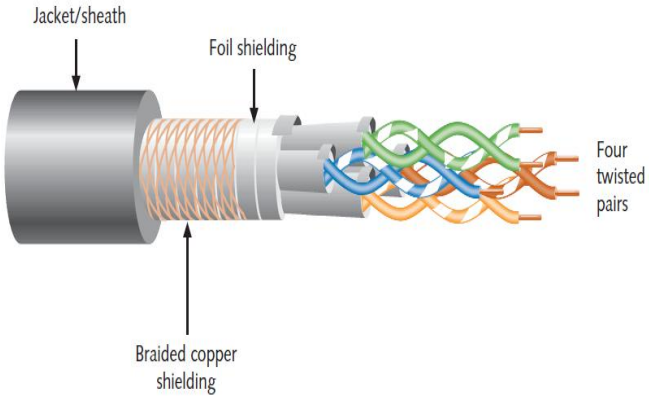



Figure 2.6. Twisted Pair Cable [1]

- A twisted pair cable is a type of cable made by putting two separate insulated wires together in a twisted pattern and running them parallel to each other.
- This type of cable is widely used in different kinds of data and voice infrastructures.
- They have 4 twisted pairs.

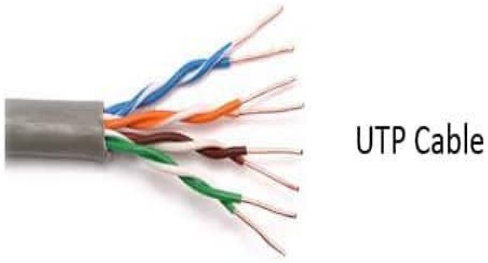



Figure 2.7. UTP [1]

**UTP**

- The most common cable used in computer networking.
- There is no metal shielding over each individual pair of copper wire as STP.


Figure 2.8. STP [1]

**STP**

- STP cabling includes metal shielding over each individual pair of copper wires.
- This type of shielding protects cable from external EMI (electromagnetic interference's).

| Category | Speed | Frequency |
|---|---|---|
| CAT 1 | Carry only voice | 1MHz |
| CAT 2 | 4Mbps | 4MHz |
| CAT 3 | 10Mbps | 16Mhz |
| CAT 4 | 16Mbps | 20Mhz |
| CAT 5 | 100Mbps | 100Mhz |
| CAT 5e | 1000Mbps | 100Mhz |
| CAT 6 | 1000Mbps | 250MHz |
| CAT 7 | 10Gbps | 600MHz |
| CAT 7a | 10Gbps | 1000Gbps |
| CAT 8 | 25Gbps | 2000Mhz |

**Figure 2.9. Unshielded & Shielded Twisted Pair Cabling Standards [1]**

**Unshielded & Shielded Twisted Pair Cabling Standards**

- **Cat 1**: Currently unrecognized by TIA/EIA. Previously used for telephone communications, ISDN and doorbell wiring.
- **Cat 2**: Currently unrecognized by TIA/EIA. Previously was frequently used on 4 Mbit/s token ring networks.
- **Cat 3**: Currently defined in TIA/EIA-568-B, used for data networks using frequencies up to 16 MHz. Historically popular for 10 Mbit/s Ethernet networks.
- **Cat 4**: Currently unrecognized by TIA/EIA. Provided performance of up to 20 MHz, and was frequently used on 16 Mbit/s token ring networks.
- **Cat 5**: Currently unrecognized by TIA/EIA. Provided performance of up to 100 MHz, and was frequently used on 100 Mbit/s ethernet networks. May be unsuitable for 1000BASE-T gigabit ethernet.
- **Cat 5e**: Currently defined in TIA/EIA-568-B. Provides performance of up to 100 MHz, and is frequently used for both 100 Mbit/s and gigabit ethernet networks.
- **Cat 6**: Currently defined in TIA/EIA-568-B. It provides performance of up to 250 MHz, more than double category 5 and 5e.
- **Cat 6a**: Future specification for 10 Gbit/s applications.

**Figure 2.10. RJ 11 (Registered Jack) Connector [1]**

**RJ 11 (Registered Jack) Connector**

- The typical RJ-11 connector has six terminals, usually, only the middle four pins are used.
- RJ11 is the cable connector that using in telephone sets.
- The POTS (Plain Old Telephone Service) residential telephone wiring generally contains two pairs of wires designed for two separate telephone lines.

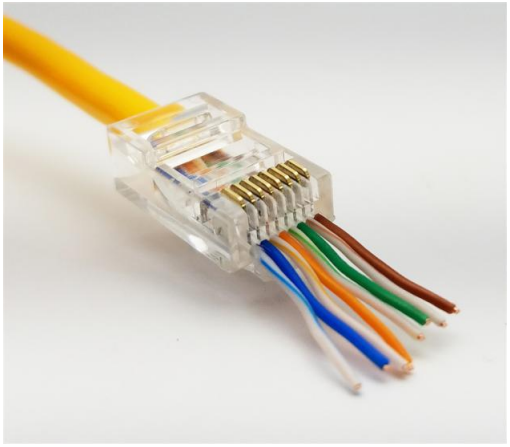


**Figure 2.12. RJ 45 Connector [1]**

**RJ 45 Connector**

- Each RJ45 connector has eight pins means an RJ45 cable contains eight separate wires.
- RJ45 is used in networking, where you connect computers or other network elements to each other.
- This cable is capable of transmitting data at speeds of up to 1000 Mbps (or 1 Gigabit per second).
- There are two wiring standards for RJ-45 wiring: T-568A and T-568B.
- Although there are 4 pairs of wires, Ethernet uses only 2 pairs: Orange and Green. The other 2 colors (blue and brown) may be used for a second Ethernet line or for phone connections.

## FIBER OPTIC CABLE

**Figure 2.13. Backbone [1]**

- A fiber optic cable is a network cable that contains strands of glass fibers inside an insulated casing.
- They're designed for long distance, high-performance data networking, and telecommunications.
- Fiber-optic cables carry information between two places using entirely optical (light-based) technology. Fiber optics transmit data in the form of light particles or photons that pulse through a fiber optic cable.

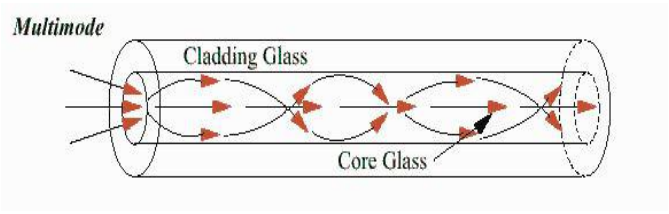



**Figure 2.14. Multi-Mode [1]**

**Multi-Mode**

- In optical fiber technology, multimode fiber is optical fiber that is designed to carry multiple light rays or modes concurrently, each at a slightly different reflection angle within the optical fiber core.
- Commonly used short distances, audio/video applications, and Local Area Networks (LANs).

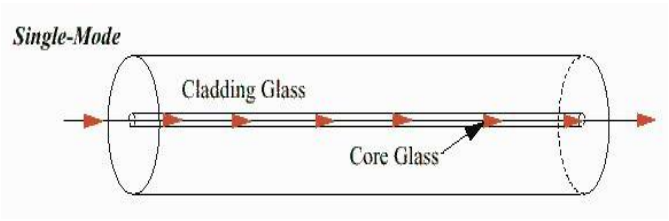



**Figure 2.15. Single-Mode [1]**

**Single-Mode**

- In fiber-optic communication, a single-mode optical fiber (SMF) is an optical fiber designed to carry only a single mode of light - the transverse mode.
- Used for long distances or higher bandwidth needs and uses a laser has its light source

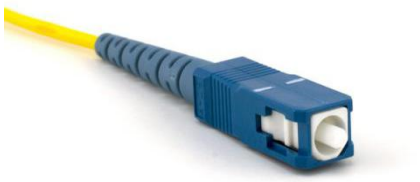


**Figure 2.16. SC Connector [1]**

**SC Connector**

- The SC connector (sometimes known also as a square connector) is another type of fiber-optic connector.
- This latching mechanism holds the connector in securely while in use and prevents it from just falling out.

**Figure 2.17.ST Connector [1]**

**ST Connector**

- They are cylindrical with twist lock coupling, 2.5mm keyed ferrule.
- ST Connectors are among the most commonly used Fiber optic connectors in networking applications

# CHAPTER 3

# WORKDONE

## 3.1. INTRODUCTION

The main aim for the project was to successfully placing the surveillance cameras around Katara Park, choosing the camera with best view, high range, waterproof, environmental protection, etc. So the camera used is IP65, which satisfies all the conditions as demanded by the clients.The camera needs to placed in an area of 1 or 2 acre of land. The setup is in our scope but accessing of camera, video playing and recording is not in our scope.We use ring topology. We have a total of 12 rings with 5 to 6 switches which are kept under the manhole, and the cameras are connected with these industrial switches. The switch we use is IE3000 We use ring topology rather than star topology. As for connecting we might need to use fibre cables, using these cables are costly, area is also big so star is not efficient. In this we use 4 core fibre, and 1 core is connected with 1 manhole. Each core has its own TX and RX module which is used to transmission and receiving respectively. The first connection formed is from the service room(TX) to one rings switch(RX), then from that switch(TX) to another switch(RX) below the manhole. This continues until service room has RX of that particular ring. The video recorded are being stored in disks which are placed in the IT rack. The main control and service room is connected with these these rings.

## 3.2. Layout and Implementation

### 3.2.1. Visual Layout

Before beginning the manually networking connection. Lots of site visits take place, analyzing the place where the cameras are supposed to be initialized at what distance they need to be initialized, etc keeping all the factors in mind the layout of installment of the cameras are done virtually using AUTOCAD. When the layout is done and finalized then proceeded.

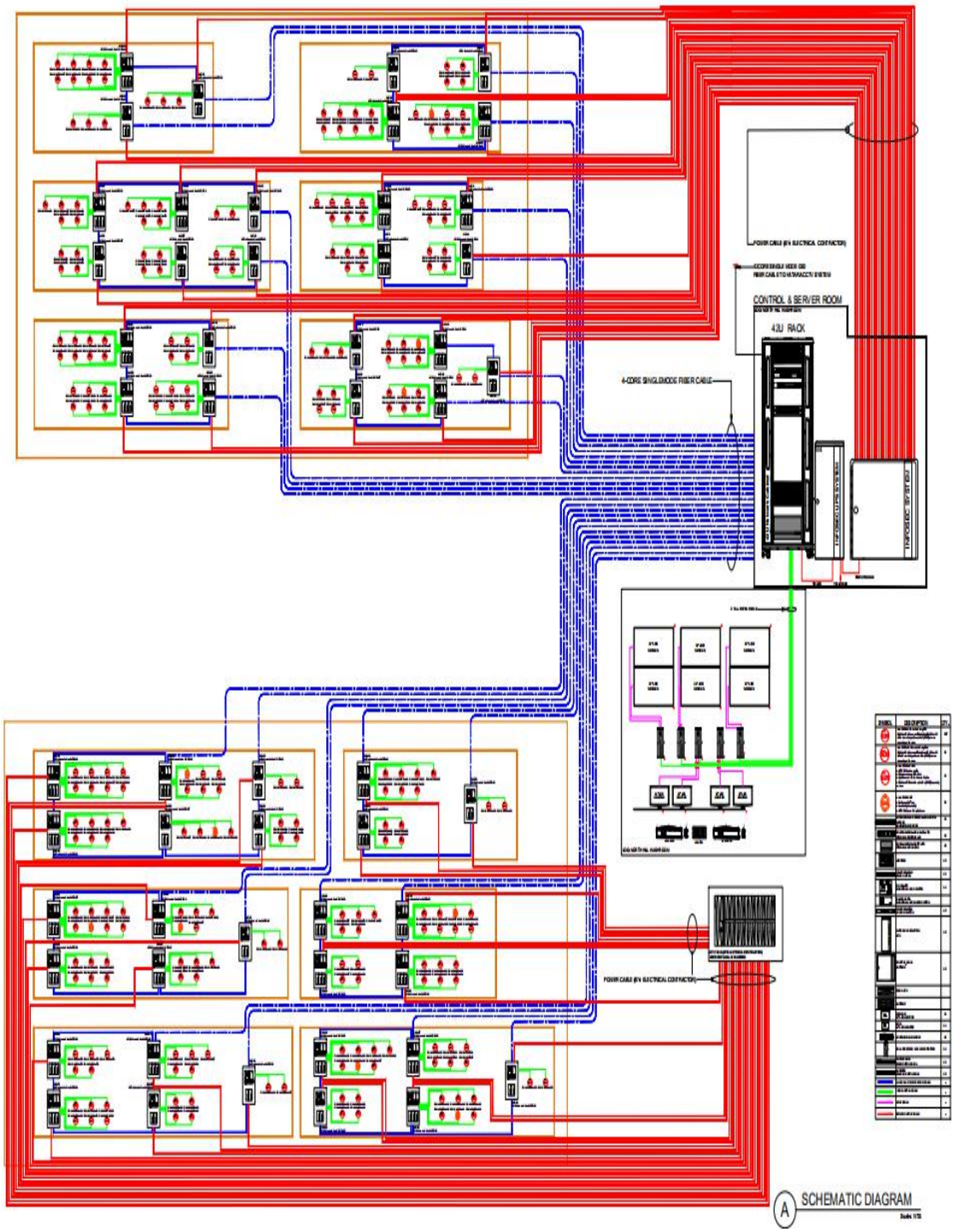



**Figure.3.1. The whole layout [5]**

This is the main virtual layout of the project.
Before physically or manually being involved in the network connection, the layout is made for the convenience and efficiently getting the output.

So this is the whole connection of how the surveillance cameras are placed and installed in the south hill and north hill.

The switches are connected in ring fashion which are placed inside the manhole.

For every switch there are few cameras connected to them.

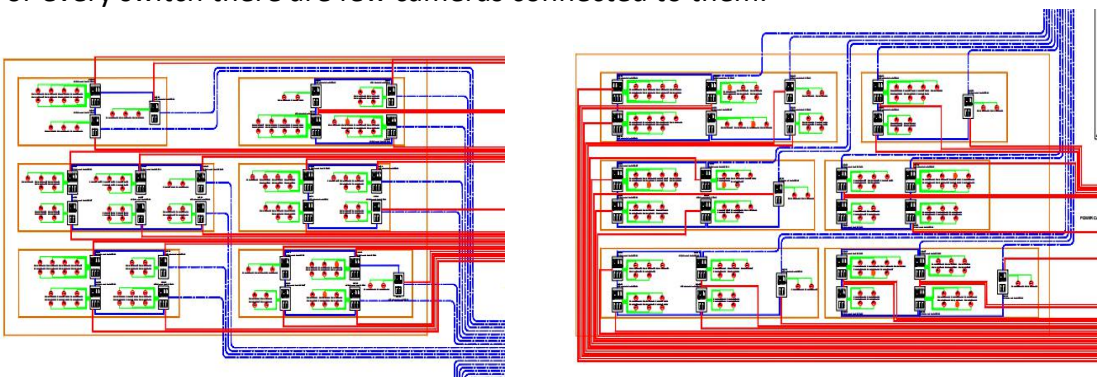


**Figure.3.2. The south and north hill connection [5]**

This is the south hill to the left and north hill to the right.
The surveillance cameras were connected in this fashion.

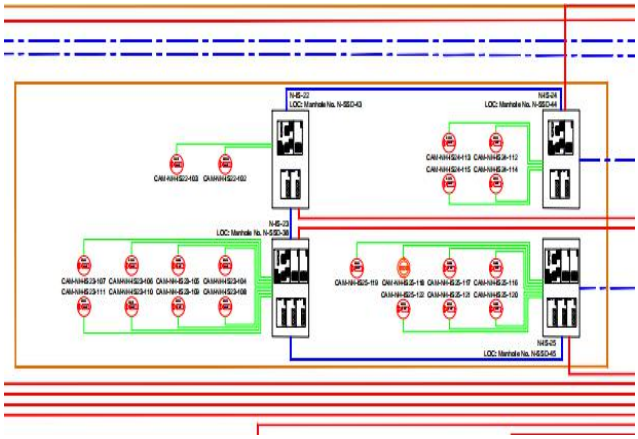


**Figure.3.3. Switches connection [5]**

The switches that are placed inside the manhole are connected in a ring fashioned topology. Each switch has 2 or more surveillance cameras connected to it.
As the switches are connected in ring fashion, there are two backbone each of 4 core for each ring connected to the IT rack.
As each of the switches have 2 backbone, one for receiving the data and other for transmitting the data.
If a backbone stops sending data, as they are connected in a ring topology fashion the data is still transmitted to the IT rack in the server room.

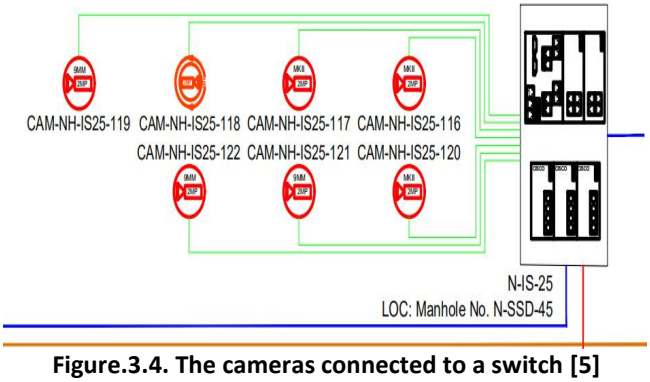



**Figure.3.4. The cameras connected to a switch [5]**

This is the way the surveillance cameras are connected to the switch, the switches which are placed inside the manhole and are connected to each other in a ring fashion.
This is one of the switches, in which there are 7 surveillance cameras connected.

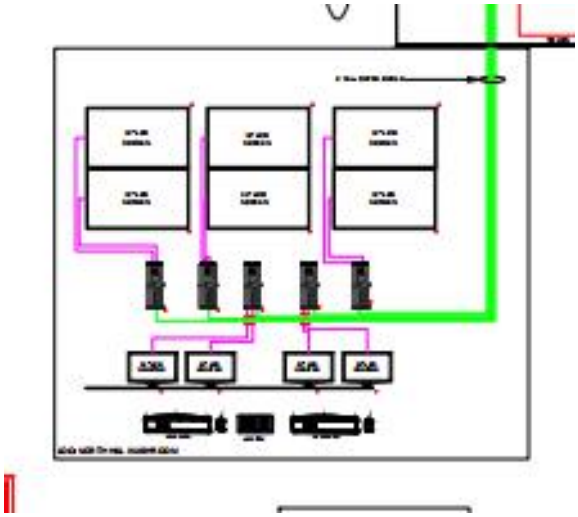


**Figure.3.5. Surveillance room [5]**

This is the surveillance room where the videos are seen, Only the authorized people have access to this place.

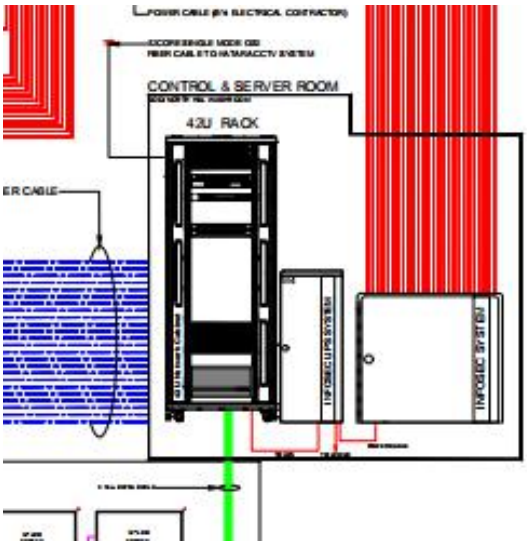



**Figure.3.6. Server room [5]**

This is the place where the IT rack is placed and the connection that starts from here and end here.
The storing of the video recording is also placed here.

## 3.2.2. THE NETWORK CONNECTIONS

The networking connection is the one in which the connections are made manually after the visual layout. The main connection is made in the IT rack of the server room.

The main process occurs here where the video captured by the cameras are transferred and stored in the storage. The required videos are displayed as per the requirements.
But before this also a visual setup is done in the Cisco Packet Tracer, where the unique id are provided to the devices and pinged to know if the network is able to transfer data or not.

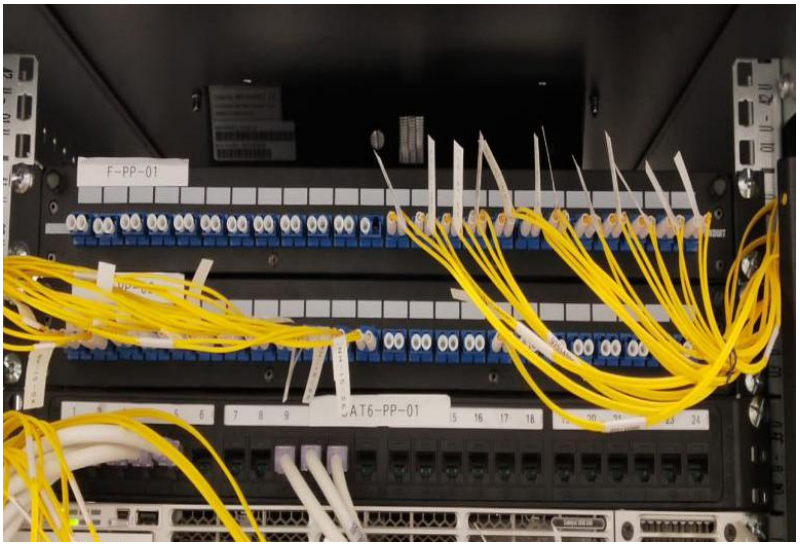



**Figure.3.7. The topmost patch panel in the IT rack**

This is the topmost setup in the IT rack. The 1st one is for the south pole and the 2nd one is for the north pole. The fiber cables as seen in the front are connected to the switch using the SFP Module.
The Fiber Cable has 2 cores(TX, RX) for a data to be transmitted and received.
As the backbone with 4 cores are used to connect the switches placed inside the manhole. Those backbones are then spliced inside the patch panel as only 2 cores are required for a normal transmission and the other 2 are kept as spare or a backup. Therefore the the patch panel half of the patch is empty and not connected to the switch1 and switch2.

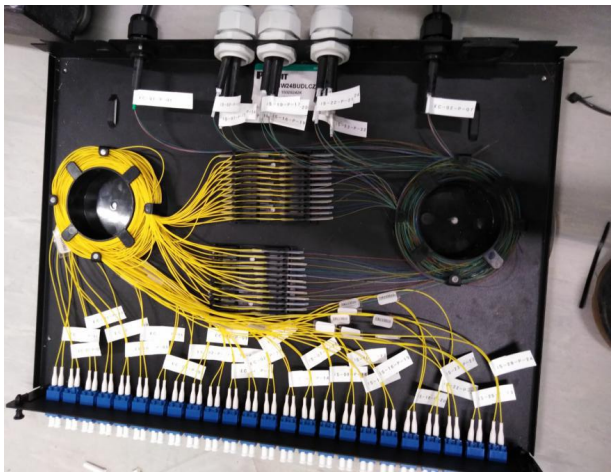


**Figure.3.8. Splicing of the backbone**

**Figure.3.9. Backbone of 4 core**

This is how the splicing looks inside the patch panel, splicing is done between the backbone of 4 core so that each backbones only 2 cores can be connected to the switch1 and switch2 from outside the patch panel.
Since in each hill there are 6 rings of switches that are placed inside the manhole. Therefore 12pair cores are being connected to the switch and the rest 12pairs are kept as spare.
So including both the hills, 24pairs cores are connected and the other 24pairs cores are kept as spares.

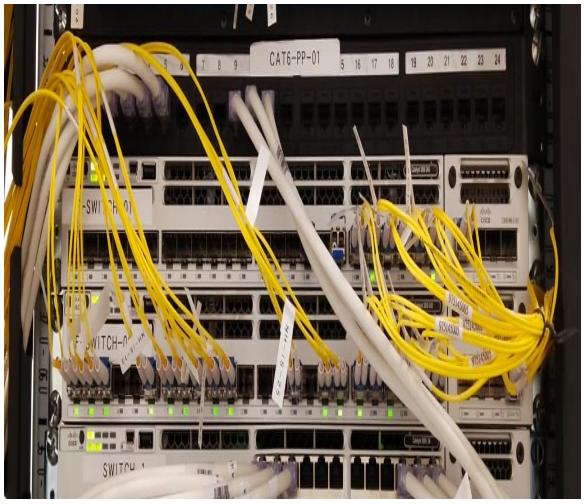



**Figure.3.10.Fiber cables connected to the switch**

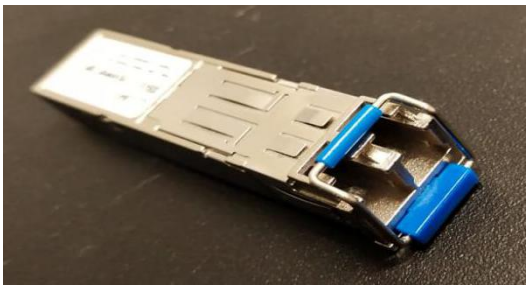


**Figure.3.11.SFP module for the fiber cables**

Afterwards the splicing, he fiber cables are then connected to the switch1 and switch2, with the help of an SFP module, as the switch has copper cables connection and fiber cables cannot be connected to them.

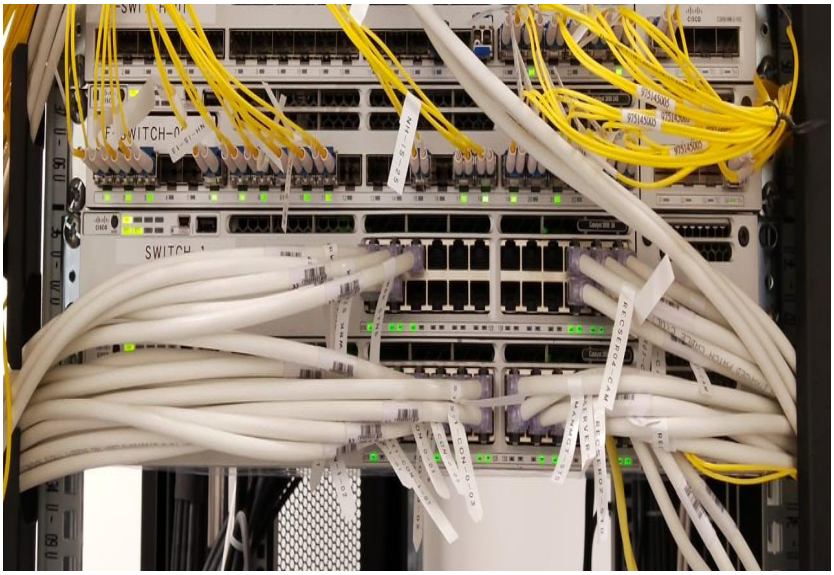


**Figure.3.12. The copper cables connected to the switch.**

This switch3 where all the cooper cables are connected are, from the previous switch1 and switch2 one pair of fiber cable connected the both with the help of a

SFP module. 2 from every server and 4 from the storage

**Figure.3.13. Behind the server rack**

This is the back view of the IT rack .This Blade server has 4 individual servers within it. Each of the server has 2 wires, 1st for camera image access to server and 2nd for server to storage which is connected to the switch3 which is in the front of the IT rack.
All the cameras are equally divided between the servers

**Figure.3.14. The camera that needs to be installed**

The connection was being made for these surveillance cameras which are placed on the North and South hills.
The cameras are connected to the switch placed in the manhole with the copper cable.
The camera used is ip365.

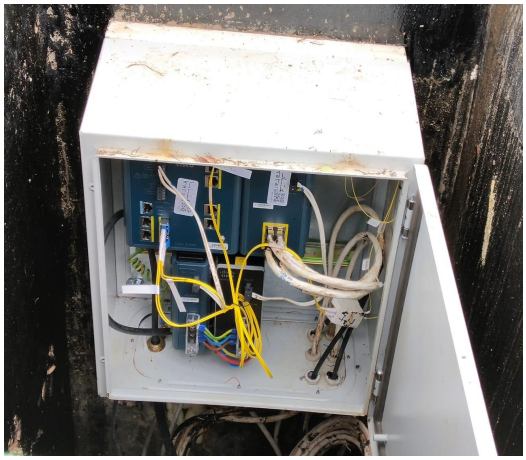


**Figure.3.15. The industrial switch inside the manhole**

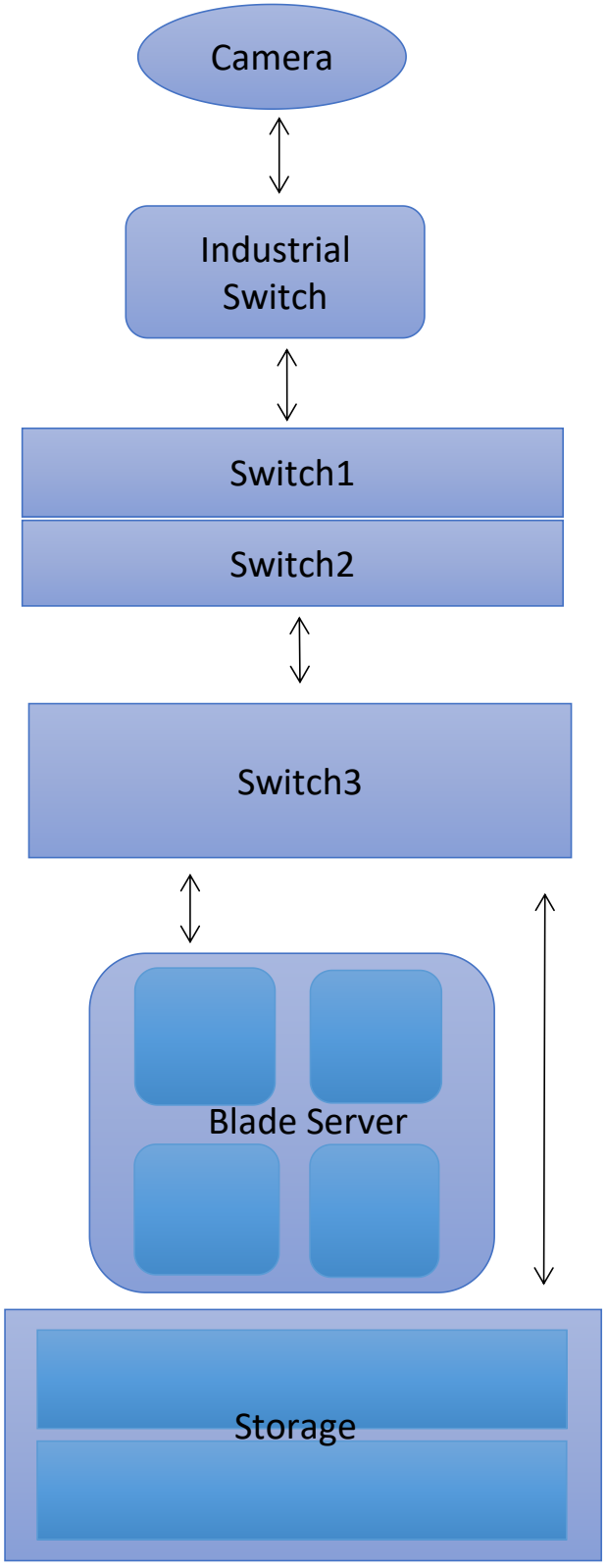
The switches are placed under the manhole are the industrial switches. Each switch is connected to 5 - 6 surveillance cameras . The switch is connected to other switches in a ring fashioned topology.

The Top left is the main switch where the backbones are spliced and connected.The Top right is the expansion module which has copper port where it used to connect with the cameras. The white cables are used. The Bottom left is for power supply to the switch. The Bottom right is for power supply to the expansion module

.

The switch has 2 backbones connected to it. One it receives the other it transmits. As the industrial switches are connected in a ring fashioned topology. The backbones are spliced and then connected to the switch (The top left Box)

**SO THE OVERALL PROCESS HOW THE VIDEO IS CAPTURED AND STORED**




So the footage captured from the camera is transferred to the industrial switch with he help of copper wire. (The white cable).

From the industrial switch it is transferred to the IT rack by the backbone. (The black cable).

As the backbone is of 4 core optical cable, it is being spliced and connected with the pigtails, then connected to switch1 and switch2.

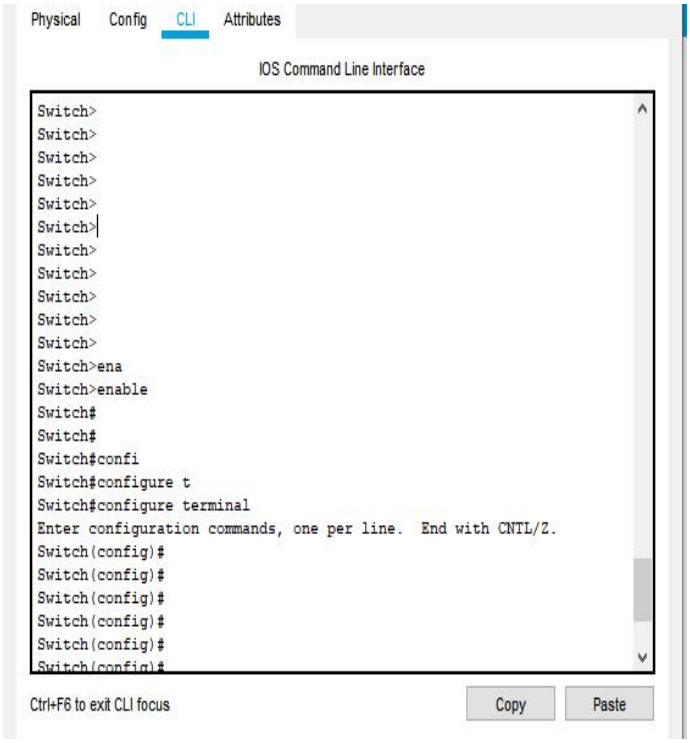
From these 2 switches it is connected to the switch3, they need to be connected with an optical fiber so the footage is accessed .

The blade server, which had 4 individual servers, each with 2 copper ports. 1st port from camera footage to server and the 2nd from server to the storage. These 8 ports are connected to the switch3. ( The white cable)

The storage has 2 blocks, each with 4 ports, which is connected to the switch3 for storage purposes. (The white cable)

**Figure.3.16. Process of Video Capture**

# 3.2.3.CISCO PACKET TRACER



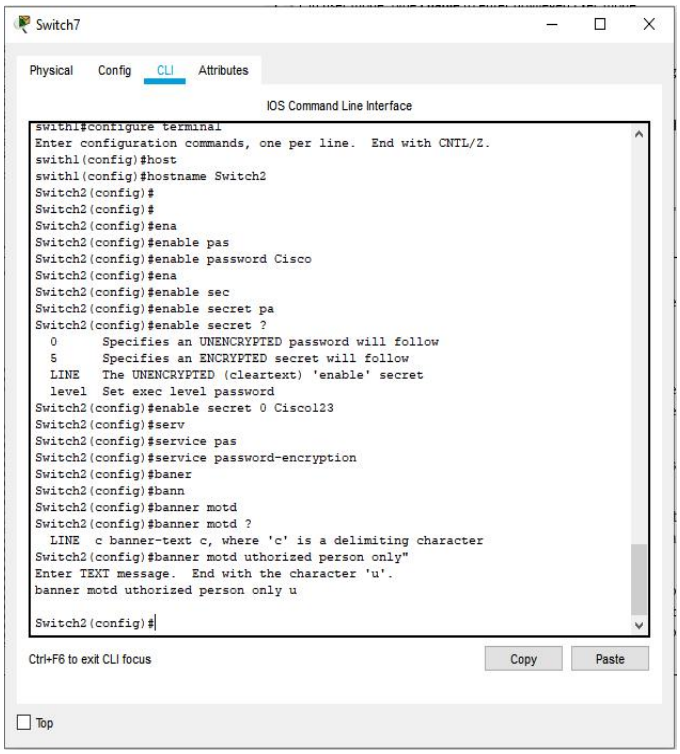

Today started with the Cisco packet tracer.
How to do the configurations of the switch according to the requirements.

Basically, it had 3 Mode

**User EXEC Mode**: allows you to access only basic monitoring commands.
(can be identified by the > prompt)

**privileged EXEC Mode:** allows users to view the system configuration, also allows all the commands that are available in user mode, type **Enable** to enter privileged Exec mode
(can be identified by the # prompt)

**Global Configuration mode**: allows users to modify the running system configuration
From privileged EXEC mode type the **configure terminal** command to enter the global configuration mode
(can be identified by (global)#
(To exit configuration mode, the user can enter "end" command or press Ctrl-Z key combination)




After entering the Global configuration mode, I have done below mention configuration in order to secure the switch.

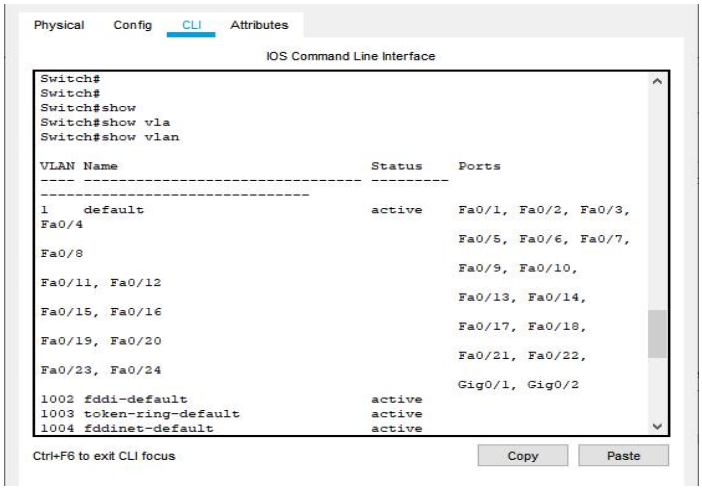
**Hostname:** Switch Name

**enable password:** The enable password doesn't encode the password and might be read in clear text within the running-config

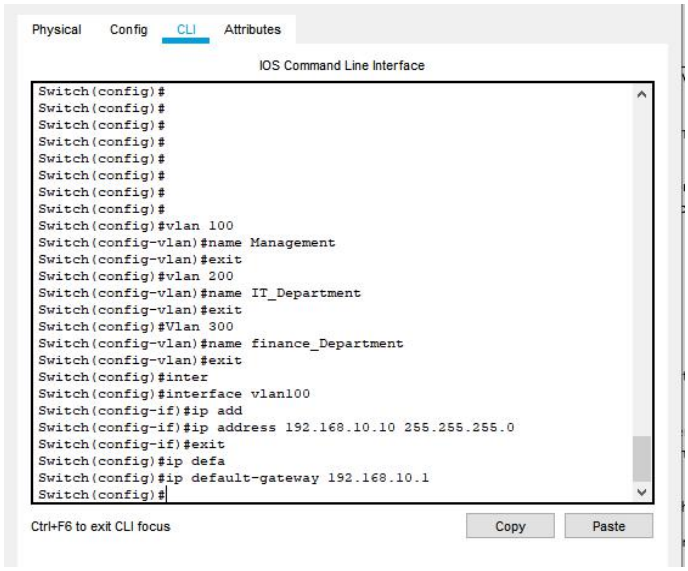
**enable secret password:** The secret password overwrites the regular password

**service password encryption:** command that encrypts **passwords** after you reload the device or do a show run command.

**Banner motd:** the message that shown when someone who is not authorizes to access the switch and inside the port, I put the warning message that I want an unauthorized person to see when they are trying to access the switch.



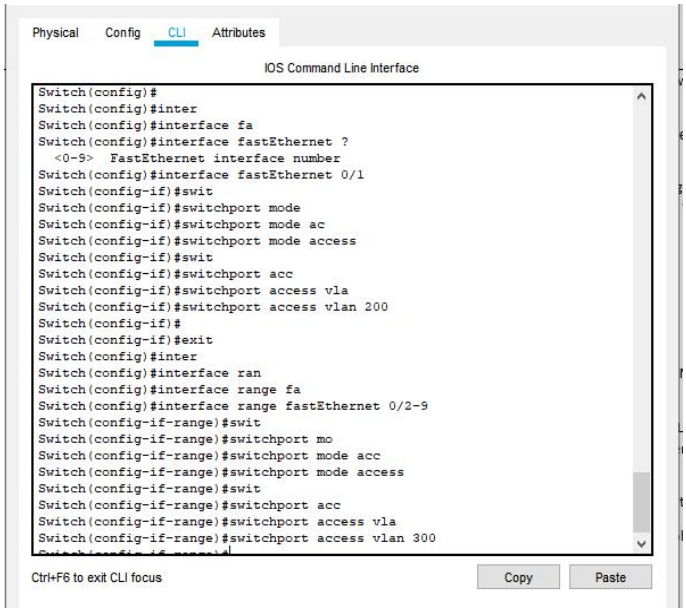

**VLAN**: In the Configuration mode, by typing show VLAN we can see all the VLANS, their status, ports, etc.
VLANs can be used for to separate network management traffic from end-user or server traffic.
After you have created the VLAN, any network segments connected to the assigned ports will become part of that VLAN.



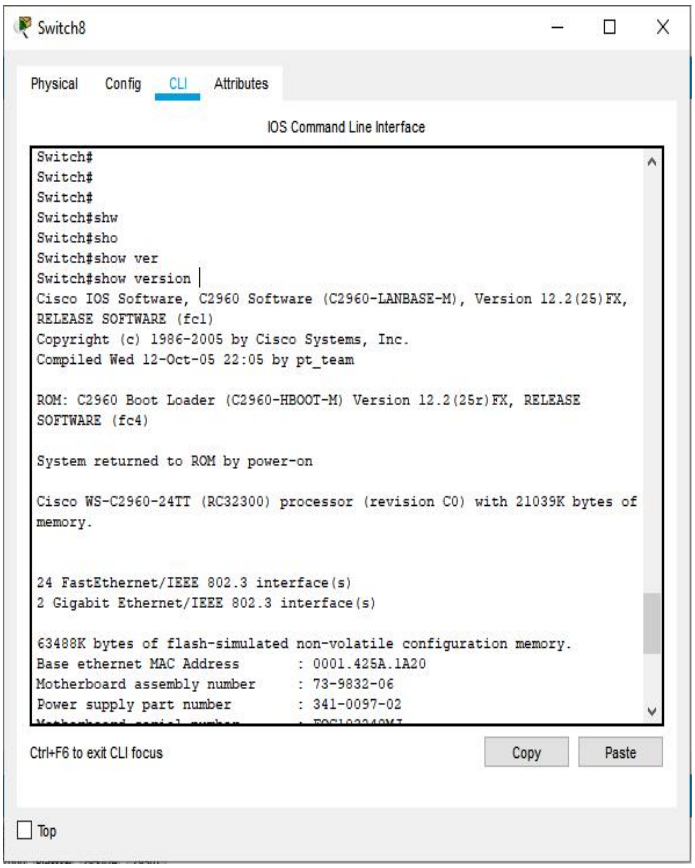

I have created 3 VLAN given below

VLAN 100 For management
VLAN 200 for IT Department
VLAN 300 For Finance Department

Then I have given IP address to management VLAN 100 followed by 24 subnet mask Eg:255.255.255.0
Then I have assigned some port into IP department VALN and Finance department VALN in order to separate the User from the organization
After that I have given the IP Default Gateway address to the Switch



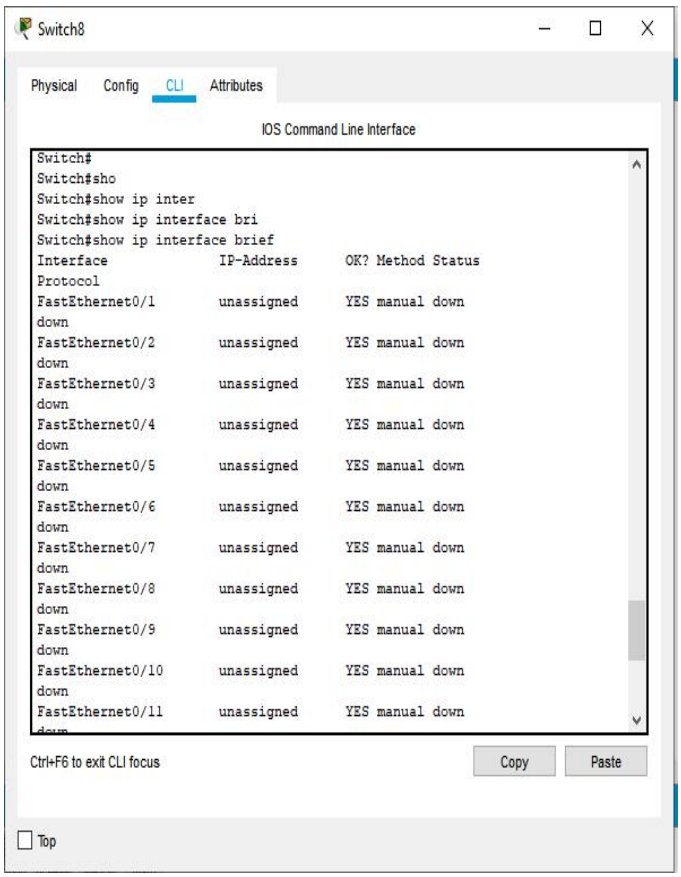

We Can assign port one by one also we can assign multiple port together by typing range command
as shown in the figure




To check the version of the device used

From the Enable mode type **show version** Command Followed by Space key to see all the details

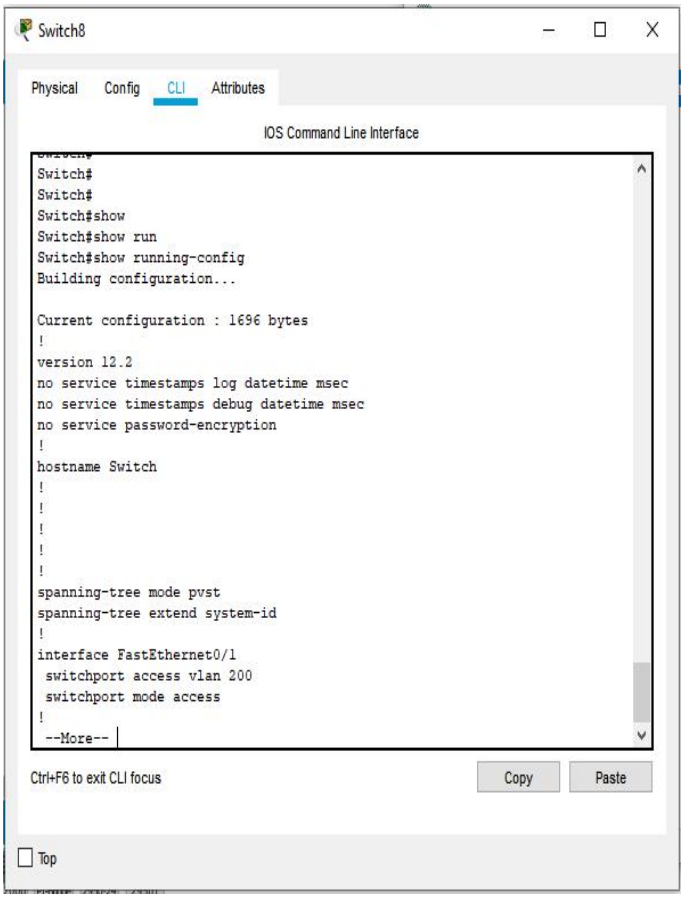
All the details are then shown




To Check the status of the port

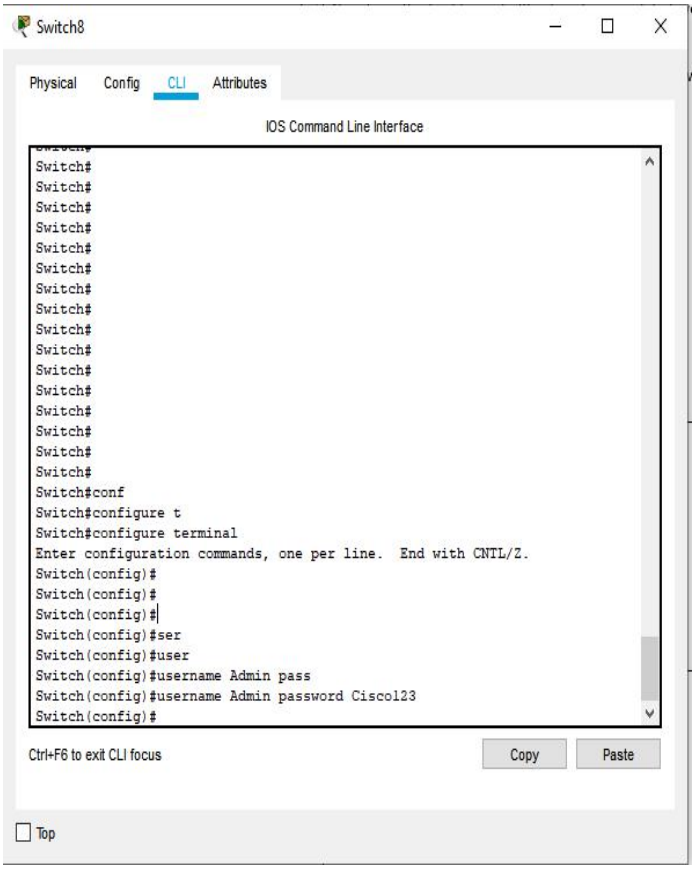
Type **show IP interface brief** Command followed by enter Space key to see for the full port status

Space key is used to see more details
And the Tab key can fulfill the command without entering full command it helps me to complete the work easily



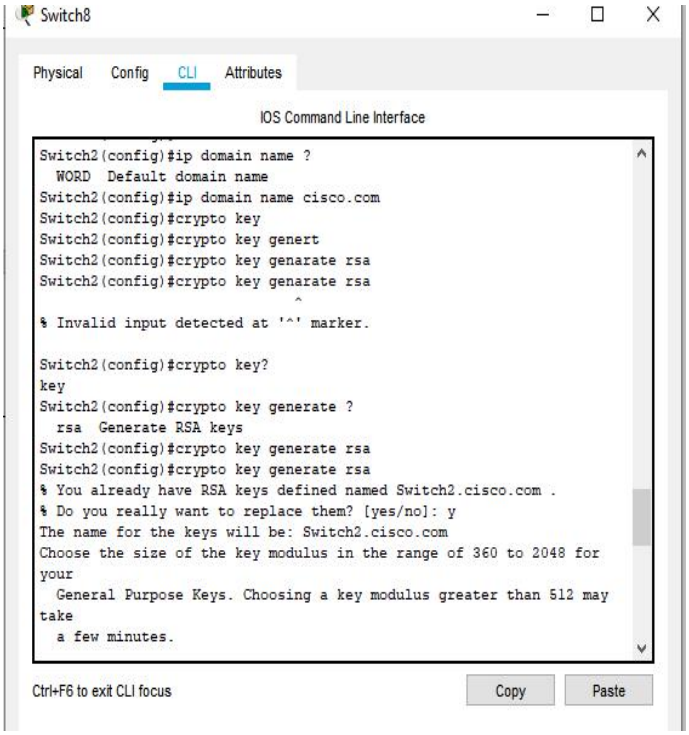

Now from the Enable mode (Privilege Exec mode), if we type show running-config
We can see the Current Running Configuration Followed by typing the space key

.




In the global configuration mode, we create a username and password in order to secure console access

The username is Admin
The password is Cisco123



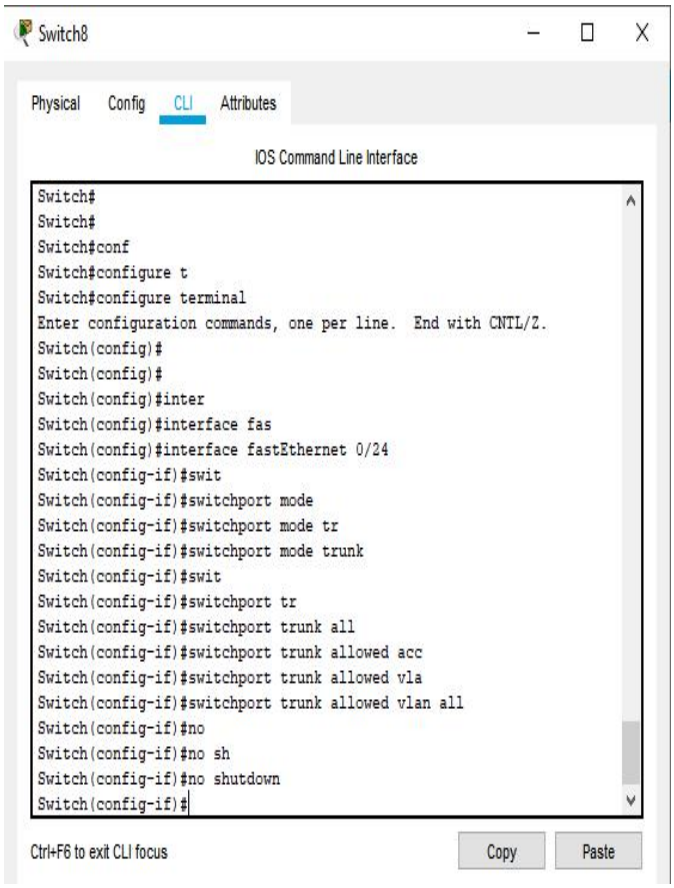

**Trunk**: A **trunk** is a communications line or link designed to carry multiple signals simultaneously to provide network access between two points. ... First, **trunks** can carry data from multiple local area networks (LANs) or virtual LANs (VLANs) across a single interconnect between switches or routers, called a **trunk** port

I have Configured the trunk and it helps me to understand the connectivity between two switch and how the network is passing using trunk mode

From the configuration mode I enter to interface mode using the command interface **gigabyte ethernet 0/9**

Then I have made this port as trunk using the Command **switch port mode Trunk**

After that I have allowed all the VLANs to pass through this trunk port to next switch using the Command **Switchport trunk allowed VLAN all**




**Telnet and SSH:**

**telnet:** doesn't use any encryption therefore the information is transmitted in a form of plain text even the password

**SSH: It** uses encryption, which means that all data transmitted over a network is secure from eavesdropping. **SSH** uses the public key encryption for such purposes.

I have successfully configured telnet and SSH as given below

In order to complete this process, we need to follow 5 steps

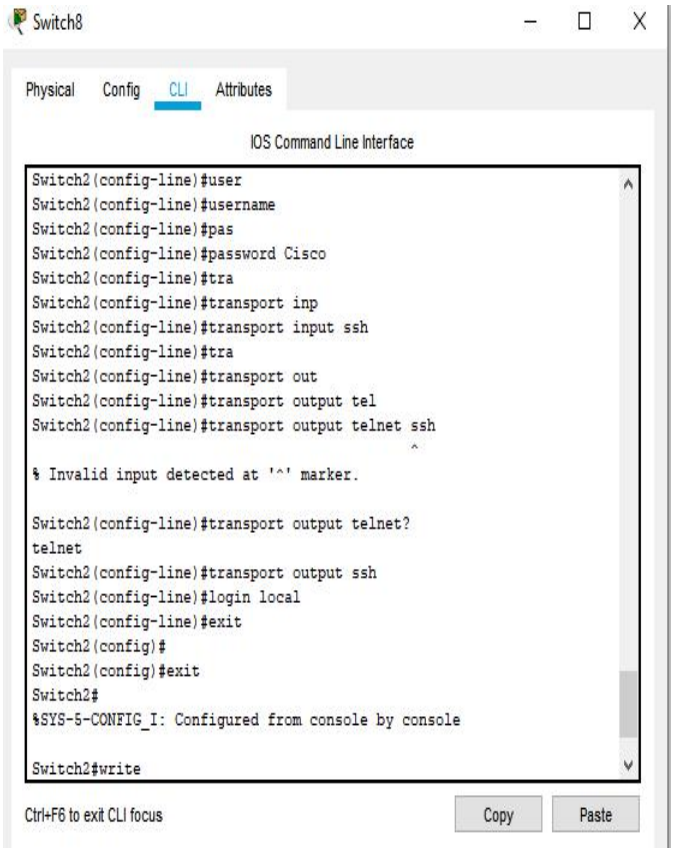
1 hostname should be configured

2 We need to create a username and password

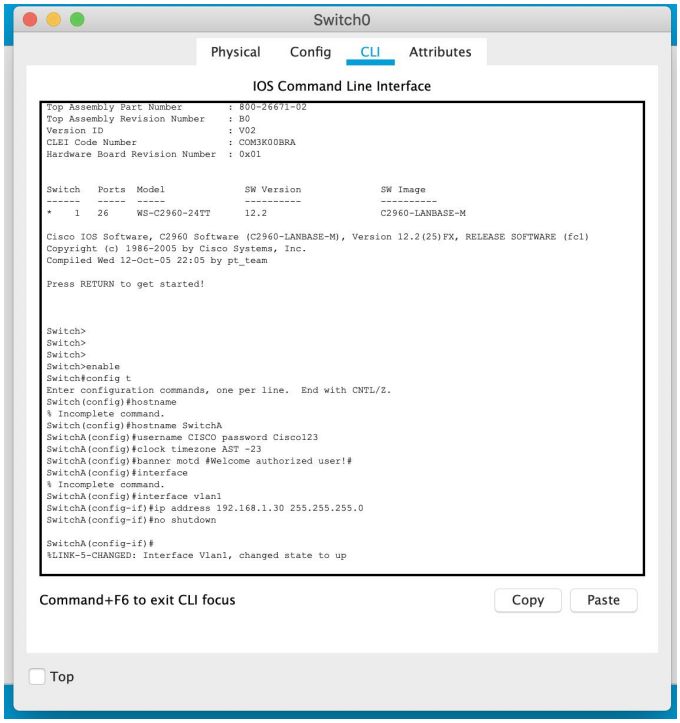
3.We have to generate the crypto key using command from the config terminal type crypto key generate rsa module hit enter then this will going to ask you how many bit for the key, as my mentor has told me to put 1024 is most recemented for getting the good result

4 IP Domain name: If you want to generate a rsa key you will need Ip domain-name in your config. For Eg: When executing command such as ping

5 enable ssh and telnet




From the configure terminal I have enter to the line vty 04 this line is for the ssh and telnet
Then I put the password in order to secure the remote connection **password Cisco**
After that I have enter the command the command **transport input SSH** and **transport output ssh telnet**
then type the command **login local**: it does us to able to use the username and password to login using remote connection without that this is not going to work




This is done by me, as my mentor wanted to check if I knew how configurations are done for a switch.

1. Create hostname
2. Create username and password
3. set time zone
4. Create a banner
5. Set an IP address for a switch

The followings are done as follows

1. enable
2. config t
3. hostname Switch2
4. username Admin password Cisco123
5. clock time zone AST -23
6. banner motd #Authorized user only! #
7. interface vlan100

Ip address 192.168.10.10 255.255.255

# CHAPTER 4

# CONCLUSION

During the course of my internship at Informatica Qatar, I got to know a lot of domain specific knowledge related to Networking. During the internship bootcamp training which lasted for fourteen days, I got to learn a lot about the company and various technologies they use in their products. Sessions were conducted on the basic knowledge on networking, without having a strong base its quite difficult to proceed with any work.

I got to contribute to the topology of the system, which aimed to reduce the overall cost, more efficient and durable. Choosing the cables, configuring the devices manually, giving them an unique id.

# REFERENCES


[1] LBS Networking Essentials.ppt
[2] https://www.geekforgeeks.com/
[3] https://www.youtube.com/
[4] https://www.cisco.com/
[5] Networking Layout
[6] http://web.opalsoft.net/qos/
[7] http://computernetworkingtopics.weebly.com/
[8] https://slideplayer.com/slide/5028490/
[9]https://medium.com/software-engineering-roundup/
[10] https://networkencyclopedia.com/
[11] https://OmniSecu.com/