SUMMER TRAINING PROJECT REPORT

On

Networking

Completed at

FTK-Centre for Information Technology, JMI, New Delhi-110025.

PROJECT NAME

"Architecture of network in JMI"

Duration:

13 June 2019 to 12 July 2019 (28 days)

Submitted in partial fulfillment of the requirement for the award of Diploma in Computer Engineering (University Polytechnic), JMI.

Design By:
Ali Abu Bakr
Md. Atif Hussain
Diploma in Computer Engineering

Computer Engineering Section
University Polytechnic, Faculty of Engineering and Technology
Jamia Millia Islamia (A Central University)
New Delhi-110025

INDEX

ACKNOWLEDGEMENT

First of all, I would like to express my gratitude to Almighty Allah to enabling me to complete this project report on **"Architecture of Network of JMI "**

It is my pleasure to be indebted to various people, who directly or indirectly contributed in the development of this project and who influenced my thinking, behavior, and acts during the course of study.

I express my sincere gratitude to **Dr. S. M. K. Quadri** (Honorary Director-CIT, JMI) and **Mr. Syed Khalid Ali** (Network Engineer-CIT, JMI) for providing me an opportunity to undergo summer training at **FTK-Centre for Information Technology (JMI).**

I am thankful to **Mr. Abuzar** (Trainer) for his support, cooperation, and motivation provided to me during the training for constant inspiration, presence and blessings.

I also extend my sincere appreciation to my group member in summer training who provided his valuable suggestions and precious time in accomplishing my project report.

Group Member:

1. Ali Abu Bakr
2. Aayan Khan
3. Aquib Raushan
4. Ibrahim Tamimi
5. Md. Asif Hussain
6. Zubair Alam

Lastly, I would like to thank the almighty and my parents for their moral support and my friends with whom I shared my day-to-day experience and received lots of suggestions that improved my quality of work.

Name: **Md. Atif Hussain**
Roll No.: 17DCS033
Diploma in Computer Engg;
(4^{th} Sem.)

Signature of student
Date:

PREFACE

The basic goal of the information technology is to efficiently capture and organize the available information in a manner that would avail the management to concretes more on decisional issue rather than daily business chores. This has been very important factor in the growth of computer technology and its quick amalgamation with the different business process.

The present project report on "Architecture of network in Jamia Millia Islamia". The objective of the summer training was to familiarize the student with the implementation of network knowledge she/he earned in the campus. The practical knowledge is far different from the bookish knowledge that a student achieves in an institution.

The major problem that I faced during my training was that there were not sufficient published documents available on the network from where I could get any information about the university. Due to limitation of time it was not possible to include all the aspects of the network. The report focus on the important aspects of architecture of network in JMI. An important thing that I feel important to mention that in some cases, some practices are performed which are not accepted theoretically.

The center today offers essential ICT services including Internet Access, Emailing, Jamia MIS, IT security, WiFi, University Portal development and maintenance, Problem diagnostics and troubleshooting etc. through a network comprising of approximately 7000+ nodes. All ICT services offered by the centre remain operational on 24x7 across the University. To provide Internet facility and access to online learning material, the Center administers a 1-Gbps link to National Knowledge Network. In addition, the centre manages an additional Internet bandwidth of 44 Mbps available through other operators.

The present is not free of limitations. There might have problems regarding lack of limitation in some aspects and also some minor mistakes such as typing mistakes. These few drawbacks have occurred merely due to time limitation and lack of secondary sources of information's. Though I have tried my best to keep the report free from errors, I apologize if any error is found which was not deliberately made. If the report can help any person in providing information, I will feel that the purpose of the report has been fulfilled. I hope that the project report made by us will be of great help to get the comprehensive knowledge of the network in JMI.

The project duration was four weeks. This commenced from 13th June to 12th July 2019.

……..
Md. Atif Hussain
Roll No.: 17DCS033
Diploma in Computer Engg. (4th Sem.)

FTK-Centre For Information Technology (JMI)

The FTK-Centre For Information Technology is a state-of-the-art centre in Jamia Millia Islamia which caters to the ICT requirements of the University. Originally it was established in the year 1984 as a Computer Center with objective of providing basic computing facilities to the students and teachers. During past three-decades the centre has evolved from a small computing facility to a critical central facility of the University. Keeping its ethos of refurbishing education and research with modernization, the Jamia Millia Islamia has been leveraging the ICT as a tool to induce strategic improvement and changes in the system. The FTK-Centre for Information Technology has thus taken an important role of IT enabler for the University.

The centre today offers essential ICT services including Internet Access, Emailing, Jamia MIS, IT security, WiFi, University Portal development and maintenance, Problem diagnostics and troubleshooting etc. through a network comprising of approximately 7000+ nodes. All ICT services offered by the centre remain operational on 24x7 across the University. To provide Internet facility and access to online learning material, the Center administers a 1-Gbps link to National Knowledge Network. In addition, the centre manages an additional Internet bandwidth of 44 Mbps available through other operators.

The FTK-Centre for Information Technology also played a critical role in making Jamia Millia Islamia a pioneer central university by implementing a fully integrated 18-module ERP system popularly known as Jamia MIS. It provides transactional support to all functional requirements of the University ranging from admission of students to conduct of classes, recruitment of staff to retirement procedures, payroll etc. Ever since implementation of Jamia MIS in 2003-2004, the FTK-Centre For Information Technology is constantly working to evolve the system further by developing new features to enhance transparency and efficiency in the system. In the World Education Summit - 2011, the Jamia Millia Islamia got the Best Jury Aaward for the “Best ICT Enabled Institution of Higher Learning” for the ‘File Tracking System’ utility developed by the FTK-Centre For Information Technology.

The center also maintains a state-of-the-art Web Portal of the University. The feature rich portal is based on Web 2.0 technologies and provides up-to-date information to the external as well as internal users of the university. New features such as Anti-plagiarism service, On-line E-Contents”, On-line Admissions, Fee payment etc. have also been recently introduced.

To promote collaboration amongst academic and administrative staff of the University, the Center recently implemented Google Apps for education. More than 1870 accounts have already been created for this facility for Jamia teaching, administrative and technical staff. In addition to the Jamia eMail service, the users get access to Google Docs, Calendars, Groups etc. The FTK-Centre For Information Technology also provide such facilities to its students under Microsoft’s Live@Edu program.

NETWORK

A network, in computing, is a group of two or more devices that can communicate. In practice, a network is comprised of a number of different computer systems connected by physical and/or wireless connections. The scale can range from a single PC sharing out basic peripherals to massive data centers located around the World, to the Internet itself. Regardless of scope, all networks allow computers and/or individuals to share information and resources.

Computer networks serve a number of purposes, some of which include:

- Communications such as email, instant messaging, chat rooms, etc.
- Shared hardware such as printers and input devices
- Shared data and information through the use of shared storage devices
- Shared software, which is achieved by running applications on remote computers

Early computer networks of the late 1950s included the U.S. military's Semi-Automatic Ground Environment (SAGE) and the commercial airline reservation system called the Semi-Automatic Business Research Environment (SABRE). Based on designs developed in the 1960s, the Advanced Research Projects Agency Network (ARPANET) was created in 1969 by the U.S. Department of Defense and was based on circuit switching – the idea that a single communication line, such as a two-party telephone connection, deserves a dedicated circuit for the duration of the communication. This simple network evolved into the present day Internet.

Some of the basic hardware components that can be used in networks include:

- **Interface Cards:** These allow computers to communicate over the network with a low-level addressing system using media access control (MAC) addresses to distinguish one computer from another.
- **Repeaters:** These are electronic devices that amplify communication signals and also filter noise from interfering with the signals.
- **Hubs:** These contain multiple ports, allowing a packet of information/data to be copied unmodified and sent to all computers on the network.
- **Bridges:** These connect network segments, which allows information to flow only to specific destinations
- **Switches:** These are devices that forward, make forwarding decisions and otherwise filter chunks of data communication between ports according to the MAC addresses in the packets of information.
- **Routers:** These are devices that forward packets between networks by processing the information in the packet.
- **Firewalls:** These reject network access requests from unsafe sources, but allow requests for safe ones.

Types of Network

The Network allows computers to connect and communicate with different computers via any medium. LAN, MAN and WAN are the three major types of the network designed to operate over the area they cover. There are some similarities and dissimilarities between them. One of the major differences is the geographical area they cover, i.e. LAN covers the smallest area; MAN covers an area larger than LAN and WAN comprises the largest of all.

There are other types of Computer Networks also, like :

PAN (Personal Area Network)

SAN (Storage Area Network)

EPN (Enterprise Private Network)

VPN (Virtual Private Network)

- **Local Area Network (LAN) –**

LAN or Local Area Network connects network devices in such a way that personal computer and workstations can share data, tools and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol. Private addresses are unique in relation to other computers on the local network. Routers are found at the boundary of a LAN, connecting them to the larger WAN.

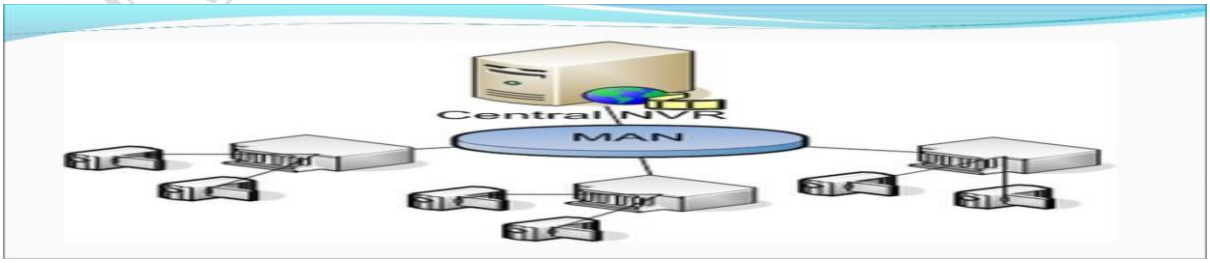
Data transmits at a very fast rate as the number of computers linked are limited. By definition, the

connections must be high speed and relatively inexpensive hardware (Such as hubs, network adapters and Ethernet cables). LANs cover smaller geographical area (Size is limited to a few kilometers) and are privately owned. One can use it for an office building, home, hospital, schools, etc. LAN is easy to design and maintain. A Communication medium used for LAN has twisted pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized.

- **Metropolitan Area Network (MAN) –**

MAN or Metropolitan area Network covers a larger area than that of a LAN and smaller area as compared to WAN. It connects two or more computers that are apart but resides in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). MAN is designed for customers who need a high-speed connectivity. Speeds of MAN ranges in terms of Mbps. It's hard to design and maintain a Metropolitan Area Network.

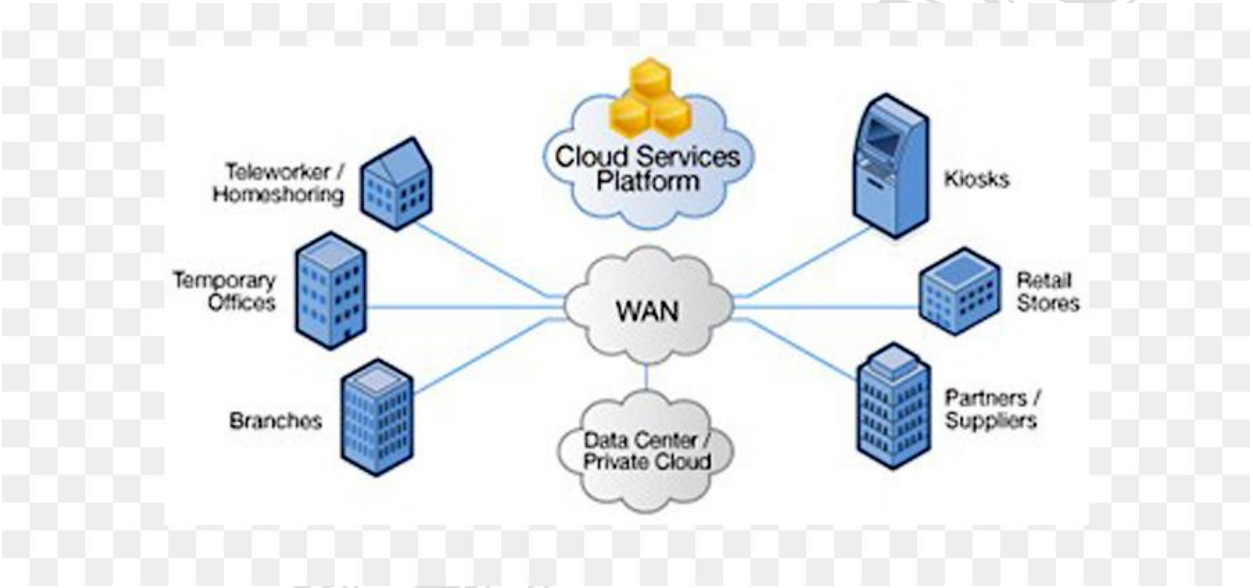
The fault tolerance of a MAN is less and also there is more congestion in the network. It is costly and may or may not be owned by a single organization. The data transfer rate and the propagation delay of MAN is moderate. Devices used for transmission of data through MAN are: Modem and Wire/Cable. Examples of a MAN are the part of the telephone company network that can provide a high-speed DSL line to the customer or the cable TV network in a city.



- **Wide Area Network (WAN) –**

WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. A WAN could be a connection of LAN connecting to other LAN's via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high speed and relatively expensive.

There are two types of WAN: Switched WAN and Point-to-Point WAN. WAN is difficult to design and maintain. Similar to a MAN, the fault tolerance of a WAN is less and there is more congestion in the network. A Communication medium used for WAN is PSTN or Satellite Link. Due to long distance transmission, the noise and error tend to be more in WAN.



OSI Model

OSI stands for Open Systems Interconnection. It has been developed by ISO – 'International Organization of Standardization', in the year 1974. It is a 7 layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.

Layers of OSI Model

Types of Layers

- Software Layer
- Hardware Layer

Heart of OSI Layer

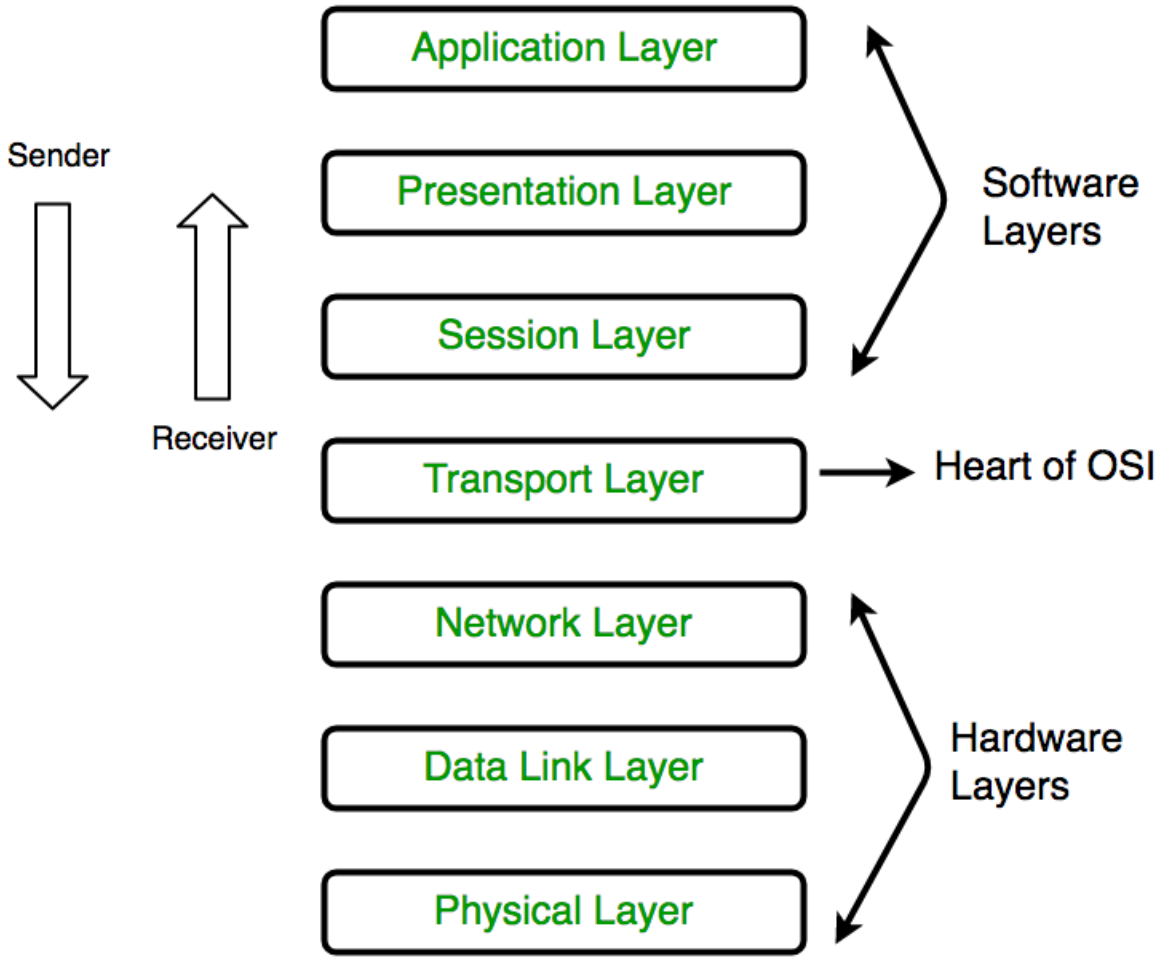
- Transport Layer

Software Layer

- Application Layer
- Presentation Layer
- Session Layer

Hardware Layer

- Physical Layer
- Data Link Layer
- Network Layer



1. Physical Layer (Layer 1) :

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual

physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for the actual physical connection between the devices. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

The functions of the physical layer are :

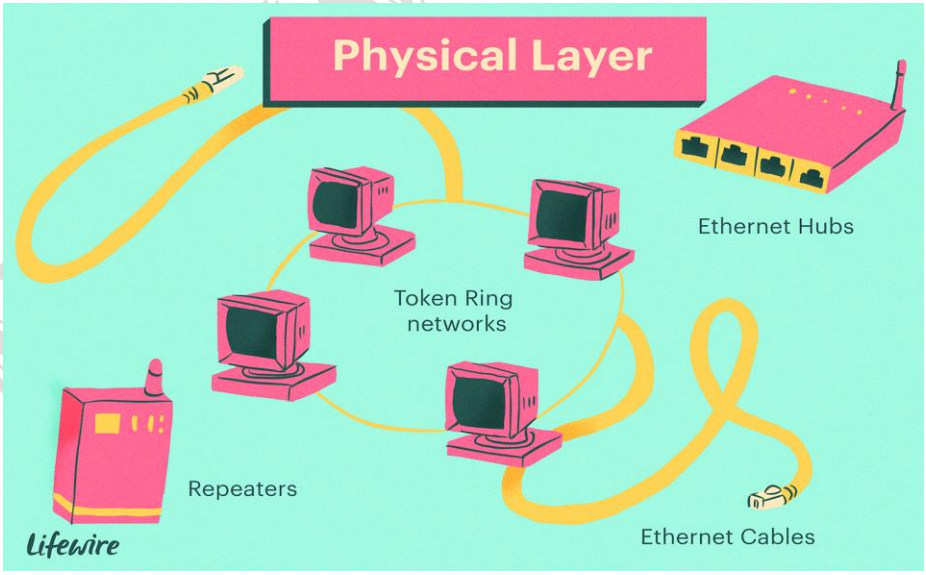
Bit synchronization: The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.

Bit rate control: The Physical layer also defines the transmission rate i.e. the number of bits sent per second.

Physical topologies: Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topolgy.

Transmission mode: Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

- Hub, Repeater, Modem, Cables are Physical Layer devices.
- Network Layer, Data Link Layer and Physical Layer are also known as Lower Layers or Hardware Layers.



2. Data Link Layer (DLL) (Layer 2) :

The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.

Data Link Layer is divided into two sub layers :

- Logical Link Control (LLC)
- Media Access Control (MAC)

The packet received from Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.

The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.

The functions of the data Link layer are :

Framing: Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.

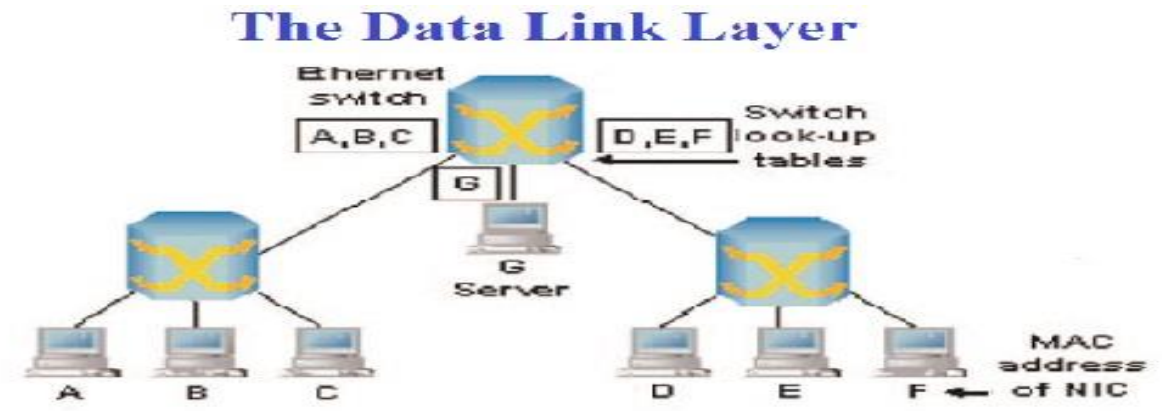
Physical addressing: After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.

Error control: Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.

Flow Control: The data rate must be constant on both sides else the data may get corrupted thus , flow control coordinates that amount of data that can be sent before receiving acknowledgement.

Access control: When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

- Packet in Data Link layer is referred as Frame.
- Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.
- Switch & Bridge are Data Link Layer devices.



3. Network Layer (Layer 3) :

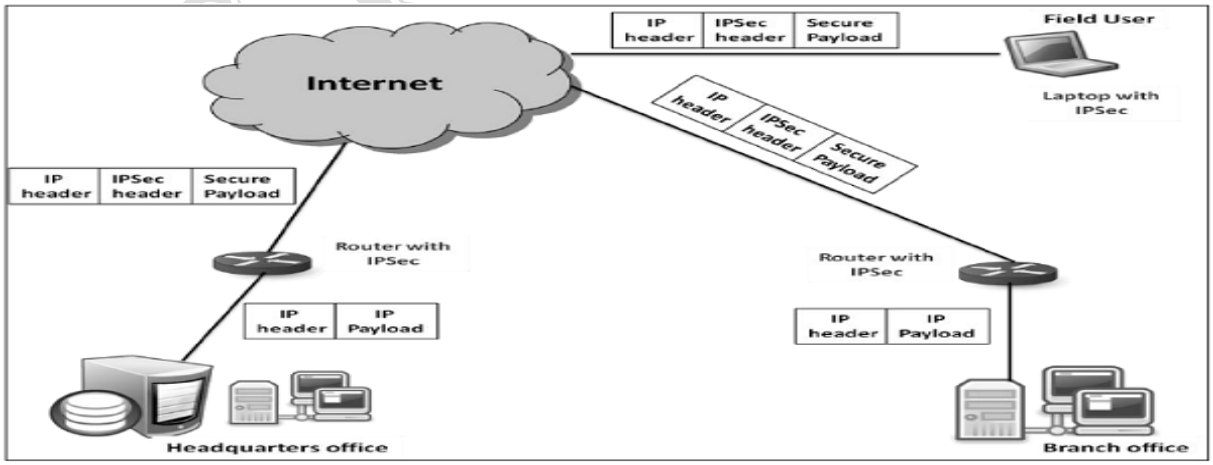
Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP address are placed in the header by network layer.

The functions of the Network layer are :

Routing: The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.

Logical Addressing: In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

- Segment in Network layer is referred as Packet.
- Network layer is implemented by networking devices such as routers.



4. Transport Layer (Layer 4) :

Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as Segments. It is responsible for the End to End delivery of the complete message. Transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

• At sender's side:

Transport layer receives the formatted data from the upper layers, performs Segmentation and also implements Flow & Error control to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.

Note: The sender need to know the port number associated with the receiver's application. Generally, this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default port assigned.

• At receiver's side:

Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

The functions of the transport layer are :

Segmentation and Reassembly: This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segment produced has a header associated with it. The transport layer at the destination station reassembles the message.

Service Point Addressing: In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

The services provided by transport layer :

Connection Oriented Service: It is a three-phase process which include

- Connection Establishment
- Data Transfer
- Termination / disconnection

In this type of transmission, the receiving device sends an acknowledgment, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.

Connection less service: It is a one phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection oriented Service is more reliable than connection less Service.

Data in the Transport Layer is called as Segments.

- Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.
- Transport Layer is called as Heart of OSI model.

5. Session Layer (Layer 5) :

This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.

The functions of the session layer are :

Session establishment, maintenance and termination: The layer allows the two processes to establish, use and terminate a connection.

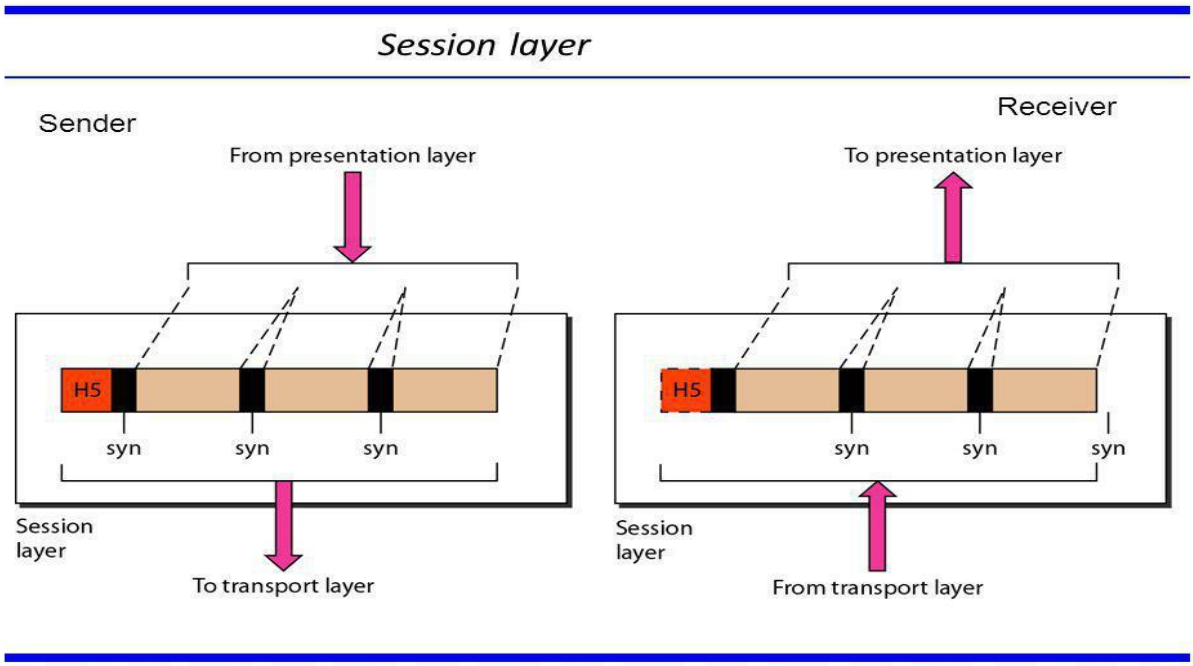
Synchronization : This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.

Dialog Controller : The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

- All the below 3 layers(including Session Layer) are integrated as a single layer in TCP/IP model as "Application Layer".
- Implementation of these 3 layers is done by the network application itself. These are also known as Upper Layers or Software Layers.

SCENARIO:

Let's consider a scenario where a user wants to send a message through some Messenger application running in his browser. The "Messenger" here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data) and converted into bits (0's and 1's) so that it can be transmitted.



6. Presentation Layer (Layer 6) :

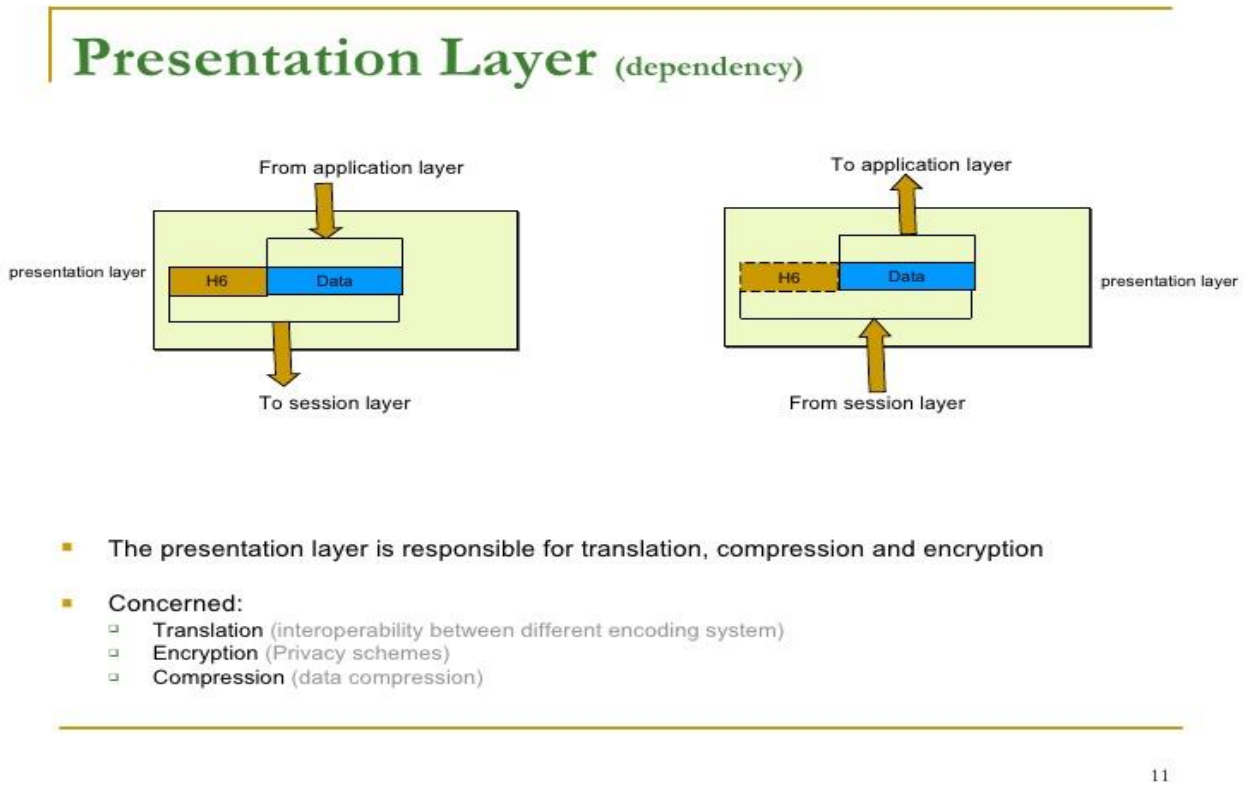
Presentation layer is also called the Translation layer.The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

The functions of the presentation layer are :

Translation : For example, ASCII to EBCDIC.

Encryption/ Decryption : Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.

Compression: Reduces the number of bits that need to be transmitted on the network.



7. Application Layer (Layer 7) :

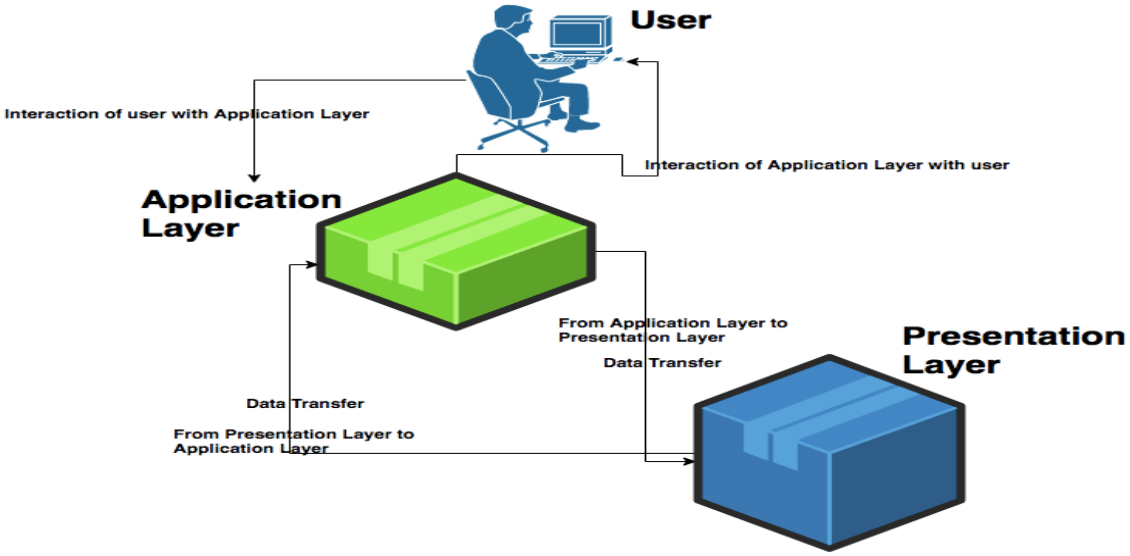
At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

Ex: Application – Browsers, Skype Messenger etc.

- Application Layer is also called as Desktop Layer.

The functions of the Application layer are :

- Network Virtual Terminal
- FTAM-File transfer access and management
- Mail Services
- Directory Services



How Application Layer Works

Networking Cables

Networking cables are networking hardware used to connect one network device to other network devices or to connect two or more computers to share printers, scanners etc. Different types of network cables, such as coaxial cable, optical fiber cable, and twisted pair cables, are used depending on the network's physical layer, topology, and size. The devices can be separated by a few meters (e.g. via Ethernet) or nearly unlimited distances (e.g. via the interconnections of the Internet).

There are several technologies used for network connections. Patch cables are used for short distances in offices and wiring closets. Electrical connections using twisted pair or coaxial cable are used within a building. Optical fiber cable is used for long distances or for applications requiring high bandwidth or electrical isolation. Many installations use structured cabling practices to improve reliability and maintainability. In some home and industrial applications power lines are used as network cabling.

Ethernet

Ethernet is the technology that is most commonly used in wired local area networks (LANs). A LAN is a network of computers and other electronic devices that covers a small area such as a

room, office, or building. It is used in contrast to a wide area network (WAN), which spans much larger geographical areas. Ethernet is a network protocol that controls how data is transmitted over a LAN. Technically it is referred to as the IEEE 802.3 protocol. The protocol has evolved and improved over time to transfer data at the speed of a gigabit per second.

Many people have used Ethernet technology their whole lives without knowing it. It is most likely that any wired network in your office, at the bank, and at home is an Ethernet LAN. Most desktop and laptop computers come with an integrated Ethernet card inside so they are ready to connect to an Ethernet LAN.

Analog to Digital Converter

From the name itself it is clear that it is a converter which converts the analog (continuously variable) signal to digital signal. This is really an electronic integrated circuit which directly converts the continuous form of signal to discrete form. It can be expressed as A/D or A-to-D or A-D or ADC. The input (analog) to this system can have any value in a range and are directly measured. But for output (digital) of an N-bit A/D converter, it should have only 2N discrete values. This A/D converter is a linkage between the analog (linear) world of transducers and discreet world of processing the signal and handling the data. The digital to analog converter (DAC) carry out the inverse function of the ADC. The schematic representation of ADC is shown below.

Figure 1

ADC Process

There are mainly two steps involves in the process of conversion. They are

- Sampling and Holding
- Quantizing and Encoding

The whole ADC conversion process is shown in figure 2.

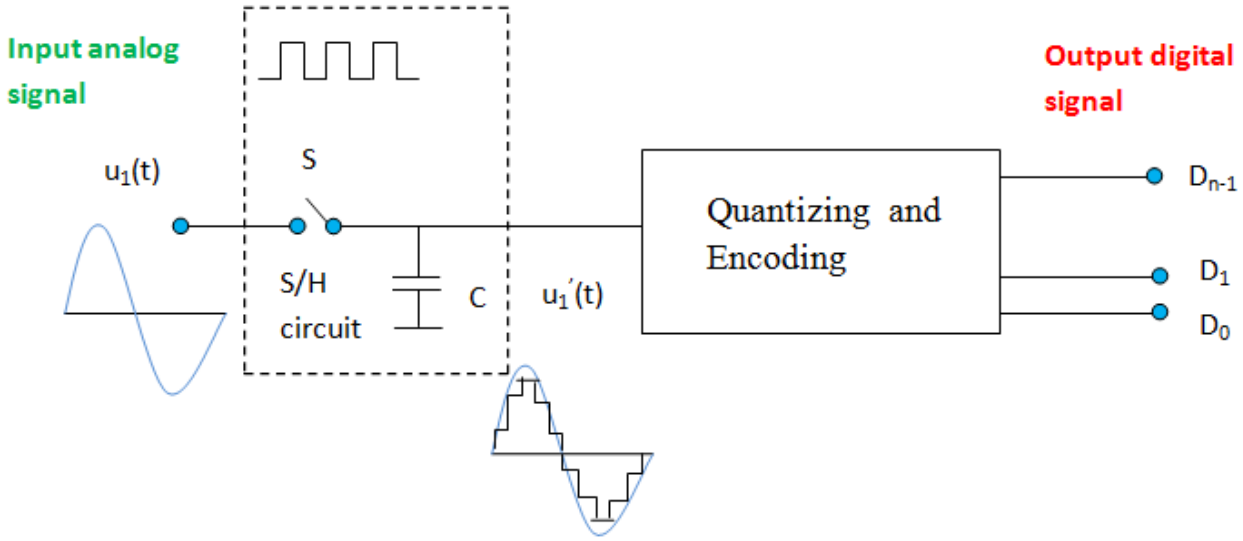


Figure 2

Sampling and Holding

In the process of Sample and hold (S/H), the continuous signal will gets sampled and freeze (hold) the value at a steady level for a particular least period of time. It is done to remove variations in input signal which can alter the conversion process and thereby increases the accuracy. The minimum sampling rate has to be two times the maximum data frequency of the input signal.

Quantizing and Encoding

For understanding quantizing, we can first go through the term Resolution used in ADC. It is the smallest variation in analog signal that will result in a variation in the digital output. This actually represents the quantization error.

V → Reference voltage range

2N → Number of states

N → Number of bits in digital output

Quantizing: It is the process in which the reference signal is partitioned into several discrete quanta and then the input signal is matched with the correct quantum.

Encoding: Here; for each quantum, a unique digital code will be assigned and after that the input signal is allocated with this digital code. The process of quantizing and encoding is demonstrated in the table below.

Analog signal			Digital o/p
7.5	7 →	7Δ=7V →	111
6.5	6 →	6Δ=6V →	110
5.5	5 →	5Δ=5V →	101
4.5	4 →	4Δ=4V →	100
3.5	3 →	3Δ=3V →	011
2.5	2 →	2Δ=2V →	010
1.5	1 →	1Δ=1V →	001
0.5	0 →	0Δ=0V →	000

From the above table we can observe that only one digital value is used to represent the whole range of voltage in an interval. Thus, an error will occur and it is called quantization error. This is the noise introduced by the process of quantization. Here the maximum quantization error is

$$\pm \frac{1}{2}\triangle V = \pm\, 0.5V$$

Improvement of Accuracy in ADC

Two important methods are used for improving the accuracy in ADC. They are by increasing the resolution and by increasing the sampling rate. This is shown in figure below (figure 3).

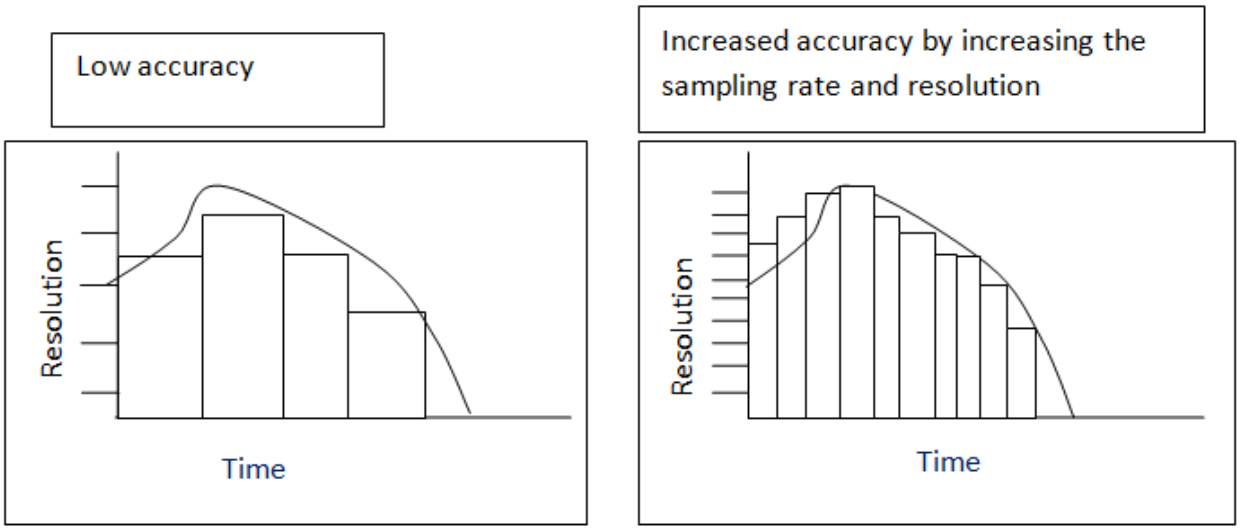


Figure 3

Types of Analog to Digital Converter

- **Successive Approximation ADC:** This converter compares the input signal with the output of an internal DAC at each successive step. It is the most expensive type.
- **Dual Slope ADC:** It have high accuracy but very slow in operation.
- **Pipeline ADC:** It is same as that of two step Flash ADC.
- **Delta-Sigma ADC:** It has high resolution but slow due to over sampling.
- **Flash ADC:** It is the fastest ADC but very expensive.
- **Other:** Staircase ramp, Voltage-to-Frequency, Switched capacitor, tracking, Charge balancing, and resolver.

Application of ADC

- Used together with the transducer.
- Used in computer to convert the analog signal to digital signal.
- Used in cell phones.
- Used in microcontrollers.
- Used in digital signal processing.
- Used in digital storage oscilloscopes.
- Used in scientific instruments.
- Used in music reproduction technology etc.

Networking Devices

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length which

the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

2. Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

Types of Hub

- **Active Hub :-** These are the hubs which have their own power supply and can clean , boost and relay the signal along the network. It serves both as a repeater as well as wiring center. These are used to extend maximum distance between nodes.
- **Passive Hub :-** These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend distance between nodes.

3. Bridge – A bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

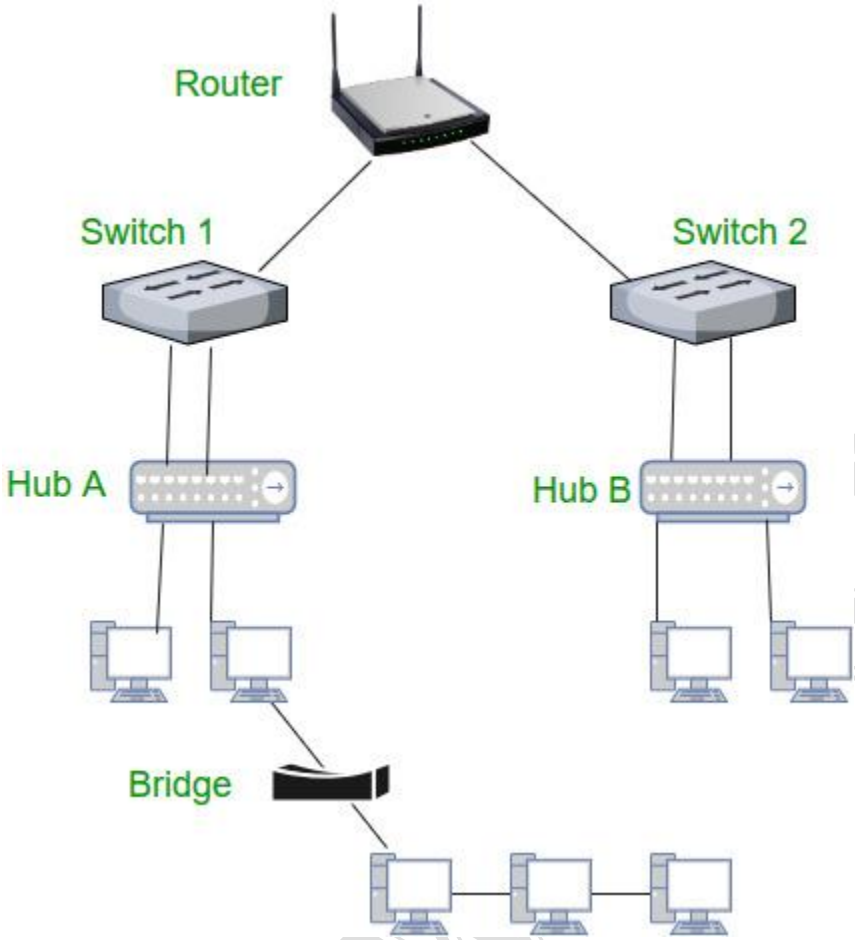
Types of Bridges

- Transparent Bridges :- These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network , reconfiguration of the stations is unnecessary. These bridges makes use of two processes i.e. bridge forwarding and bridge learning.
- Source Routing Bridges :- In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The hot can discover frame by sending a specical frame called discovery frame, which spreads through the entire network using all possible paths to destination.

4. Switch – A switch is a multi port bridge with a buffer and a design that can boost its efficiency(large number of ports imply less traffic) and performance. Switch is data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the

data packets. Router divide broadcast domains of hosts connected through it.



6. Gateway – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

7. Brouter – It is also known as bridging router is a device which combines features of both bridge and router. It can work either at data link layer or at network layer. Working as router, it is capable of routing packets across networks and working as bridge, it is capable of filtering local area network traffic.

Internet Protocol(IP)

An Internet Protocol address (IP address) is a logical numeric address that is assigned to every single computer, printer, switch, router or any other device that is part of a TCP/IP-based network.

The IP address is the core component on which the networking architecture is built; no networkexists without it. An IP address is a logical address that is used to uniquely identify every node in the network. Because IP addresses are logical, they can change. They are similar to addresses in a town or city because the IP address gives the network node an address so that it can communicate with other nodes or networks, just like mail is sent to friends and relatives.

The numerals in an IP address are divided into 2 parts:

- The network part specifies which networks this address belongs to and
- The host part further pinpoints the exact location.

IPv4 and IPv6 addresses

IPv4 addresses are 32 bits long (four bytes). An example of an IPv4 address is 216.58.216.164, which is the front page of Google.com.

The maximum value of a 32-bit number is 232, or 4,294,967,296. So the maximum number of IPv4 addresses, which is called its address space, is about 4.3 billion. In the 1980s, this was sufficient to address every networked device, but scientists knew that this space would quickly become exhausted. Technologies such as NAT have delayed the problem by allowing many devices to use a single IP address, but a larger address space is needed to serve the modern Internet.

A major advantage of IPv6 is that it uses 128 bits of data to store an address, permitting 2128 unique addresses, or 340,282,366,920,938,463,463,374,607,431,768,211,456. The size of IPv6's address space — 340 duodecillion — is much, much larger than IPv4.

IP address classes

With an IPv4 IP address, there are five classes of available IP ranges: Class A, Class B, Class C, Class D and Class E, while only A, B, and C are commonly used. Each class allows for a range of valid IP addresses, shown in the following table.

Class	Address range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or research and development purposes.

Ranges 127.x.x.x are reserved for the loopback or localhost, for example, 127.0.0.1 is the loopback address. Range 255.255.255.255 broadcasts to all hosts on the local network.

Static vs. dynamic IP addresses

IP addresses are assigned in two different ways. They may be dynamically assigned (they can change automatically) or statically assigned (they're intended not to change, and must be changed manually). Most home networks use dynamic allocation. Your router uses DHCP to temporarily assign, or "lease," an IP address to your device. After a period of time, this lease "expires," and the router renews your old address or assigns you a new one, depending on the needs of the network and the configuration of the router.

The most common default addresses assigned by home routers are shown below.

192.168.1.0: This number, called the network number, identifies the network as a whole, and is not assigned to a device.

192.168.1.1: The common default address assigned to the gateway device. In most home networks, the gateway is the router itself.

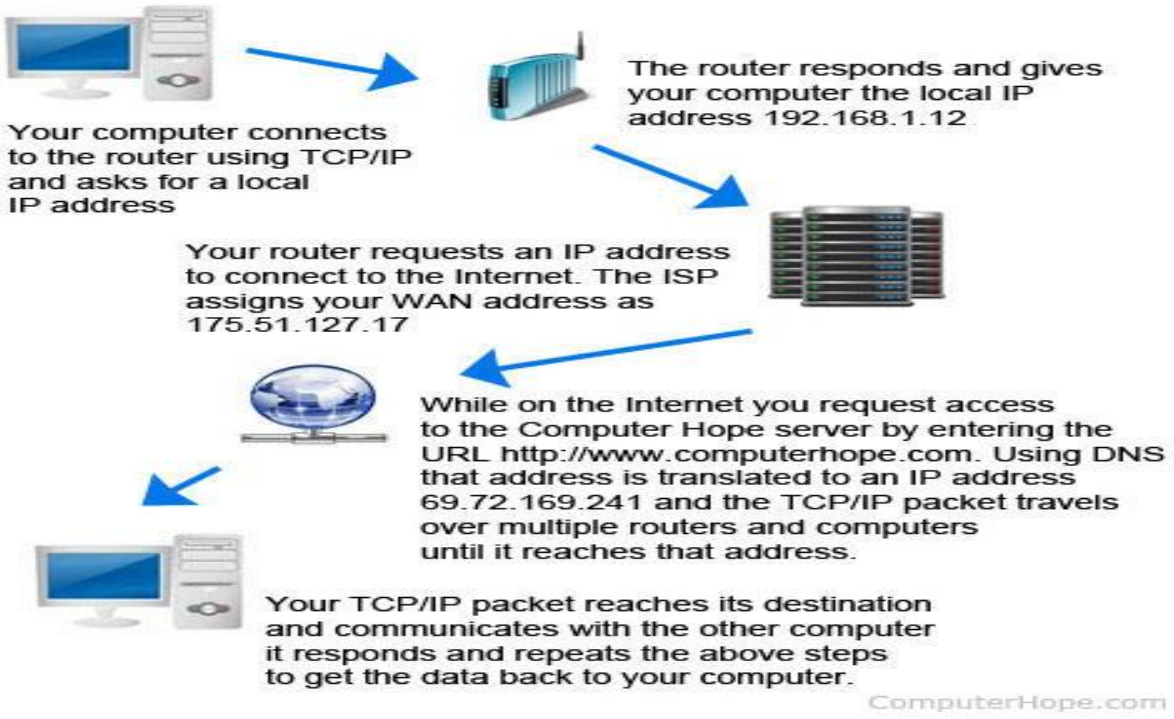
192.168.1.2: Another common gateway address. Or, it may be assigned to a device on the network.

192.168.1.3–254: Assigned to devices on the network.

192.168.1.255: The broadcast address of the network. Data sent to this address is automatically broadcast to addresses 1–254.

How data is sent to an IP address on another network

The following diagram illustrates how your home computer might obtain an IP address and send data to an IP address on another network.



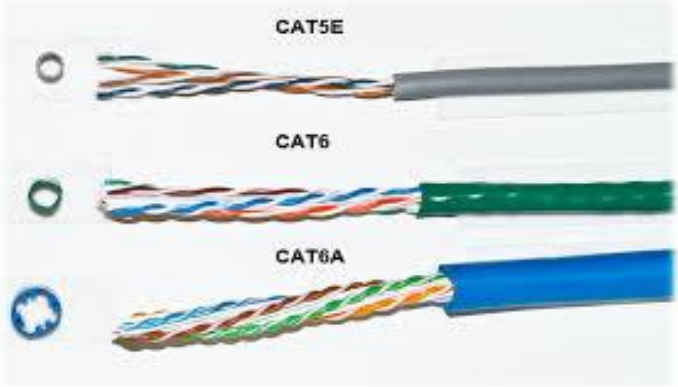
CATEGORY 5 & 6 CABLE

Category 5 cable, commonly referred to as Cat 5, is a twisted pair cable for computer networks. Since 2001, the variant commonly in use is the Category 5e specification (Cat 5e). The cable standard provides performance of up to 100 MHz and is suitable for most varieties of Ethernet over twisted pair up to 1000BASE-T (Gigabit Ethernet). Cat 5 is also used to carry other signals such as telephony and video.

Category 6 cable, commonly referred to as Cat 6, is a standardized twisted pair cable for Ethernet and other network physical layers that is backward compatible with the Category 5/5e and Category 3 cable standards.

Cat 6 has to meet more stringent specifications for crosstalk and system noise than Cat 5 and Cat 5e. The cable standard specifies performance of up to 250 MHz, compared to 100 MHz for Cat 5 and Cat 5e.

Whereas Category 6 cable has a reduced maximum length of 55 meters when used for 10GBASE-T, Category 6A cable (or Augmented Category 6) is characterized to 500 MHz and has improved alien crosstalk characteristics, allowing 10GBASE-T to be run for the same 100 meter maximum distance as previous Ethernet variants.

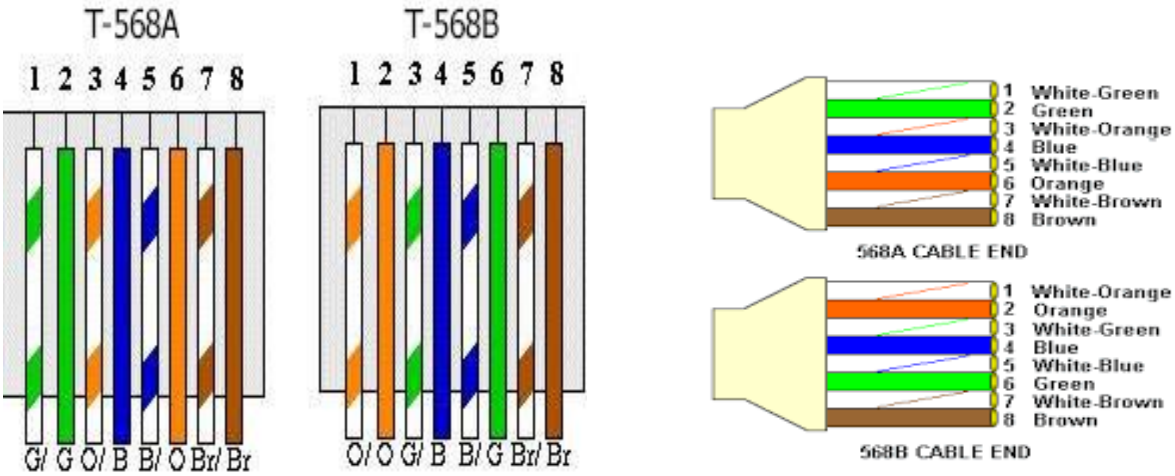


REGISTOR JACK 45 (RJ45)

A registered jack (RJ) is a standardized telecommunication network interface for connecting voice and data equipment to a service provided by a local exchange carrier or long distance carrier. Registration interfaces were first defined in the Universal Service Ordering Code (USOC) system of the Bell System in the United States for complying with the registration program for customer-supplied telephone equipment mandated by the Federal Communications Commission (FCC) in the 1970s. They were subsequently codified in title 47 of the Code of Federal Regulations Part 68.[2][3][4]

T-568A & T-568B

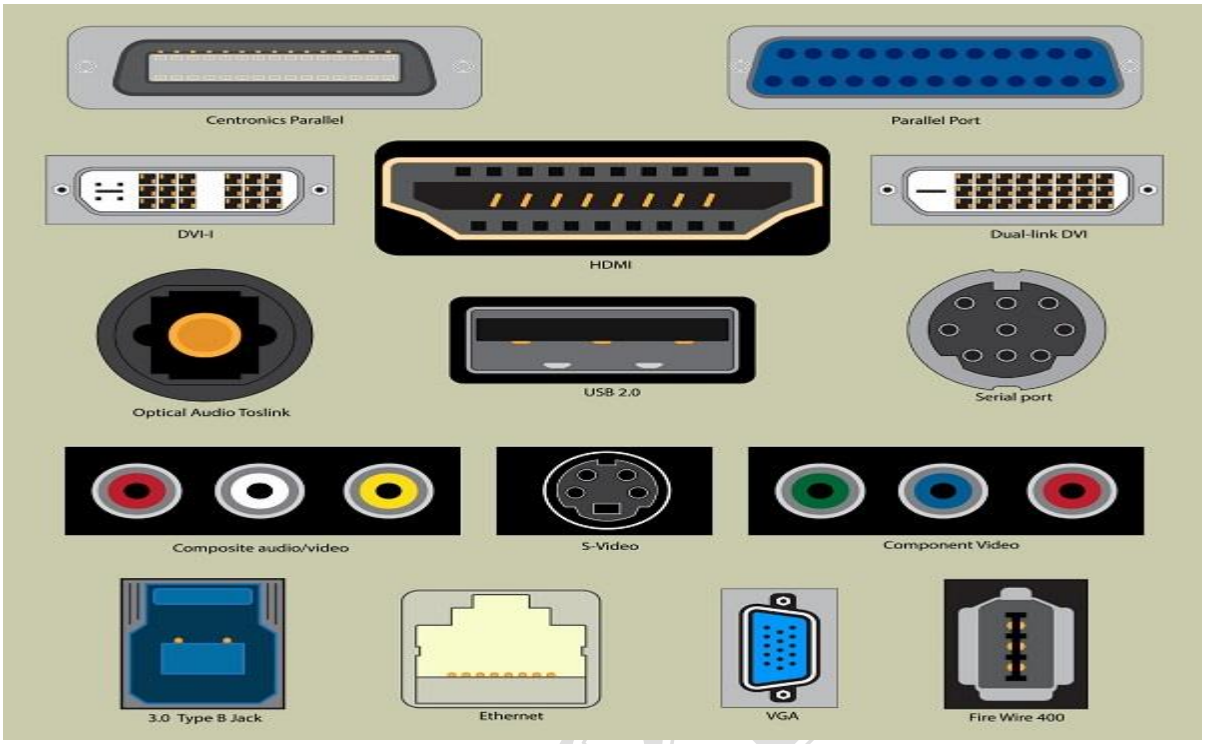
T568A and T568B are the two color codes used for wiring eight-position RJ45 modular plugs. Both are allowed under the ANSI/TIA/EIA wiring standards. The only difference between the two color codes is that the orange and green pairs are interchanged.



Input/ Output Ports And Connectors

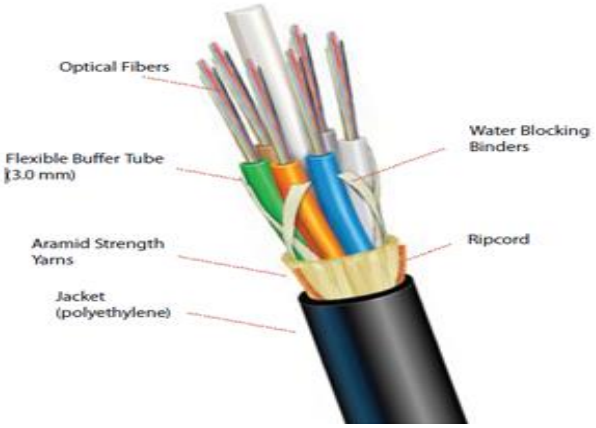
A connection point that acts as interface between the computer and external devices like mouse, printer, modem, etc. is called port. Ports are of two types −

- Internal port − It connects the motherboard to internal devices like hard disk drive, CD drive, internal modem, etc.
- External port − It connects the motherboard to external devices like modem, mouse, printer, flash drives, etc.



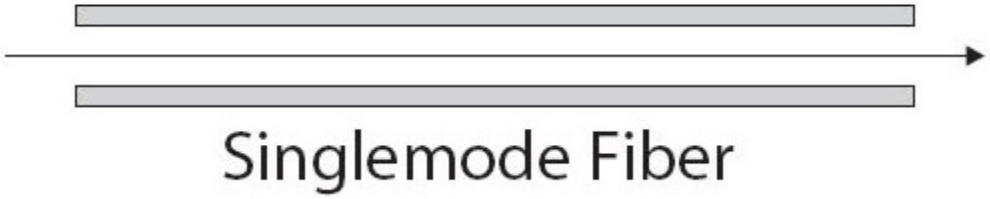
Optical Fiber Cable (OFC)

An optical fiber cable, also known as a fiber optic cable, is an assembly similar to an electrical cable, but containing one or more optical fibers that are used to carry light. 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. Different types of cable[1] are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.



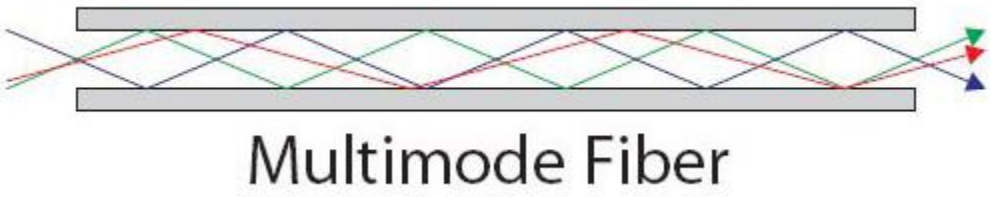
Types of OFC

Single mode optical fiber



- As the name suggests, this type of optical fiber transmits only one mode of light. To put it another way, it can carry only one wavelength of light across its length.
- This wavelength is usually 1310nm or 1550nm.
- Interestingly, single mode fibers came into existence after multimode fibers. They are more recent than the multimode cables.
- Only lasers are used as a light source. To point out, the light used in single mode fibers are not in the visible spectrum.
- Since the light travels in a straight direction, there are fewer losses, and it can be used in applications requiring longer distance connections.
- An obvious disadvantage of single mode fiber is that they are hard to couple.

Double mode optical fiber



- As the name implies, these types of optical fibers allow multiple modes of light to travel along their axis.
- To explain physically, they can do this by having a thicker core diameter.
- The wavelengths of light waves in multimode fibers are in the visible spectrum ranging from 850 to 1300 nm.
- The reflection of the waves inside the multimode fiber occurs at different angles for every mode. Consequently, based on these angles the number of reflections can vary.
- We can have a mode where the light passes without striking the core at all.
- We can have a slightly higher mode which will travel with appropriate internal reflections.

CISCO

Cisco Systems, Inc. is an American multinational technology conglomerate headquartered in San Jose, California, in the center of Silicon Valley. Cisco develops, manufactures and sells networking hardware, telecommunications equipment and other high-technology services and products.[3] Through its numerous acquired subsidiaries, such as OpenDNS, WebEx, Jabber and Jasper, Cisco specializes into specific tech markets, such as Internet of Things (IoT), domain security and energy management.

Cisco stock was added to the Dow Jones Industrial Average on June 8, 2009, and is also included in the S&P 500 Index, the Russell 1000 Index, NASDAQ-100 Index and the Russell 1000 Growth Stock Index.

Cisco Systems was founded in December 1984 by Leonard Bosack and Sandy Lerner, two Stanford University computer scientists. They pioneered the concept of a local area network (LAN) being used to connect geographically disparate computers over a multiprotocol router system. By the time the company went public in 1990, Cisco had a market capitalization of $224 million. By the end of the dot-com bubble in the year 2000, Cisco had a more than $500 billion market capitalization.

History of CISCO

Cisco Systems was founded in December 1984 by Sandy Lerner, a director of computer facilities for the Stanford University Graduate School of Business. Lerner partnered with her husband, Leonard Bosack, who was in charge of the Stanford University computer science department's computers.

Cisco's initial product has roots in Stanford University's campus technology. In the early 1980s students and staff at Stanford; including Bosack, used technology on the campus to link all of the school's computer systems to talk to one another, creating a box that functioned as a multiprotocol router called the "Blue Box". The Blue Box used software that was originally written at Stanford by research engineer William Yeager. Due to Yeager's well-designed invention, the underlying architecture was what was, in part, the key to Cisco's early success as the design scaled very well.

In 1985, Bosack and Stanford employee Kirk Lougheed began a project to formally network Stanford's campus.They adapted Yeager's software into what became the foundation for Cisco IOS, despite Yeager's claims that he had been denied permission to sell the Blue Box commercially. On July 11, 1986, Bosack and Lougheed were forced to resign from Stanford and the university contemplated filing criminal complaints against Cisco and its founders for the theft of its software, hardware designs, and other intellectual properties.In 1987, Stanford licensed the router software and two computer boards to Cisco. In addition to Bosack, Lerner, Lougheed, Greg Satz (a programmer), and Richard Troiano (who handled sales), completed the early Cisco team.[7] The company's first CEO was Bill Graves, who held the position from 1987 to 1988. In 1988, John Morgridge was appointed CEO.

The name "Cisco" was derived from the city name San Francisco, which is why the company's engineers insisted on using the lower case "cisco" in its early years. The logo is intended to depict the two towers of the Golden Gate Bridge.

On February 16, 1990, Cisco Systems went public with a market capitalization of $224 million, and was listed on the NASDAQ stock exchange. On August 28, 1990, Lerner was fired. Upon hearing the news, her husband Bosack resigned in protest. The couple walked away from Cisco with $170 million, 70% of which was committed to their own charity.

Although Cisco was not the first company to develop and sell dedicated network nodes, it was one of the first to sell commercially successful routers supporting multiple network protocols.Classical, CPU-based architecture of early Cisco devices coupled with flexibility of operating system IOS allowed for keeping up with evolving technology needs by means of frequent software upgrades. Some popular models of that time (such as Cisco 2500) managed to stay in production for almost a decade virtually unchanged. The company was quick to capture the emerging service provider environment, entering the SP market with product lines such as Cisco 7000 and Cisco 8500.[citation needed]

Between 1992 and 1994, Cisco acquired several companies in Ethernet switching, such as Kalpana, Grand Junction and most notably, Mario Mazzola's Crescendo Communications,which together formed the Catalyst business unit. At the time, the company envisioned layer 3 routing and layer 2 (Ethernet, Token Ring) switching as complementary functions of different intelligence and architecture—the former was slow and complex, the latter was fast but simple. This philosophy dominated the company's product lines throughout the 1990s.[citation needed].

Cisco Systems' products and services focus upon three market segments—enterprise and service provider, small business and the home.

Cisco has grown increasingly popular in the Asia-Pacific region over the last three decades[when?] and is the dominant vendor in the American market with leadership across all market segments.[citation needed] It uses its Australian office as one of the main headquarters for the Asia-Pacific region, offering a diverse product portfolio for long-term stability, and integration in a sustainable[citation needed] competitive advantage.

VoIP services

Cisco became a major provider of Voice over IP to enterprises, and is now moving into the home user market through its acquisitions of Scientific Atlanta and Linksys. Scientific Atlanta provides VoIP equipment to cable service providers such as Time Warner, Cablevision, Rogers Communications, UPC and others; Linksys has partnered with companies such as Skype, Microsoft and Yahoo! to integrate consumer VoIP services with wireless and cordless phones.

Hosted Collaboration Solution (HCS)

Cisco partners can offer cloud-based services based on Cisco's virtualized Unified Computing

System (UCS). A part of the Cisco Unified Services Delivery Solution that includes hosted versions of Cisco Unified Communications Manager (UCM), Cisco Unified Contact Center, Cisco Unified Mobility, Cisco Unified Presence, Cisco Unity Connection (unified messaging) and Cisco Webex Meeting Center.

Network Emergency Response

As part of its Tactical Operations initiative, Cisco maintains several Network Emergency Response Vehicles (NERV)s.[20] The vehicles are maintained and deployed by Cisco employees during natural disasters and other public crises. The vehicles are self-contained and provide wired and wireless services including voice and radio interoperability, voice over IP, network-based video surveillance and secured high-definition video-conferencing for leaders and first responders in crisis areas with up to 3 Mbit/s of bandwidth (up and down) via a 1.8-meter satellite antenna.

NERVs are based at Cisco headquarters sites in San Jose, California and at Research Triangle Park, North Carolina, allowing strategic deployment in North America. They can become fully operational within 15 minutes of arrival. High-capacity diesel fuel-tanks allow the largest vehicles to run for up to 72 hours continuously. The NERV has been deployed to incidents such as the October 2007 California wildfires; hurricanes Gustav, Ike and Katrina; the 2010 San Bruno gas pipeline explosion, tornado outbreaks in North Carolina and Alabama in 2011; and Hurricane Sandy in 2012.

The Tactical Operations team maintains and deploys smaller, more portable communication kits to emergencies outside of North America. In 2010, the team deployed to assist in earthquake recovery in Haiti and in Christchurch (New Zealand). In 2011, they deployed to flooding in Brazil, as well as in response to the 2011 earthquake and tsunami in Japan.

In 2011, Cisco received the Innovation Preparedness award from the American Red Cross Silicon Valley Chapter for its development and use of these vehicles in disasters.

Fig: CISCO COMPUTER

Fig: CISCO ROUTER

AVAYA

In 1995, Lucent Technologies was spun off from AT&T, and Lucent spun off units of its own in an attempt to restructure its struggling operations.

Avaya was then spun off as its own company in 2000. It remained a public company from 2000 to 2007, when it was purchased by private equity firms.

In 2001, the Mark Avaya Interaction Center for customer relationship management began, enabling businesses to draw multi-platform call centers to multimedia, multi-site contact centers. A proposed "converged communications" road map focused on the role that applications would play in making communications improve business performance.

On December 15, 2017, it again became a public company, trading under the stock ticker AVYA.

Acquisitions

Since 2001, Avaya has sold and acquired several companies, including VPNet Technologies, VISTA Information Technologies, Quintus, RouteScience, Tenovis, Spectel, NimCat Networks, Traverse Networks, Ubiquity Software Corporation, Agile Software NZ Limited, Konftel, Sipera, Aurix, Radvision and Esnatech.Through Nortel bankruptcy proceedings, assets related to their Enterprise Voice and Data business units were auctioned. Avaya placed a $900 million bid, and was announced as the winner of the assets on September 14, 2009.

Avaya Product

Cisco 2900 Series Integrated Services Routers

Services-rich router for medium-sized branches

Cisco 2900 Series Integrated Services Routers (ISR) are designed to meet the application demands of today's medium-sized branches and to evolve to cloud-based services. They deliver virtualized applications and highly secure collaboration through the widest array of WAN connectivity at high performance that offers concurrent services at up to 75 Mbps.

AVAYA Switches

Fig:Avaya Ethernet Routing Switches 4800 Series

A cost effective, feature rich solution, the Avaya Ethernet Routing Switch (ERS) 3000 series is a family of standalone or stackable Fast Ethernet and Gigabit Ethernet switching products perfectly suited to the unique requirements of small offices. The ERS 3000 series support Layer 2 switching and Layer 3 routing, advanced convergence features including support for PoE and PoE+ as well as a wide range of security features. The new ERS 3600 (v6.0) provides improved performance and IP services capability for the growing sophistication needed by SME and small midmarket customers.

Features & Benefits

Energy efficient: On average 36% more energy efficient than competitive solutions,* energy saver functionality further reduces power consumption for both Switch and IP Phone without losing telephony connectivity.

Powerful: Wire-speed performance, true pay-as-you-grow Stackable Chassis capabilities, delivering up to 400 ports and 384 Gbps of virtual backplane throughput.

Secure : Standards-based 802.1x with integration with Avaya's Identity Engines portfolio for centralized, policy-based authenticated network access.

Flexible : Mix-and-match best-in-class stacking capabilities with support for PoE/PoE+ and optional 1GbE / 10GbE SFP+ uplinks.

Fabric-ready : Support for Avaya Fabric Connect that extends virtual fabric services from the data center all the way to the wiring closet.

Ethernet Routing Switch 5600 Series

Fig:Ethernet Routing Switch 5600 Series

Ethernet Routing Switch 5600 Series or (ERS 5600) in computer networking terms are stackable routers and switches designed and manufactured by Avaya. The ERS 5600 Switches can be stacked up to 8 units high to create a 1.152 Tbit/s backplane through the Flexible Advanced Stacking Technology (FAST) stacking technology configuration. The 5600 Series consists of five stackable models that can be mixed and matched together with other ERS 5600 models or other ERS 5500 models to meet configuration requirements.Additionally the ports on the switches incorporates the Avaya Energy Saver (AES) which can manage and dim down (reduce the wattage requirements of each port and/or the PoE wattage) the power requirements to save energy across all switches in the enterprise.

Cisco Aironet 1700 Series Access Points

Entry-Level 802.11ac Access Points

The entry-level Cisco Aironet 1700 Series Access Points take advantage of the latest 802.11ac Wi-Fi technology. Designed to meet the growing needs of today's small and medium-sized, wireless, enterprise networks, the Aironet 1700 Series Access Point offer the right value to help customers ease into 802.11ac networking.

Features and Capabilities

The Cisco Aironet 1700 Series is a component of our flagship, 802.11ac-enabled Aironet Series Access Points that deliver high-performance, comprehensive mobility experiences. The series offers

- Entry-level access points for small to midsize organizations
- An attractive price and performance for migrating to 802.11ac
- 802.11ac Wave 1 support with 3x3 multiple input, multiple output (MIMO) equalization
- Cisco CleanAir Express Spectrum Intelligence across 20-, 40-, and 80-MHz-wide channels
- Optimized Roaming intelligently decides proper access points as people move.

The Cisco Aironet 3700 Series Access Point

The Cisco Aironet 3700 Series Access Point supports 802.11ac Wave 1. But if you're looking to expand your wireless network or deploy a new one, consider the next-generation Cisco Aironet 3800 Series Access Point. It supports the latest Wi-Fi standard, 802.11ac Wave 2, for speeds up to 2.34 Gbps. That’s up from 1.3 Gbps in Wave 1.

Features and benefits

Integrated Wave 1 radio: The 3700 Series is the industry's first wireless access point with integrated 802.11ac Wave 1 radio to support a 4x4 MIMO with three spatial streams

CleanAir Technology: Meet and exceed your needs for high-density network environments. This series supports Cisco High Density Experience (HDX) technology, including CleanAir support for 20-, 40-, and 80-MHz channels.

Cisco ClientLink 3.0: Boost performance for all clients, including 802.11ac, with the updated ClientLink for high-density wireless networks.

Two versions: The 3700i model has integrated antennas for typical office deployments. The 3700e model requires external dual-band antennas, and is for RF-challenging indoor environments. Both have dual-band 2.4/5-GHz integrated radios.

Optional hyperlocation: Add the Cisco Hyperlocation Module solution for exceptional location accuracy for indoor Wi-Fi.

CISCO Nexus 93108 TC-FX

Fig: CISCO Nexus 93108 TC-FX

Cloud Scale technology, 10GBASE-T switching

Get high-density, nonblocking, and low-power 48 x 100M/1/10GBASE-T ports in the Cisco Nexus 93108TC- FX switch. Ideal for leaf-and-spine deployment in enterprise, service provider facilities, large virtualized, and cloud computing environments, it supports Cisco Tetration Analytics for deep telemetry and Cisco Application Centric Infrastructure (ACI).

Features and Capabilities

Architectural Flexibility:

- Leaf node support for Cisco ACI architecture with flexible port configuration
- 100-Mbps, 1 and 10 GBASE-T server connectivity
- Easy migration with 6 uplinks ports that can be configured as 40/100-Gbps Ethernet or FCoE ports.

Rich features:

- Automated policy-based systems management with Cisco ACI
- Open APIs enable third-party integration with our partners
- Better management of speed mismatch between access and uplink ports with 40 MB of shared buffer space

Top-notch security

- Whitelist model, policy enforcement, and application security with Cisco ACI micro-segmentation
- Wire-rate MACsec encryption on all ports
- Real-time visibility and telemetry
- Built-in Cisco Tetration sensors for rich traffic flow telemetry and line-rate data collection
- Get actionable insights in less than1 second
- Get visibility into everything in your data center

Highly available and efficient design:

- High-performance, non-blocking architecture
- Easily deployed into either a hot-aisle or cold-aisle configuration
- Redundant, hot-swappable power supplies and fan trays

Simplified operations

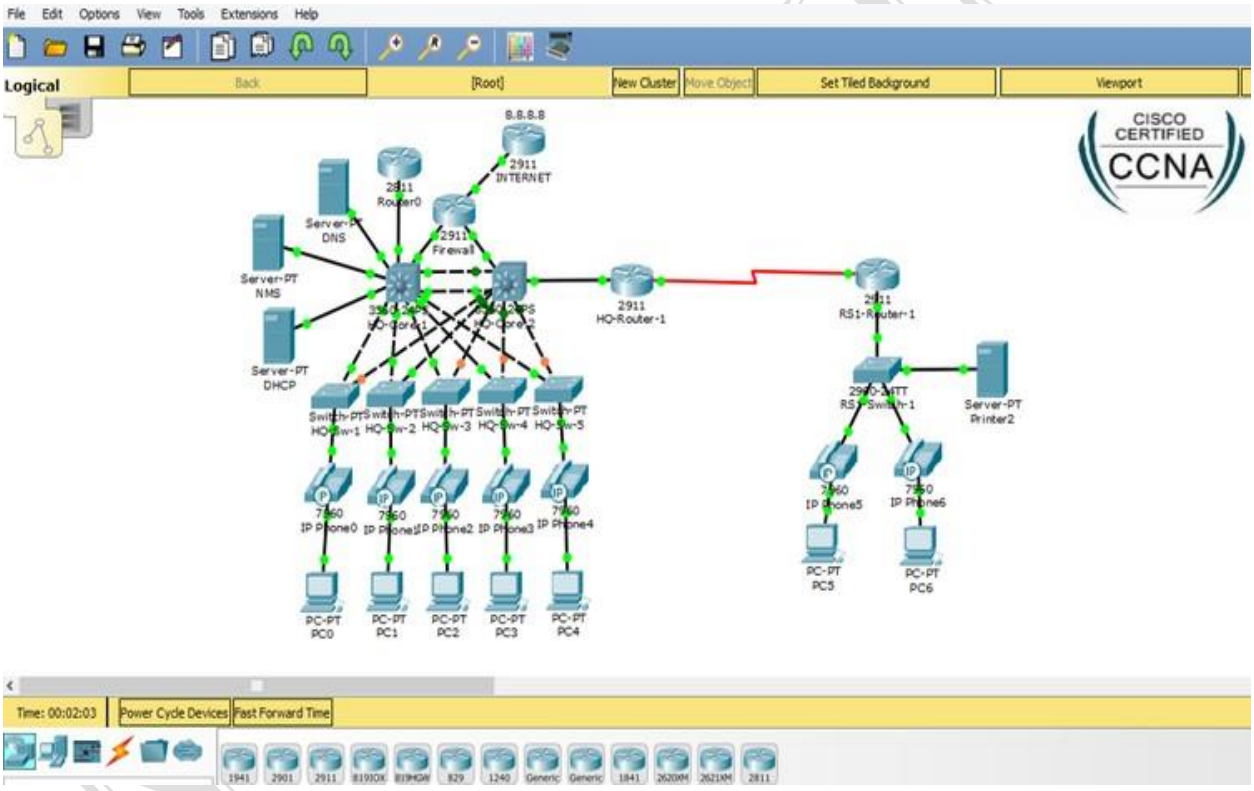
- Automate IT work flows and shorten app deployment from weeks to minutes with Cisco ACI
- Investment protection
- With 1/10GBASE-T support, get 10 Gigabit Ethernet over existing copper cabling, enabling a low-cost upgrade.

CISCO PACKET TRASER

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused towards Certified Cisco Network Associate Academy students as an educational tool for helping them learn fundamental CCNA concepts. Previously students enrolled in a CCNA Academy program could freely download and use the tool free of charge for educational use.

Packet Tracer can be run on Linux and Microsoft Windows and also macOS Only. Similar Android[3] and iOS[4] apps are also available. Packet Tracer allows users to create simulated network topologies by dragging and dropping routers, switches and various other types of network devices. A physical connection between devices is represented by a "cable" item. Packet Tracer supports an array of simulated Application Layer protocols, as well as basic routing with RIP, OSPF, EIGRP, BGP, to the extents required by the current CCNA curriculum. As of version 5.3, Packet Tracer also supports the Border Gateway Protocol.

In addition to simulating certain aspects of computer networks, Packet Tracer can also be used for collaboration. As of Packet Tracer 5.0, Packet Tracer supports a multi-user system that enables multiple users to connect multiple topologies together over a computer network.[6] Packet Tracer also allows instructors to create activities that students have to complete.[2] Packet Tracer is often used in educational settings as a learning aid. Cisco Systems claims that Packet Tracer is useful for network experimentation.



Task 1: Wipe the switch

Your first action is to clear any existing configuration. You can do this by resetting it back to all of its default settings.

- Enter EXEC mode by entering enable at the switch's operating system prompt. If prompted for a password, use class. The prompt character will change from ">" to "#."
- Type in delete flash:vlan.dat and press ENTER. You will be asked twice to confirm the deletion. Press ENTER each time. If the vlan.dat file doesn't exist you will see an error message.
- Type in erase startup-config and press ENTER. Again, the system will ask you twice to confirm the deletion. Press ENTER each time.
- Type show vlan and press ENTER. The readout should only show the default VLAN 1. If previous VLANs are shown, restart the switch by unplugging the power socket and then plugging it in again. If all previous VLANs have been removed, you don't need to do a hardware reset. Enter reload and press ENTER. This is a software restart. You will be prompted to save changes. Enter n and press ENTER. You will be asked to confirm this instruction. Press ENTER.
- On reloading, the prompt will display the message "Would you like to enter the initial configuration dialog? [yes/no]:" Type n and press ENTER. You will see the message "Press RETURN to get started!" Press ENTER to finish the reset process.

Task 2: Check the default configuration

- Make sure that your work removing the old configuration was successful.
- Enter EXEC mode by entering enable at the switch's operating system prompt and press ENTER.
- Query the configuration by typing show running-config and pressing ENTER. The report of this command will show you how many Fast Ethernet and Gigabit Ethernet interfaces are available.
- Check that startup procedures have been removed. Enter show startup-config and press ENTER. The report should be "startup-config is not present."
- Look at the default VLAN settings by typing show interface vlan1 and pressing ENTER. You will be able to see whether any addresses are logged for the switch.
- Take a deeper look at the IP address with the command show ip interface vlan1.
- Check out the base operating system information with the command show version. The report should show you the system image file name and the base MAC address as well as the version of the operating system.
- The image file is important because this will enable you to back up the configuration of your switch and monitor for any unauthorized changes to the setup of the switch. Taking a copy of the file also enables you to roll back any accidental or malicious changes to the configuration and it will also enable you to update all of your switches from one single

approved configuration. You can get more information on tools that will organize these image files for you in 10 best network config tools and software.

Task 3: Create a basic configuration setup

- The startup-config and running-config were wiped out when you cleared the existing configuration. You can create these files again so that they are ready for your new configuration. Start by giving the switch a name. In this example, the switch will be called "S1." You need to still be in the EXEC mode to carry out this task.
- Type in configure terminal and press ENTER. Write hostname S1, press ENTER and then type exit. Instead of typing exit, you can also just press CTRL-Z.
- Save this change in non-volatile RAM (NVRAM) with copy running-config startup-config. At the following prompt, press ENTER to save the file.
- Check the contents of the startup file with the command show startup-config.

Task 4: Set up switch passwords

- Set up your configuration in stages. Make sure that the basic configuration details are correct before moving to advanced settings. In this task, you will set passwords for the switch and set up its address. In this example, all passwords will be set to "system."
- Enter configure terminal to get into the configuration line mode.
- Enter line console 0, press ENTER, type password system, press ENTER, enter login, and press ENTER.
- Before leaving configuration line mode, set up the passwords for vty lines 0 to 15. Enter line vty 0 15, press ENTER, type in password system, press ENTER, type login, and then press ENTER.
- Set up the command mode password by entering enable secret system. This password is for the EXEC mode and the password "class" is often used for this. However, using a non-standard password, such as "system" improves security.
- Press CTRL-Z to exit configuration line mode.

Task 5: Set up switch addresses

- The switch currently has one VLAN set up, which is the default VLAN 1. It is better to create a new VLAN and make it the connection over which you will manage the switch remotely. This new VLAN will be called VLAN 99 and you need to give the switch an address so that your network management console can contact it over the network. In this example, the switch is given the address 172.17.99.09. Use the subnet mask 255.255.255.255.
- Go into configure line mode by entering configure terminal.
- Type vlan 99 and press ENTER. On the next line, type exit. This will create VLAN 99.

- Type interface vlan 99 and press ENTER. Type IP address 172.17.99.09 255.255.255.255 and press ENTER. Type no shutdown, press ENTER and type exit on the next line.
- If you haven't sorted out the address space for your network yet, you should check out The Ultimate Guide to Subnetting for tips on how to organize addresses.

Task 6: Assign all user ports to the admin VLAN

- The VLAN 99 interface will report as being offline because it has no ports assigned to it. Add all the user switch ports to the new VLAN.
- Enter configure terminal to get into configure line mode.
- Type interface range fa0/1 – 24 and press ENTER. Type switchport access vlan 99 and press ENTER.
- Type exit on the next line to get out of configure line mode. You will see the messages "Line protocol on Interface Vlan1, changed state to down" and "Line protocol on Interface Vlan99, changed state to up".
- Check on the status of the new VLAN with the command show interface vlan 99.

Task 7: Assign a default gateway to the switch

- The switch will need to partner with a router – the switch deals with the Network Layer and uses MAC addresses and the router uses IP addresses and the Internet Layer. In order to get traffic moving around your network identified by IP address, you should have a router on it. You need to tell the switch the address of the router that it will be working with. This is termed its "default gateway." In this example, the router's IP address is 172.17.99.1, but you should substitute the address of your router.
- Enter configure terminal to get into configure line mode.
- Type IP default-gateway 172.17.99.1 and press ENTER.
- Enter exit on the next line to exit configure line mode.

Task 8: Assign IP addresses to each device connected to the switch

- This is a task that you will perform away from the switch. You will either assign the addresses manually on each device or manage the addresses from a central DHCP server. In each case, you should set the device's default gateway to the IP address of the switch and not the router. You can now access the switch from your connected management console PC. Ping the address of the switch from your console to check that communications are flowing correctly.
- At this point, you have the switch set up and working and all of the devices connected to it able to communicate to it and through it. You can now proceed to the advanced settings.

Task 9: Save basic switch configuration

- You have already seen how to back up the configuration of the switch in the switch wiping section above. Once you have the basic configuration tasks completed, store the status of the switch with the command copy running-config startup-config.

Use the show startup-config command to check that the configuration has been saved.

Task 10: Set up the MAC address table

- The Cisco switch should discover the addresses of all of the devices connected to it. As the switch is a Layer 2 device, it communicates by MAC addresses. You can record the MAC addresses of the computers that you have connected to the switch by running ipconfig /all at the command line of each computer.

- At the switch, issue the command show-mac-address-table to see the addresses that the switch has stored. Check these against the list you gathered by running ipconfig on each computer. If an address is missing, force communication by issuing a ping to the switch from the computer that isn't listed in the MAC address table. Use the show-mac-address table to check whether the switch has now registered that missing address.

Task 11: Configure the Fast Ethernet interfaces

- You can specify the parameters of each interface on your switch. Here is how to define the port speed and duplex type for each. By default, the Ethernet interfaces use autosensing to coordinate speed and duplex type. The option to manually set these parameters should only be used if a port is only able to function at a specific speed and duplex setting.

- In this example, the commands will specify the settings for Fast Ethernet 0/12. You need to be in EXEC mode in order to perform this task.

- Enter configure line mode with the configure terminal command.
- Type interface fastethernet 0/12 and press ENTER. This enters a deeper level of command line with all subsequent lines relating to the named interface.
- Type speed 100 and press ENTER.
- Set the duplex condition with duplex full.
- Enter end to get out of the specifications for the named interface.
- You will see messages on the screen that show the settings of the interface have been changed. Repeat the above steps for each of the interfaces on your switch.

- Check on the new status of the interface with the command, show interface fastethernet 0/12.

Further Cisco switch commands

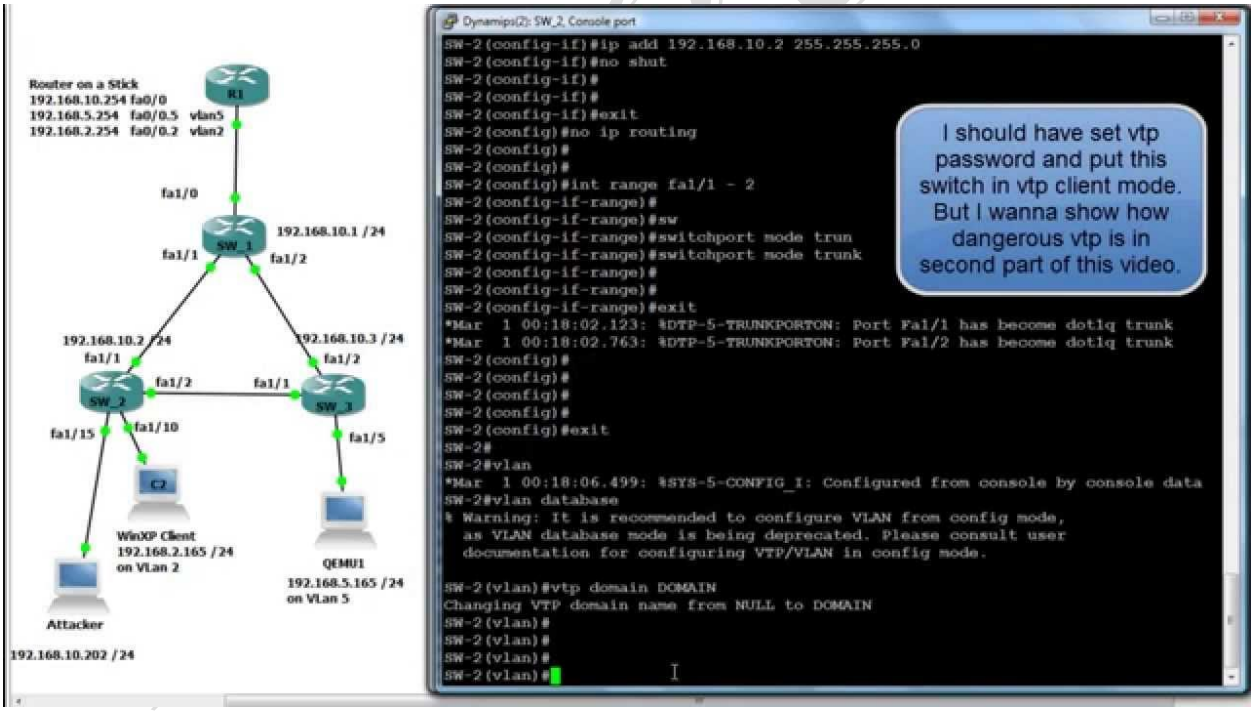
The show commands that you have seen used throughout this guide are just a few examples of a long list of commands that can be used to query statuses on Cisco switches. You can find out more useful query options in the Cisco Router Show Commands Cheat Sheet.

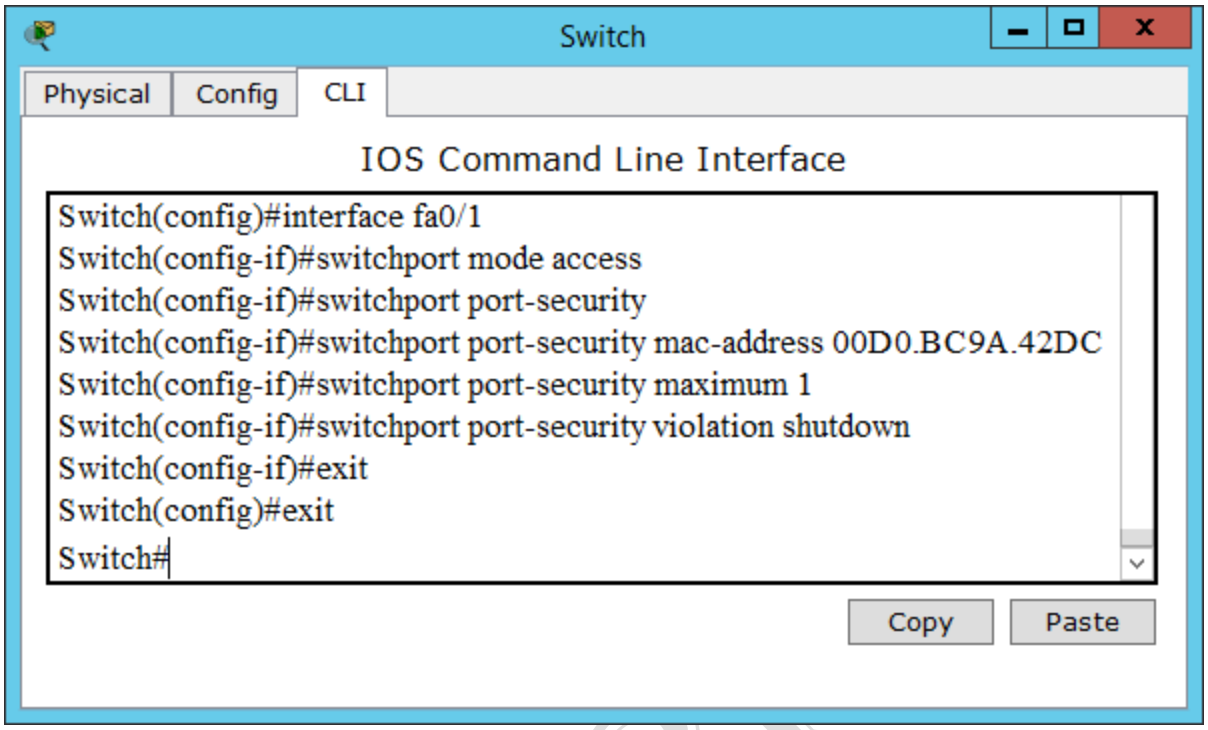
Managing Cisco switches

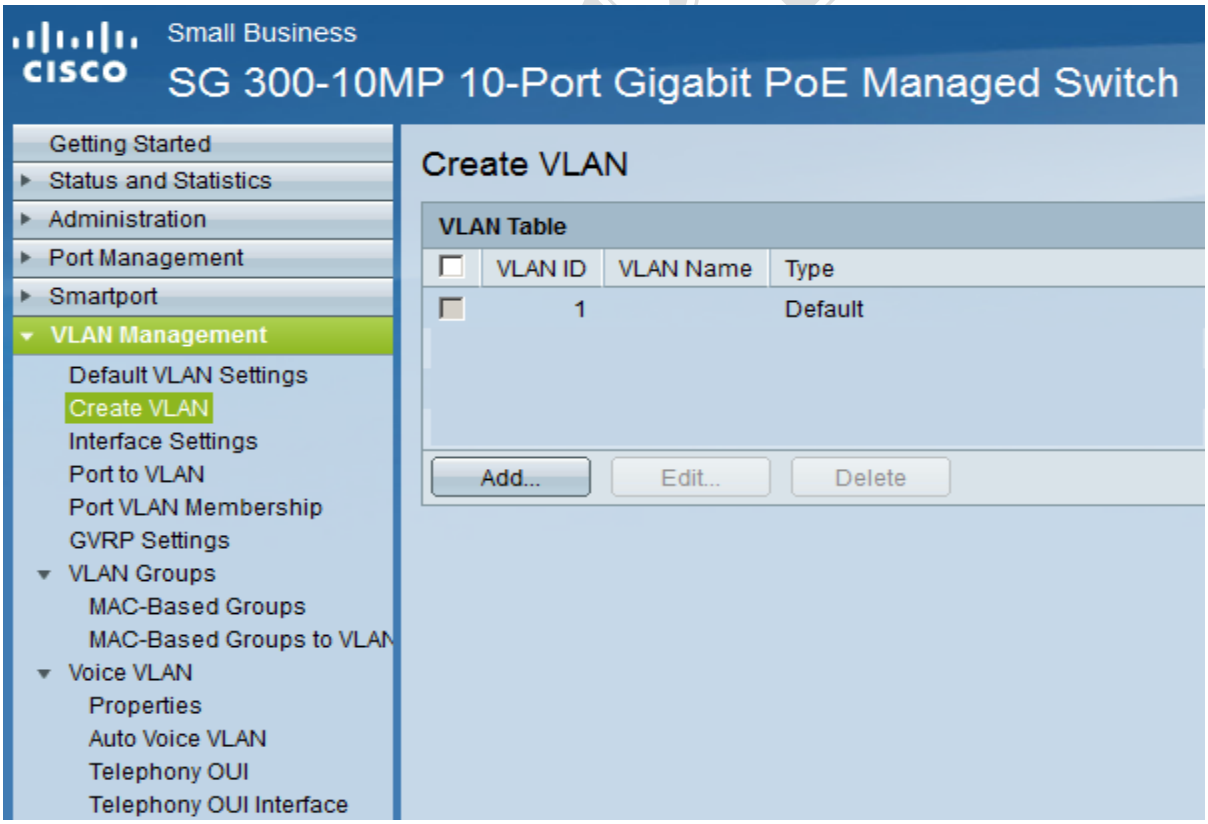
Once you have several switches on your network, you will find it too time-consuming to log into each switch and monitor its status. With all of the network management tasks that you need to perform, you will find it essential to install a network monitoring system. You can also use your Cisco switch's built-in messaging system, called NetFlow, to gather traffic data. Look for a network analyzer tool to make sense of the data that you gather.

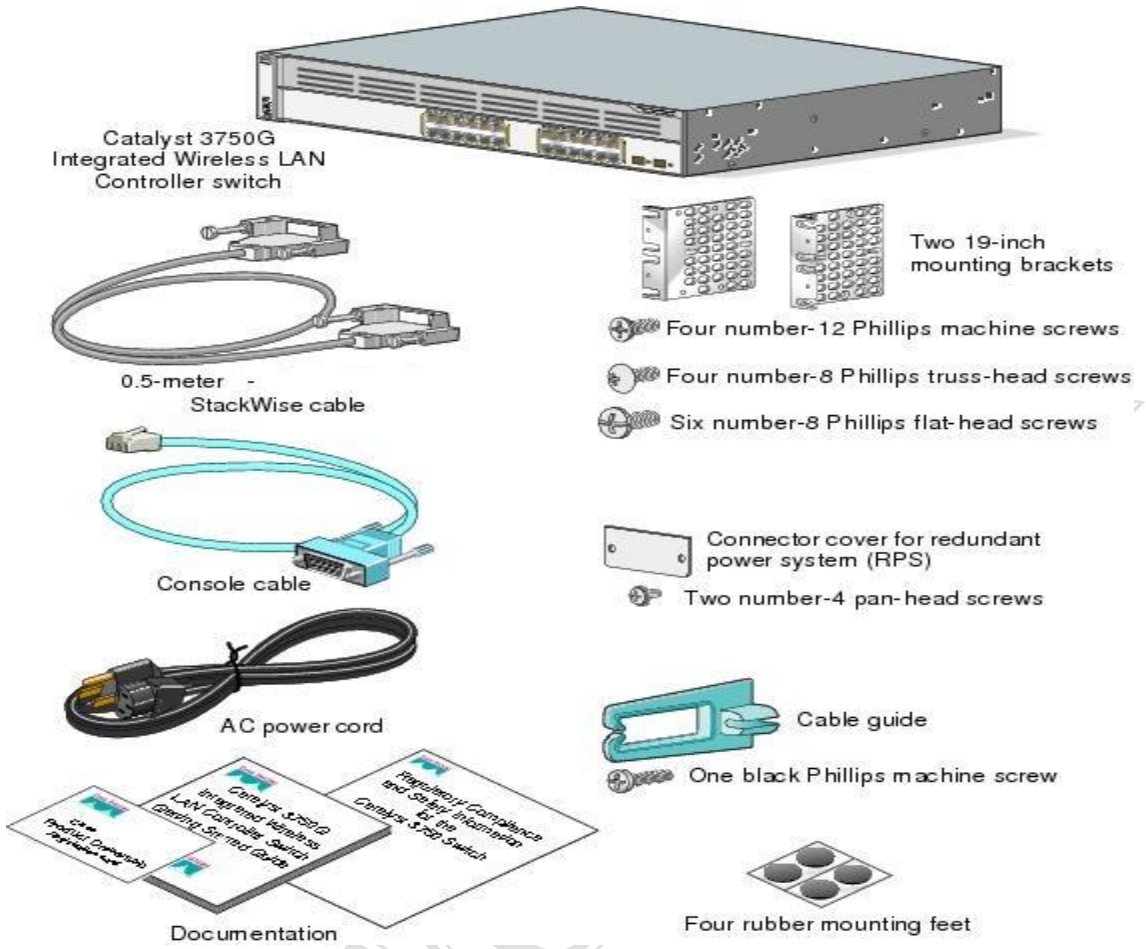
Getting a switch operating

Once you have managed to set up one Cisco switch, you will find the task of configuring more switches very easy. You can even replicate a standard configuration from one switch to another just by copying over the image file.




Switch
Physical
Config
CLI
IOS Command Line Interface
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address 00D0.BC9A.42DC
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
Switch(config)#exit
Switch#
Copy
Paste


Small Business
SG 300-10MP 10-Port Gigabit PoE Managed Switch
Getting Started
Status and Statistics
Administration
Port Management
Smartport
VLAN Management
Default VLAN Settings
Create VLAN
Interface Settings
Port to VLAN
Port VLAN Membership
GVRP Settings
VLAN Groups
MAC-Based Groups
MAC-Based Groups to VLAN
Voice VLAN
Properties
Auto Voice VLAN
Telephony OUI
Telephony OUI Interface
Create VLAN
VLAN Table
VLAN ID
VLAN Name
Type
1
Default
Add...
Edit...
Delete



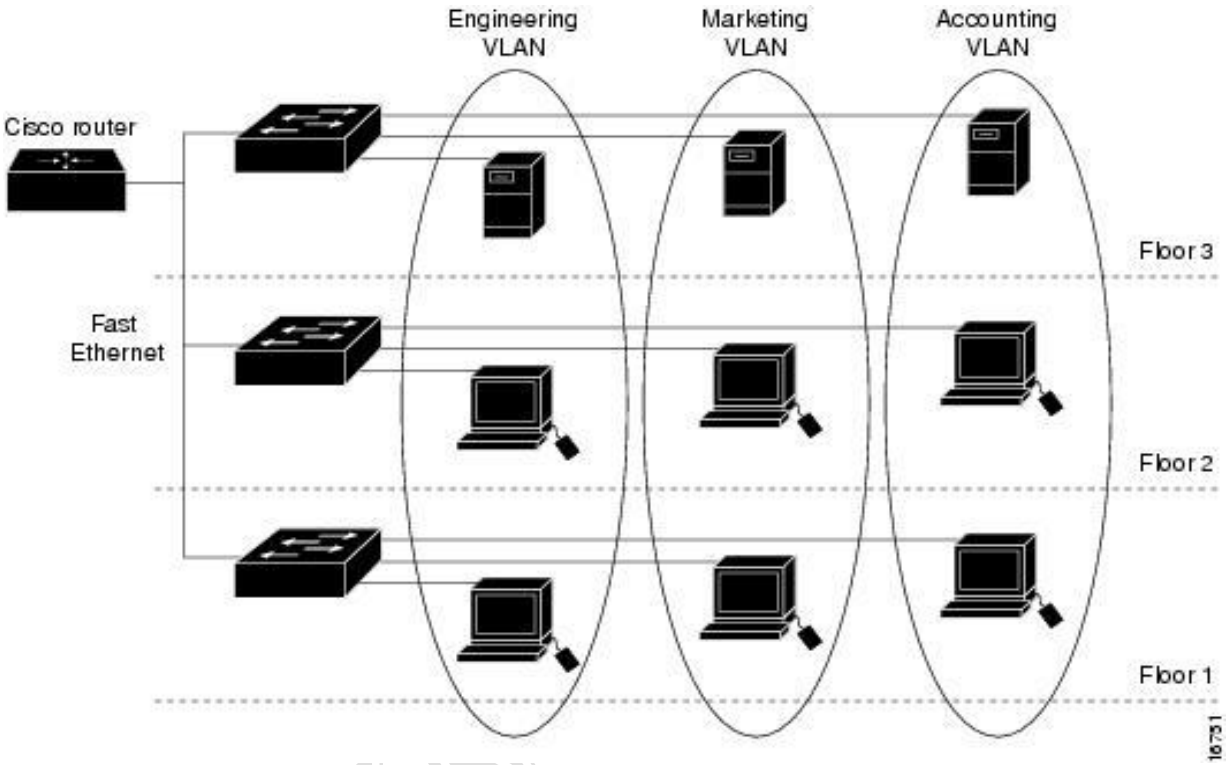
VLAN IN CISCO

VLANs (Virtual LANs) are logical grouping of devices in the same broadcast domain. VLANs are usually configured on switches by placing some interfaces into one broadcast domain and some interfaces into another. VLANs can be spread across multiple switches, with each VLAN being treated as its own subnet or broadcast domain. This means that frames broadcasted onto the network will be switched only between the ports within the same VLAN.

A VLAN acts like a physical LAN, but it allows hosts to be grouped together in the same broadcast domain even if they are not connected to the same switch. Here are the main reasons why you should use VLANs in your network:

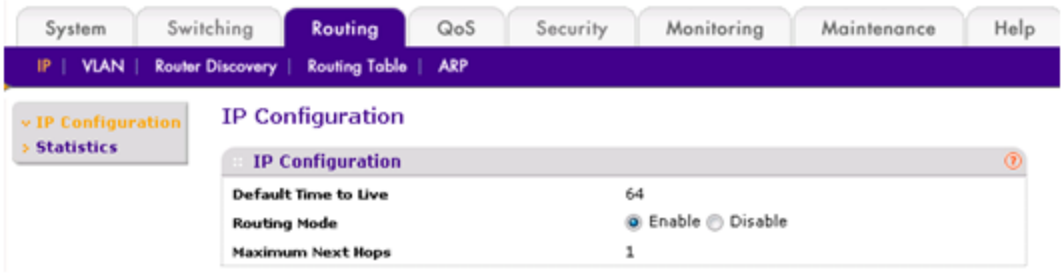
- VLANs increase the number of broadcast domains while decreasing their size.
- VLANs reduce security risks by reducing the number of hosts that receive copies of frames that the switches flood.

- you can keep hosts that hold sensitive data on a separate VLAN to improve security.
- you can create more flexible network designs that group users by department instead of by physical location.
- network changes are achieved with ease by just configuring a port into the appropriate VLAN.

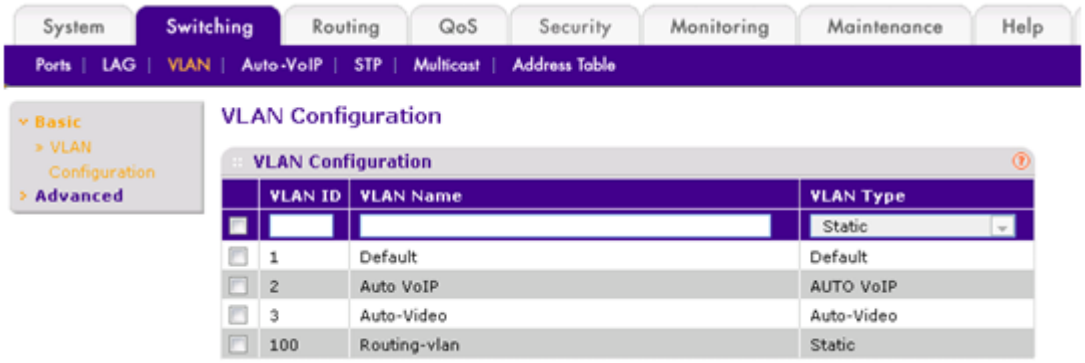


VLAN CONFIGURATIONS GUIDELINES

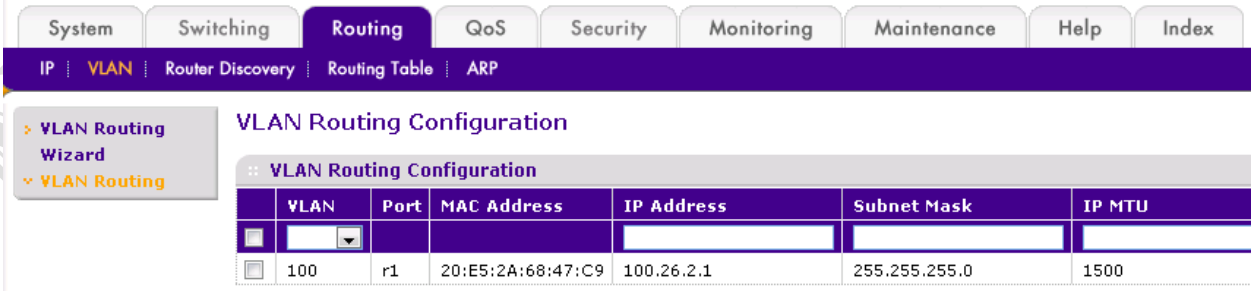
- Determine the IP addresses that you want to assign to the VLAN interfaces on the switch.For the switch to route between VLANs, the VLAN interfaces must have IP addresses. When the switch receives a packet that is destined for a VLAN or subnet, the switch forwards the packet to the destination VLAN interface based on the information in the routing table. The destination VLAN interface forwards the packet to the port to which the end device is attached.
- Open a web browser.
- In the browser address field, type the IP address of the smart switch.
- The default IP address is 192.168.0.239 and the default subnet mask is 255.255.255.0.
- You are prompted to enter your password.
- Type the password in the Password field.
- The default password is password. Passwords are case-sensitive.



- Click the Login button.
- After the system authenticates you, the System Information screen displays.
- Select Routing>IP>IP Configuration.
- Next to Routing Mode, select the Enable radio button.
- Click the Apply button.
- Routing is now enabled.
- Select Switching>VLAN>Basic > VLAN Configuration.



- Create a static VLAN by specifying a VLAN ID and VLAN name, and, from the VLAN Type menu, selecting Static.
- Click the Add button.
- The new VLAN is added to the configuration.
- Select Routing> VLAN > VLAN Routing.



- Enable routing on the VLAN that you just created and assign an IP address and subnet mask
- From the VLAN menu, select the VLAN that you just created.
- In the IP address field, type the IP address that you want to assign to the VLAN routing interface.

- In the Subnet Mask field, type the subnet mask that you want to assign to the VLAN routing interface.
- In the IP MTU field, type 1500.
- 1500 is the default MTU size.
- Click the Add button.
- The VLAN routing interface is added to the configuration and becomes active.
- Repeat steps 9—14 for all VLANs that you want to designate as VLAN routing interfaces.

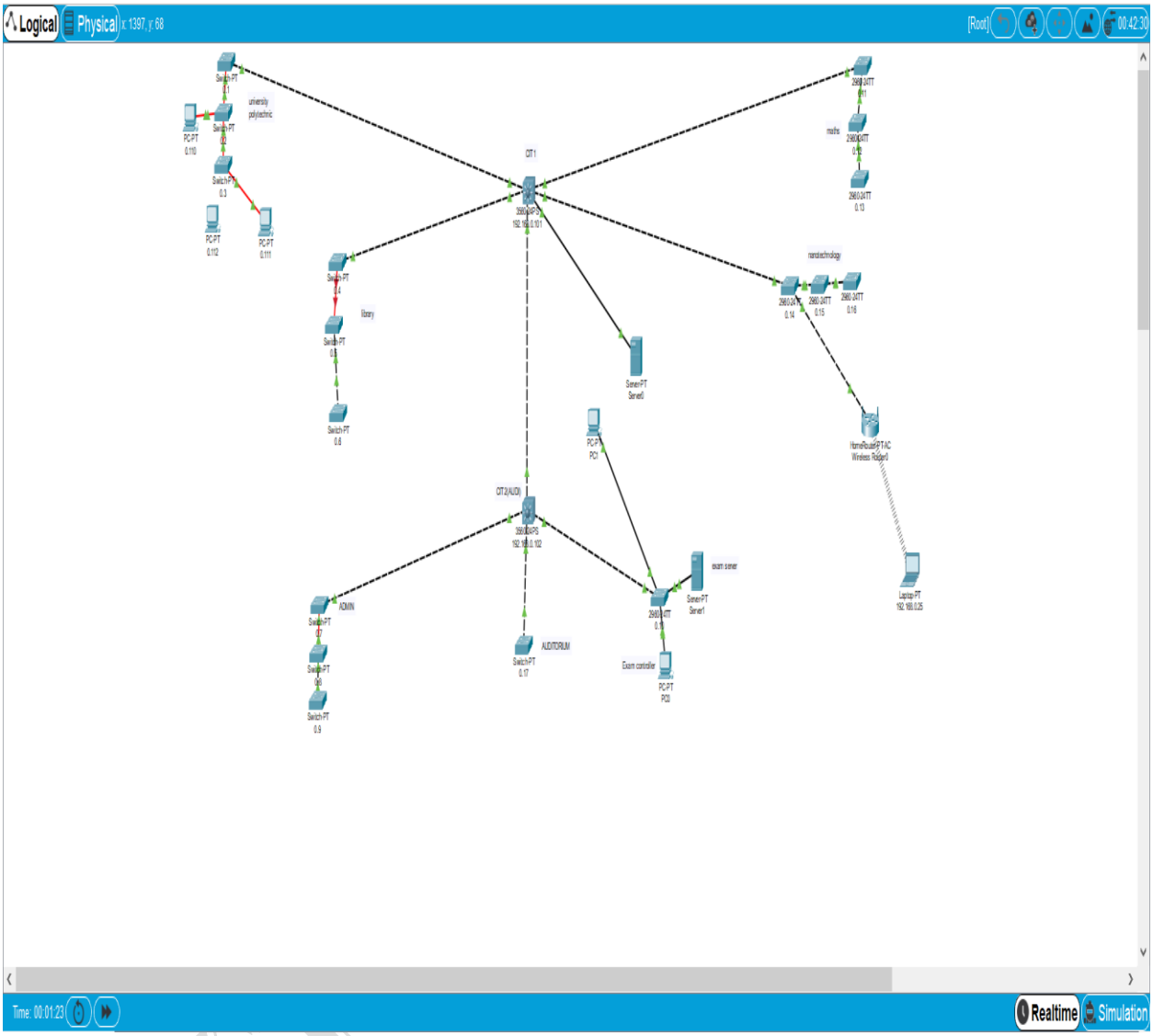
Network Switches

A network switch (also called switching hub, bridging hub, officially MAC bridge[1]) is a computer networking device that connects devices on a computer network by using packet switching to receive, process, and forward data to the destination device.

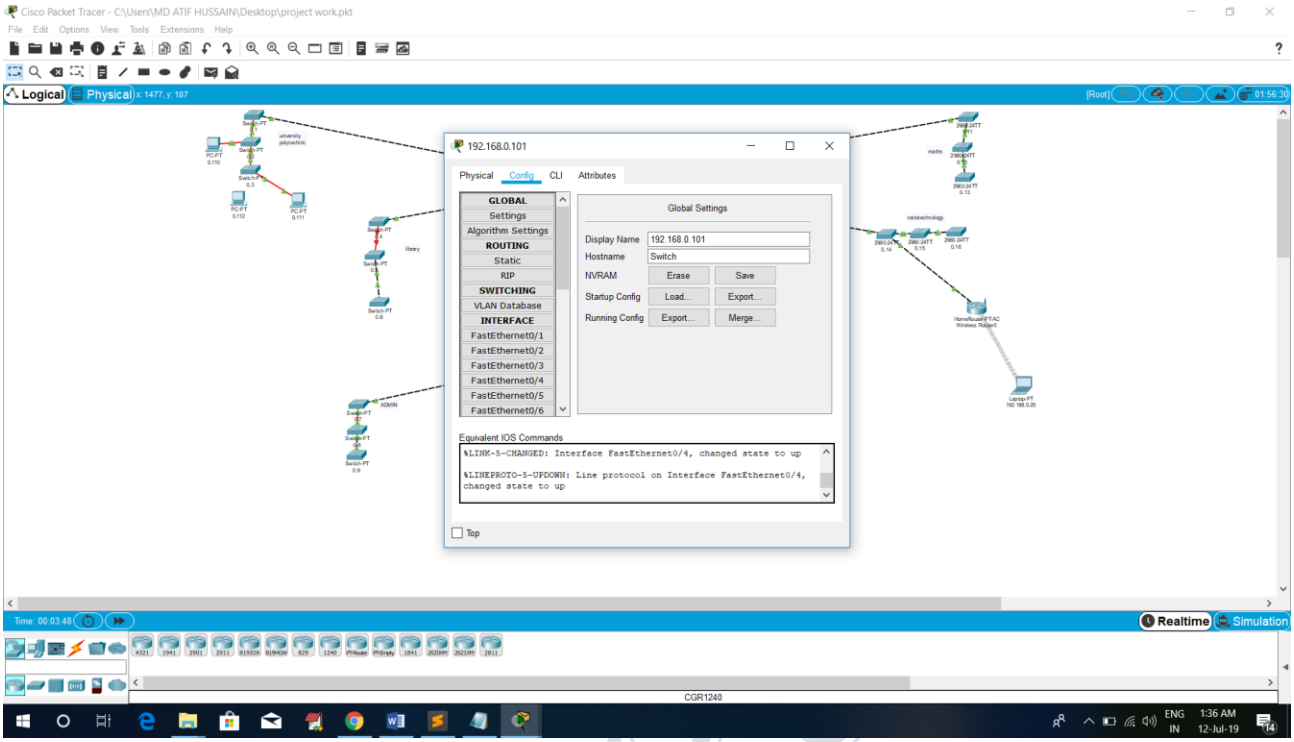
A network switch is a multiport network bridge that uses hardware addresses to process and forward data at the data link layer (layer 2) of the OSI model. Some switches can also process data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.[2]

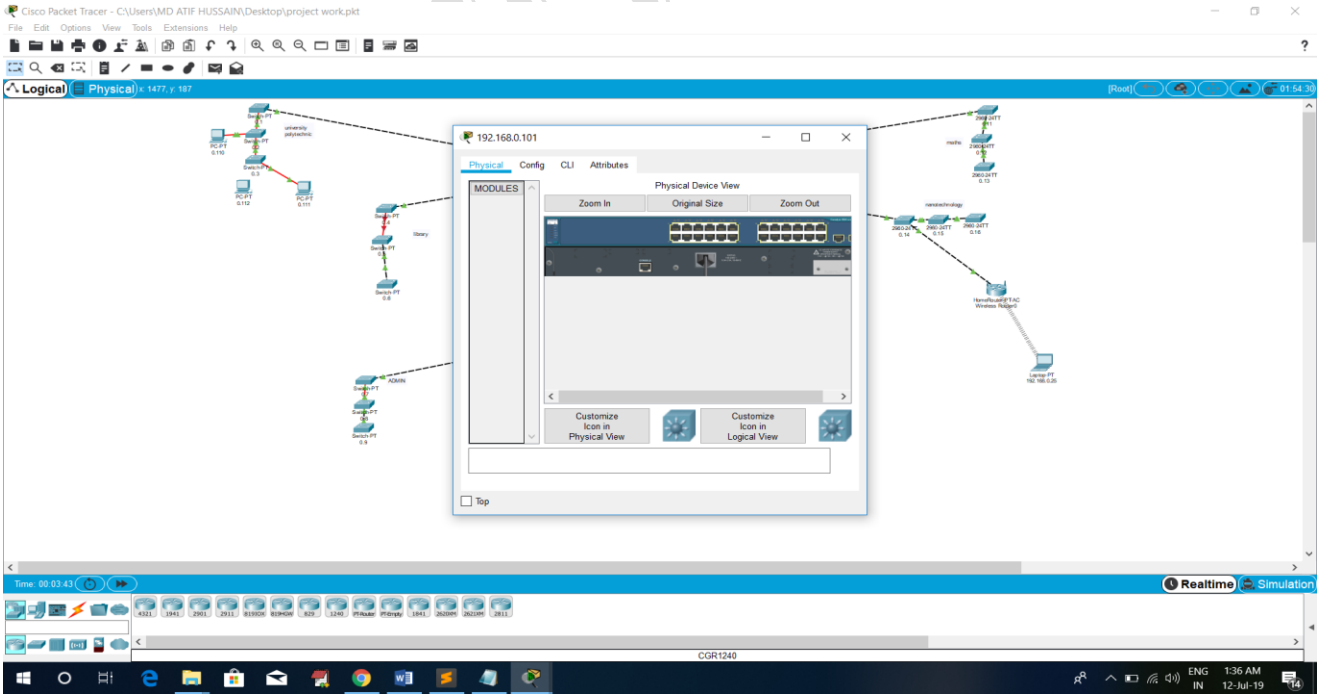
Switches for Ethernet are the most common form of network switch. The first Ethernet switch was introduced by Kalpana in 1990.[3] Switches also exist for other types of networks including Fibre Channel, Asynchronous Transfer Mode, and InfiniBand.

Unlike less advanced repeater hubs, which broadcast the same data out of each of its ports and let the devices decide what data they need, a network switch forwards data only to the devices that need to receive it.



Basic Architecture of Network in JMI


Cisco Packet Tracer - C:\Users\MD ATIF HUSSAIN\Desktop\project work.pkt
File Edit Options View Tools Extensions Help
Logical Physical
192.168.0.101
Physical Config CLI Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/1
FastEthernet0/2
FastEthernet0/3
FastEthernet0/4
FastEthernet0/5
FastEthernet0/6
Global Settings
Display Name 192.168.0.101
Hostname Switch
NVRAM Erase Save
Startup Config Load... Export...
Running Config Export... Merge...
Equivalent IOS Commands
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up
Top
Realtime Simulation
CGR1240
ENG IN 1:36 AM 12-Jul-19


Cisco Packet Tracer - C:\Users\MD ATIF HUSSAIN\Desktop\project work.pkt
File Edit Options View Tools Extensions Help
Logical Physical
192.168.0.101
Physical Config CLI Attributes
MODULES
Physical Device View
Zoom In Original Size Zoom Out
Customize Icon in Physical View
Customize Icon in Logical View
Top
Realtime Simulation
CGR1240
ENG IN 1:36 AM 12-Jul-19

Conclusion

Computer Networking is a very vast project in the present developing era of electronics and communication. Now a days, computers are used in a wider range. All the organization are using multiple computers within their departments to perform their day to day work. Computer Network allows the user to share data, share folders and files with other users connected in a network. Computer Networking has bound the world in a very small area with it wide networking processes like LAN, MAN, WAN.

Applications

- Communication Field
- Industries
- Medical Field
- Research Field
- Organizations
- School
- Colleges

References

- **www.google.com**
- **www.greeksforgreeks.com**
- **www.microsoft.com**
- **www.digitechengineers.com**
- **4-in-1 MCSE study material**
- **Network essential module**
- **CISCO Network Certified Associate**
- **Wikipedia**
- **https://issuu.com/sanjaykumargupta**
- **Mr. Abuzar (Technical Assistant)**