AN INTERNSHIP REPORT

Submitted by

SURYADEVARA MANOJ - 412420106070

In Partial fulfillment for the award of the degree

of

BACHELOR OF ENGINEERING

in

ELECTRONICS AND COMMUNICATION ENGINEERING

SRI SAI RAM INSTITUTE OF TECHNOLOGY

(An Autonomous Institution; Affiliated to Anna University, Chennai-600025)

ANNA UNIVERSITY::CHENNAI - 600 025

APRIL 2024

BONAFIDE CERTIFICATE

Certified that this internship report **"TELECOMUNICATION"** and **"NETWORKING"** are the Bonafide works of **"SURYADEVARA MNAOJ (412420106070)"** who carried out the internship works in the **"CHENNAI METRO RAIL LIMITED**" and **" VERZEO EDUTECH PRIVATE LIMITED ".**

Dr. S. Rajarajan, Professor
Dean/ Academics

Dr. G. ThamaraiSelvi, Professor
HoD/ ECE

Dr. P. Saravanan, Assoc. Prof
Strategist

Mrs. R. Janaki, Assoc. Prof
Talent Enabler

Mrs. K . Sivasankari, AP
Placement facilitator

Mrs.S. Sweetline Shamini, AP
Internship Incharge

Mrs. G .Valarmathi, Asst. Prof

Student Mentor

Submitted for the internship review held on _____

at Sri Sai Ram Institute of Technology, Chennai- 600 044.

DETAILS OF INTERNSHIP

SECTION NO	COMPANY NAME	MODE OF INTERNSHIP	YEAR/SEM
I	CHENNAI METRO RAIL LIMITED (CMRL)	OFFLINE	III/ VI
II	VERZEO EDUTECH PRIVATE LIMITED	ONLINE	II/ IV

SECTION I

TABLE OF CONTENTS

SECTION -I

LIST OF FIGURES

ABSTRACT

The internship outlines a comprehensive program aimed at providing students with practical experience in telecommunications systems and technologies. Through a blend of classroom instruction, laboratory exercises, and real-world industry projects, participants will gain proficiency in telecommunications hardware, software, and networking techniques tailored to telecommunication environments. With hands-on experience, mentorship, and professional development opportunities, the program aims to equip students with the technical skills, problem-solving abilities, and industry insights necessary for successful careers in the field of telecommunications. With the rapid advancement of telecommunications technologies revolutionizing communication networks and services, the internship aims to bridge the gap between theoretical knowledge and practical application in telecommunications systems and automation.

CHAPTER 1

ABOUT THE COMPANY

NAME OF THE COMPANY – CHENNAI METRO RAIL LIMITED

NSIC CIN NO: U60100TN2007SGC065596

The Chennai Metro is a fast transport system that serves the city of Chennai, Tamil Nadu, India. It is India's fourth-longest metro system. After the first phase of the project's construction was largely completed, the system went into service in 2015. The existing network comprises of two coloured lines that span 54 kilometres (34 miles) in length.The Chennai Metro was constructed and is run by the Chennai Metro Rail Limited (CMRL), a joint venture between the governments of Tamil Nadu and India. The system uses standard gauge and contains a mixture of elevated and underground stops. The services are available every day from 5:30 till 2:00 at a frequency that varies from 2 to 8 minutes.

VISION

"Moving people, sustaining growth"

MISSION

"We shall provide a safe, fast, reliable ,accessible, convenient ,comfortable ,efficient and affordable public transport service preferred by all in a sustainable manner."

CMRL CORE VALUES

➢ Concern for customers: We Commit to provide safe, clean, reliable, on-time, courteous service for all categories of our clients and customers

➢ Integrity: We commit to be transparent and fair in our transactions with all our clients.

➢ Sustainability: We commit to base our decisions on principles of sustainability (Refuse,Reduce, Reuse, Recycle and Rethink) towards reducing greenhouse emissions.

➢ Responsibility: We commit to honour the trust reposed in us by the public by managing CMRL resources financial and non-financial with the highest degree of responsibility.

➢ Creativity & Innovation: We commit to strive together as a team to continuously to develop and deploy creativity, innovation and technology to add value to our customers and other stakeholders.

➢ Punctuality: We Commit to render prompt service to our customers and instil a culture of punctuality in all aspects of our business.

Fig. 1 CMRL Logo

Title of the Internship: TELECOMUNICATION

Internship Period: 26/06/2023 to 10/07/2023 (Two Half weeks)

Mode of Internship: Offline

CHAPTER 2

ABOUT THE INTERNSHIP

2.1 TELECOMUNICATION

Chennai Metro Rail comprises of new build sites and rail routes which will require the provision of a full complement of telecommunications sub-systems. For efficient Railway Management and Operations, it is essential to have well equipped telecommunication Network covering strategic locations like OCC, Stations, Rolling Stock and Depots.

It is also equally essential to have reliable links between strategic locations, moving Trains and Staff working along the Railway Track. The Telecommunication System provides all necessary communication channels / links for carrying Voice, Data and Video Signals for Management Control and Operations.

The various telecommunication subsystems are listed below,

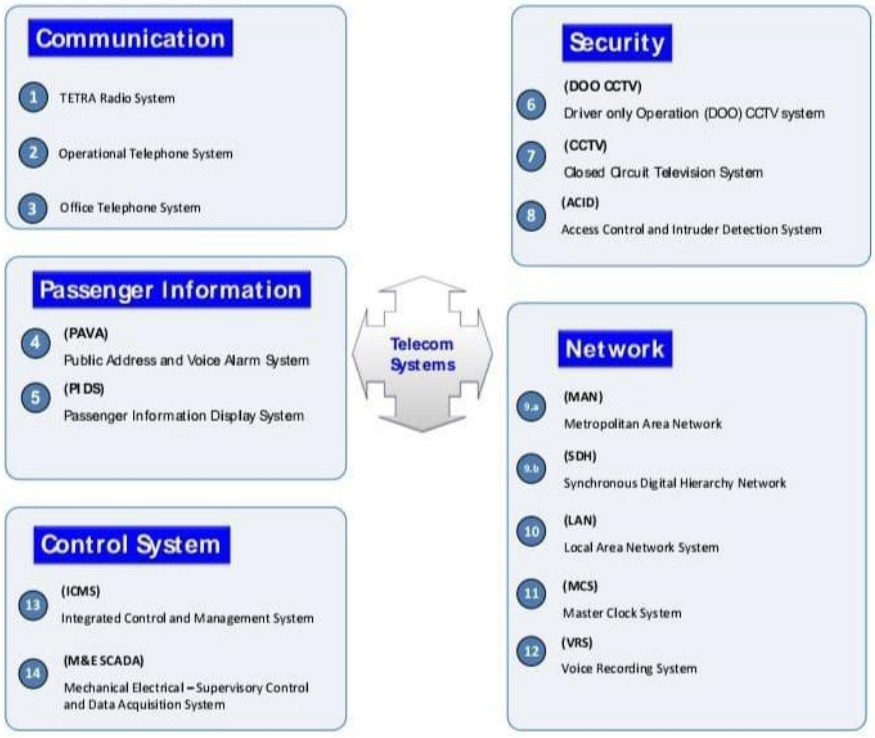


Fig:1 TELECOMMUNITCATION SYSTEM

2.2 TETRA RADIO SYSTEM

TETRA is the acronym for Terrestrial Trunked Radio, which is a European Open Standard for Digital Trunked Radio. The system is digital where in speech is coded and passed through the system as digital data. The system supports both speech and data transmissions.

2.2.1 PURPOSE

- Instant communication between Traffic Controller, Chief Controller, Other controllers, Train Driver, maintenance staff &Security staff working at OCC, DCC, RSS, Depot, Station, Viaduct and Other Locations.
- Public announcement to Train from OCC.

- Data Communication between Train Radio system and ATO. The ATO will send train information of Rake ID, All Modes of Train, Train Location (Mainline or Depot), Master Cab Location, Triggering of Event Recording (Activation, Deactivation and Failure of Emergency call), and Health status of train.

2.2.2 SYSTEM FEATURES (Mode of Operation)

Trucking Mode In this mode of operation all the infrastructure like BTS and MSO are connected with each other. Here all the calls are controlled by the MSO in the central location. Local Site Trucking (LST) Mode LST is a feature that enables each base station to act as a standalone system when communication lost with MSO. Direct Mode Operation (DMO) It is a mode of operation, which allows subscriber radios to communicate directly with each other without using BS. It works within a radius of 2km with line of sight. When the local BTS is not in working mode then the user has to switch to DMO mode.

2.2.3 CALL FEATURES TETRA

Radio will support various types of call features like individual Calls, Group Calls, Broadcast Calls, Data Calls, Emergency Calls, Telephone Interconnect calls. The group call service allows a MS or dispatcher console to initiate a one-to much half duplex communication with a group of users defined by their talk group affiliation. Individual Calls Tetra supports individual call, private communication between two individual MSs, or between a dispatcher console and Handset. This feature supports both “point to point” and “point to multipoint” services. Emergency Calls Each Handset is equipped with an easily accessible emergency button. The Mobile Station (MS) user can invoke emergency mode by activating this button.

2.2.4 Radio Access Unit (RAU) & Radio Control Panel (RCP)

Total 12 Nos. (Min) RAU is provided to various controller positions

Total 34 Nos. RCP is provided to the Station Controller positions.

Fig:2 Radio Access Unit (RAU) & Radio Control Panel (RCP)

2.2.5 Rain borne Radio

Total 84 Nos. Train Mobile Radio is provided in the Train (2 Radio/Train)

Fig:3 Rain borne Radio

2.3 OPERATIONAL TELEPHONE SYSTEM

Operation Telephone system is a circuit switched based EPBX system which support railway operational processes involving train movements and activities related to those operations. This will be for Voice Traffic only.

2.3.1 PURPOSE

- To meet the communication requirement of O&M staff in designated plant room, equipment room, control room, sub-station, and other staff rooms.
- Operation Telephone system also provides Direct Lines and emergency line for operational needs.

2.3.2 SYSTEM FEATURES

Homogeneous numbering plan (up to 8 digits)

Call Back

Call forward

Caller party extension number display

Call pick-up

Call transfer

2.4 OFFICE TELEPHONE SYSTEM

Office Telephone system is an IP based PBX (IP-PBX) for internal and external routine office telephone communication.

2.4.1 PURPOSE

- For office routine voice communication to inside and outside metro rail system.
- Voice communication to outside world of the metro system by Direct PSTN line. This is separate system available in each station and used in emergency situation.

Analoge Phone

Fig: 4

VOIP Phone

Fig: 5

2.5 PUBLIC ADDRESS AND VOICE ALRAM SYSTEM

The Public Address / Voice Alarm (PA/VA) System supports the broadcast of live voice announcements, pre-recorded messages, fire alarm messages to public.

Fig:6 Public Address / Voice Alarm (PA/VA)

2.5.1 PURPOSE

- The PA/VA equipment at OCC facilitates broadcasting of live and pre-recorded announcements from OCC to selected zones.
- The OCC PA/VA System enables the broadcast of messages to different stations. In case of different messages are being broadcasted to the same zone, the message with the higher priority is broadcasted.
- PA/VA provides the station controllers at each Station Control Room (SCR) with the ability to address individual platform, concourse, non-public area or entire station.

2.6 PASSENGER INFORMATION DISPLAY SYSTEM

PIDS provides relevant information on train times and train destinations and also facilitate the timely dissemination of important, current and up-to-date travel information to the passengers through

display units.

2.6.1 PURPOSE

The primary purpose of PIDS is to display:

- Expected Train Arrival/Departure time and Destination
- Expected Train arrival time for next two/three trains.
- Emergency Message Management Pre-formatted / instantly constructed Normal and Emergency messages.
- Operational Messages Management.

Fig: 7 DISPLAY

2.7 CLOSED CIRCUIT TELEVISION (CCTV)

- Closed-circuit television (CCTV) is the use of cameras to transmit video signals to a specific place, on a limited set of monitors for surveillance purpose.
- As the name implies, Closed Circuit Television (CCTV) is a system in which the circuit is closed and all the elements are directly connected.

2.7.1 PURPOSE

- The purpose of the CCTV system is to provide security and surveillance throughout the station premises, depot, OCC, ventilation shaft, electrical 14 sub-stations and selected line side locations, like tunnel cross passages and line portals.

2.8 SYSTEM COMPONENT

- Cameras [Fixed & PTZ (Pan Tilt Zoom)]
- DVRs (Digital Video recorders)
- Display Monitors & Video walls
- Servers, Storages & HMI(workstations)

Fig: 8 CCTV

2.8.1 Driver only Operation (DOO) CCTV:

The cameras are set up on the platforms with a view of passenger entering and departing off the train . A monitor with the four views is setup such that it is viewed by the train operator from their cabin . This is helpful in monitoring the status of passengers so that they can close the doors of the train. The systems support drivers making decisions regarding the safe dispatch of trains. CCTV cameras strategically positioned along the platform, capture video images of the Platform to Train Interface (PTI). Images of the carriage doors beyond the yellow line along the platform edge are displayed either in the train cab or on platform monitors. With responsibility for the safety of so many others, real-time, high

quality image presentation is vital to underpin quick sure action

2.8.2 CCTV/DOO SYSTEM:

In any kind of facility, CCTV cameras are employed for security surveillance and monitoring. Closed-circuit television, or CCTV for short, refers to how CCTV systems broadcast visual data over a single channel, effectively forming a closed circuit. This means that instead of being broadcast to the public, CCTV footage is only shown on a small number of personal monitors and screens.

2.9 Types of Camera

- Bullet Camera

Bullet cameras offer a sleek design and a flexible range of areas they can be placed, including on walls. The shape of a bullet camera allows it to accommodate a large lens, giving it a longer range than many other cameras. This makes it ideal for monitoring over long distances. Bullet cameras' good recording quality, motorized zoom capabilities, and infrared make them ideal for outdoor use and use in industries such as manufacturing, property management and farming

Fig 9.Bullet Camera

- Dome Camera

Dome cameras are generally used indoors and mounted on ceilings. This allows them to survey large areas at a wide angle. Dome CCTV cameras are great

for retail establishments, restaurants, hotels, and casinos, as they can completely monitor a large room. They are also well-suited to environments that get dirty easily, such as kitchens and warehouses. Dome cameras offer smaller, more discreet hardware than other camera types.

Fig 10.Dome Camera

- PTZ Camera

  PTZ (pan, tilt, zoom) cameras are shaped like dome cameras, but they allow users to remotely move the camera using an app, joystick, or computer program. This is ideal for panning certain areas and focusing in when the camera detects movement. With the ability to move and “look” around a room, PTZ cameras provide 360-degree coverage, and can do the job of several static cameras. PTZ cameras are great for protecting valuable objects, such as in retail settings.

Fig 11.PTZ Came

2.10 ACCESS CONTROL AND INTRUSION DETECTION SYSTEM (ACID):

An access control and intrusion detection system is an integrated framework that allows users to monitor and regulate physical access to specific regions. Access control is in charge of regulating and giving access to specific people into specific places. The purpose of this type of software is to minimise unauthorised access to locations, assets, and systems. Identification and authorization are crucial for intrusion detection. This means that users can only gain access to restricted places or equipment after properly identifying themselves and obtaining level clearance.

Below diagram shows the working of an access control and intrusion System (ACID).

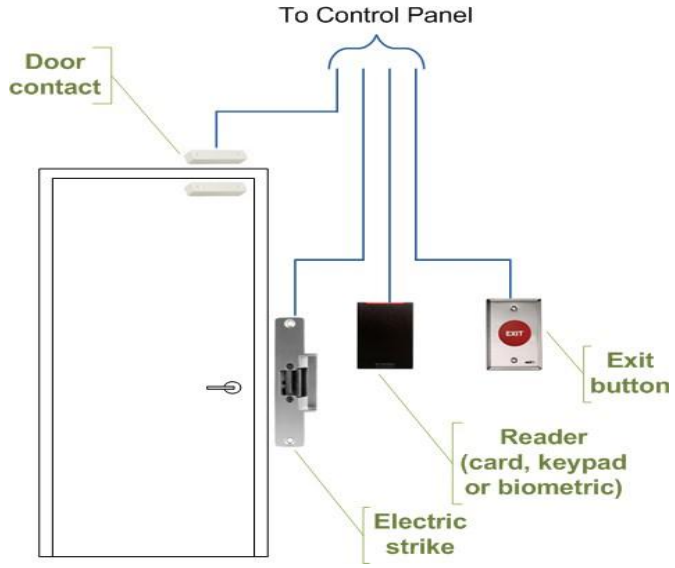


Fig 12.Access control and intrusion detection system

The components involved in this system are card reader,door open alarm,break glass, Quad door Control Unit (QDCU). Each QDCU will control upto four doors. To permit access we can also use the fingerprint or PIN along with the card reader using the software. For other staff to access those rooms , we can also set time to let the door open as per our need.

2.11 MASTER CLOCK SYSTEM

The Master Clock System is a source of high precision and stable time signals for network synchronization and reference timing.

2.11.1 PURPOSE

Master Clock System is provided to distribute a GPS based time and date signal from a Master Clock equipment to OCC, Stations, Depot and other location systems.

2.11.2 SYSTEM FEATURES

The Master clock receives the time from dedicated GPS receivers. The Master Clock derives the Universal Time Code (UTC).

The internal time is adjusted to the GPS in one step or small adjustable micro steps to avoid time leaps. The accuracy is further increased by continuous compensation of the quartz drift and aging. Holdover of Master clock system is at least 24hours of synchronization from time source.

2.11.3 DIGITAL CLOCK:

This is a seven segment LED numerical display clock, available in dimensions of 333x118x39mm and 510 x 169 x 39mm.

2.11.4 ANALOUGE CLOCK:

The Analogue Display Clock provides easily readable and traditional round clock shaped. Available in dimensions of 40cm and 50cm.

Fig: 13 Fig 14

2.12 VOICE RECORDING SYSTEM (VRS)

Voice recordings include selected voice communications within the OCC, between the OCC and sites on the Corridor 1 and 2, between the OCC and the PSTN. Multi-channel digital voice recorders are available that automatically and continuously record IP, analogue and digital speech channels along with the logging of all recorded calls.

2.12.1 PURPOSE

The voice recording solution covers the recording of:

- Analogue and digital phones of Operational Telephone system.
- Tetra radio IP feeds from the Tetra Radio System.

2.12.3 SYSTEM COMPONENTS

- Recorders: Two multi-channel, rack-mounted, voice recorders are available at Corridor 1 and Corridor 2 Control Equipment Room. Each voice recorder serves as a back-up to the other. Each voice recorder is equipped with DVD drives to allow archiving facilities.
- Operator's HMI: A single HMI Terminal headset is provided within the OCC Recording Room to provide operator access to all relevant functions of the Corridor 1 and Corridor 2 recorders for operation, playback, system and alarm management and archiving.

- Engineering terminal: A colour display that provides the functions operators HMI.

2.13 INTEGRATED CONTROL AND MANAGEMENT SYSTEM (ICMS)

The ICMS is an integration of various subsystems in the OCC and stations to support the operation and maintenance needs of the Metrorail systems.

2.13.1 PURPOSE

- It provides a central repository for system wide alarms and events recording, an integrated graphical Human Machine Interface (HMI) capability and advance reporting capability.
- The ICMS will enable the control room operators, with appropriate operating privileges, to operate, monitor and/or control the equipment/devices from OCC.

2.14 VIDEO AND COMMUNICATION (PICT) HMI

An integrated PICT HMI is provided to enable an authorized operator to operate the dispatching function of the following subsystems: Public Address and Voice Alarm System (PAVA), Closed Circuit Television (CCTV), Passenger Information Display System (PIDS), Access Control and

Intruder Detection System (ACID).

2.15 TELECOM SUBSYSTEMS MANAGEMENT WORK STATIONS

Maintenance and configuration facilities for the telecommunication subsystems are provided by software deployed in the management workstations located in the OCC Maintenance Centre and the station equipment room.

M&E SCADA SYSTEM (HMI)

The M&E SCADA system provides the Operational and Maintenance interface with various electrical & mechanical systems (including monitoring of high-level alarms of AFC, other SCADA systems and monitoring of detailed alarms of all telecom sub-systems)

OCC

Fig:15

Chief Controller

Fig:16

METRO DRIVER CABIN (Cockpit):

Fig: 17

2.18 ASSIGNMENT I

How To Configure The IP Address For An Ethernet Interface:

1. Determine the name of your Ethernet interface: This could be something like "eth0" or "Ethernet."
2. Open the network settings: Access the network settings or control panel on your computer.
3. Find the Ethernet interface: Look for the section or tab that displays your Ethernet interface settings.
4. Choose the IP configuration method: Decide whether you want to set the IP address manually or obtain it automatically.

Manual (Static) IP Configuration: Select the option to manually configure the IP address. Then, enter the IP address, subnet mask, default gateway (router IP), and DNS server addresses. Use valid IP addresses for your network. Dynamic IP Configuration (DHCP): Choose the option to obtain an IP address automatically from a DHCP server. The network will assign the IP address, subnet mask, default gateway, and DNS server addresses.

5. Save and apply the changes: After configuring the IP settings, save the changes and apply them. Your Ethernet interface will now use the newly configured IP address.

2.18 ASSIGNMENT II

IP address
An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.
Class A Address
The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.
The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (27-2) and 16777214 hosts (224-2).
Class A IP address format is thus:
0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH
Class B Address
An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.
Class B has 16384 (214) Network addresses and 65534 (216-2) Host addresses.
Class B IP address format is:
10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH
Class C Address
The first octet of Class C IP address has its first 3 bits set to 110,
Class C gives 2097152 (221) Network addresses and 254 (28-2) Host addresses.
Class C IP address format is:
110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH
Class D Address
Very first four bits of the first octet in Class D IP addresses are set to 1110
Class D has IP address range from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.
Class E Address
This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

CHAPTER 3

IMPACT OF THE INTERNSHIP

I completed wireless communication, Antenna and Networking papers in my 6th semester. In that paper, I learnt about In your wireless communication, antenna, and networking papers, you likely learned about concepts related to wireless transmission of data, including modulation techniques, multiplexing, channel coding, wireless standards (like Wi-Fi, Bluetooth, 4G/5G cellular networks), and protocols for wireless communication and in antennas (such as dipole, patch, Yagi-Uda, and parabolic antennas), antenna arrays, radiation patterns, antenna measurements, and antenna performance parameters like gain, directivity, and bandwidth.networking protocols (TCP/IP, UDP, HTTP, etc.), network architectures (client-server, peer-to-peer, mesh networks), network devices (routers, switches, gateways), network security, Quality of Service (QoS), and network management. To gain more knowledge in the fields, I attended this internship. The training helped me to learn new concepts and gain knowledge about telecommunication system .As telecommunication cover wireless system ,antenna and computer networks .this internship help us to learn real time system installation and also the maintenance telecommunication system Upon completing telecommunication training, I acquire the following skills:

- Technical Knowledge: I developed a deeper understanding of telecommunications hardware, software, and networking technologies by installation of system
- Problem-Solving: I improved my ability to troubleshoot and solve technical issues related to telecommunication systems by maintenance of system
- Communication Skills: I learned effective communication methods within telecommunication environments, enhancing my ability to convey ideas and information clearly by assignment.
- Teamwork: I gained experience working collaboratively in projects, improving my teamwork and collaboration skills by assignment.
- Industry Insights:I gained insights into current trends and advancements in telecommunications, keeping me updated with industry standards and practices.
- Increased efficiency and productivity in designing and maintaining automation systems

PROOF OF COMPLETION

Chennai Metro Rail Limited
(A Joint Venture of Govt. of India and Govt. of Tamil Nadu)

No.436/CMRL/HR/IPT/2023 **Date: 10/07/2023**

TO WHOMSOEVER IT MAY CONCERN

This is to certify that Mr. Suryadevara Manoj (ID No. SIT20EC086) from Sri Sai Ram Institute of Technology (West Tambaram, Chennai – 600 044) has done his Internship in Chennai Metro Rail Limited from 26th June 2023 to 10th July 2023.

During the Internship his conduct was good.

We wish him all the best for his better future.

S. Raja Ram
Assistant Manager (Admin)

S. RAJARAM
Assistant Manager - Admin
CHENNAI METRO RAIL LIMITED
METROS, Anna Salai,
Nandanam, Chennai - 600035

METROS, Anna Salai, Nandanam, Chennai - 600 035.
Email: chennaimetrorail@cmrl.in / Website: www.chennaimetrorail.org
CIN : U60100TN2007SGC065596

SECTION II

TABLE OF CONTENTS

SECTION -II

LIST OF FIGURES

SECTION II

ABSTRACT

Networking involves the practice of linking computers and various devices to facilitate resource and information sharing. This connection enables seamless communication among devices, facilitating data exchange and providing access to shared assets like printers, files, and internet services. Networking serves as a fundamental pillar of modern computing, serving businesses, organizations, and individuals by fostering communication, collaboration, and resource accessibility. It empowers the sharing of resources such as files and printers, enabling devices to connect to the internet and other networks. Networking plays a pivotal role in facilitating the creation and deployment of various applications and services, including email, web browsing, and video conferencing. Its significance extends to offering opportunities to engage in real-world projects, contributing to the advancement and implementation of innovative networking solutions. Through networking, individuals and entities can harness the power of interconnected systems to enhance productivity, communication, and the seamless flow of information across diverse platforms and environments.

CHAPTER 1

ABOUT THE COMPANY

NAME OF THE COMPANY – CISCO SYSTEMS (CISCO NETWORKING ACADEMY)

CISCO CIN NO: U72200KA2011FTC056691

Cisco Systems, Inc., is an ISO 9001:2015 Certified renowned multinational technology company that specializes in designing, manufacturing, and selling networking hardware, software, telecommunications equipment and other hightechnology services and products. Cisco specializes in specific tech markets, such as the Internet of Things (IoT), domain security, and energy management with leading products including Webex, OpenDNS, Jabber, Duo Security, and Jasper.

Cisco's mission: 'To shape the future of the internet by creating unprecedented value and opportunity for our customers, employees, investors, and ecosystem partners'. It aims to shape the future of the internet by delivering high-quality

products and services that meet its customer's needs and exceed their expectations.

Cisco's vision: Cisco's vision is aimed at changing the way we work, live, play, and learn.

Technology Support: Cisco hardware, software, and service offerings are used to create the Internet solutions that make networks possible--providing easy access to information anywhere, at any time. Since the company's inception, Cisco engineers have been leaders in the development of Internet Protocol (IP)based networking technologies. Today, with more than 71,000 employees worldwide, this tradition of innovation continues

with industry-leading products and solutions in the company's core development areas of routing and switching, as well as in advanced technologies such as home networking, IP telephony, optical networking, security, storage area networking, and wireless technology. In addition to its products, Cisco provides a broad range of service offerings, including technical support and advanced services. Cisco sells its products and services, both directly through its own sales force as well as through its channel partners, to large enterprises, commercial businesses, service providers, and consumers.

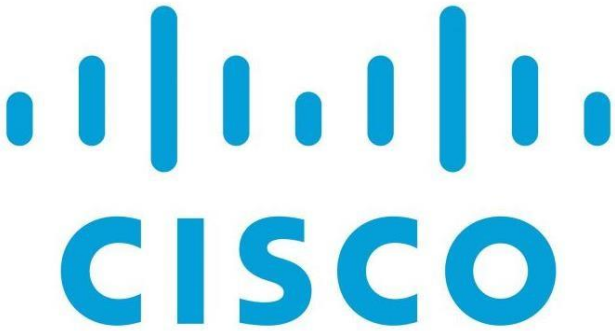


Fig. 1 CISCO Logo

Title of the Internship: Cybersecurity

Internship Period: 01/08/2023 to 21/09/2023 (Two months)

Mode of Internship: Online

CHAPTER 2
ABOUT THE INTERNSHIP

A computer network is a system that connects numerous independent computers in order to share information (data) and resources. The integration of computers and other different devices allows users to communicate more easily.

It is a collection of two or more computer systems that are linked together. A network connection can be established using either cable or wireless media. Hardware and software are used to connect computers and tools in any network.It consists of various kinds of nodes. Servers, networking hardware, personal computers, and other specialized or general-purpose hosts can all be nodes in a computer network. Host names and network addresses are used to identify them.

2.1 CISCO Packet Tracer:

Cisco Packet Tracer is a network simulation and visualization tool developed by Cisco Systems. It is used for teaching and learning networking concepts and skills, as well as for designing, configuring, and troubleshooting networks. Packet Tracer provides a virtual environment where users can create and simulate networks using a variety of Cisco devices and technologies.It provides a safe and controlled environment for students to experiment with networking technologies and gain hands-on experience. Packet Tracer is also used by networking professionals for designing, testing, and troubleshooting networks in real-world scenarios.

2.2 NETWORKING DEVICES

Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one

another. For example Repeater, Hub, Bridge, Switch, Routers, Gateway, Brouter, and NIC, etc.

- **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 to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they not only amplify the signal but also regenerate it. It is a 2-port device.

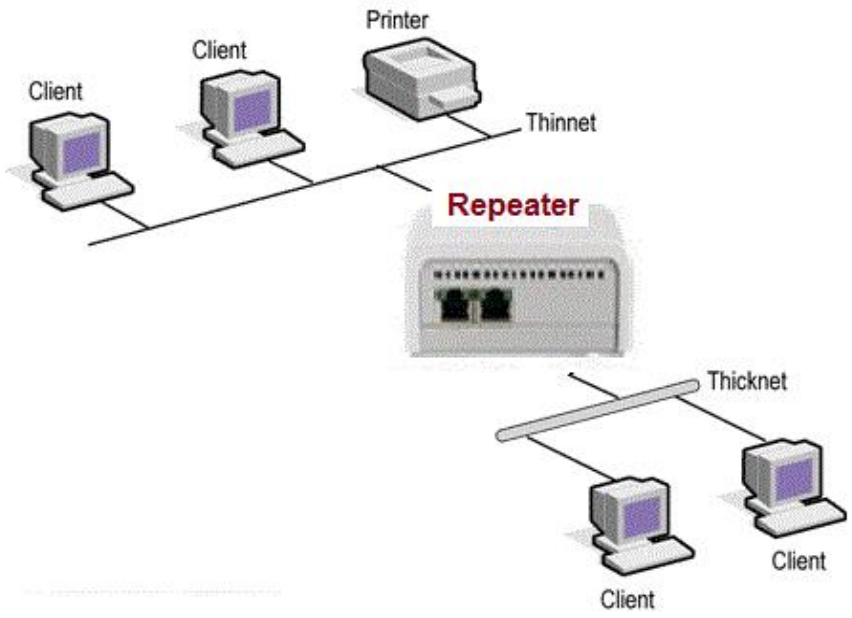


Fig.2 **Repeater**

- **Hub**

A hub is a basically multi-port 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. It do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

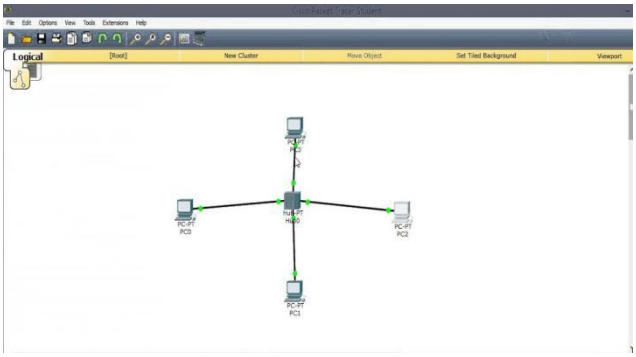


Fig 3 **Hub**

- **Bridge**

A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the 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.

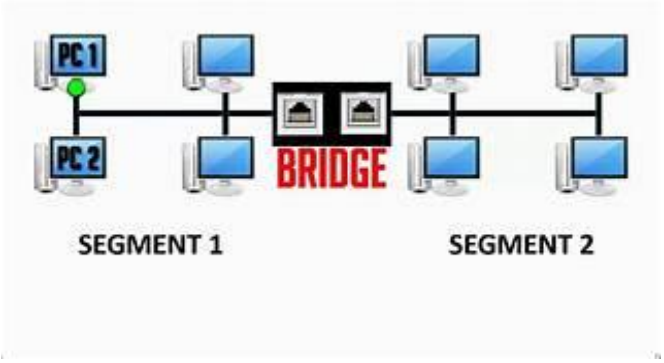


Fig 4 Bridge

- **Switch**

A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking

before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

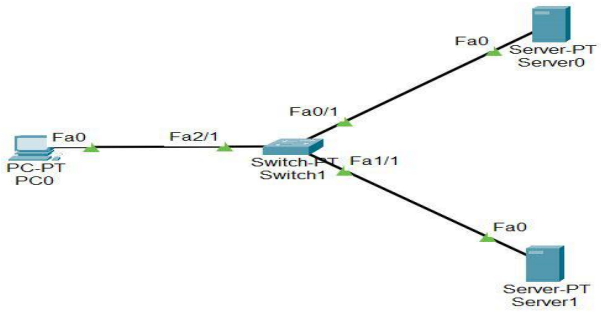


Fig 5 Switch

- **Routers**

A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.

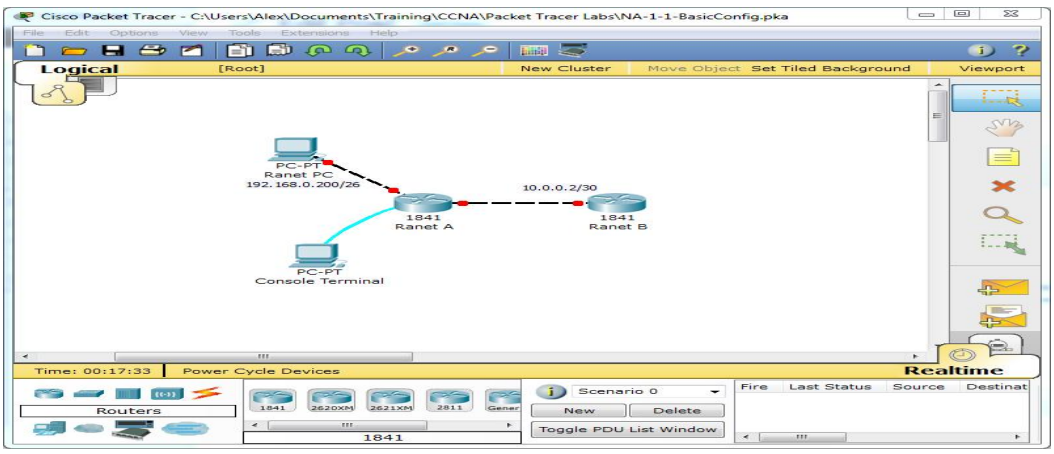


Fig 6 **Routers**

2.3TOPOLOGY

The structure of the network and how each component is connected to the others are defined by the network topology. Topology comes in two flavours: logical topology and physical topology.

2.3.1 TYPES OF TOPOLOGY

- **Bus Topology**

Every computer and network device is connected to a single cable in a bus topology network. Linear Bus topology is defined as having exactly two terminals.

Advantages

Installation is simple.Compared to mesh, star, and tree topologies, the bus utilizes less cabling.

Disadvantages

Difficulty in reconfiguring and isolating faults.

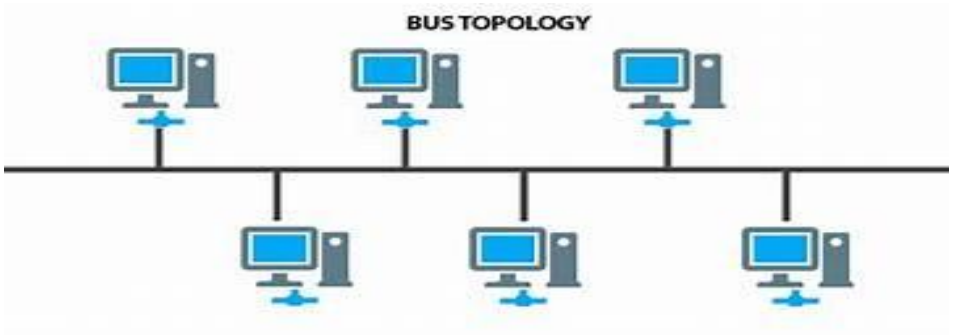


Fig 7 Bus Topology

- **Ring Topology**

The topology is named ring topology because one computer is connected to another, with the final one being connected to the first. Exactly two neighbors for each device. A signal is passed along the ring in one direction. Each ring incorporates a repeater.

Advantages

Data transmission is relatively straightforward because packets only move in one direction.There is no requirement for a central controller to manage communication between nodes.

Disadvantages:In a Unidirectional Ring, a data packet must traverse through all nodes.All computers must be turned on in order for them to connect with one another.

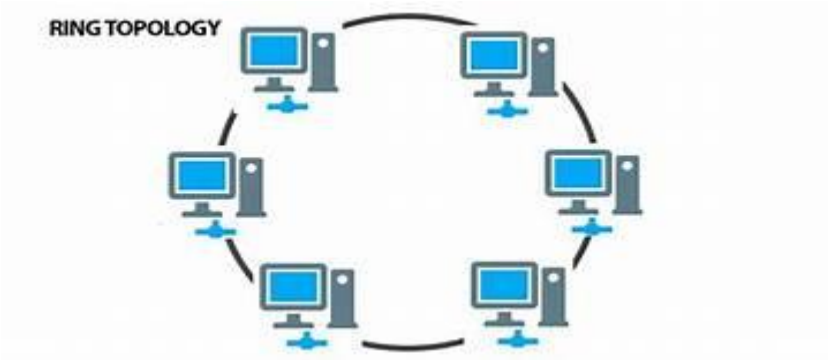


Fig 8 Ring Topology

- **Star Topology**

Each device in a star topology has a dedicated point-to-point link to a central controller, which is commonly referred to as the HUB. There is no direct connection between the devices. Traffic between the devices is not allowed in this topology. As an exchange, the controller is used.

Advantages

- It's simple to set up and configure.
- Identifying and isolating faults is simple.
- Less Expensive than mesh

Disadvantages

- Nodes attached to the hub, switch, or concentrator is failed if they fail.
- Because of the expense of the hubs, it is more expensive than linear bus topologies.
- More cable is required compared to a bus or ring
- Too much dependency on Hub.

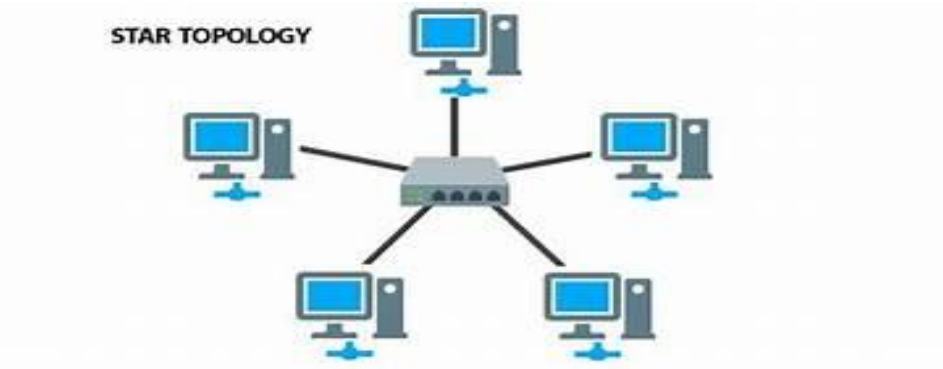


Fig 9 Star Topology

- ## Mesh Topology

Every device in a mesh topology has dedicated point-to-point connectivity to every other device. The term “dedicated” refers to the fact that the link exclusively transports data between the two devices it links. To connect n devices, a fully connected mesh network contains n *(n-1)/2 physical channels.

Advantages

- Data can be sent from multiple devices at the same time. This topology can handle a lot of traffic.
- Even if one of the connections fails, a backup is always available. As a result, data transit is unaffected.
- Physical boundaries prevent other users from gaining access to messages
- Point to Point links make fault transmission & fault isolation easy

Disadvantages

- The amount of cabling and the number of I/O ports that are necessary.
- The sheer bulk of wiring can be greater than the available space can accommodate.
- It is difficult to install and reconfigure.

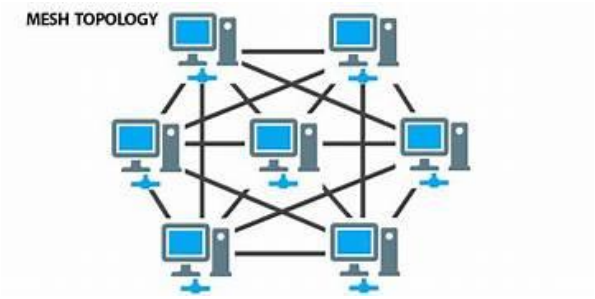


Fig 10 Mesh Topology

- **Tree Topology:**

The topology of a tree is similar to that of a star. Nodes in a tree, like those in a star, are connected to a central hub that manages network traffic. It has a root node, which is connected to all other nodes, producing a hierarchy. Hierarchical topology is another name for it. The number of Star networks is connected via Bus in Tree Topology.

Advantages

- Network expansion is both possible and simple.
- We partition the entire network into pieces (star networks) that are easier to manage and maintain.
- Other segments are unaffected if one segment is damaged.

Disadvantages

- Tree topology relies largely on the main bus cable because of its basic structure, and if it fails, the entire network is handicapped.
- Maintenance becomes more challenging when more nodes and segments are added.

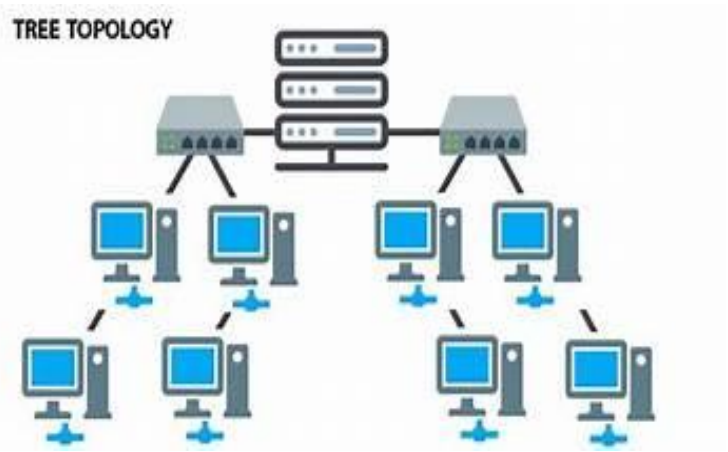


Fig 11 Tree Topology

2.4 NETWORKING MODELS:

A networking model is a set of guidelines and standards that defines how data is transmitted and received over a network. It is also known as a networking architecture or a networking blueprint. It provides a common framework for network devices and software to communicate with each other.

There are many networking models, but the most widely used are the OSI (Open Systems Interconnection) model and the TCP/IP(Transmission Control Protocol/Internet Protocol) . Both models are layered architectures that divide the communication process into layers. The OSI model divides the communication process into seven layers, each responsible for a specific set of functions. These layers are:

2.4.1 Similarities between OSI Model and TCP/IP Model

OSI and TCP/IP both are logical models. One of the main similarities between the OSI and TCP/IP models is that they both describe how information is transmitted between two devices across a network. Both models define a set of layers. Each layer performs a specific set of functions to enable the transmission of data.

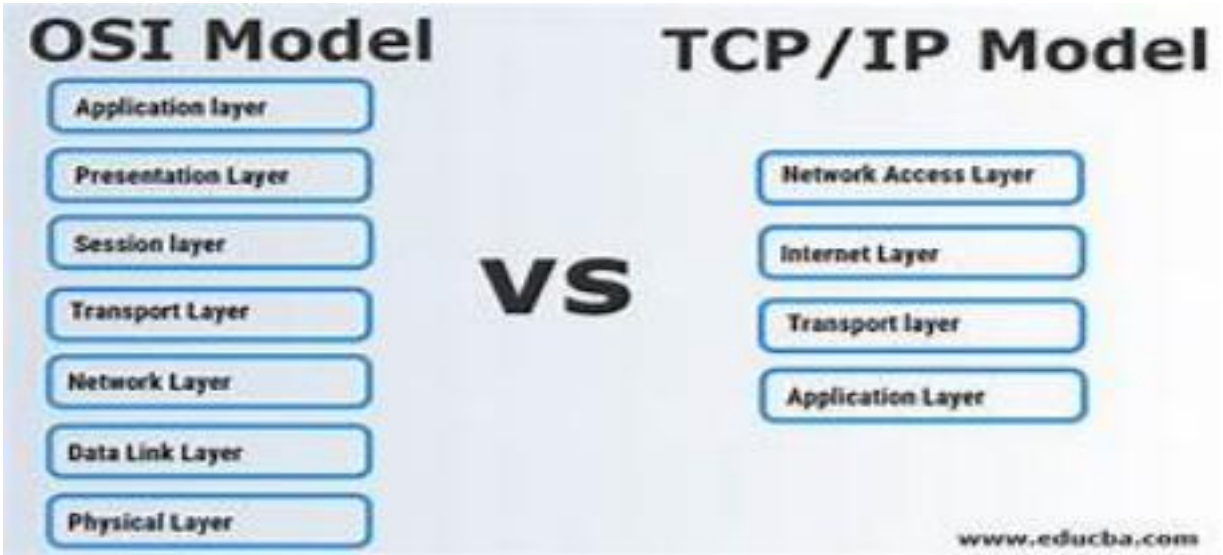


Fig 12 Similarities between OSI Model and TCP/IP Model

2.4.2 Different layers in OSI and TCP/IP Model:

Physical Layer: This layer deals with the physical connection between devices. It includes specifications for cables, connectors, and other physical aspects of networking.

Data Link Layer: This layer is responsible for establishing, maintaining, and terminating connections between devices. It also handles error detection and correction.

Network Layer: This layer is responsible for routing data packets between devices on different networks. It determines the best path for data to travel and handles addressing and packet forwarding.

Transport Layer: This layer is responsible for ensuring that data is delivered reliably and in the correct order. It also handles flow control and error recovery.

Session Layer: This layer is responsible for establishing, maintaining, and terminating connections between applications. It also handles synchronization and check pointing.

Presentation Layer: This layer is responsible for translating data between different formats and character sets. It also handles encryption and decryption.

Application Layer: This layer is responsible for providing network services to applications. It includes protocols like HTTP, FTP, and SMTP.

2.4.3 TCP/IP Model:

- **Link Layer**: This layer is similar to the OSI Data Link Layer and includes protocols like Ethernet and Wi-Fi.
- **Internet Layer**: This layer is similar to the OSI Network Layer and

includes the IP protocol, which is responsible for routing data packets between devices on different networks.

- **Transport Layer**: This layer is similar to the OSI Transport Layer and includes the TCP and UDP protocols, which are responsible for ensuring reliable delivery of data.
- **Application Layer**: This layer is similar to the OSI Application Layer and includes protocols like HTTP, FTP, and SMTP.

The main difference between the OSI model and the TCP/IP model is that the OSI model has seven layers, while the TCP/IP model has four layers. Additionally, the TCP/IP model combines the OSI Session Layer, Presentation Layer, and Application Layer into a single Application Layer.

2.4.4 IP ADDRESSING AND SUBNETTING:

Network Addressing is one of the major responsibilities of the network layer. Network addresses are always logical, i.e., software-based addresses. A host is also known as end system that has one link to the network. The boundary between the host and link is known as an interface. Therefore, the host can have only one interface .A router is different from the host in that it has two or more links that connect to it. When a router forwards the datagram, then it forwards the packet to one of the links. Each IP address is 32 bits long, and they are represented in the form of "dot-decimal notation" where each byte is written in the decimal form, and they are separated by the period. An IP address would look like 193.32.216.9 where 193 represents the decimal notation of first 8 bits of an address, 32 represents the decimal notation of second 8 bits of an address.

2.4.5 Class full Addressing

An IP address is 32-bit long. Classful addressing is an IPv4 addressing architecture that divides addresses into five groups Class A,Class B,Class C,Class D, Class E.

An ip address is divided into two parts:

- **Network ID:** It represents the number of networks.
- **Host ID:** It represents the number of hosts.

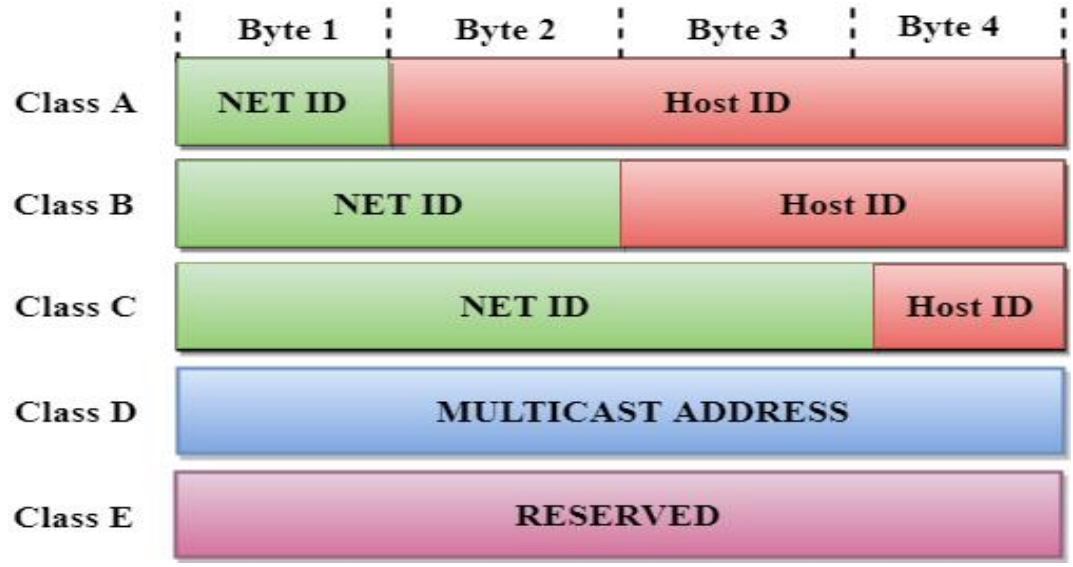


Fig 13 IP Class

Class A

In Class A, an IP address is assigned to those networks that contain a large number of hosts

- The network ID is 8 bits long.
- The host ID is 24 bits long.

In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.

The total number of networks in Class A = 2^7 = 128 network address

The total number of hosts in Class A = 2^{24} - 2 = 16,777,214 host address

Class B

In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks.

- The Network ID is 16 bits long.
- The Host ID is 16 bits long.

In Class B, the higher order bits of the first octet is always set to 10, and the remaining14 bits determine the network ID. The other 16 bits determine the Host ID.

The total number of networks in Class B = 2^{14} = 16384 network address

The total number of hosts in Class B = 2^{16} - 2 = 65534 host address

Class C

In Class C, an IP address is assigned to only small-sized networks.

- The Network ID is 24 bits long.
- The host ID is 8 bits long.

In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID. The 8 bits of the host ID determine the host in a network.

The total number of networks = 2^{21} = 2097152 network address

The total number of hosts = 2^8 - 2 = 254 host address

Class D

In Class D, an IP address is reserved for multicast addresses. It does not possess subnetting. The higher order bits of the first octet is always set to 1110, and the remaining bits determines the host ID in any network.

Class E

In Class E, an IP address is used for the future use or for the research and development purposes. It does not possess any subnetting. The higher order bits of the first octet is always set to 1111, and the remaining bits determines the host ID in any network.

Rules for assigning Host ID:

- The Host ID must be unique within any network.
- The Host ID in which all the bits are set to 0 cannot be assigned as it is used to represent the network ID of the IP address.

- The Host ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

Rules for assigning Network ID:

- The network ID cannot start with 127 as 127 is used by Class A.
- The Network ID in which all the bits are set to 0 cannot be assigned as it is used to specify a particular host on the local network.
- The Network ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

2.4.6 Classful Network Architecture

Classless addressing, also called **Classless Inter-Domain Routing (CIDR)**, is an improved IP addressing system. It increases the effectiveness of IP address allocation because of the absence of class distribution.

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Fig 14 Classful Network Architecture

Structure

The CIDR block comprises two parts. These are as follows:

- **Block id** is used for the network identification, but the number of bits is not pre-defined as it is in the classful IP addressing scheme.
- **Host id** is used to identify the host part of the network.

2.4.7 SUBNETTING:

A subnet, or subnetwork, is a part of a larger network. Subnets are a logical part of an IP network into multiple, smaller network components. The Internet Protocol (IP) is the method for transmitting data from one computer to another over the internet network. Each computer, or host, on the internet, has at least one IP address as a unique identifier.

Subnetting is a technique for creating logical sub-networks from a single physical network (subnets). A company can grow its network via subnetting without asking for a new network number from its ISP. Subnetting hides network complexity while assisting in the reduction of network traffic.

Subnet Masks on Octet Boundaries

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of hosts
/8	255.0.0.0	nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh 11111111.00000000.00000000.00000000	16,777,214
/16	255.255.0.0	nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh 11111111.11111111.00000000.00000000	65,534
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	254

Fig 15 subnet masks

Subnetting Network 10.0.0.0/8 using a /16

Subnet Address (256 Possible Subnets)	Host Range (65,534 possible hosts per subnet)	Broadcast
10.0.0.0/16	**10.0**.0.1 - **10.0**.255.254	**10.0**.255.255
10.1.0.0/16	**10.1**.0.1 - **10.1**.255.254	**10.1**.255.255
10.2.0.0/16	**10.2**.0.1 - **10.2**.255.254	**10.2**.255.255
10.3.0.0/16	**10.3**.0.1 - **10.3**.255.254	**10.3**.255.255
10.4.0.0/16	**10.4**.0.1 - **10.4**.255.254	**10.4**.255.255
10.5.0.0/16	**10.5**.0.1 - **10.5**.255.254	**10.5**.255.255
10.6.0.0/16	**10.6**.0.1 - **10.6**.255.254	**10.6**.255.255
10.7.0.0/16	**10.7**.0.1 - **10.7**.255.254	**10.7**.255.255
...	...	...
10.255.0.0/16	**10.255**.0.1 - **10.255**.255.254	**10.255**.255.255

Fig 16 sub netting network

Subnet a /24 Network

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh 11111111.11111111.11111111.**1**0000000	**2**	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh 11111111.11111111.11111111.**11**000000	**4**	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh 11111111.11111111.11111111.**111**00000	**8**	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh 11111111.11111111.11111111.**1111**0000	**16**	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh 11111111.11111111.11111111.**11111**000	**32**	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh 11111111.11111111.11111111.**111111**00	**64**	2

Fig 17 sub net a/24 network

2.4.8 MAC ADDRESS:

It is the 48 bits unique identifier address of a device. The other name of this address is hardware address. Every device has a unique physical address which identifies it between whole network devices.These addresses are assigned to the devices by the manufacturer vendors.

MAC Address is the abbreviation of Media Access Control Address. It is assigned to NIC of the devices. NIC is Network Interface Controller.ipconfig/all command to display ip information and mac address on your PC.

Physical addresses are expressed with Hexadecimal numbers. Hexadecimal numbers use decimal 0-9 numbers and A, B, C, D, E, F letters. So, in a Media Access Control Address, any of these numbers or letters can be used.

The total length of a MAC address is 48 bits (6 bytes). Physical addresses consist of 6 groups. Each group has two hexadecimal numbers. Each number is defined with 4 bits and these two numbers are total 8 bits. In other words, every group is 8 bits long.

The switch maintains an address table called the MAC address table in order to efficiently switch frames between interfaces. So basically a switch stores information about the other (Ethernet interfaces) to which it is connected on a network. when a switch receives a frame, it associates the MAC address of the sending device with the switch port on which it was received.

Physical address examples:

C2-E2-82-AD-B5-56

45-78-92-AA-33-12

Static: The switch administrator must manually add static items to the table. Dynamic entries are less important than static entries. Static entries are active until the switch administrator deletes them.

Dynamic: The switch retrieves the source mac address(and VLAN ID, if present) of each Ethernet packet received on a port, dynamic entries are automatically added to the table. If the table does not already include the obtained address, it is added. Dynamic entries are automatically erased after being present in the table for a certain period of time (specified by the command mac-address-table age-time).

2.5 SWITCHING:

When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as switching.

Switching in a computer network is achieved by using switches. A switch is a small hardware device which is used to join multiple computers together with one local area network (LAN).Network switches operate at layer 2 (Data link layer) in

the OSI model.Switching is transparent to the user and does not require any configuration in the home network.Switches are used to forward the packets based on MAC addresses.A Switch is used to transfer the data only to the device that has been addressed. It verifies the destination address to route the packet appropriately.It is operated in full duplex mode.

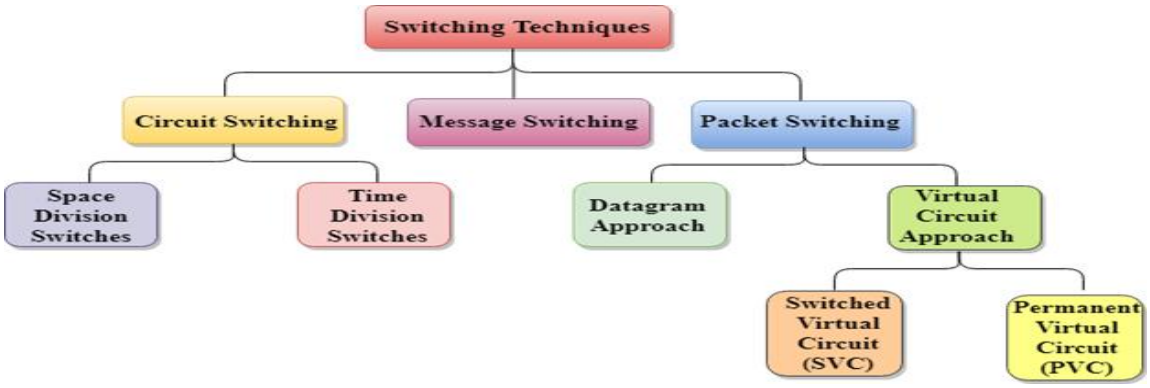


Fig 18 Classification Of Switching Techniques

2.5.1 Circuit Switching:

Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.Circuit switching in a network operates in a similar way as the telephone works.A complete end-to-end path must exist before the communication takes place.In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.

2.5.2 Communication through circuit switching has 3 phases:

- Circuit establishment
- Data transfer
- Circuit Disconnect

2.6 MESSAGE SWITCHING:

Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the

message.Message switches are programmed in such a way so that they can provide the most efficient routes.Each and every node stores the entire message and then forward it to the next node. This type of network is known as store and forward network.

Message switching treats each message as an independent entity.

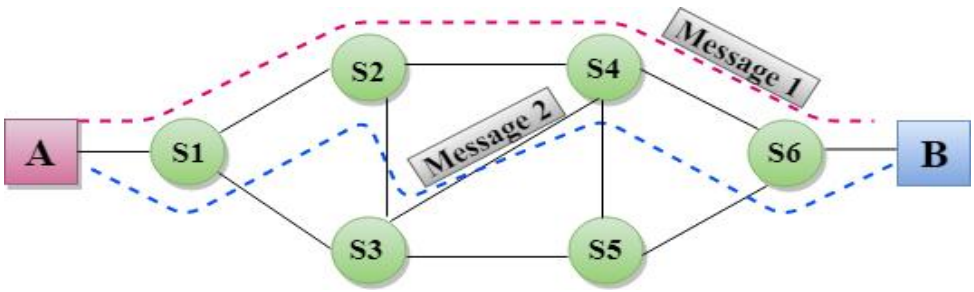


Fig 19 Message Switching

2.6.1 Packet Switching

The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.Every packet contains some information in its headers such as source address, destination address and sequence number.Packets will travel across the network, taking the shortest path as possible.

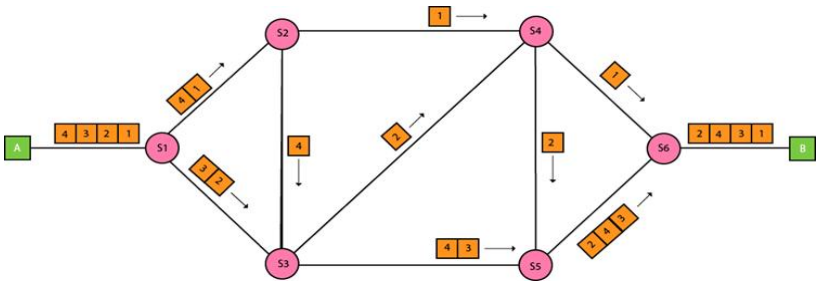


Fig 20 Packet Switching

2.7 ROUTING:

- A Router is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.
- A Router works at the network layer in the OSI model and internet layer in TCP/IP model
- A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.
- The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.

- The routing protocols use the metric to determine the best path for the packet delivery. The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc. used by the routing algorithm to determine the optimal path to the destination.
- The routing algorithm initializes and maintains the routing table for the process of path determination.

2.7.1 Types of Routing:

- Static Routing
- Default Routing
- Dynamic Routing

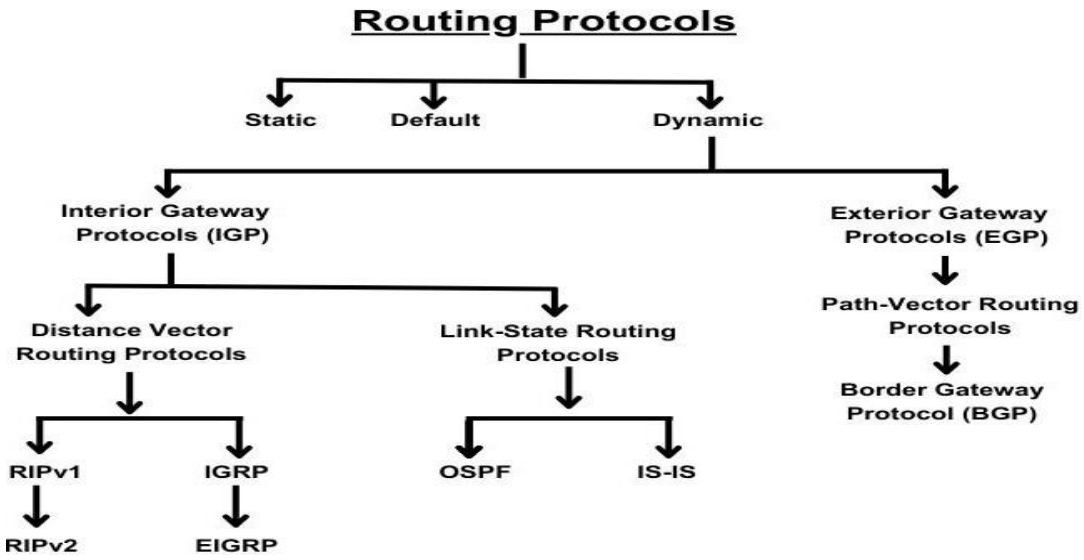


Fig 21 routing proctocls

2.7.2 Static Routing

Static Routing is also known as Nonadaptive Routing.It is a technique in which the administrator manually adds the routes in a routing table.A Router can send the packets for the destination along the route defined by the administrator.In this technique, routing decisions are not made based on the condition or topology of the networks.

2.7.3 Default Routing

Default Routing is a technique in which a router is configured to send all the packets to the same hop device, and it doesn't matter whether it belongs to a particular network or not. A Packet is transmitted to the device for which it is configured in default routing.Default Routing is used when networks deal with the single exit point.It is also useful when the bulk of transmission networks have to transmit the data to the same hp device.

2.7.4 Dynamic Routing

It is also known as Adaptive Routing.It is a technique in which a router adds a new route in the routing table for each packet in response to the changes in the condition or topology of the network.Dynamic protocols are used to discover the new routes to reach the destination.In Dynamic Routing, RIP and OSPF are the protocols used to discover the new routes.If any route goes down, then the automatic adjustment will be made to reach the destination.

- **Interior Gateway Protocol (IGP)**

The Interior Gateway Protocol was built to overcome the shortcomings of RIP. IGP is majorly used by the routers to transit the data within the autonomous systems. They are more suitable for large-sized networks as it contains a count of 255 and broadcast after every 90-sec interval. It is fruitful for loop routing as it can automatically update the route whenever any kind of change takes place.

- **Link State Routing Protocol**

The Link State Routing Protocol, as the name suggests, follows a unique method to get the best route by calculating the speed of the path for reaching the

destination and the cost of resources. This protocol maintains a separate table to get the best and backup route information. Thus, it is appropriate for inter-network compared to any other distance vector protocol. It does not consume any extra bandwidth as it follows triggered updates. But when there is any change in the topology, it triggers a partial update. Therefore, there is no update required at the point where the whole routing table is exchanged.

- **Distance Vector Routing Protocol (DVR)**

Distance Vector Routing Protocol shares the routing table with each node which is a directly connected neighbour at a specific time but has slow convergence and high bandwidth. When the route is unavailable, the routing table gets updated with new information.

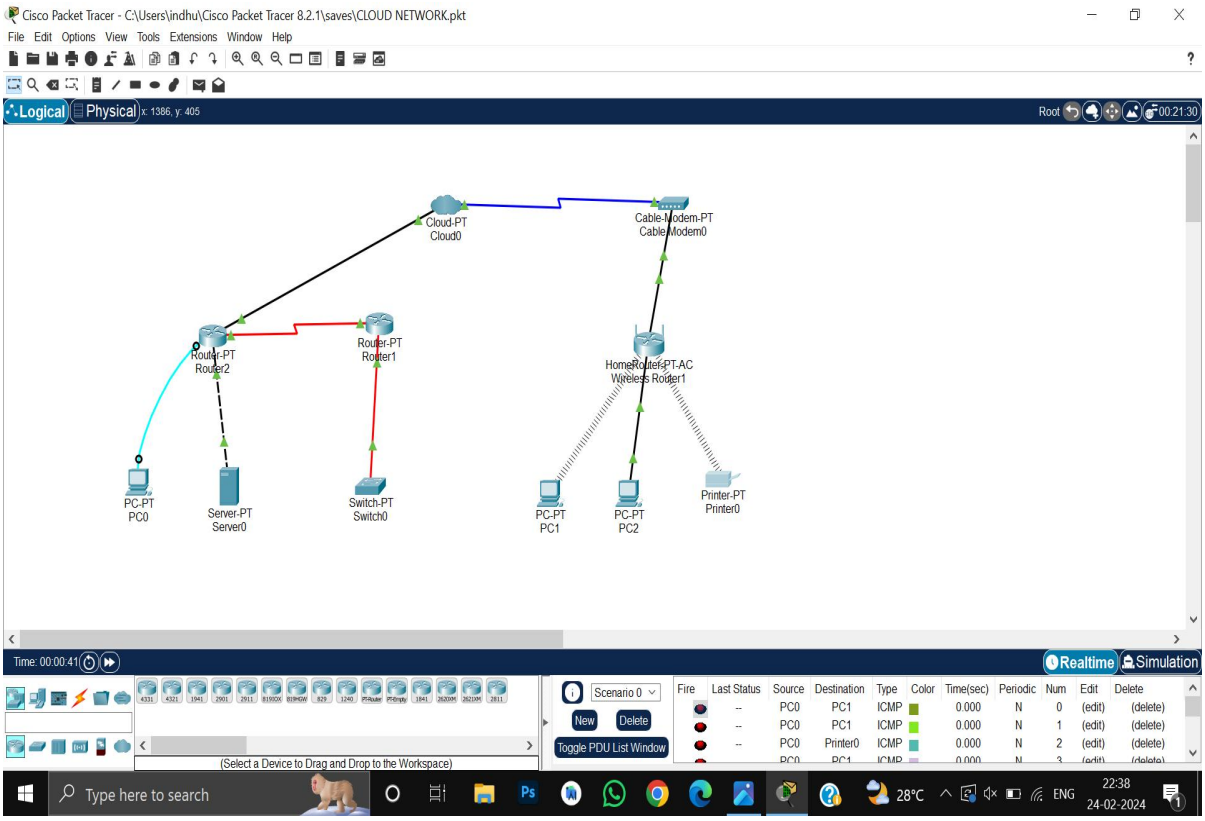
- **Exterior Gateway Protocol**

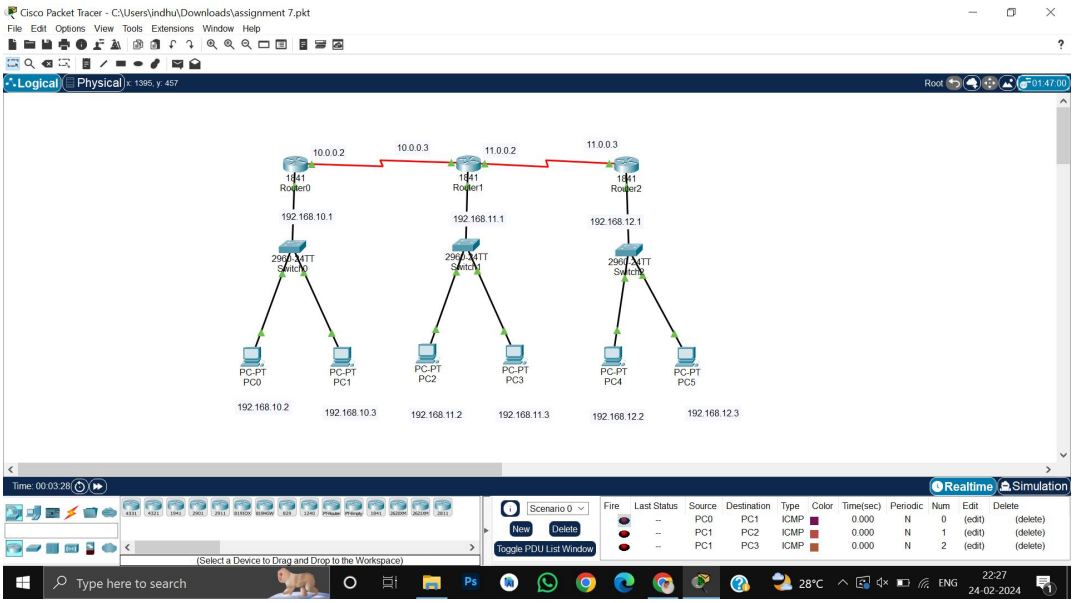
Exterior Gateway Protocol (EGP) is the mechanism that allows the exterior gateway of an autonomous system to share routing information with exterior gateways on other autonomous systems.

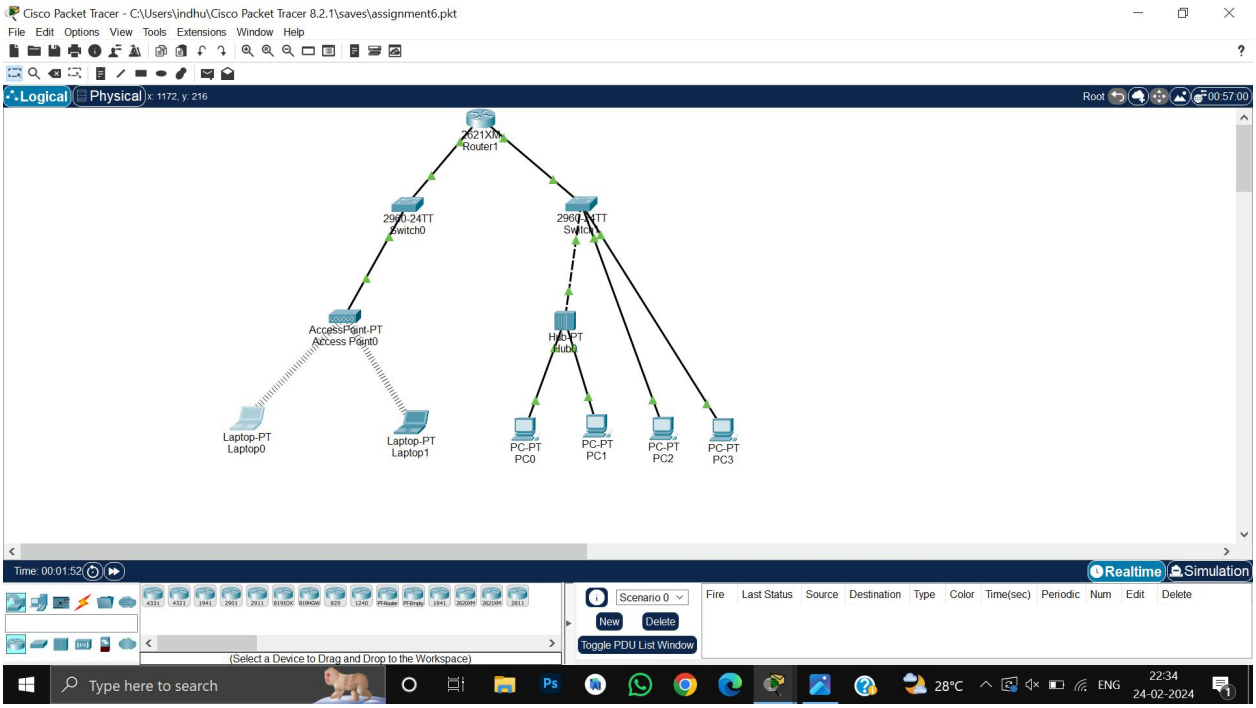
- **Path Vector Protocol**

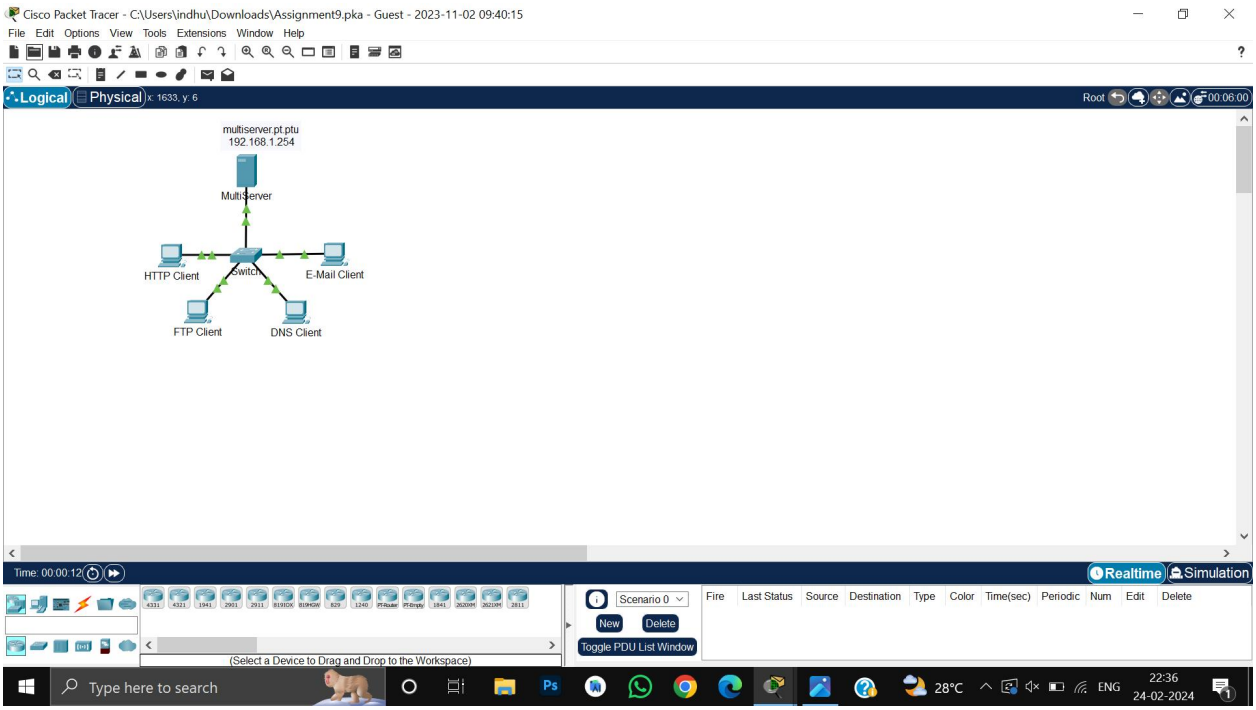
The path vector protocol is a routing protocol that keeps track of path information that is updated dynamically. The path vector protocol does not rely on the reachability to the destination, instead determines whether the path is loop-free or not. The path vector does the analysis of the path to determine whether the path is loop-free or not.

2.8 MINI PROJECTS:


Cisco Packet Tracer - C:\Users\indhu\Cisco Packet Tracer 8.2.1\saves\CLOUD NETWORK.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical
Cloud-PT Cloud0
Cable-Modem-PT Cable Modem0
Router-PT Router2
Router-PT Router1
HomeRouter-PT-AC Wireless Router1
PC-PT PC0
Server-PT Server0
Switch-PT Switch0
PC-PT PC1
PC-PT PC2
Printer-PT Printer0
Realtime Simulation
Scenario 0
New Delete
Toggle PDU List Window
(Select a Device to Drag and Drop to the Workspace)
Type here to search
28°C ENG 22:38 24-02-2024


Cisco Packet Tracer - C:\Users\indhu\Downloads\assignment 7.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical
10.0.0.2
10.0.0.3
11.0.0.2
11.0.0.3
1841 Router0
1841 Router1
1841 Router2
192.168.10.1
192.168.11.1
192.168.12.1
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
PC-PT PC4
PC-PT PC5
192.168.10.2
192.168.10.3
192.168.11.2
192.168.11.3
192.168.12.2
192.168.12.3
Realtime Simulation
Scenario 0
New Delete
Toggle PDU List Window
(Select a Device to Drag and Drop to the Workspace)
Type here to search
28°C ENG 22:27 24-02-2024


Cisco Packet Tracer - C:\Users\indhu\Cisco Packet Tracer 8.2.1\saves\assignment6.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 1172, y: 216
Root 00:57:00
2621XM Router1
2960-24TT Switch0
2960-24TT Switch1
AccessPoint-PT Access Point0
Hub-PT Hub0
Laptop-PT Laptop0
Laptop-PT Laptop1
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
Time: 00:01:52
Realtime Simulation
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
(Select a Device to Drag and Drop to the Workspace)
Type here to search
28°C ENG 22:34 24-02-2024


Cisco Packet Tracer - C:\Users\indhu\Downloads\Assignment9.pka - Guest - 2023-11-02 09:40:15
File Edit Options View Tools Extensions Window Help
Logical Physical x: 1633, y: 6
Root 00:06:00
multiserver.pt.ptu
192.168.1.254
Multiserver
HTTP Client
Switch
E-Mail Client
FTP Client
DNS Client
Time: 00:00:12
Realtime Simulation
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
(Select a Device to Drag and Drop to the Workspace)
Type here to search
28°C ENG 22:36 24-02-2024

CHAPTER 3

IMPACT OF THE INTERNSHIP

I completed Computer Networking papers in my 6th semester. In that paper, I learnt about In your wireless communication, antenna, and networking papers, you likely learned about concepts related to networking protocols (TCP/IP, UDP, HTTP, etc.), network architectures (client-server, peer-to-peer, mesh networks), network devices (routers, switches, gateways), network security, Quality of Service (QoS), and network management. To gain more knowledge in the fields, I attended this internship. The training helped me to learn new concepts and gain knowledge about networking system .As networking cover computer networks .this internship help us to learn real time system installation and also the maintenance networking system

- Practical Exposure: An internship at Cisco, a renowned networking technology leader, promises hands-on experience with state-of-the-art networking equipment and software. This firsthand experience is invaluable when pursuing careers in Networking, Packet Tracer, and Routing Protocols within Computer Networks.

- Networking Prospects: Engaging in a Cisco internship within the "NETWORKING" domain opens doors to connect with industry professionals, both within the organization and through participation in industry events and conferences. Building a professional network plays a pivotal role in accessing job opportunities and progressing in one's career.

- Enhanced Resume Appeal: Including a Cisco Internship Certificate on our resume elevates our profile for potential employers, showcasing our exposure to cutting-edge technology and training from a top networking company.

- Skill Enhancement: Cisco internships offer training and mentorship opportunities, fostering the development of technical competencies in networking. This

encompasses learning about Cisco's products and solutions, along with gaining expertise in networking protocols and technologies.

- Future Employment Potential: Many companies, Cisco included, use internships as a talent pipeline for future hiring. Excelling during the internship may lead to prospects for joining Cisco as a full-time employee post-graduation.

- Industry Esteem: Cisco's esteemed reputation in the networking sector adds significant value to our resume, signalling to other employers our proficiency in networking fundamentals and adaptability to dynamic, innovative work environments.

- Learning from Industry Leaders: With a pool of top networking experts at Cisco, interns have the opportunity to learn from these professionals and stay abreast of the latest industry trends and advancements.

PROOF OF COMPLETION


VERZEO

Certificate Of Course Completion

Manoj Suryadevara

has successfully completed Internet of Things course
from 01-08-2022 to 30-09-2022.

During this course, we found the student to be a keen and enthusiastic candidate.

P Athulitha
Course Co-ordinator

T. Nikhil
Academic Head

Verified Certificate

Certificate ID: 447750115
Date: 27-02-2023

Our Course Completion certificates are verified and are recognized
by eminent industries and universities all over the world.