COMPUTER NETWORKS

LAB MANUAL

Created By

Hashim Yaseen Mulug-1501

School of Information Technology

MUL, Lahore

Table of Contents

CHAPTER # 0: COMMANDS

1. HOSTNAME

```
PS C:\Users\hashi> hostname
Hashymhh
```

Fig 1.1

My computer`s Host name: Hashymhh

2. IP CONFIG:

```
Windows IP Configuration


Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::bba6:2585:b616:c75f%13
   IPv4 Address. . . . . . . . . . . : 192.168.37.246
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.37.1

Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::fb6:47ae:397b:212d%7
   IPv4 Address. . . . . . . . . . . : 192.168.137.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
PS C:\Users\hashi>
```

Fig 2.1

Basically, in screenshot you can see media disconnected, because windows never show media connected instead it displays their ipv4 address, or subnet or default gateways.
My current Pc is connected or linked with 4 connections
3 of them is disconnected and one is connected

3. IP CONFIG/ALL:

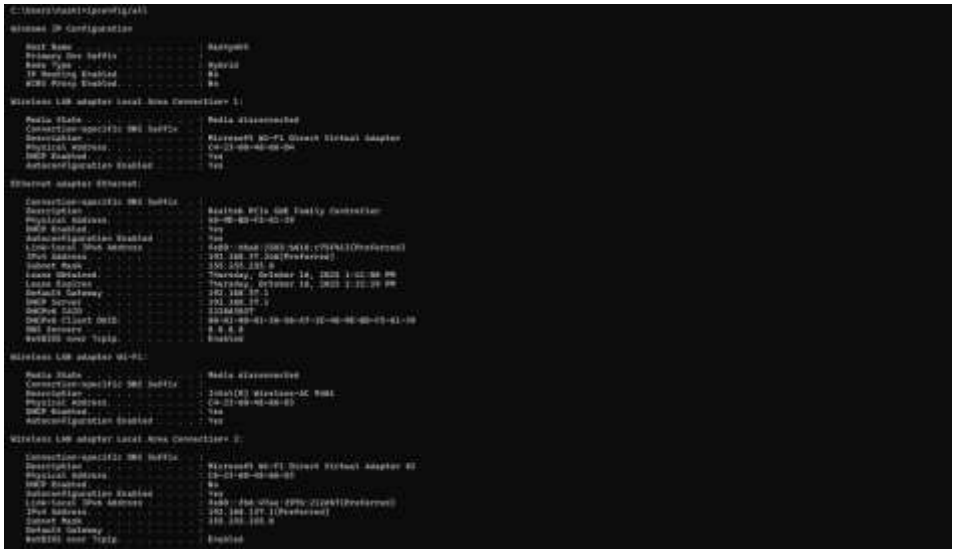


Fig 3.1

4. GET MAC:

```
PS C:\WINDOWS\system32> getmac

Physical Address    Transport Name
=================== ============================================================
C4-23-60-48-66-D3   \Device\Tcpip_{B92DCC02-0668-477C-8AD3-B441ECD08B67}
48-9E-BD-F5-81-39   Media disconnected
C4-23-60-48-66-D7   Media disconnected
PS C:\WINDOWS\system32>
```

Fig 4.1

5. PING:

```
C:\Users\hashi>ping youtube.com

Pinging youtube.com [142.250.202.14] with 32 bytes of data:
Reply from 142.250.202.14: bytes=32 time=48ms TTL=115
Reply from 142.250.202.14: bytes=32 time=37ms TTL=115
Reply from 142.250.202.14: bytes=32 time=47ms TTL=115
Reply from 142.250.202.14: bytes=32 time=40ms TTL=115

Ping statistics for 142.250.202.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 37ms, Maximum = 48ms, Average = 43ms

C:\Users\hashi>ping instagram.com

Pinging instagram.com [157.240.227.174] with 32 bytes of data:
Reply from 157.240.227.174: bytes=32 time=41ms TTL=51
Reply from 157.240.227.174: bytes=32 time=42ms TTL=51
Reply from 157.240.227.174: bytes=32 time=41ms TTL=51
Reply from 157.240.227.174: bytes=32 time=41ms TTL=51

Ping statistics for 157.240.227.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 41ms, Maximum = 42ms, Average = 41ms

C:\Users\hashi>ping tiktok.com

Pinging tiktok.com [2.19.193.27] with 32 bytes of data:
Reply from 2.19.193.27: bytes=32 time=342ms TTL=51
Request timed out.
Reply from 2.19.193.27: bytes=32 time=341ms TTL=51
Reply from 2.19.193.27: bytes=32 time=332ms TTL=51

Ping statistics for 2.19.193.27:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 332ms, Maximum = 342ms, Average = 338ms
```

Fig 5.1

```
C:\Users\hashi>ping netflix.com

Pinging netflix.com [54.246.79.9] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 54.246.79.9:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\hashi>ipconfig youtube.com

Error: unrecognized or incomplete command line.
```

Fig 5.2

CHAPTER # 1

INTRODUCTION TO CISCO PACKET TRACER

Cisco Packet Tracer is a free network simulation and visualization tool from Cisco Systems that lets users design, build, and test network topologies and configurations in a virtual environment. It provides a drag-and-drop interface to add simulated devices like routers and switches and allows users to configure them using a command-line interface, making it a valuable educational tool for learning fundamental networking concepts

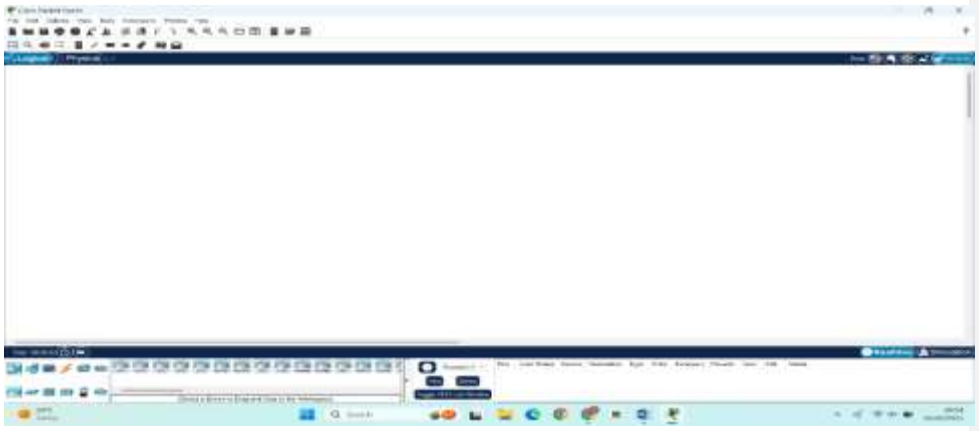


Fig 1.1

It is a network simulation tool developed by Cisco Systems that allows users to create virtual networks to practice

designing, configuring and troubleshooting the networks.

The tool is so powerful using it efficiently will help you in many aspects.

1. TOP BAR

Fig 1.1

This includes all the general functions such as copy paste, new, delete etc. But below are few features which we will use a lot, so we have got to be very clear about their purpose and shortcuts:

1.1 New File:

Creates a new project and starts a fresh workspace. Clears everything and opens a blank topology.

Shortcut: Ctrl + N

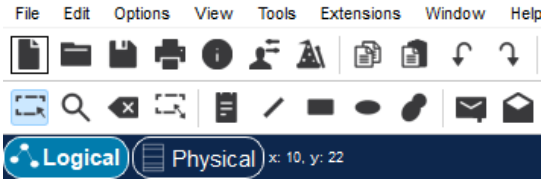


Fig 1.1.1

1.2 Open File:

Load an existing .pkt file. Also, reopen saved work.

Shortcut: Ctrl + O

Fig 1.1.2

1.3: Save File:

Save the current project, store changes into the same file and update the existing .pkt file.

Shortcut: Ctrl + S

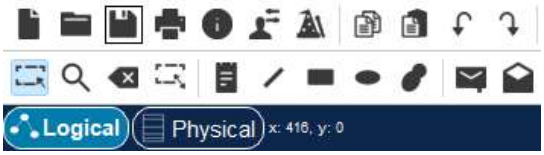


Fig 1.3.1

1.4

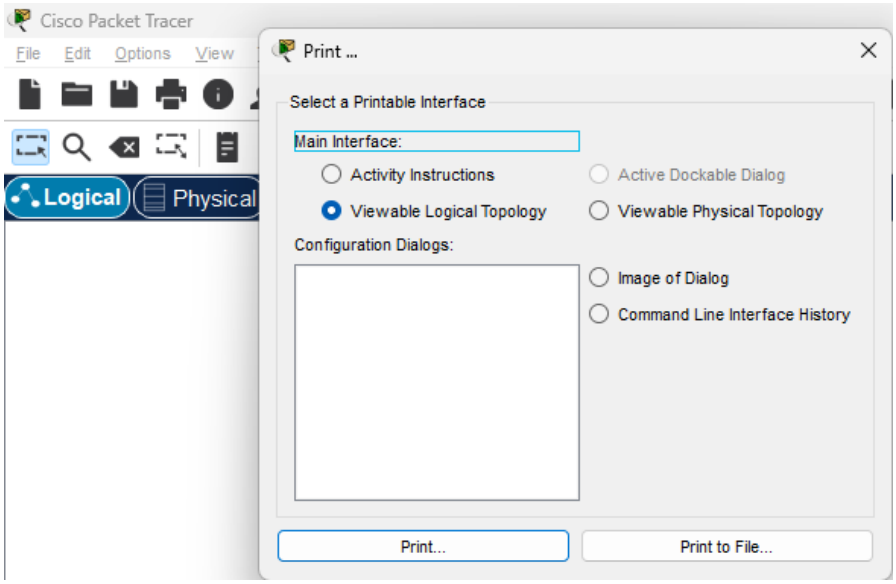


Fig 1.4.1

1.5: Network Information

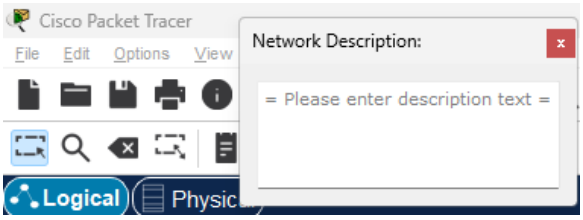


Fig 1.5.1

1.6: User Profile:

Definition: Shows the user's details logged into Cisco NetAcad, used for PT assessments, saving progress.
It doesnot have any short cut key.

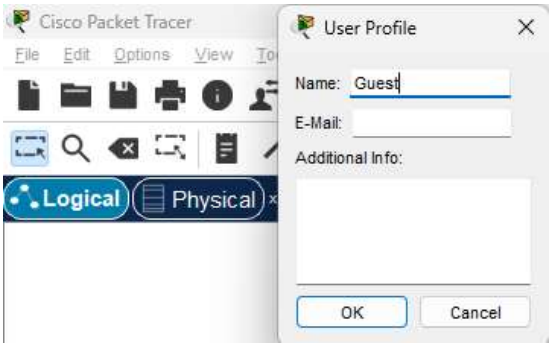


Fig 1.6.1

1.7: Activity Wizard:

Definition: Tool to create custom scoring activities.

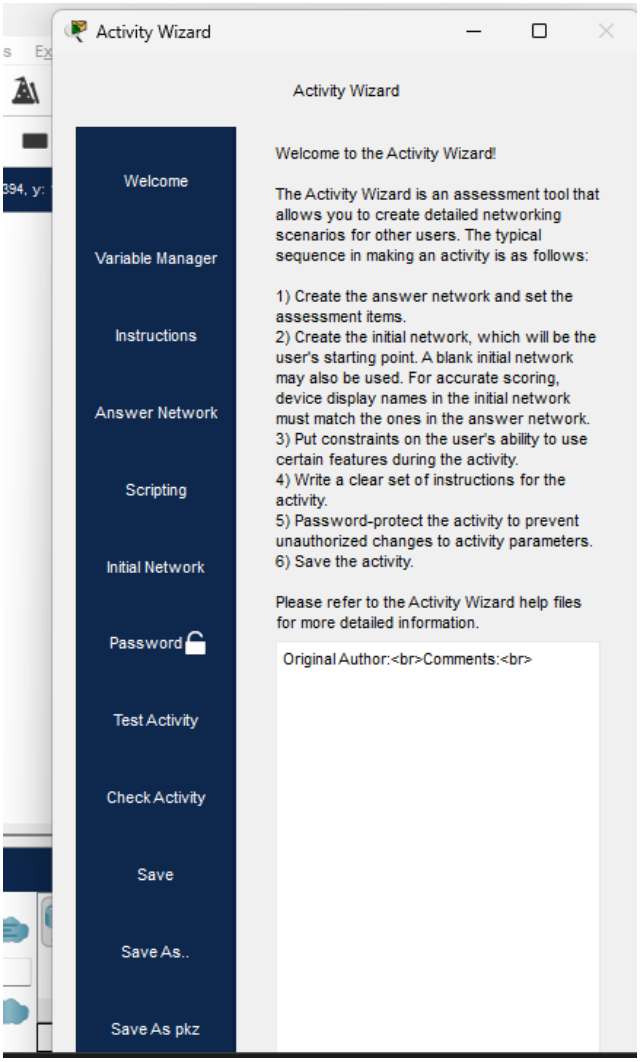
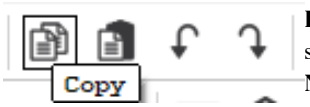

Activity Wizard
Activity Wizard
Welcome
Variable Manager
Instructions
Answer Network
Scripting
Initial Network
Password
Test Activity
Check Activity
Save
Save As..
Save As pkz
Welcome to the Activity Wizard!
The Activity Wizard is an assessment tool that allows you to create detailed networking scenarios for other users. The typical sequence in making an activity is as follows:
1) Create the answer network and set the assessment items.
2) Create the initial network, which will be the user's starting point. A blank initial network may also be used. For accurate scoring, device display names in the initial network must match the ones in the answer network.
3) Put constraints on the user's ability to use certain features during the activity.
4) Write a clear set of instructions for the activity.
5) Password-protect the activity to prevent unauthorized changes to activity parameters.
6) Save the activity.
Please refer to the Activity Wizard help files for more detailed information.
Original Author:
Comments:

Fig 1.7.1

1.8: Copy



Definition: Copies selected devices, drawings, notes, or shapes.
Note: Does not copy configurations fully for some devices.
Shortcut: Ctrl + C

Fig 1.8.1

1.9:Paste

Definition: Pastes copied items into workspace.
Shortcut: Ctrl + V

Fig 1.9.1

1.10: View Port

Shows a small minimap of your workspace useful to Navigate large networks.
E.g., to view Big WAN topologies.
It does not have any shortcut key

Fig 1.10.1

1.11: Workspace Lists:

Displays all workspaces (Logical & Physical), Switch between views. It does not have any shortcut key.

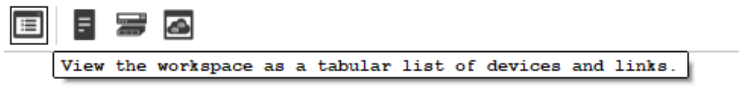


Fig 1.11.1

1.12: View Logs:

Shows the CLI commands executed in devices, used for debugging and learning CLI.It does not have any shortcut key.

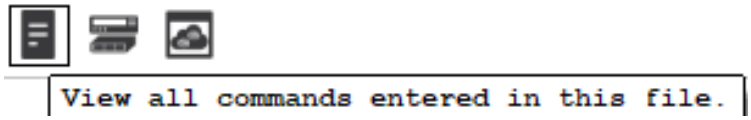


Fig 1.12.1

1.13: Custom dialouge:

Window for creating/editing custom devices. It does not have any shortcut key.

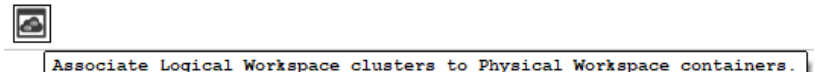
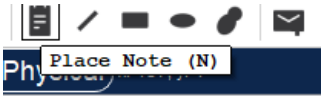


Fig 1.13.1

1.14 Place Note:



Short Cut Key: N

This is used to add text in the cisco workspace.

Fig 1.14.1

1.15 Draw Line:

Definition: Draw straight lines.
Shortcut: L

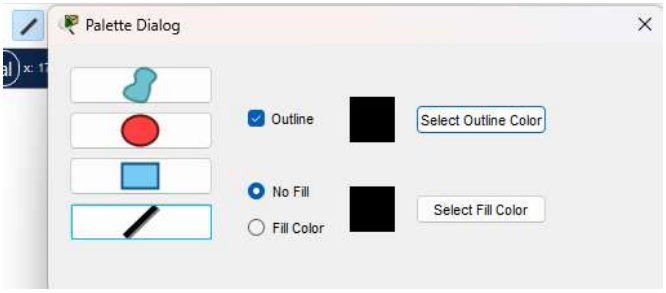


Fig 1.15.1

You can draw a line to point/demonstrate stuff in workplace

1.16 Draw Rectangle:

Definition: Create rectangular shapes.
Shortcut: R

Fig 1.16.1

Can draw rectangles to isolate networks from one to another

1.17 Draw Ellipse:

Definition: Draw circular/oval shapes.
Shortcut: E
(Add img)

Also use to isolate nodes from one to another

1.18 Draw Freeform:

(Add img)

Another designing tool for discrimination among the network devices.

1.19 Add PDU:

Definition: Opens advanced packet configuration options. Testing TCP, HTTP,DHCP, email, etc.
Shortcut: C

Fig 1.19.1

Allows you to create detailed packets and configure protocol behavior for simulations.

1.20 Del:

You can delete unwanted material from your workplace.

Shortcut: Delete key

Fig 1.20.1

1.21 Select:

Select and operate functions on them like shifting through this button.

Shortcut: Delete key

Fig 1.21.1

1.22 Zoom:

Fig 1.22.1

You can zoom in or out or reset the vision for your efficiency.

1.23 Undo/redo:

Fig 1.23.1

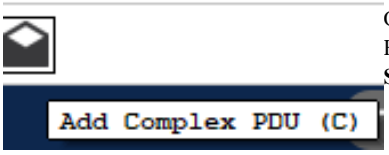
Undo or redo any of your actions

1.24 ESC:

(add img)

Escape from the current mode and reverse to normal

1.25 Add Complex PDU:



Opens advanced packet configuration options. Testing TCP, HTTP, DHCP, email, etc.
Shortcut: C

Fig 1.25.1

1.26 Resize:

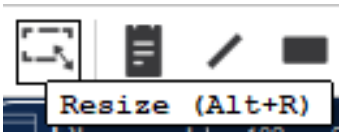
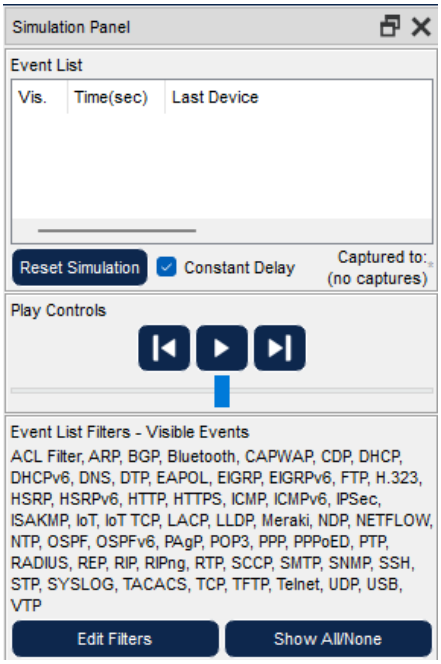


Fig 1.26.1

Bottom bar

The area for all types of nodes, you can get multiple devices with great categorization and placements

Stimulation mode



Allows you to stimulate the network you build so you can check if it works or not in real life.

Time controls

You can pause or forward the packets sent over internet to complete your tasks.

Network devices

All the network devices and nodes will be available here for you to use them according to your network requirements.

CHAPTER # 2

NETWORK TOPOLOGIES

TOPOLOGIES:

A network topology is the arrangement of devices (nodes) and connections (links) in a computer network. It shows how computers, servers, and other devices are connected and how data flows between them. There are two main types of topologies:

Physical Topology:

The actual physical layout of cables and devices.

Logical Topology:

How data moves across the network, regardless of physical layout.

1. Peer to Peer

Point-to-point topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point-to-Point provides high bandwidth.

Fig 1.1

This topology works as an interlink within only 2 pcs, A single cable line is used to connect nodes with each other.

Nodes:	Links:	IP Addresses:
PC0	Copper Cross over	192.168.10.6
PC2	Copper Cross over	192.168.10.5

1.1 Assigning IP Addresses:

Step 1: Click on the PC

Fig 1.1.1

A window will open.

- Go to the config tab
- Select FastEthernet0

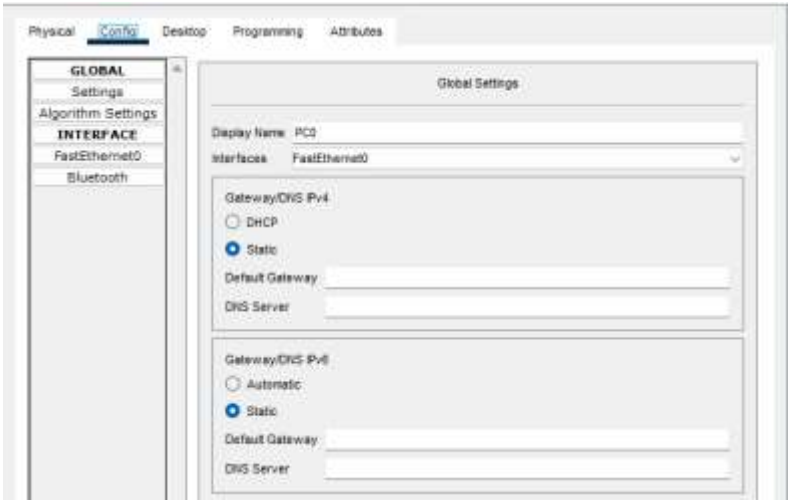


Fig 1.1.2

- Add IP4 Address
- And make sure all devices have unique ip addresses.

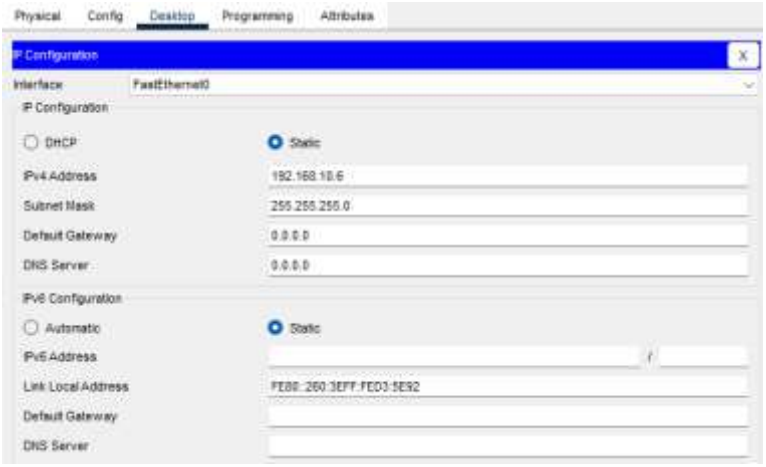


Fig 1.1.3

Step 2: Checking Connectivity

- PING: USE PING COMMAND TO CHECK CONNECTIVITY

Fig 1.1.4

- For that Go to the **Desktop tab**
- select command prompt and write PING IP address**.** e.g. to connect PC0 to PC1 write PING 192.168.10.02.

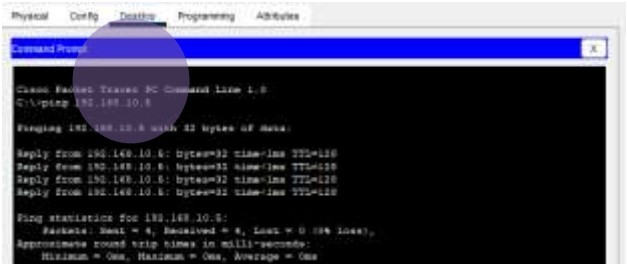


Fig 1.1.5

2. RING:

In a Ring Topology, it forms a ring connecting devices with exactly two neighboring devices. A number of repeaters are used for Ring topology with many nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data where, Token passing is a network access method in which a token is passed from one node to another node & Token is a frame that circulates around the network**.**

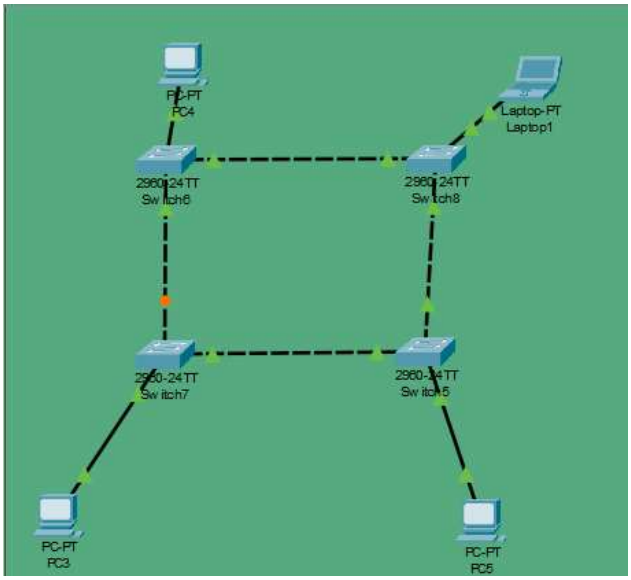


Fig 2.1

This network represents a Ring Topology, where each switch is connected to two neighboring switches, forming a closed loop. Each PC acts as a node connected to one

switch in the ring or you can say In ring topology, each node is connected to every other node ensuring the connections of the devices in a closed loop.

Nodes	**Links**	**Connected with**	**Ip Addresses**
PC3	ST wire	S7	192.168.10.2
PC4	ST wire	S6	192.168.10.1
PC5	ST wire	S5	192.168.10.3
Laptop 1	ST wire	S8	192.168.10.4
Switch 5	ST & CT	S7, S8, PC5	N/A
Switch 6	ST & CT	S7, S8, PC4	N/A
Switch 7	ST & CT	S5, S6, PC3	N/A
Switch 8	ST & CT	S6, S5, Laptop 1	N/A

3. BUS

Bus Topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

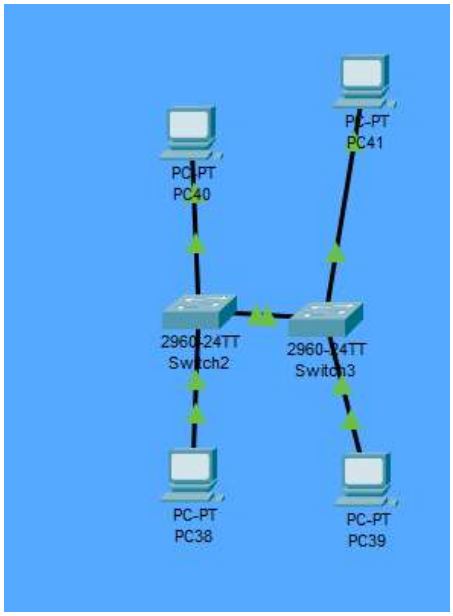


Fig 3.1

A bus is linear type of interconnected device, in which each node is connected through a single wire that behaves as the backbone of the entire network. Thus, all the information traveled in this network will be communicating unidirectionally.

The theoretical setup of buses cannot be structured in real life, because a PC can be connected only through one wire and continuing the network is not possible this way

4. STAR:

In Star Topology, all the devices are connected to a single central nod through a cable. This hub is the central node and all other nodes are connected to the central node.

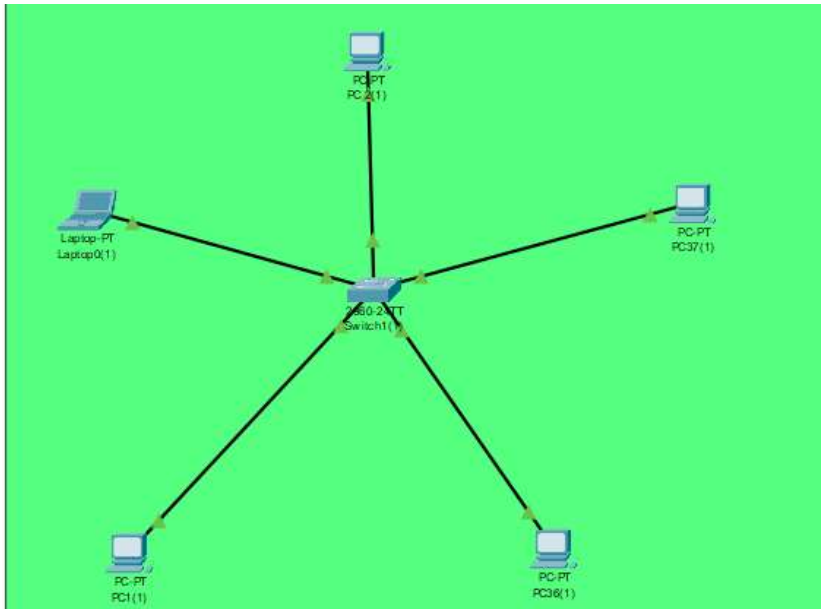


Fig 4.1

The star Topology consists of nodes connected centrally through a HUB/ Switch.

The structure of this network topology is like a star and usually has 5 nodes but that can be scaled according to the usage.

CHAPTER # 3
INTRODUCTION TO NETWORK DEVICES

Network devices are fundamental hardware components in computer networking that operate across different layers of the OSI and TCP/IP models. They facilitate data transmission, regulate traffic flow, provide interconnectivity between heterogeneous networks, and enforce security policies.

Functions of Network Devices

- Enable communication by transmitting and receiving data between devices.
- Allow devices to connect to networks efficiently and securely.
- Improve network performance by reducing congestion and managing traffic.
- Provide security by controlling access and preventing unauthorized activities.
- Extend network coverage and solve signal loss or attenuation problems.

Types of networking devices:

1. Repeater:

Fig 1.1

A repeater is signal reviving device, through which the dead signals are regenerated, it just captures the weak signal and generates strong signals.

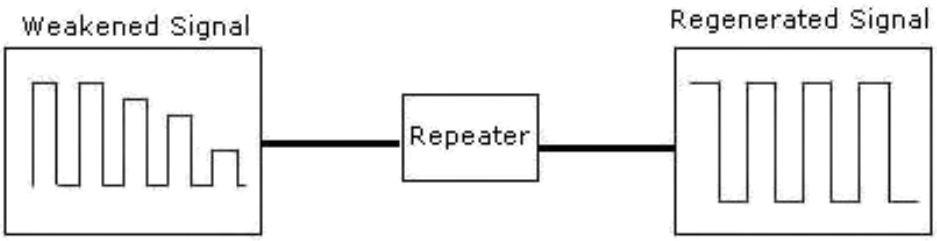
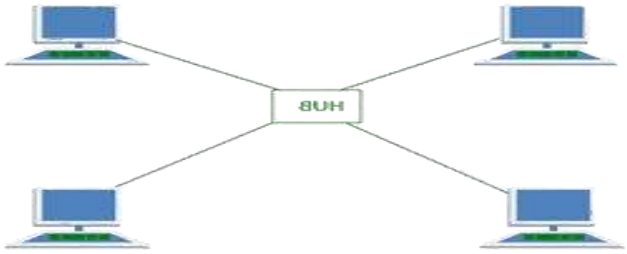


Fig 1.2

2. Hub

A Hub is small area network device that is used to connect nodes in a small network, it has several ports that can connect a small number of nodes in a small geographical area.

Fig 2.1



(ulti ha yeh)

3. Bridge

A bridge behaves as the connector between two Local Area Networks.

A bridge behaves as a connection between Two Local Area Networks so that each can communicate with the other.

Fig 3.1

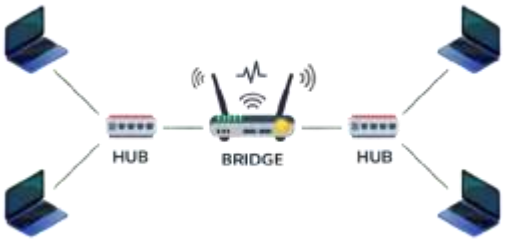


Fig 3.2

4. Switch

A switch is a most used network device that is used to connect devices inside a Local Area Network. The purpose of this device is to connect as many nodes as needed in a limited geographical area, maintaining features like security, Data Protection etc.

Fig 4.1

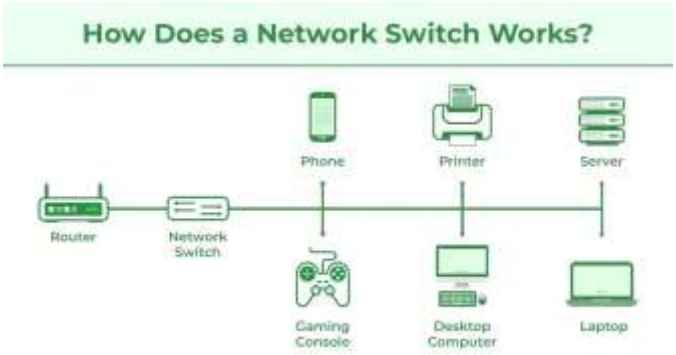


Fig 4.2

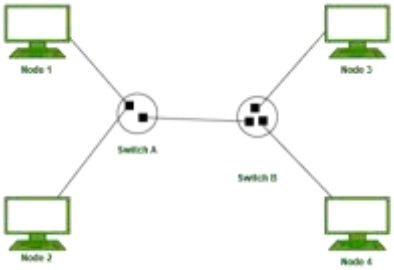


Fig 4.3

5. Router

A router is routing device that is used to connect Multiple Local Area Networks to connect and able to communicate within.

A router can connect many LANs thus creating a WAN.

Fig 5.1

Functions of a Router

- **Forwarding:** Receives packets, examines headers, and forwards them to the correct output port.
- **Routing:** Determines the optimal path for packets using routing tables and algorithms.
- **Network Address Translation (NAT):** Translates private IPs to a public IP for Internet access.
- **Security:** Supports firewalls and other security measures.
- **VPN Connectivity:** Provides secure remote access to networks.
- **Bandwidth Management:** Controls data flow to prevent congestion.
- **Monitoring & Diagnostics:** Tracks traffic and helps troubleshoot network issues.

Fig 5.2

Commented [1]: Types of Routers
Below, we have discussed different types of routers that are being used for various purposes in almost every industry.
1. Wireless Router
Wireless routers are devices that are mainly used to connect a computer to the internet modem and make the network available without wires. This is where several devices, for example, smart phones, laptops, tablets. Smart TVs, etc., can access the Internet without wires.
Wireless routers operate through the use of radio signals. They are simple to install and suitable for residential, commercial or any area where individuals employ a range of wireless devices.
Wireless routers that are being produced today can handle high speeds, and you also get options such as dual-band or tri-band routers that help in getting less interference. It makes communication easy and offers better solutions for all your internet-related issues.
2. Core Router
A core router is defined as extremely valuable equipment that is applied in big networks, like Internet providers or large companies. Its primary function is to guide the flow of data frames inside or across a network at a very fast pace. Unlike traditional routers, core routers are purposely built to deal with large traffic and are implemented with high speed.
It links different parts of a network and helps communication between those two parts. Hubs or core routers usually do not transmit Wi-Fi signals; they are just responsible for controlling the traffic between network centers. These routers support thousands of connections and, therefore, are best suited for large networking environments such as data centers and telecom service providers.
3. Edge Router
Next in the list of types of routers is Edge Router. An edge router is a device that provides communication between internal networks, including business or home networks, and external networks or the internet. It is situated at the periphery of a network and performs data entry into and out of a network.
Edge routers are also used to determine by which path the data is to be transferred from your private network to other public networks. Edge routers
have Firewalls and VPN capabilities as well as provide you with the protection from external threats to your network.
Examples of edge routers are CISCO ISR, MikroTik EdgeRouter, Juniper MX Series and Ubiquiti EdgeRouter. These devices are most used by businesses and ISPs to proficiently manage flow at the network edge.
4. SOHO (Small Office/Home Office) Router
A SOHO router is specifically intended for use in small offices or home offices. It is equipped with the internet as well as intended and designed networking solutions for small settings better known as office environments. These routers are not very complicated and are all in one device that can act as standard routers, provide wireless connectivity and even basic security features ...

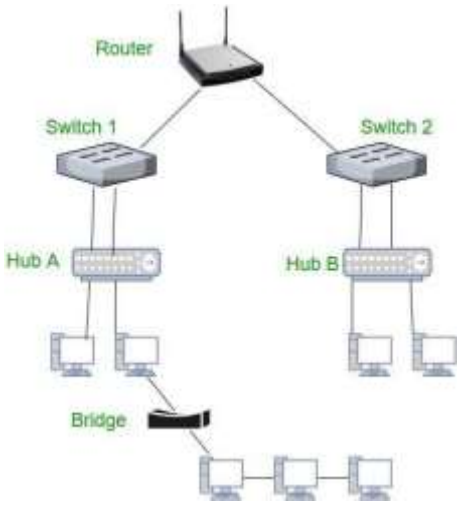


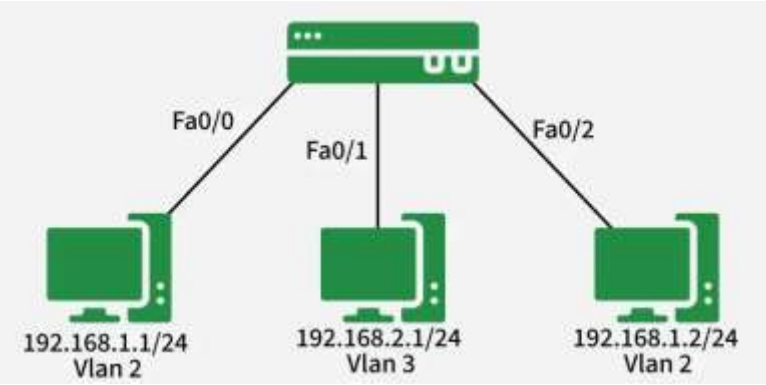
Fig 5.3

CHAPTER # 4

VLAN

VLAN

In Cisco Packet Tracer, a VLAN (Virtual LAN) lets you split one physical switch into



multiple logical networks. Instead of buying separate switches for departments like Sales, HR, or IT, you use one switch and logically isolate their traffic. Devices in one VLAN (e.g., Sales) cannot see or interact with devices in another VLAN (e.g., HR) unless you add routing.

1. Why VLANs are used

- **Broadcast Control:**
  Without VLANs, every broadcast hits every device on the switch. VLANs break the network into smaller broadcast domains, keeping unnecessary traffic contained.
- **Security and Isolation:**
  Sensitive traffic stays separated. For example, student devices and admin devices run on the same hardware but are logically isolated.
- **Organization:**
  Devices are grouped by purpose instead of physical location. An HR user on the 1st floor and another on the 3rd floor can still belong to the same VLAN with the same policies.

The following image shows how a switch forwards broadcast messages when it has two VLANs.

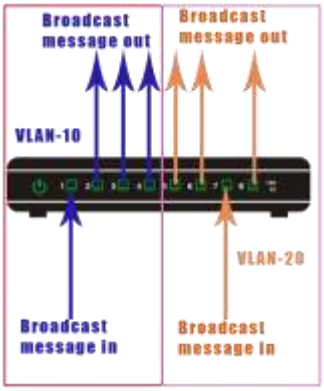


Fig 1.1

2. Basic setup in Packet Tracer

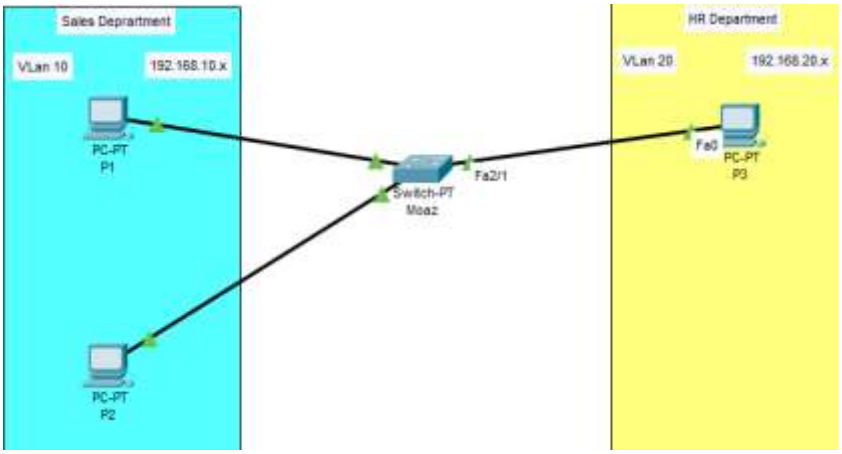


Fig 2.1

Step 1:

- After placing PCs and switches, assign IP addresses by clicking each PC → **IP Configuration** → **IPv4**.
- Then move to the switch CLI:

```
> enable

# no shutdown

# exit
```

Fig 2.2

Step 2:

- configure the interface you're using. Example for FastEthernet 0/1:

```
Switch(config)# interface fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
# exit
```

Fig 2.3

Step 3: Common VLAN commands

Create a VLAN:

```
Switch(config)# vlan 10
Switch(config-vlan)# name Sales
```

Fig 2.4

Assign a port as an access port for that VLAN:

```
Switch(config)# interface fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
```

Fig 2.5

```
# Create VLANs
Switch(config)# vlan 2
Switch(config-vlan)# name Accounts

Switch(config)# vlan 3
Switch(config-vlan)# name HR

# Assign switch ports to VLANs
Switch(config)# interface fa0/0
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2

Switch(config)# interface fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 3
```

Fig 2.6

LAB TASK

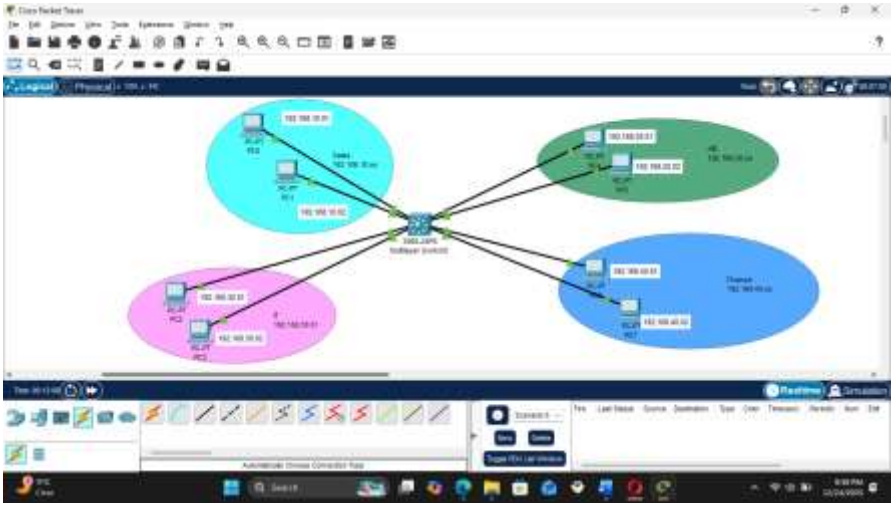


Fig 1.1

Nodes (End Devices):

SALES VLAN

PC2 – IP: 192.168.10.01

PC3 – IP: 192.16.10.02

HR VLAN

PC4 – IP: 192.168.20.01

PC5 – IP: 192.16.20.02

IT VLAN

PC6 – IP: 192.168.30.01

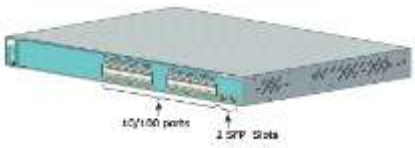
PC7 – IP: 192.16.30.02

Finance VLAN

PC8 – IP: 192.168.40.01

PC9 – IP: 192.16.40.02

About Switch:



The Cisco Catalyst 3560-24PS (specifically model number WS-C3560-24PS-S or -E) is a fixed-configuration, enterprise-class, 24-port Fast Ethernet switch with Power over Ethernet (PoE) and Layer 3 switching capabilities.

Fig 1.2

Links:

All PCs are connected to the switch using copper straight-through cables:

PC2 → Switch0

PC3 → Switch0

PC4 → Switch0

PC5 → Switch0

PC6 → Switch0

PC7 → Switch0

PC8 → Switch0

PC9 → Switch0

Each cable provides a dedicated connection to the switch.

1.1 VLAN Configuration on the Switch:

Step 1: Write the enable and config terminal command.

- Click on the switch and select CLI.

- Write the following commands for VLAN Configuration on the Switch:

Enable: The enable command is used to enter privileged EXEC mode (also known as enable mode).

switch>enable

Configure Terminal: The configure terminal command is used to enter global configuration mode.

```
switch#Configure terminal
```

Step 2: Create the VLANs.

- Commands:

```
Switch(config-vlan)#Vlan 10
Switch(config-vlan)#name Sales
Switch(config-vlan)#exit
```

- Note: use these commands to create all Vlans.

```
Switch>vlan 10
           ^
% Invalid input detected at '^' marker.

Switch>enable
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name sales
Switch(config-vlan)#exit
```

Fig 1.1.1

- Naming the Vlan 20 as HR

```
Switch(config)#vlan 20
Switch(config-vlan)#name HR
Switch(config-vlan)#exit
```

Naming the vlan 30 as IT

```
Switch(config)#vlan 30
Switch(config-vlan)#name IT
Switch(config-vlan)#exit
```

```
Switch(config)#vlan 40
Switch(config-vlan)#name Finance
Switch(config-vlan)#exit
Switch(config)#
```

Finally name the Vlan 40 as Finance.

Step 3: Assigning Switch Ports to a VLAN.

```
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#
```

In this step, FastEthernet port 0/1 is configured as an access port and assigned to VLAN 10. This ensures that the PC connected to this port becomes part of the Sales VLAN.

```
Switch(config)#interface fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#
```

In this step, FastEthernet port 0/2 is configured as an access port and assigned to VLAN 10. This ensures that the PC connected to this port becomes part of the Sales VLAN.

```
Switch(config)#interface range fa0/3 - 4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
```

Using the range code, we assign both ports to vlan 20 at once.

```
Switch(config)#interface range fa0/5 - 6
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
```

same assigning the fa0/5 and fa0/6 to

vlan 30.

```
Switch(config)#interface range fa0/7 - 8
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 40
Switch(config-if-range)#exit
Switch(config)#
```

And same goes for here assigning fa0/7 and 0/8 to vlan 40

CHAPTER # 5:
OSI Layers

1. OSI MODEL: Cisco Packet Tracer Simulation Analysis

The OSI (Open Systems Interconnection) Model is a set of rules that explains how different computer systems communicate over a network. OSI Model was developed by the International Organization for Standardization (ISO). The OSI Model consists of 7 layers, and each layer has specific functions and responsibilities. This layered approach makes it easier for different devices and technologies to work together.

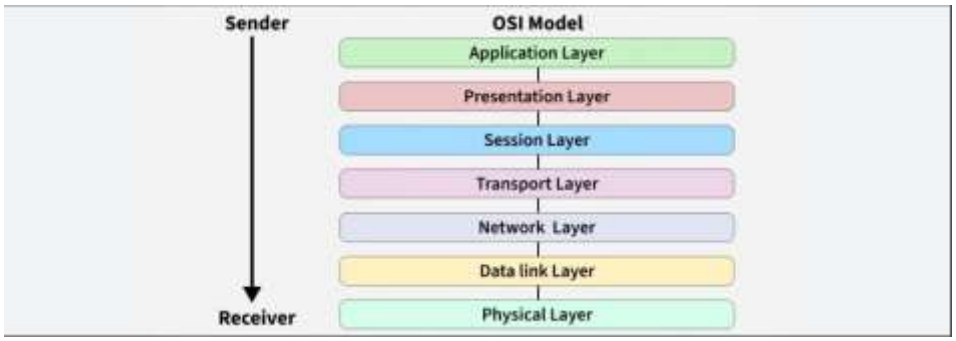


Fig 1.1

2. Network:

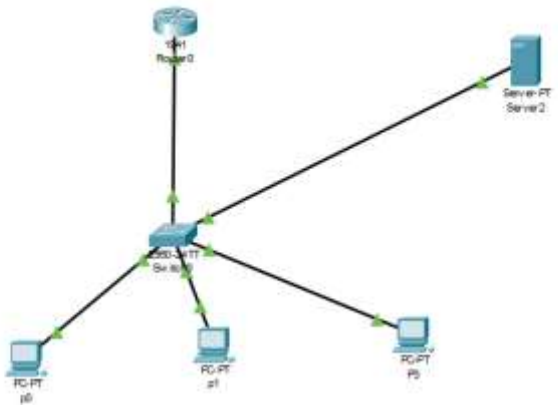


Fig 2.1

Router Configuration:

- Click on the Router and go to the CLI tab.

```
Router>enable
Router#configure terminal
```

Fig 2.2

- Configure the interface connected to the Switch:

```
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
Router#write memory
```

Fig 2.3

CLI:

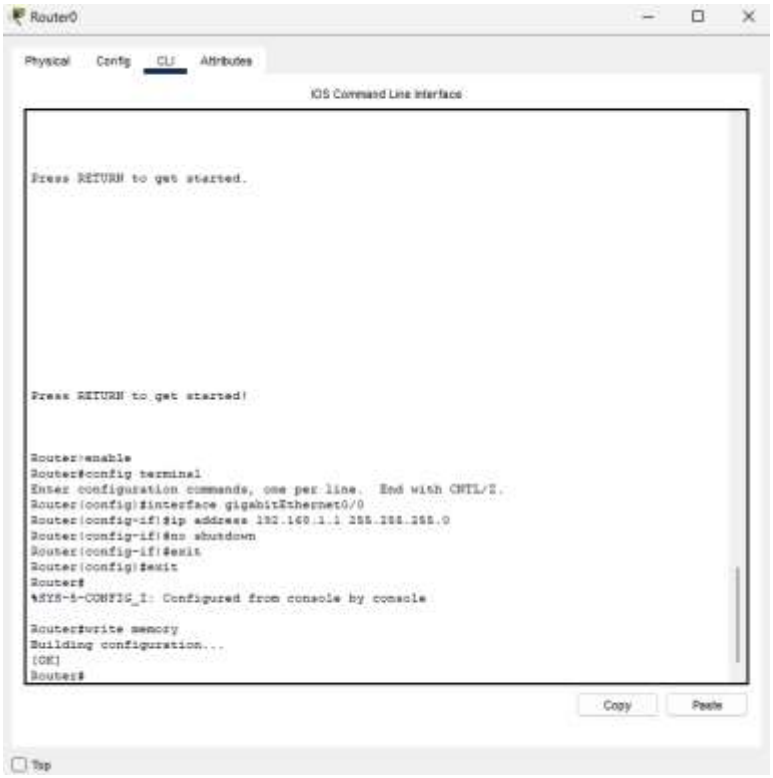


Fig 2.4

3. OSI MODEL - LAYERS

3.1 Layer 7: Application Layer:

At the very top of the OSI Reference Model stack of layers, we find the Application Layer which is implemented by the network applications. These applications produce data 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.
- Protocols used in the Application layer are SMTP, FTP, DNS, etc.

Fig 3.1

3.2 Layer 6: Presentation Layer

The 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. Protocols used in the Presentation Layer are TLS/SSL (Transport Layer Security / Secure Sockets Layer).JPEG, MPEG, GIF, are standards or formats used for encoding data, which is part of the presentation layer's role.

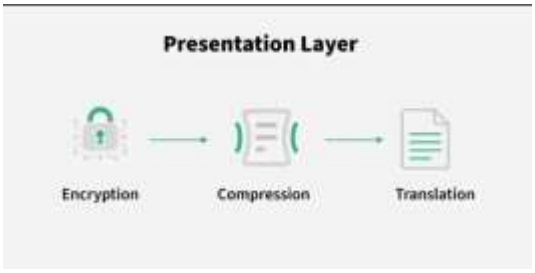


Fig 3.2

3.3 Layer 5: Session Layer

Session Layer in the OSI Model is responsible for the establishment of connections, management of connections, and termination of sessions between two devices. It also provides authentication and security. Protocols used in the Session Layer are NetBIOS, PPTP.

Fig 3.3

3.4 Layer 4: Transport Layer:

The Transport Layer provides services to the application layer and takes services from the 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.

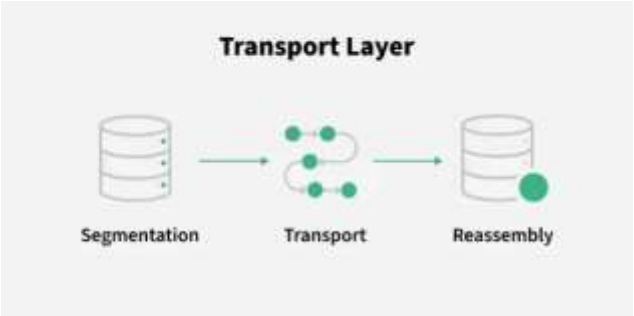


Fig 3.4

3.5 Layer 3: Network Layer

The 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 and receiver's IP address are placed in the header by the network layer. Segment in the Network layer is referred to as Packet**.**
- Network layer is implemented by networking devices such as routers and switches.

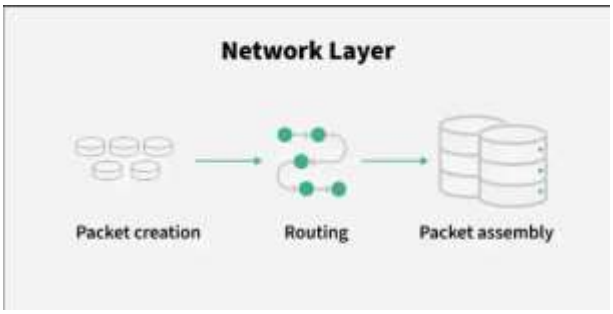


Fig 3.5

3.6 Layer 2: Data Link Layer

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 the DLL to transmit it to the Host using its MAC address.
- Packet in the Data Link layer is referred to as Frame. Switches and Bridges are common Data Link Layer devices.

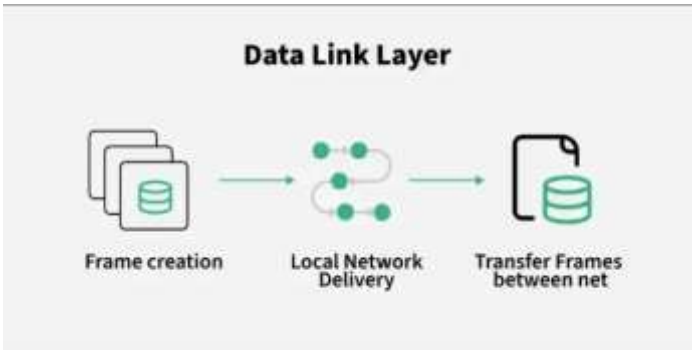


Fig 3.6

3.7 Layer 1: Physical Layer:

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.

- Physical Layer is responsible for transmitting individual bits from one node to the next.
- 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.

Fig 3.7

Example:

Identifying Layer 3: The Routing and Addressing Layer

- **Scenario:**

PC1 (192.168.1.11) sends an ICMP Echo Request (Ping) to SRV1 (192.168.1.100).

- **Observation Point: PC1 (The Source)**
- **Encapsulation:**

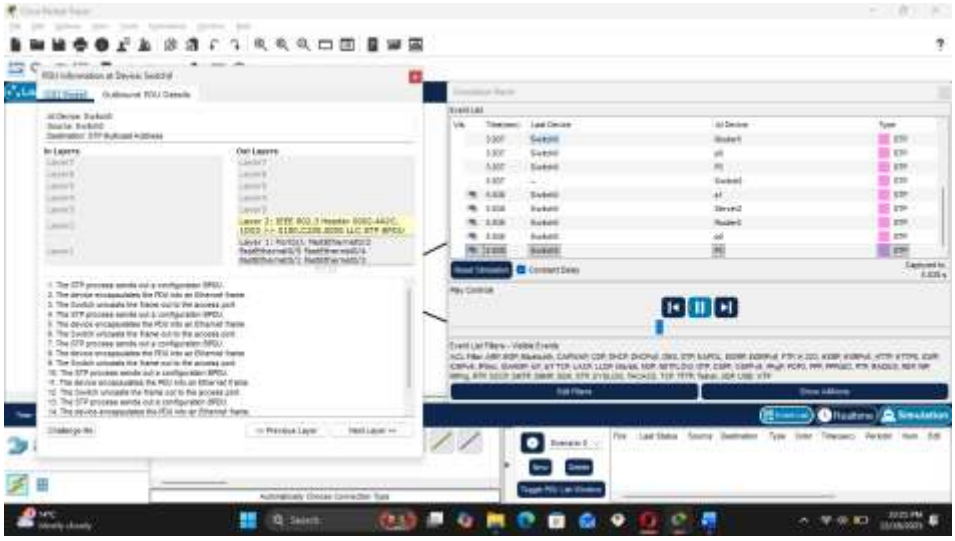
As the ICMP data leaves the Transport Layer (Layer 4), it is passed down to the Network Layer (Layer 3).

- **PDU Name:**

The Layer 3 Protocol Data Unit (PDU) is now called a Packet.

Key Action: PC1 adds an **IP Header** to the data. You can inspect this header in the "Outbound PDU Details" window.

- **Stimulation View**



- **Stimulation Panel**

When you click on the colored PDU envelope at each hop (PC1, Switch, Server), the "PDU Information" window appears. This window is split into three main sections: OSI Model, Inbound PDU Details, and Outbound PDU Details.

- **PDU Information at Device: Server 1**

When the PDU arrives at the Server, it’s a moment of truth. The Server must confirm that the data is for it and then process the request. It does this by moving the data up the OSI stack, removing the headers one by one.