

Practical – 1

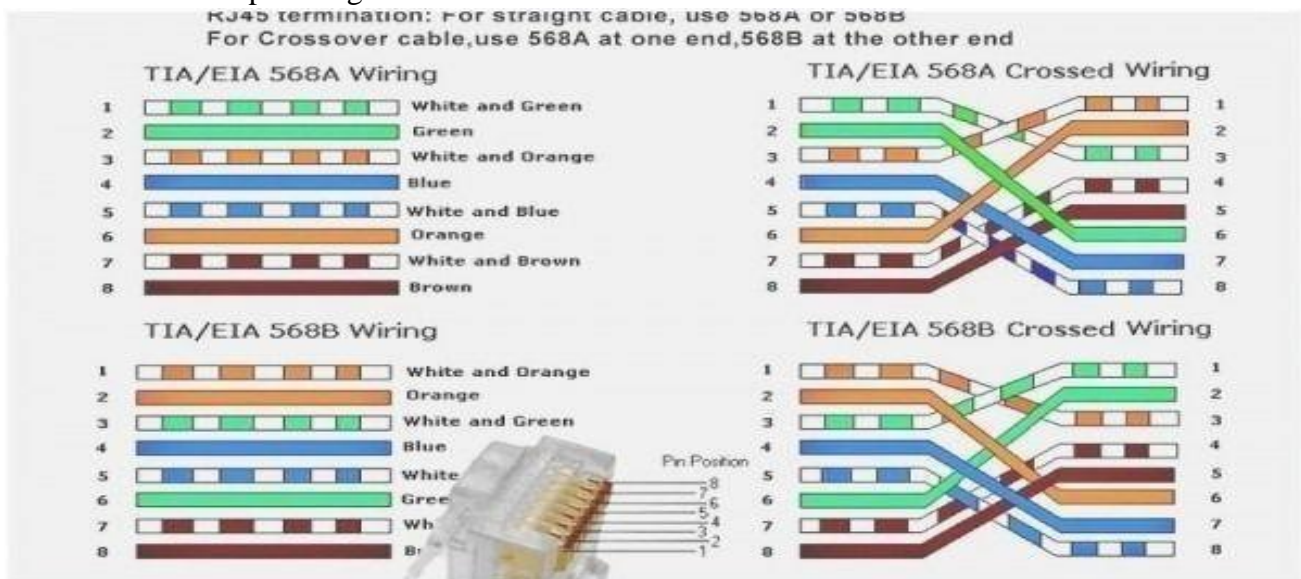
Objective:

To Understand various types of cables:

- CAT5
- CAT6
- Optical Fibre Cable
- Coaxial Cable

CAT5

Alternatively known as an Ethernet cable or LAN cable, a Cat 5 or category 5 is a network cable that consists of four twisted pairs of copper wire terminated by an RJ-45 connector. The picture shows an example of a Cat 5 cable. A Cat 5 cable contains 8 wires and has a specific wire order. If the wires are in a different order, the cable does not work. There are two standards, T568A and T568B, for the order of the wires. Each standard is similar in performance and does not provide an advantage over the other. However, you must use the same wire order on each end of the Cat 5 cable, providing data transmission speeds of up to 100 Mbps. The maximum recommended length of a Cat 5 cable is 100 meters. Exceeding this length without the aid of a bridge or other network device could cause network issues, including data packet loss and data transmission speed degradation.



Application:

- Cat 5 cable is used in home and business networks.
- Category 5 cable is used in structured cabling for computer networks such as Ethernet over twisted pair.
- Cat 5 is also used to carry other signals such as telephony and video.
- Cat 5 can carry two conventional telephone lines as well as 100BASE-TX in a single cable.

Advantages:

- Cheaper
- High Transfer Speed
- Versatile
- Easy Installation
- Easy Usage

Disadvantages:

- Limited Data Transfer
- Interference sensitive
- Limited Flexibility

CAT6

Cat 6 or Category 6 is a network cabling that consists of four twisted pair wires, has a data rate of 10,000 Mbps, and is used in Ethernet and Gigabit Ethernet. Cat 6 cable can be identified by the printing on the side of the cable sheath. Cat 6 patch cables are normally terminated in 8P8C modular connectors, using either T568A or T568B pin assignments; performance is comparable provided both ends of a cable are terminated identically. If Cat 6-rated patch cables, jacks and connectors are not used with Cat 6 wiring, overall performance is degraded and may not meet Cat 6 performance specifications. The Cat 6 specification requires conductors to be pure copper.

**Application:**

- Installers often use Cat6 cables at the network's backbone in conjunction with fibre optics.
- Cat6 cable is more reliable at longer distances.
- Cat6 cable currently dominates home and enterprise networks as the cable of choice.

Advantages:

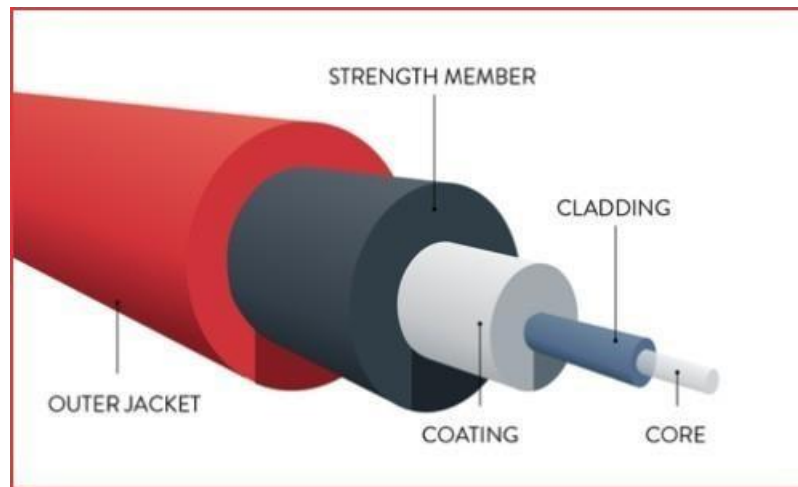
- High Speed
- Fast performance
- Produces high bandwidth
- Upgradable

Disadvantages:

- Expensive
- Does not guarantee full speed
- Little complicated usage

Optical Fibre Cable

A fibre-optic cable is composed of very thin strands of glass or plastic known as optical fibres; one cable can have as few as two strands or as many as several hundreds of them. These optical fibre cables carry information in the form of data between two places using optical or light-based technology. Once the light beams travel down the optical fibre cable (OFC), they would emerge at the other end. A photoelectric cell will be required to turn the pulses of light back into electrical information the computer can understand. While traveling down fibre optic cable, light bounces repeatedly off the walls. The beam of light does not leak out of the edges because it hits the glass at really shallow angles. And then it reflects back again as if the glass were really a mirror. This is called total internal reflection. The other factor that keeps it in the pipe is the cable structure.



Application:

- Medical Industry
- Communication
- Defence
- Industries
- Broadcasting
- Lighting and Decorations
- Mechanical Inspections

Advantages:

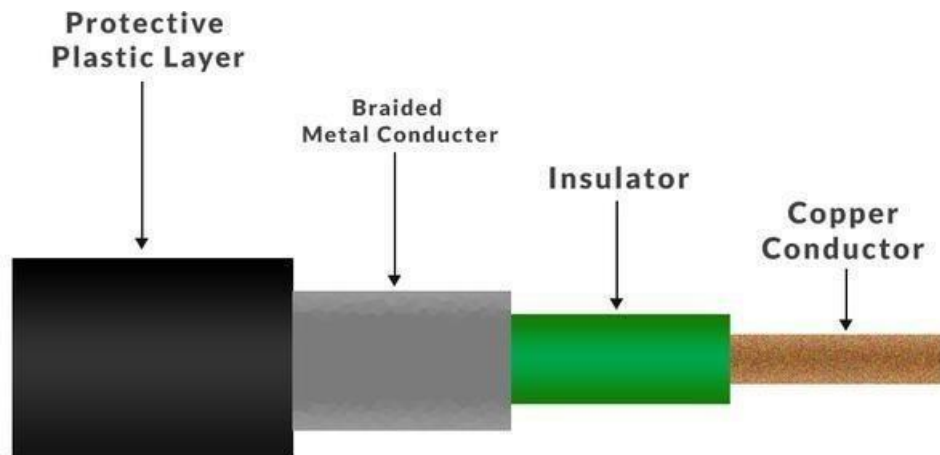
- Higher Bandwidth
- High Speed broadband
- Cannot be tapped easily
- Lower latency
- Long Lasting

Disadvantages:

- Difficult to splice
- Expensive to install
- Cannot be curved
- High susceptible

Coaxial Cable

Coaxial cable is a type of copper cable specially built with a metal shield and other components engineered to block signal interference. Coaxial cable received its name because it includes one physical channel that carries the signal surrounded after a layer of insulation by another concentric physical channel, both running along the same axis. The outer channel serves as a ground. Many of these cables or pairs of coaxial tubes can be placed in a single outer sheathing and, with repeaters, can carry information for a great distance.



Application:

- It is primarily used by cable TV companies to connect their satellite antenna facilities to customer homes and businesses.
- It is also sometimes used by telephone companies.
- Some homes and offices use coaxial cable, too.
- Historically, coaxial cables were also used as an early form of Ethernet.
- Cables are also used in automobiles, aircraft, military and medical equipment.

Advantages:

- Rugged
- High Bandwidth
- Provide Power
- Less in diameter

Disadvantages:

- Expensive Installation
- High maintenance
- Inflexible
- Bulky
- Security problem
- Low-speed transmission

Understanding the various connector and passive devices:

1. RJ11
2. RJ45
3. SL-SC
4. SFP
5. LIU
6. POE

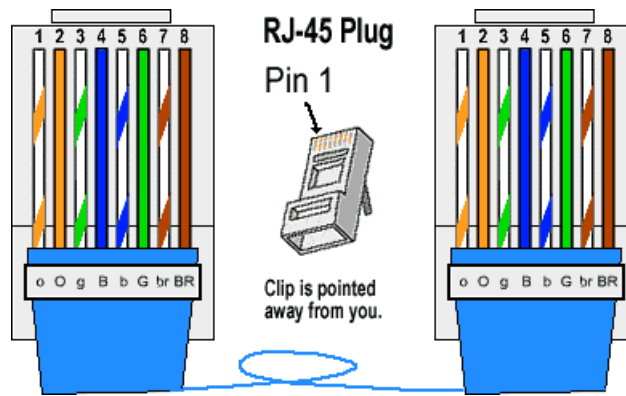
RJ11

A Registered Jack, or RJ, is a standardized telecommunication network interface for connecting voice and data equipment to a service provided by a local exchange carrier or long-distance carrier. RJ11 connector is one of the earliest versions of modular connectors used for telephone and modem lines. It is a six-position, four-conductor modular plug or jack. RJ11 is a 6P4C registered jack. That is the connector of RJ11 has 6 positions(sockets) and 4 wires. These 4 wires are used in 2 pairs to make connections . One pair of wires in RJ11 is left unused. It is considered as an extra pair, to be used in case of failure of the working pair. RJ11 is smaller in size compared to the other registered jacks. It connects a telephone with the wall socket and handset to the telephone. RJ11 jack or socket is available in two forms to use on telephone lines: RJ11C and RJ11W.



RJ45

Using RJ45 is an efficient way to achieve high-speed internet on your laptop and computers. Although you can use the Wi-Fi connection on a laptop, this may not give you a higher speed. Also, wireless connections are more vulnerable to connection failures. 4 in 'RJ45' signifies that it has 4 pairs of cables. And to decrease the capacitance formed by the closely spaced cables, 5 twists per inch are provided to the cable. Hence the number 45 in 'RJ45'. An RJ45 connector is connected with an RJ45 cable (Ethernet cable). Based on the standard of RJ45 cable, it can either be T568A or T568B.



SL-SC

SLSC is the platform for signal conditioning, routing and faulting, SLSC offers on the one hand standardized connections and on the other hand a modular approach for signal conditioning, fault simulation and more test requirements. Switch Load and Signal Conditioning (SLSC) extends the PXI or Compact RIO platform with the ability to add custom front-end modules. With a standardized connectivity and form factor, it eliminates the fault-prone process of point-to-point wiring, simplifying the overall system. Accelerate Time to First Test—SLSC brings a commercial-off-the shelf approach to the signal conditioning, loads, and switching that are a part of every validation and production system. Utilize a variety of modules to integrate and commission systems sooner while maintaining the customizability you need. Reduce Design and Integration Costs—SLSC has an open architecture that partners and end users can utilize to build custom boards. It eliminates the need to design mechanical and software integration infrastructure that is typically needed with custom hardware. Meet Custom Test Demands—SLSC extends PXI and Compact RIO measurement hardware with high-power relays for signal switching, power loads, and additional inline signal-conditioning capability. SLSC provides more power, cooling, and board space, which makes it ideal for adding I/O types and loads that are not natively supported in those platforms.



Small form-factor pluggable, or SFP, devices are hot-swappable interfaces used primarily in network and storage switches. The SFP ports on a switch and SFP modules enable the switch to connect to fiber and Ethernet cables of different types and speeds. Specified by a multi-source agreement (MSA), SFP connector was first introduced in early 2000 and designed to replace the previous gigabit interface converter (GBIC) connector in fibre optic and Ethernet high-speed networking systems. Based on the IEEE 802.3, SFF-8472 protocol specification, SFP module connectors have the ability to handle up to 4.25Gb/s with greater port density than the GBIC, which is why SFP is also known as mini GBIC. This allowed it to quickly become

the connector of choice for system administrators who liked the idea of being able to significantly increase their output per rack. The SFP connectors can support Gigabit Ethernet, Fibre Channel, Synchronous Optical Network (SONET) and other communication standards.

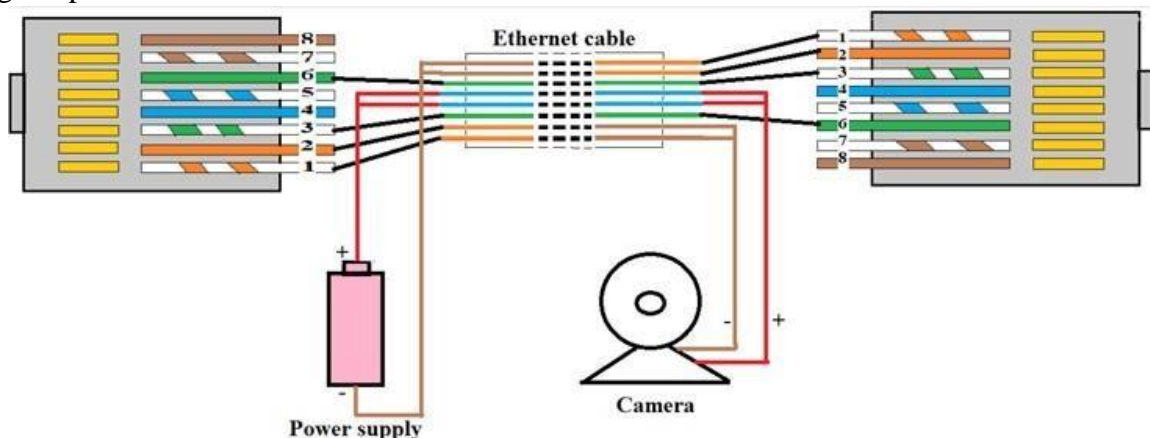
LIU

Light interface units are extensively used for wired communication networks. The LIUs are used for routing, terminating and managing optical cable terminations. These light interface units can be wall mounted or rack mounted for ease of use.



PoE

Power over Ethernet (PoE) is a technique for delivering DC power to devices over copper Ethernet cabling, eliminating the need for separate power supplies and outlets. While PoE doesn't add Ethernet data capabilities, it does offer expanded options for how and where Ethernet end devices can be placed. Power over Ethernet (PoE) is technology that passes electric power over twisted-pair Ethernet cable to powered devices (PD), such as wireless access points, IP cameras, and VoIP phones in addition to the data that cable usually carries. It enables one RJ45 cable to provide both data connection and electric power to PDs instead of having a separate cable for each.



Practical – 2

Objective:

Study of various devices-

1. Media converter

2. L2 switch

3. Catalyst Switch

4. Broadcast Switch

5. Wireless Access Point and Wireless Modem with Router

6. L3 Switch

7. Multilayer

switch 8. Router

9. Firewall

Media Converter

A media converter is a networking device that transparently converts Ethernet or other communication protocols from one cable type to another type, usually copper CAT x/UTP to fibre. Media converters are often used in pairs to insert a fibre segment into copper networks to increase cabling distances and enhance immunity to electromagnetic interference. They can also extend LANs, and convert link speeds and fibre modes.

Types of Media Converters

1. Copper-to-Fibre Media Converters

Copper-to-fibre media converters enable connections of copper-based Ethernet equipment over a fibre optic link. This extends links over greater distances with fibre optic cable, protects data from noise and interference, and future-proofs a network with additional bandwidth capacity.

2. Fibre-to-Fibre Media Converters

Fibre-to-fibre media converters connect different fibre optic networks and support conversion from one wavelength to another. They provide connectivity between single-mode and multimode fibre, as well as between dual and single fibre.

3. PoE Media Converters

Power-over-Ethernet (PoE) media converters provide reliable and cost-effective fibre distance extension to PoE-powered devices. PoE media converters can power devices like IP phones, videoconferencing equipment, IP cameras and Wi-Fi devices over copper UTP cabling.

4. Stand-Alone vs. Chassis-Based Media Converters

Stand-alone media converters are compact and can be AC or DC powered. They are commonly used to convert one copper link to fibre in point-to-point installs. These converters are easy to deploy and offer a range of useful functionality for your network, such as auto-MDI/MDIX, link fault pass through and more.

Layer.2 Switch

A layer 2 switch is a type of network switch or device that works on the data link layer (OSI Layer 2) and utilizes MAC Address to determine the path through where the frames are to be forwarded. It uses hardware-based switching techniques to connect and transmit data in a local area network (LAN). A layer 2 switch can also be referred to as a multi-port bridge

Layer 2 switches similar to bridges. They interconnect networks at layer 2, most commonly at the MAC sub layer, and operate as bridges, building tables for the transfer of frames among networks.

Historically, layer 2 switches emerged to alleviate the contention problem of shared media LAN. As structured cabling emerged and star-based connectivity to network centers was adopted, the exploitation of existing cabling and existing network adapters led to the continuation of using typical LAN, such as Ethernet and Token Ring, but enabled the development of layer 2 switches. The original goal of these switches was to enable use of a single LAN segment, if feasible, per attached end system, minimizing contention delays that existed in the older shared segments. For example, with an Ethernet switch and a dedicated Ethernet segment per attached system, collisions are avoided and delay is minimized.

Catalyst Switch

Catalyst switches offer advanced customization and manageability. The switches can be configured using a serial console, telnet or Secure Shell. Simple Network Management Protocol (SNMP) allows monitoring of many states, and measurement of traffic flows. Many devices can also run an HTTP server.

Wireless access point

In computer networking, a wireless access point (WAP), or more generally just access point (AP), is a networking hardware device that allows other Wi-Fi devices to connect to a wired network. As a standalone device, the AP may have a wired connection to a router, but, in a wireless router, it can also be an integral component of the router itself. An AP is differentiated from a hotspot which is a physical location where Wi-Fi access is available. An AP connects directly to a wired local area network, typically Ethernet, and the AP then provides wireless connections using wireless LAN technology, typically Wi-Fi, for other devices to use that wired connection. APs support the connection of multiple wireless devices through their one wired connection

Wireless modem

A cable modem is a hardware device that uses a coax cable to connect your computer devices with your Internet service provider (ISP). A cable modem connects to the Internet. There are a few different types of modems: analog modems (dial-up), digital subscriber line (DSL) or cable modems. Typically, your Internet Service Provider (ISP) rent modems to their subscribers, that can come with some added benefits. The option to buy or purchase your own modem can save you from paying monthly rental fees (sometimes up to \$150 per year* depending on your current rental fees). Your modem will give you a reliable, wired Internet connection. If you only have one device that needs to connect to the Internet, like a PC or laptop, you can get away with just having a modem. But if you have multiple devices, or want to use your devices wirelessly (WiFi), then you will need a router, too.

L-3 Switch

A layer 3 switch combines the functionality of a switch and a router. It acts as a switch to connect devices that are on the same subnet or virtual LAN at lightning speeds and has IP routing intelligence built into it to double up as a router. It can support routing protocols, inspect incoming packets, and can even make routing decisions based on the source and destination addresses.

Advantages-:

1. Support routing between virtual LANs. Improve fault isolation.
2. Simplify security management. Reduce broadcast traffic volumes.
3. Ease the configuration process for VLANs, as a separate router isn't required between each VLAN.
4. Separate routing tables, and as a result, segregate traffic better.
5. Simplifying troubleshooting as fixing problems in the L2 layer is tedious and time-consuming.

6. Support flow accounting and high-speed scalability.
7. Lower network latency as a packet doesn't have to make extra hops to go through a router.

Router

A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork (e.g. the Internet) until it reaches its destination node.

Applications:-

A router may have interfaces for different types of physical layer connections, such as copper cables, fibre optic, or wireless transmission. It can also support different network layer transmission standards. Each network interface is used to enable data packets to be forwarded from one transmission system to another. Routers may also be used to connect two or more logical groups of computer devices known as subnets, each with a different network prefix. Routers may provide connectivity within enterprises, between enterprises and the Internet, or between internet service providers' (ISPs) networks. The largest routers (such as the Cisco CRS-1 or Juniper PTX) interconnect the various ISPs, or may be used in large enterprise networks.[5] Smaller routers usually provide connectivity for typical home and office networks.

Advantages:-

1. It provides sophisticated routing, flow control, and traffic isolation Reduce network traffic by creating collision domains
2. Reduce network traffic by creating broadcast domains
3. Can connect different network architecture, such as Ethernet and token ring
4. They are configurable which allows the network manager to make policy based on routing decisions
5. It can choose the best path across the internetwork using dynamic routing algorithms
6. It can reduce network traffic by creating collision domains and also by creating broadcast domains
7. Allow achieving loop so that redundant paths are available

Disadvantages:-

1. A router is more expensive than bridge or repeaters
2. Router only work with rotatable network protocol, not all protocol are routable
3. The router is slower than bridge or repeaters because they must analyze data transmission from the physical to the network layer
4. Dynamic router communication causes additional network traffic Are relatively complex device
5. Can require a considerable amount of initial configuration
6. They are protocol dependent devices which must understand protocol they are forwarding

Firewall

A Firewall is a necessary part of any security architecture and takes the guesswork out of host level protections and entrusts them to your network security device. Firewalls, and especially Next Generation Firewalls, focus on blocking malware and application-layer attacks, along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls can react quickly and seamlessly to detect and react to outside attacks across the whole network.

Application:-

Firewalls, especially Next Generation Firewalls, focus on blocking malware and application-layer attacks. Along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls are able to react quickly and seamlessly to detect and combat attacks across the whole network. Firewalls can act on previously set policies to better protect your network and can carry out quick assessments to detect invasive or suspicious activity, such as malware, and shut it down.

Repeaters

Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters. When an electrical signal is transmitted via a channel, it gets attenuated depending upon the nature of the channel or the technology. This poses a limitation upon the length of the LAN or coverage area of cellular networks. This problem is alleviated by installing repeaters at certain intervals. 17 Repeaters amplifies the attenuated signal and then retransmits it. Digital repeaters can even reconstruct signals distorted by transmission loss. So, repeaters are popularly incorporated to connect between two LANs thus forming a large single LAN.

Gateway

It is a state of a network that can get to different networks. Typically, in the intranet, a node or router can

go about as a router or the gateway node that interfaces the networks are called gateways. In big companies, the PCs that deal with the traffic between enterprise networks are named gateway nodes.

For

example, the PCs utilized by Internet service providers to connect fluctuated users at the moment time to

the web are gateway nodes.

Hubs

A hub is a physical layer networking device which is used to connect multiple devices in a network. They are generally used to connect computers in a LAN. A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination or not.

Bridges

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.

Types of Bridges

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

NIC

NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC card is a layer 2 device which means that it works on both the physical and data link layers of the network model

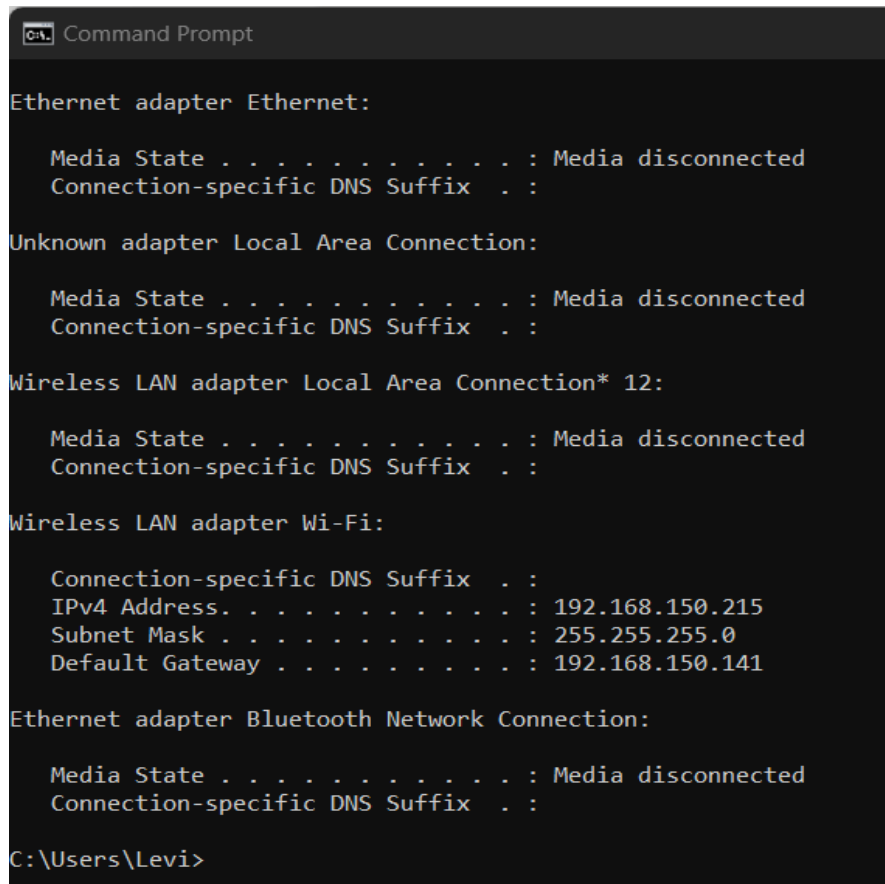
Practical – 3

Objective: Working And Analysis Of Various Networking Commands

1. Ipconfig

This command displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. This command is mainly used to view the IP addresses on the computers that are configured to obtain their IP address automatically.

The following image shows the sample output of this command.



```
Command Prompt

Ethernet adapter Ethernet:

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

Unknown adapter Local Area Connection:

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

Wireless LAN adapter Local Area Connection* 12:

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

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    IPv4 Address. . . . . : 192.168.150.215
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.150.141

Ethernet adapter Bluetooth Network Connection:

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

C:\Users\Levi>
```

2. Ping

The ping command is used to test connectivity between two hosts. It sends ICMP echo request messages to the destination. The destination host replies with ICMP reply messages. If the ping command gets a reply from the destination host, it displays the reply along with round-trip times.

If you specify the hostname as an argument, the ping command uses the configured DNS client service to automatically translate the hostname into the IP address

If you want to send specific number of ICMP packets. For example if you want to ping Google 50 times, Run ping command with "-n" option.

```
Command Prompt

C:\Users\Levi>ping localhost

Pinging MSI [::1] with 32 bytes of data:
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms

Ping statistics for ::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Levi>
```

3. Traceroute

This command is used to diagnose path-related problems. On an IP network, routers exchange IP packets between the source and the destination. They take IP packets from the source host and forward them in a sequence until they reach the destination host. The sequence of routers between the source and destination is known as the path. A path consists of all routers in a sequence that IP packets sent from the source host traverse to reach the destination host.

The tracert command prints the path. If all routers on the path are functional, this command prints the full path. If a router is down on the path, this command prints the path up to the last operational router.

```
Command Prompt

C:\Users\Levi>tracert www.google.com

Tracing route to www.google.com [172.217.161.4]
over a maximum of 30 hops:

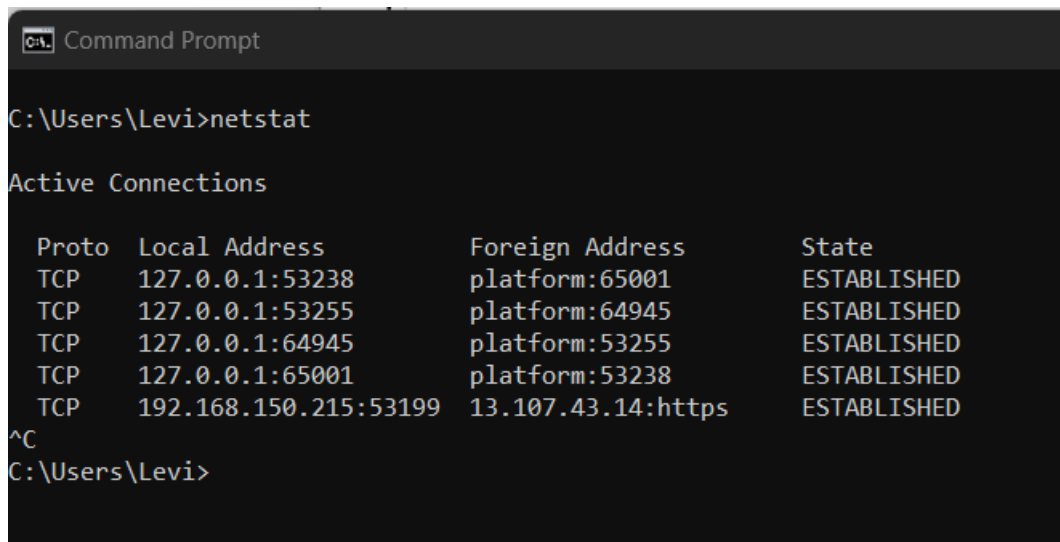
  0  10 ms  3 ms  1 ms  192.168.150.141
  1  *      *      *      Request timed out.
  2  54 ms  45 ms  41 ms  56.8.83.197
  3  54 ms  27 ms  40 ms  172.26.101.38
  4  52 ms  37 ms  37 ms  172.26.101.51
  5  61 ms  28 ms  37 ms  172.25.111.0
  6  *      *      *      Request timed out.
  7  *      *      *      Request timed out.
  8  85 ms  280 ms  74 ms  74.125.32.0
  9  76 ms  120 ms  80 ms  108.170.248.209
 10 100 ms  97 ms  64 ms  108.170.248.218
 11 97 ms  78 ms  62 ms  216.239.48.65
 12 117 ms  93 ms 102 ms  ^C

C:\Users\Levi>
```

4. Netstat

This command displays active connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, and IP statistics.

The output of this command is organized in rows and columns. Each row represents a new connection or an entry in the output. It contains four columns. These columns provide the following information about the row.



```
C:\Users\Levi>netstat

Active Connections

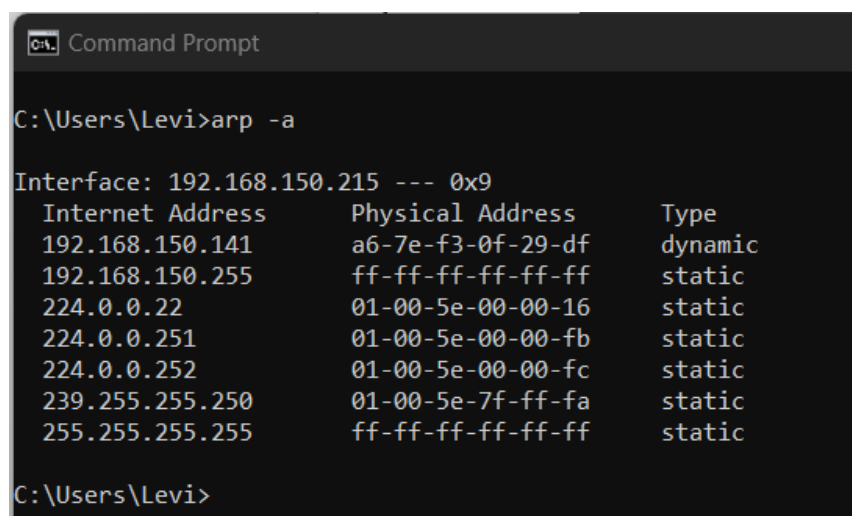
Proto Local Address          Foreign Address         State
TCP   127.0.0.1:53238         platform:65001          ESTABLISHED
TCP   127.0.0.1:53255         platform:64945          ESTABLISHED
TCP   127.0.0.1:64945         platform:53255          ESTABLISHED
TCP   127.0.0.1:65001         platform:53238          ESTABLISHED
TCP   192.168.150.215:53199   13.107.43.14:https      ESTABLISHED
^C
C:\Users\Levi>
```

5.

ARP

To send IP packets, a computer needs two addresses. These addresses are the MAC address and the IP address. A MAC address is the physical or hardware address of the NIC. An IP address is the logical or software address of NIC. If a computer knows the IP address of the destination computer but it does not know the MAC address of the destination computer, it uses the ARP protocol to know the MAC address of the destination computer.

The ARP protocol broadcasts a given IP address over a local network. The corresponding host responds to the broadcast with its MAC address. To avoid repetition, ARP stores the answer in a table known as ARP table. ARP maintains a separate ARP table for each NIC.



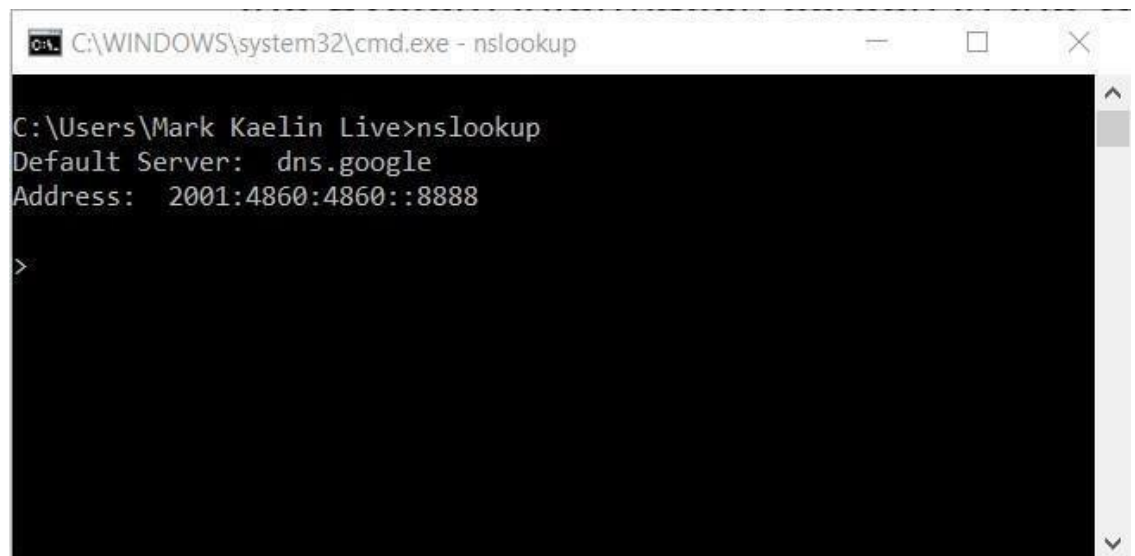
```
C:\Users\Levi>arp -a

Interface: 192.168.150.215 --- 0x9
Internet Address      Physical Address        Type
192.168.150.141       a6-7e-f3-0f-29-df      dynamic
192.168.150.255       ff-ff-ff-ff-ff-ff      static
224.0.0.22            01-00-5e-00-00-16      static
224.0.0.251           01-00-5e-00-00-fb      static
224.0.0.252           01-00-5e-00-00-fc      static
239.255.255.250       01-00-5e-7f-ff-fa      static
255.255.255.255       ff-ff-ff-ff-ff-ff      static
C:\Users\Levi>
```

6.

NSLOOKUP

NSLookup is a great utility for diagnosing DNS name resolution problems. Just type the NSLookup command, and Windows will display the name and IP address of the device's default DNS server. From there, you can type host names in an effort to see if the DNS server is able to resolve the specified host name.



```
C:\WINDOWS\system32\cmd.exe - nslookup
C:\Users\Mark Kaelin Live>nslookup
Default Server:  dns.google
Address:  2001:4860:4860::8888
>
```

7.

HOSTNAME

NbtStat command can provide you with the host name that has been assigned to a Windows device, if you know which switch to use with the command. However, if you're just looking for a fast and easy way of verifying a computer's name, then try using the Hostname command. Typing Hostname at the command prompt returns the local computer name.



```
C:\>hostname
ws5
C:\>
```


Practical-4

OBJECTIVE: - Installation of Cisco Packet Tracer and Analysis of Various Tools, Functioning, Tasks in Logical Platform, Basic PC Interconnection and Creation of LAN.

CISCO PACKET TRACER: -

The main purpose of Cisco Packet Tracer is to help students learn the principles of networking with hands-on experience as well as develop Cisco technology specific skills. Since the protocols are implemented in software only method, this tool cannot replace the hardware Routers or Switches. Interestingly, this tool does not only include Cisco products but also many more networking devices.

WORKSPACE: -

1. **Logical:** - Logical workspace shows the logical network topology of the network the user has built. It represents the placing, connecting and clustering virtual network devices.
2. **Physical:** - Physical workspace shows the graphical physical dimension of the logical network. It depicts the scale and placement in how network devices such as routers, switches and hosts would look in a real environment. It also provides geographical representation of networks, including multiple buildings, cities and wiring closets.

KEY FEATURES: -

- Unlimited devices
- E-learning
- Customize single/multi user activities
- Interactive Environment
- Visualizing Networks
- Real-time mode and Simulation mode
- Self-paced
- Supports majority of networking protocols
- International language support
- Cross platform compatibility

NETWORK DEVICES: -

1. **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.

Router devices emulated in Cisco Packet Tracer: -

- Cisco 1841 ISR router.
- Cisco 2620XM ISR router.
- Cisco 2621XM ISR router.
- Cisco 2811 ISR router.
- Cisco 1941 ISR router.
- Cisco 2901 ISR router.
- Cisco 2911 ISR router.
- Cisco 819 ISR router.

2. **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.
3. **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. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

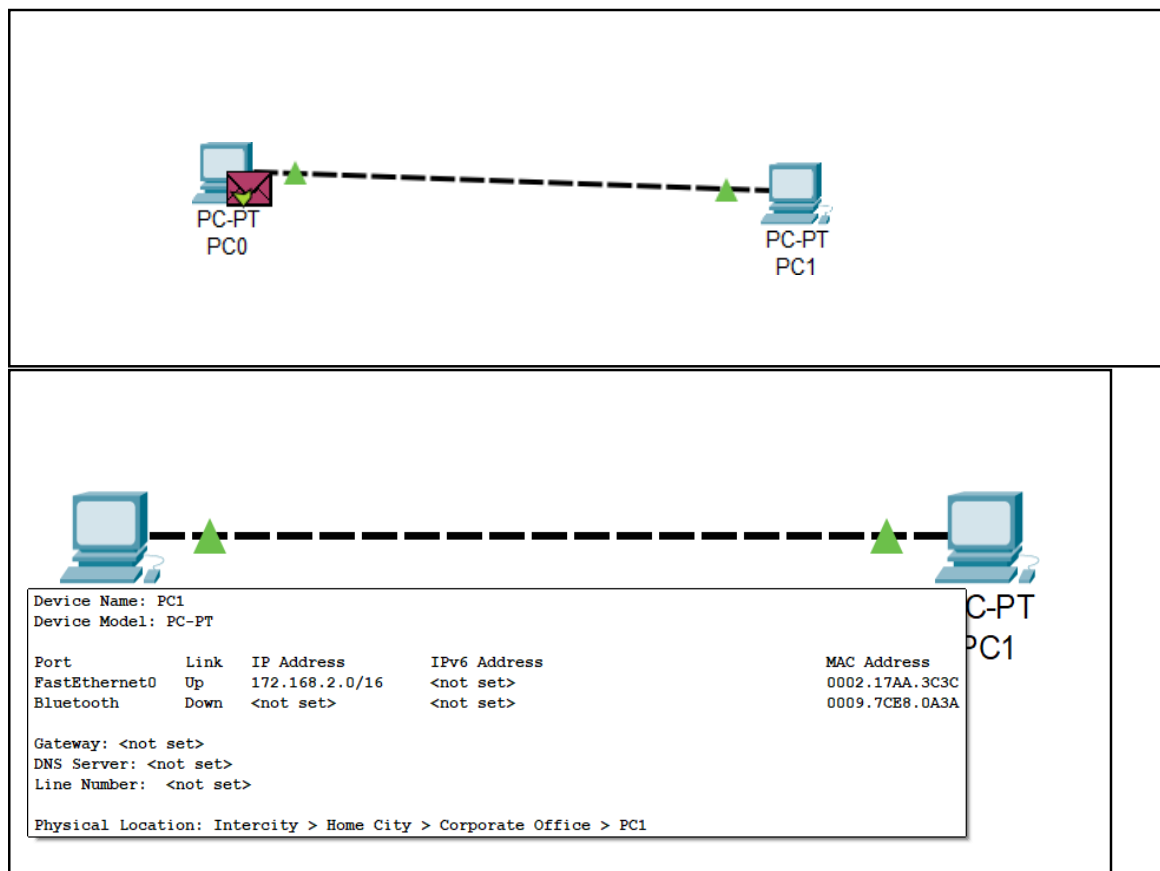
Types of Hub: -

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

END DEVICES: -

End devices are the source and destination devices, which are used for data sent over any internet network. In order to determine one end device from another, each end device on a network is determined by an address. When an end device starts communication, it uses the address of the destination end device to determine where the message should be transmitted.

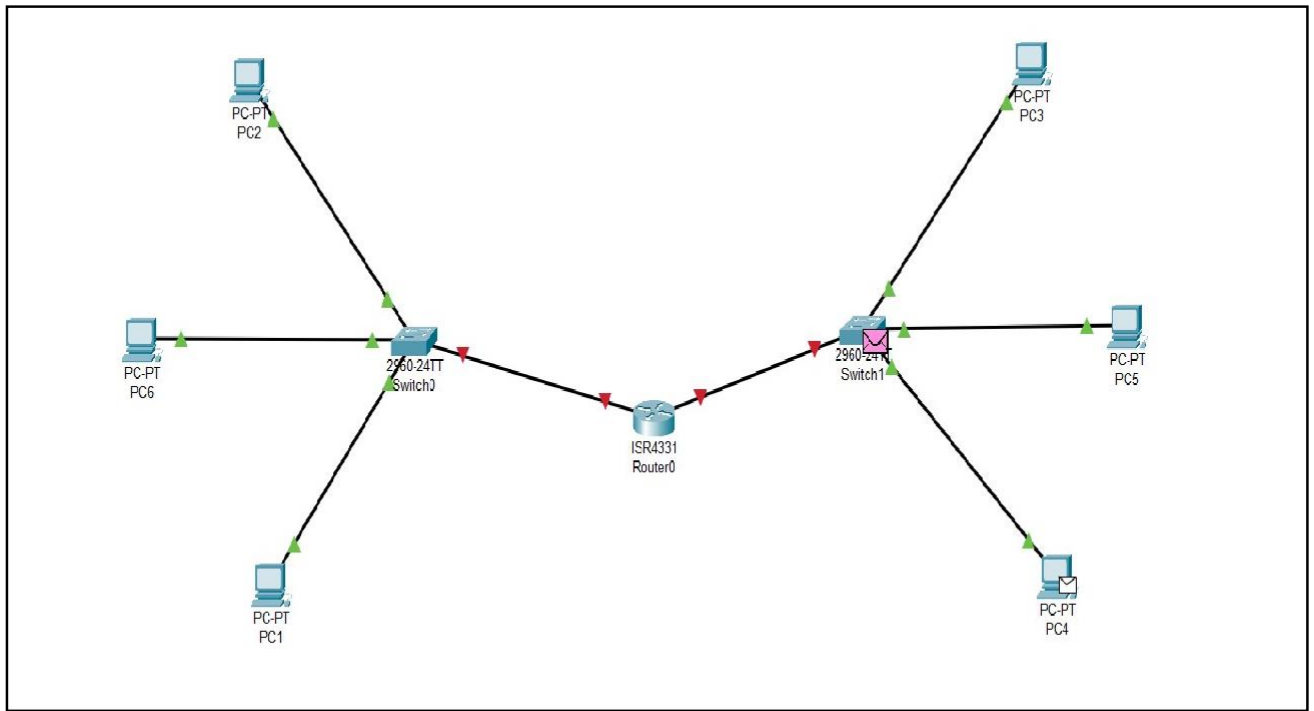
BASIC PC INTERCONNECTION: -



LAN SEGMENT: -

- LAN Segment is a physical portion of a local area network (LAN) that is separated from other portions by bridges or routers.
- LANs are often “segmented” using bridges in order to improve network performance. Bridges are smart devices that build MAC-level routing tables that forward network traffic on the basis of the destination MAC address of each frame.
- If the destination address of a frame is a machine in the local LAN segment, bridges attached to that segment will not allow the frame to pass; this reduces unneeded network traffic in other segments attached to the bridge.

LAN Segmentation improves performance: - Segmentation improves the performance of Ethernet networks by reducing the number of stations in each segment of the LAN that must compete with each other for access to the network. Bridges are generally used for segmenting smaller LANs because they are cheaper and require no special configuration. You place a bridge between your department or workgroup hub and the main network backbone to improve traffic on your local segment.



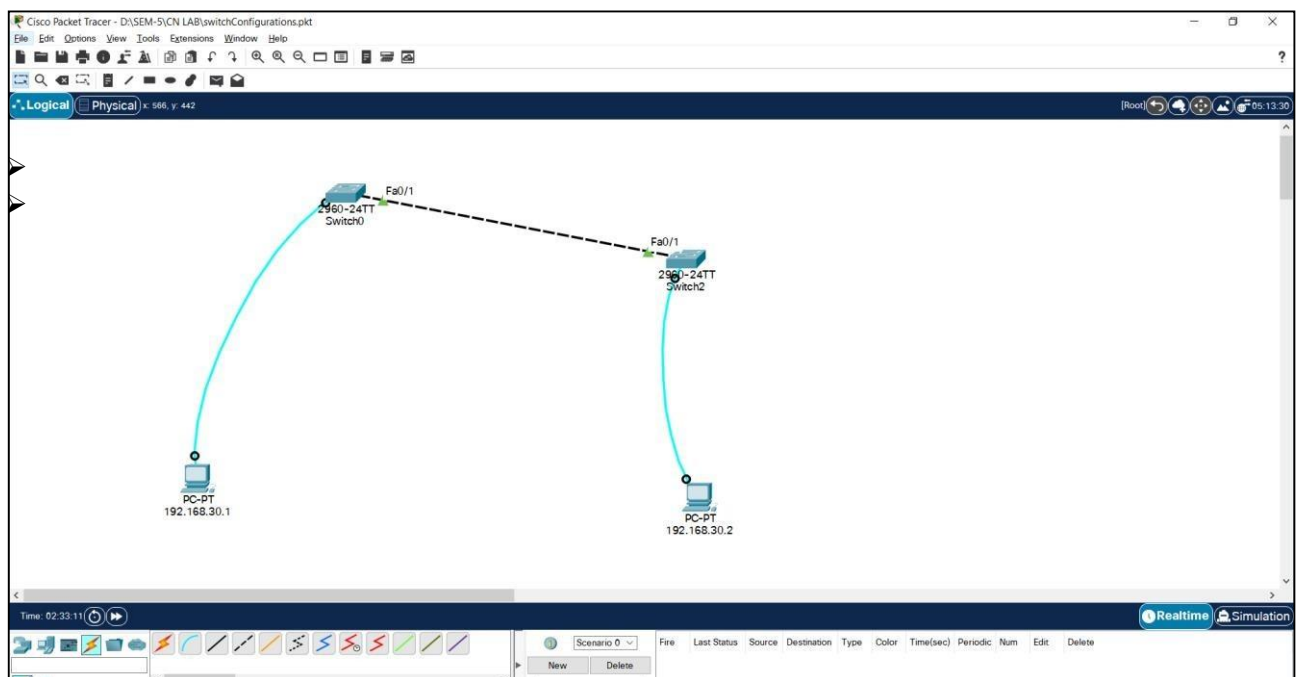
Practical-5

OBJECTIVE: - Basic configuration of devices(switch) using cisco packet tracer: user mode,

Privileged mode, name setting,password, and others.

- **Configuring the switch using PC and setting password protection to switch.**
- Requirements –
 - 2 switches
 - 2 PC's

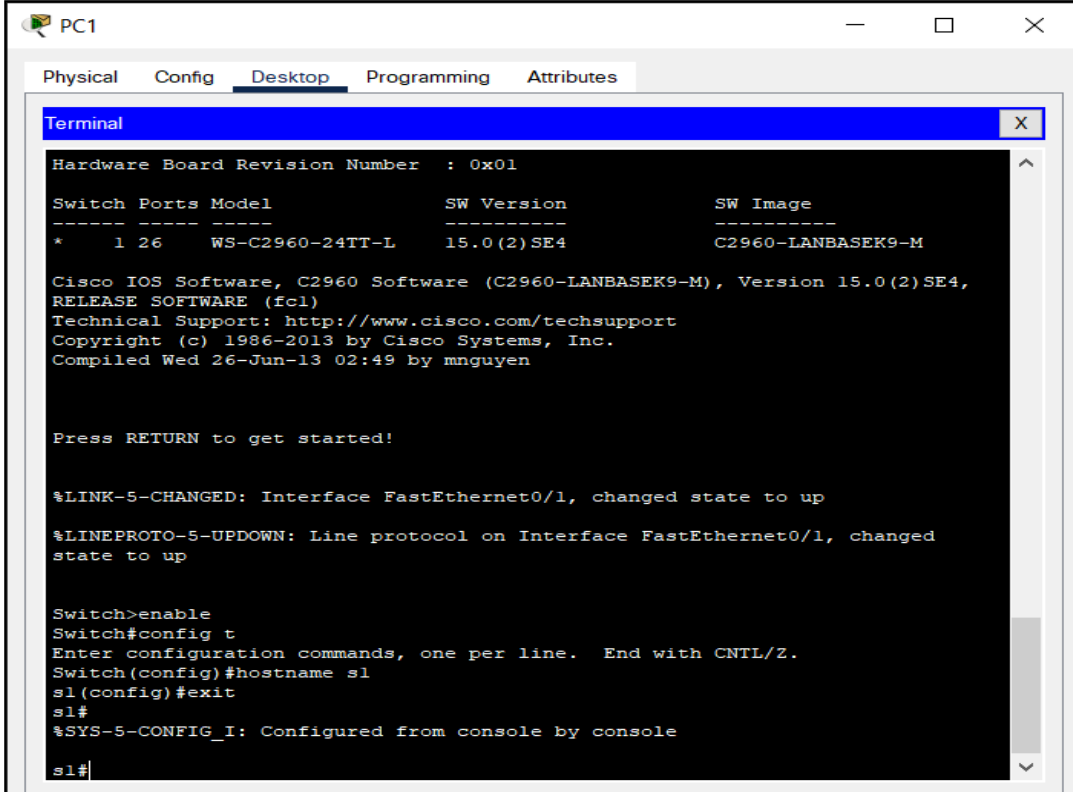
Connect both switches with Cross-over cable and then connect 1-1 PC to respective switch with console cable. Connect the console part of switch with RS 232 part of PC.



➤ Configuring switch using PC

Open PC 1 settings then Desktop -> Terminal -> Press OK
Now press Enter and write these commands

- enable
- config t
- hostname s1
- exit



The screenshot shows a PC window titled 'PC1' with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is active, displaying a terminal window. The terminal output shows the switch's boot sequence, including hardware revision, port details, and software version. It then prompts the user to press RETURN to get started. After pressing RETURN, the terminal shows the switch entering the enable mode, then the configuration mode (config t), where the hostname is set to s1. Finally, the user exits the configuration mode and returns to the enable mode.

```
Hardware Board Revision Number : 0x01

Switch Ports Model          SW Version  SW Image
-----
*   1 26   WS-C2960-24TT-L   15.0(2)SE4   C2960-LANBASEK9-M

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4,
RELEASE SOFTWARE (fcl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnnguyen

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up

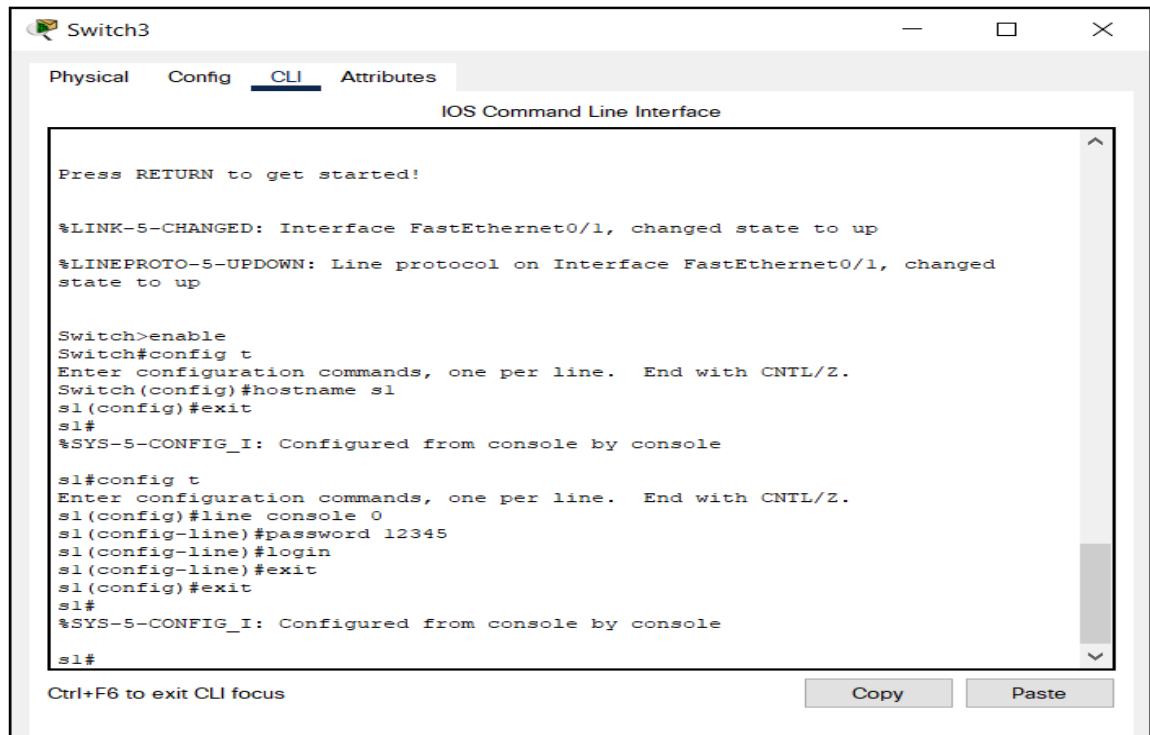
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname s1
s1(config)#exit
s1#
%SYS-5-CONFIG_I: Configured from console by console

s1#
```

➤ Setting Password in switch using switch CLI(For Main Mode)

Now open switch CLI and write these commands

- config t
- line console 0
- password 12345(our password)
- login
- exit
- exit
- exit

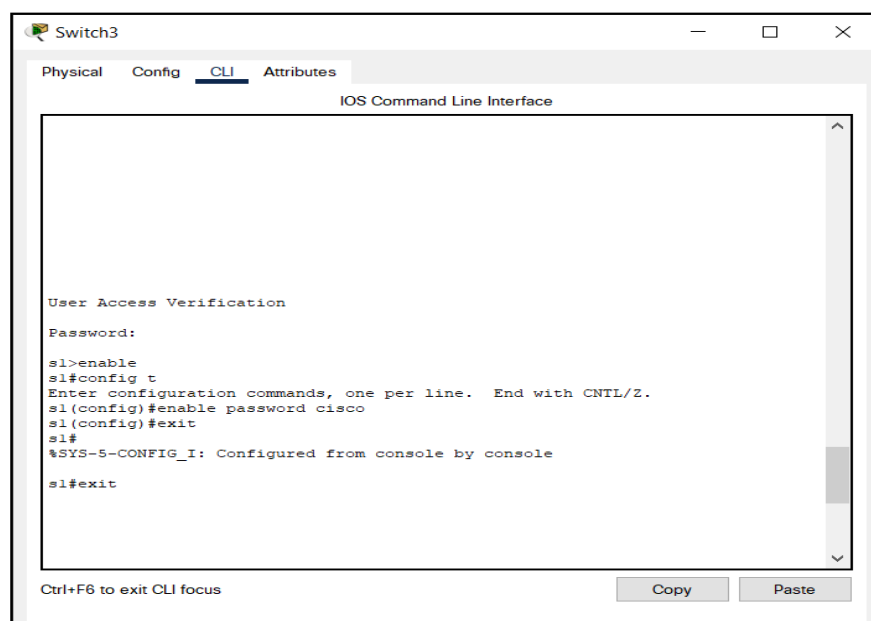


➤ Setting Password in switch(For Privilege Mode)

Now write these commands

Enter the Main Password first

- enable
- config t
- enable password cisco(our password)
- exit
- exit



Here it wants the password, so enter the password(Main Mode) and Press enter

Here it wants another password, so enter the password(Privilege Mode) and Press Enter

- show running-config

This Configuration shows both the passwords we have set.

So we need to encrypt them.

Switch3

Physical Config CLI Attributes

IOS Command Line Interface

User Access Verification

Password:

s1>enable

Password:

s1#show running-config


Building configuration...

Current configuration : 1123 bytes

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname s1
!
enable password cisco
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
--More--
```

Ctrl+F6 to exit CLI focus

Copy Paste



Switch1

Physical Config CLI Attributes

IOS Command Line Interface

```
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
  no ip address
  shutdown
!
!
!
!
line con 0
  password 7 08701E1D5D4C
  login
!
line vty 0 4
  login
line vty 5 15
  login
!
!
!
!
end

sl#
sl#
sl#
```

Ctrl+F6 to exit CLI focus

Copy Paste

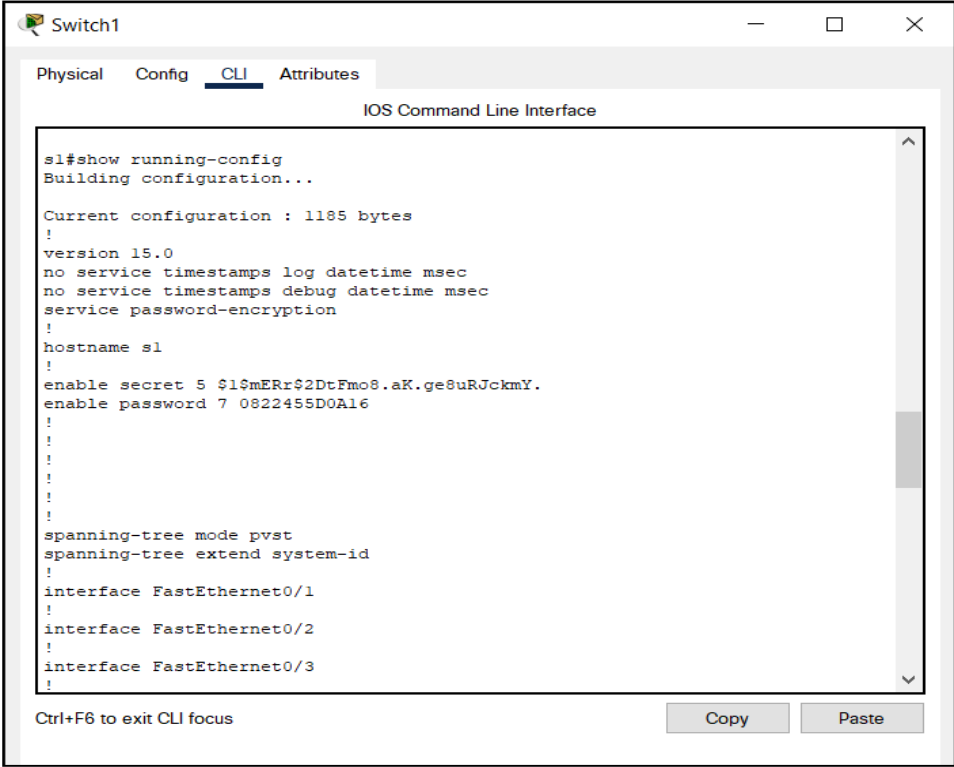
➤ Encrypting Privilege Mode Password in switch

The switch is in Privilege Mode so go to configuration mode and writes these commands

- config t
- enable secret abc123(our secret password)
- exit
- exit

➤ Encrypting All Passwords in switch

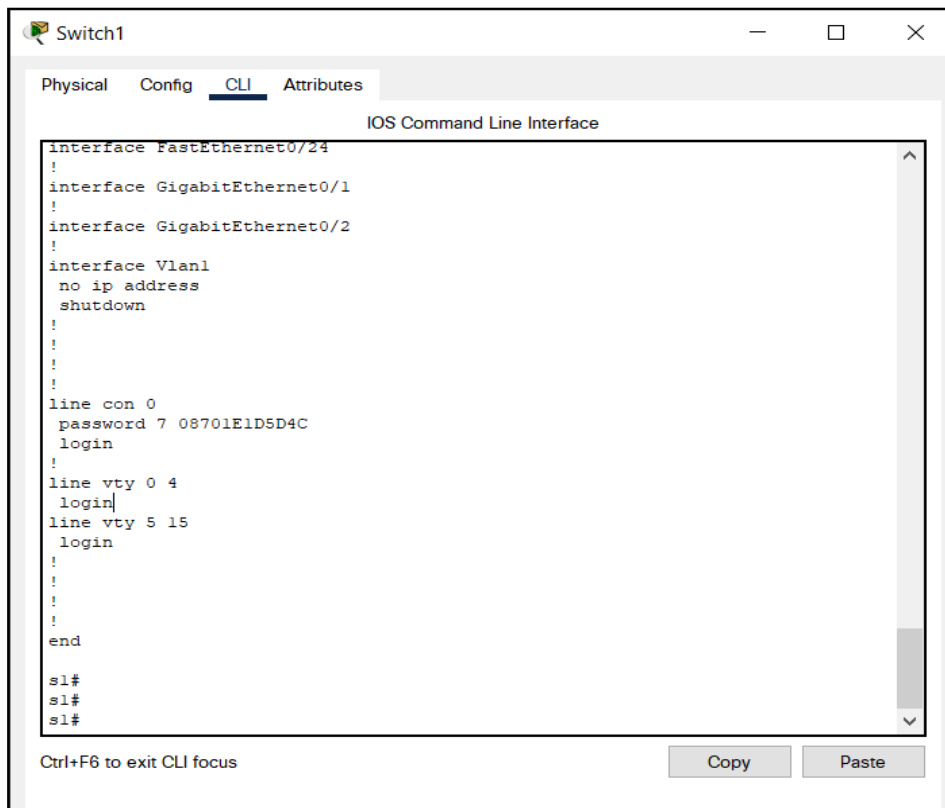
- Enter Main Password
- enable
- Enter Privilege Mode Password(secret)
- config t
- service password-encryption
- exit



```
s1#show running-config
Building configuration...

Current configuration : 1185 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname s1
!
enable secret 5 $1$mERr$2DtFmo8.aK.ge8uRJckmY.
enable password 7 0822455D0A16
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
```

- exit



Practical-6

AIM – Configuration of Router and its interfaces.

- Configuring Router and making a connection and sending packet from one network to another.
- Requirement –
 - 2 Routers
 - 2 switches
 - 4 PC's

Connect 2 PC's with 1st switch and rest 2 PC's with 2nd switch with Copper Straight Through cable. Connect both the switches to both Routers respectively with Copper Straight Through cable. Connect both Routers with Copper Cross-over cable.

Default Gateway for Router 1st -> 10.1.1.1

Default Gateway for Router 2nd -> 10.1.1.2

Default Gateway for Switch 1st -> 192.168.30.1

Default Gateway for Switch 2nd -> 192.168.40.1

Now assign IP address and Default Gateways to all PC's

1st PC -> 192.168.30.2

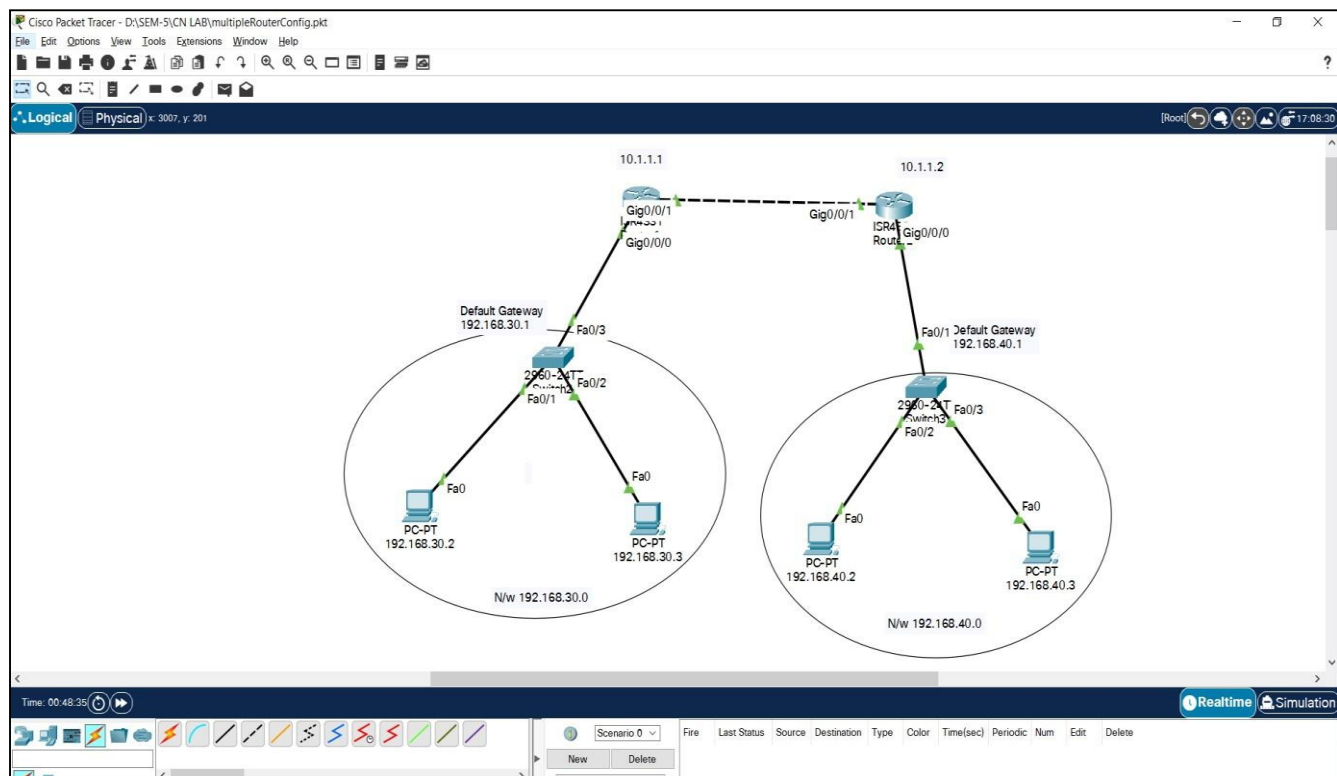
2nd PC -> 192.168.30.3

3rd PC -> 192.168.40.2

4th PC -> 192.168.40.3

Network Address for 1st Network -> 192.168.30.0

Network Address for 2nd Network -> 192.168.40.0



If we ping now From PC 1 to PC 2 we get the reply successful.
But if we ping from PC 1 to PC 3 or PC 4 we get Request Timed Out.

```

PC4
Physical Config Desktop Programming Attributes
Command Prompt
Request timed out.

Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.30.3

Pinging 192.168.30.3 with 32 bytes of data:

Reply from 192.168.30.3: bytes=32 time<1ms TTL=128
Reply from 192.168.30.3: bytes=32 time<1ms TTL=128
Reply from 192.168.30.3: bytes=32 time<1ms TTL=128
Reply from 192.168.30.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.40.2

Pinging 192.168.40.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.40.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>

```

So for this we have to configure the interfaces of Router.

➤ **Configuring Router and its interfaces**

➤ **Configuring Router 1**

Open the Router CLI and write these commands

- enable
- config t

Configuring 1st interface (1st Switch Side)

- interface g0/0/0
- ip address 192.168.30.1 255.255.255.0
- no shutdown
- exit

Configuring 2nd interface (Router Side)

- config t
- interface g0/0/1
- ip address 10.1.1.1 255.0.0.0
- no shutdown
- exit
- exit

➤ **Configuring Router 2**

Open the Router CLI and write these commands

- enable
- config t

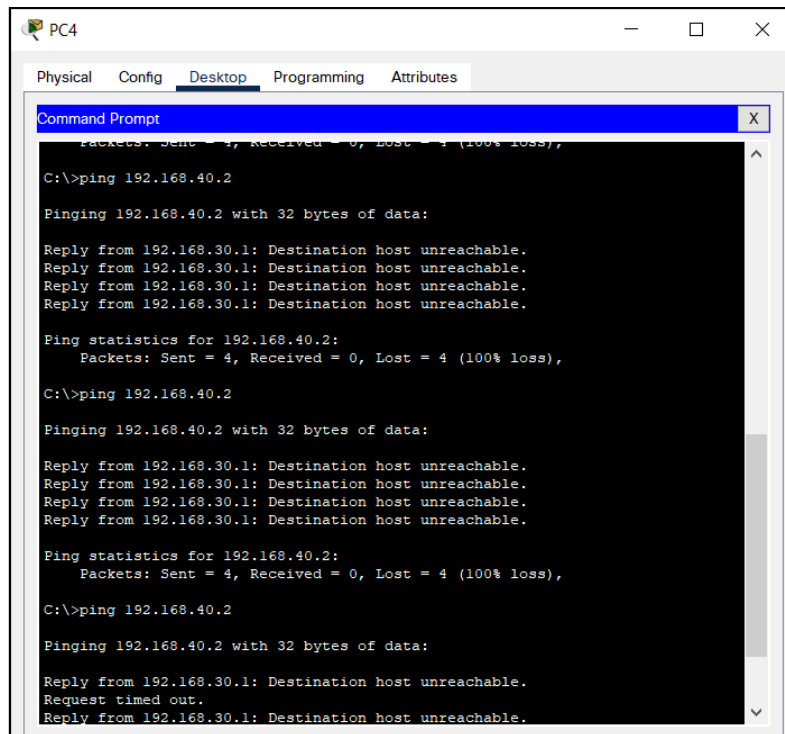
Configuring 1st interface (2nd Switch Side)

- interface g0/0/0
- ip address 192.168.40.1 255.255.255.0
- no shutdown
- exit

Configuring 2nd interface (Router Side)

- config t
- interface g0/0/1
- ip address 10.1.1.2 255.0.0.0
- no shutdown
- exit
- exit

Now If we ping now From PC 1 or PC 2 to PC 3 or PC 4 we get the reply as Destination Host Unreachable. This means that the packet travelled till Router only and not to next router.



The screenshot shows a window titled 'PC4' with tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The Command Prompt shows the results of three ping commands to the IP address 192.168.40.2. Each command shows that all four packets sent were lost, resulting in a 100% loss rate. The first two commands show 'Destination host unreachable' replies from 192.168.30.1. The third command shows a 'Request timed out' message.

```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.40.2

Pinging 192.168.40.2 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 192.168.40.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.40.2

Pinging 192.168.40.2 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 192.168.40.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.40.2

Pinging 192.168.40.2 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Request timed out.
Reply from 192.168.30.1: Destination host unreachable.
```

So we have set or configure the route of packet.

- **Configuring Packet Route**
- **Configuring Router 1**

Open the Router CLI and write these commands

- enable
- config t
- ip route 192.168.40.0 255.255.255.0 10.1.1.2
- exit
- write
- exit

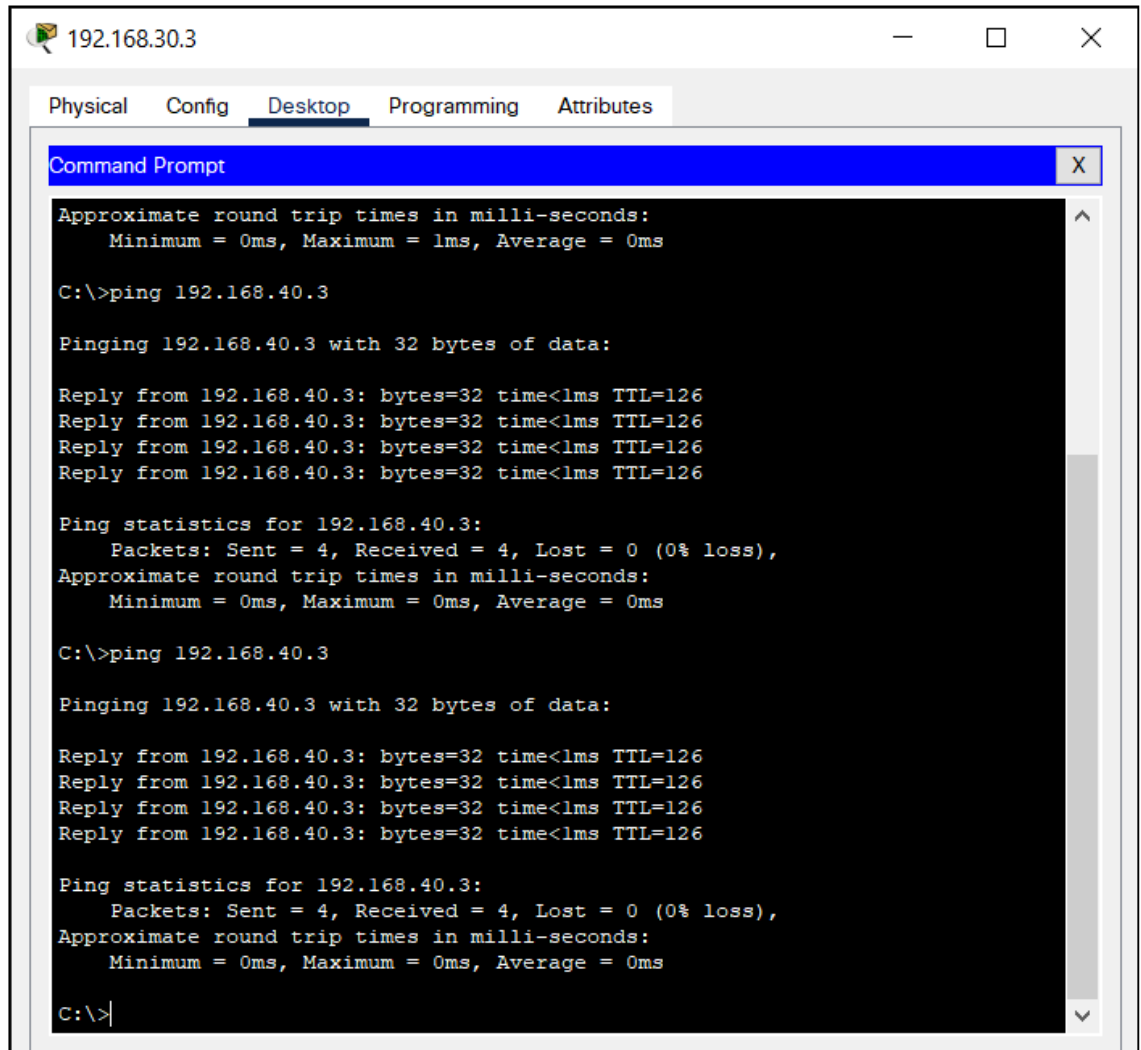
➤ **Configuring Router 2**

Open the Router CLI and write these commands

- enable
- config t
- ip route 192.168.30.0 255.255.255.0 10.1.1.1
- exit

- write
- exit

Now If we ping now From PC 1 or PC 2 to PC 3 or PC 4 we get the reply successful as we have configured our Route of Packet.



```
192.168.30.3
Physical Config Desktop Programming Attributes
Command Prompt
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.40.3

Pinging 192.168.40.3 with 32 bytes of data:

Reply from 192.168.40.3: bytes=32 time<1ms TTL=126
Reply from 192.168.40.3: bytes=32 time<1ms TTL=126
Reply from 192.168.40.3: bytes=32 time<1ms TTL=126
Reply from 192.168.40.3: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.40.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.40.3

Pinging 192.168.40.3 with 32 bytes of data:

Reply from 192.168.40.3: bytes=32 time<1ms TTL=126
Reply from 192.168.40.3: bytes=32 time<1ms TTL=126
Reply from 192.168.40.3: bytes=32 time<1ms TTL=126
Reply from 192.168.40.3: bytes=32 time<1ms TTL=126

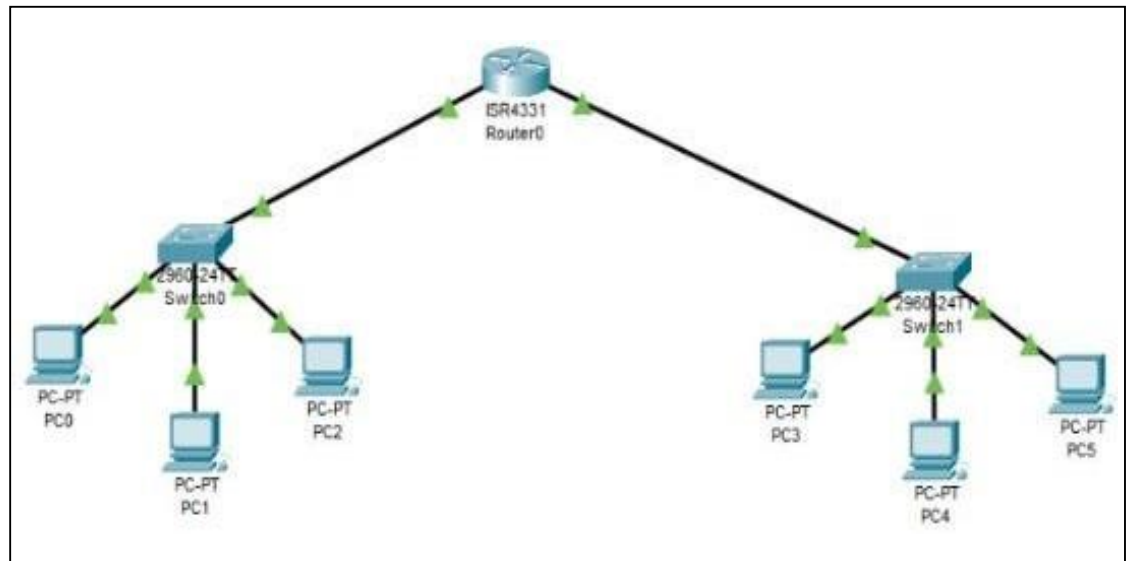
Ping statistics for 192.168.40.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```


Practical-7

Objective:- How to Connect Two Different Networks Using Router

Simulation:-



Simulation Panel				
Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC0	ICMP
	0.001	PC0	Switch0	ICMP
	0.002	Switch0	Laptop1	ICMP
	0.003	Laptop1	Switch0	ICMP
	0.004	Switch0	PC0	ICMP
Visible	1.518	--	Switch0	STP

DIFFERENT NETWORK CONFIGURATION: -

Network – 1: -

IP Address: - 192.168.1.2, 192.168.1.3, 192.168.1.4

Default Gateway: - 192.168.1.1

Interface: - g0/0/0

Network – 2: -

IP Address: - 192.168.2.2, 192.168.2.3, 192.168.2.4

Default Gateway: - 192.168.2.1

Interface: - g0/0/1

Router: -

For Network-1:

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface g0/0/0

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#exit

For Network – 2: -

Router(config)#interface g0/0/1

Router(config-if)#ip address 192.168.2.1 255.255.255.0

Router(config-if)#no shutdown

For Saving: -

Router#wr

For Checking State: -

Router#sh ip int br

Practical-8

Aim:- Configure DHCP on cisco router

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to any device, or node, on a network so they can communicate using IP (Internet Protocol). DHCP automates and centrally manages these configurations. There is no need to manually assign IP addresses to new devices. Therefore, there is no requirement for any user configuration to connect to a DHCP based network.

DHCP can be implemented on local networks as well as large enterprise networks. DHCP is the default protocol used by the most routers and networking equipment. DHCP is also called RFC (Request for comments) 2131.

DHCP does the following:

- DHCP manages the provision of all the nodes or devices added or dropped from the network.
- DHCP maintains the unique IP address of the host using a DHCP server.
- It sends a request to the DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to a network. The server acknowledges by providing an IP address to the client/node/device.

DHCP is also used to configure the proper subnet mask, default gateway and DNS server information on the node or device.

There are many versions of DHCP are available for use in IPV4 (Internet Protocol Version 4) and IPV6 (Internet Protocol Version 6).

How DHCP works

DHCP runs at the application layer of the TCP/IP protocol stack to dynamically assign IP addresses to DHCP clients/nodes and to allocate TCP/IP configuration information to the DHCP clients. Information includes subnet mask information, default gateway, IP addresses and domain name system addresses.

DHCP is based on client-server protocol in which servers manage a pool of unique IP addresses, as well as information about client configuration parameters, and assign addresses out of those address pools.

The DHCP lease process works as follows:

- First of all, a client (network device) must be connected to the internet.
- DHCP clients request an IP address. Typically, client broadcasts a query for this information.
- DHCP server responds to the client request by providing IP server address and other configuration information. This configuration information also includes time period, called a lease, for which the allocation is valid.
- When refreshing an assignment, a DHCP clients request the same parameters, but the DHCP server may assign a new IP address. This is based on the policies set by the administrator.

Components of DHCP

When working with DHCP, it is important to understand all of the components. Following are the list of components:

- **DHCP Server:** DHCP server is a networked device running the DHCP service that holds IP addresses and related configuration information. This is typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.
- **DHCP client:** DHCP client is the endpoint that receives configuration information from a DHCP server. This can be any device like computer, laptop, IoT endpoint or anything else that requires connectivity to the network. Most of the devices are configured to receive DHCP information by default.
- **IP address pool:** IP address pool is the range of addresses that are available to DHCP clients. IP addresses are typically handed out sequentially from lowest to the highest.
- **Subnet:** Subnet is the partitioned segments of the IP networks. Subnet is used to keep networks manageable.
- **Lease:** Lease is the length of time for which a DHCP client holds the IP address information. When a lease expires, the client has to renew it.
- **DHCP relay:** A host or router that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client. DHCP relay can be used to centralize DHCP servers instead of having a server on each subnet.

Benefits of DHCP

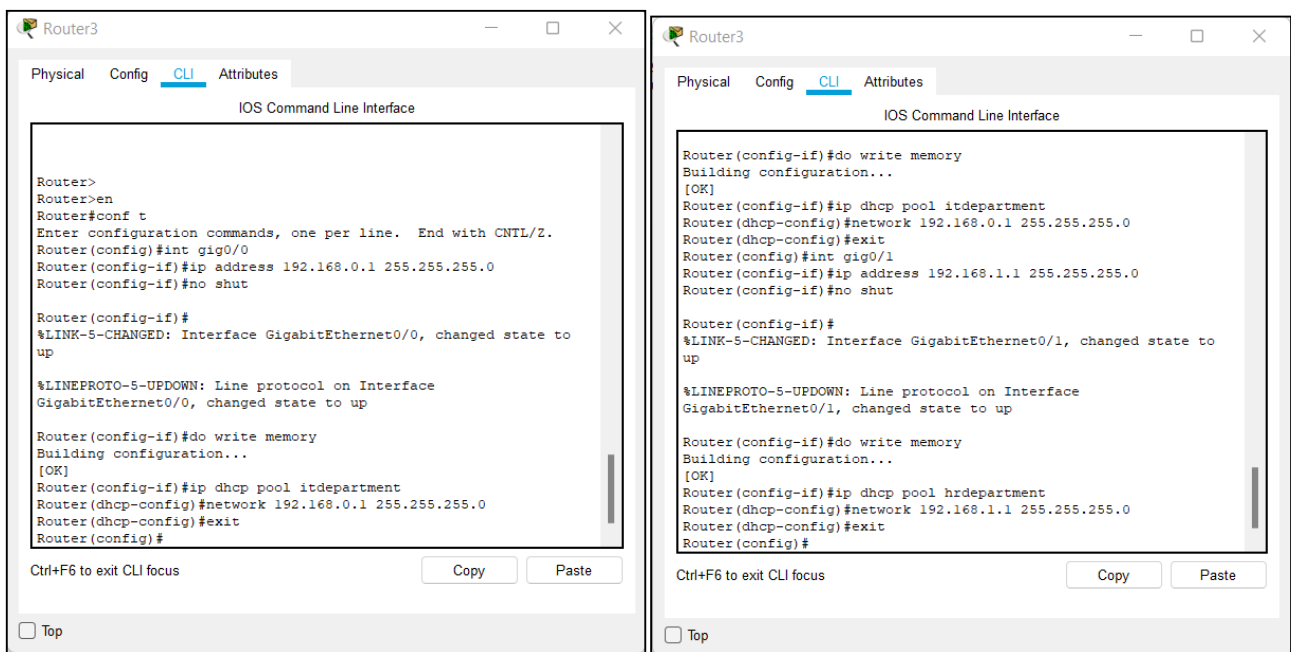
There are following benefits of DHCP:

Centralized administration of IP configuration: DHCP IP configuration information can be stored in a single location and enables that administrator to centrally manage all IP address configuration information.

Dynamic host configuration: DHCP automates the host configuration process and eliminates the need to manually configure individual host. When TCP/IP (Transmission control protocol/Internet protocol) is first deployed or when IP infrastructure changes are required.

Seamless IP host configuration: The use of DHCP ensures that DHCP clients get accurate and timely IP configuration IP configuration parameter such as IP address, subnet mask, default gateway, IP address of DND server and so on without user intervention.

Flexibility and scalability: Using DHCP gives the administrator increased flexibility, allowing the administrator to move easily change IP configuration when the infrastructure changes.



PC1

Physical Config **Desktop** Programming Attributes

IP Configuration [X]

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static DHCP request successful.

IP Address 192.168.0.2

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address /

Link Local Address FE80::230:F2FF:FE22:9566

IPv6 Gateway

IPv6 DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

☐ Top

PC4

Physical Config **Desktop** Programming Attributes

IP Configuration [X]

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static DHCP request successful.

IP Address 192.168.1.2

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address /

Link Local Address FE80::207:ECFF:FE9B:B9EC

IPv6 Gateway

IPv6 DNS Server

802.1X

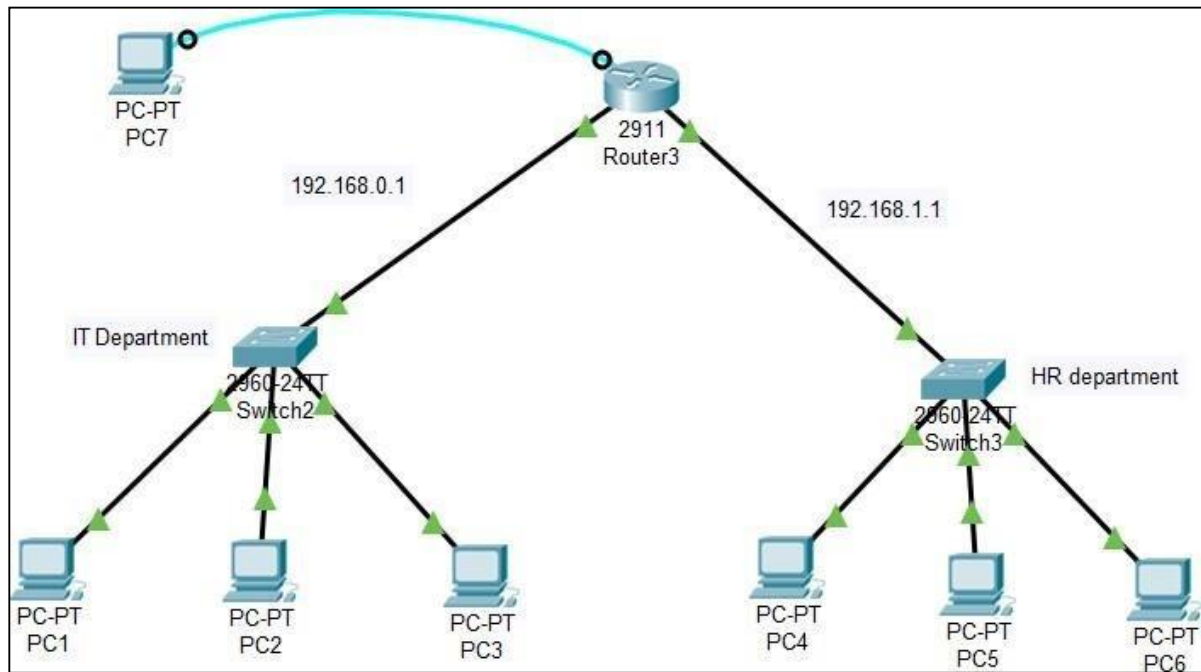
☐ Use 802.1X Security

Authentication MD5

Username

Password

☐ Top



Practical-9

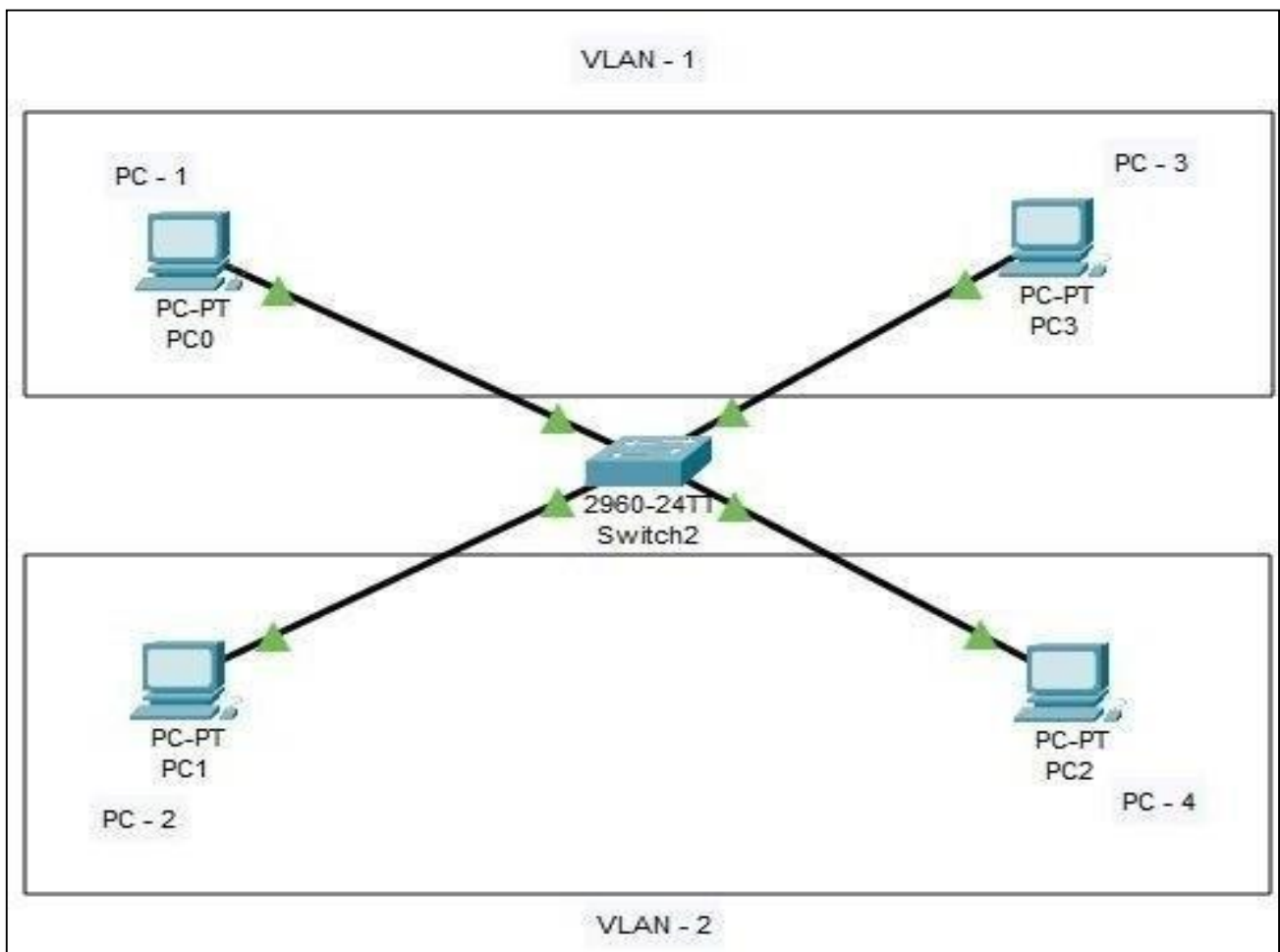
Objective: - Implementation of Virtual LAN

Virtual LAN: -

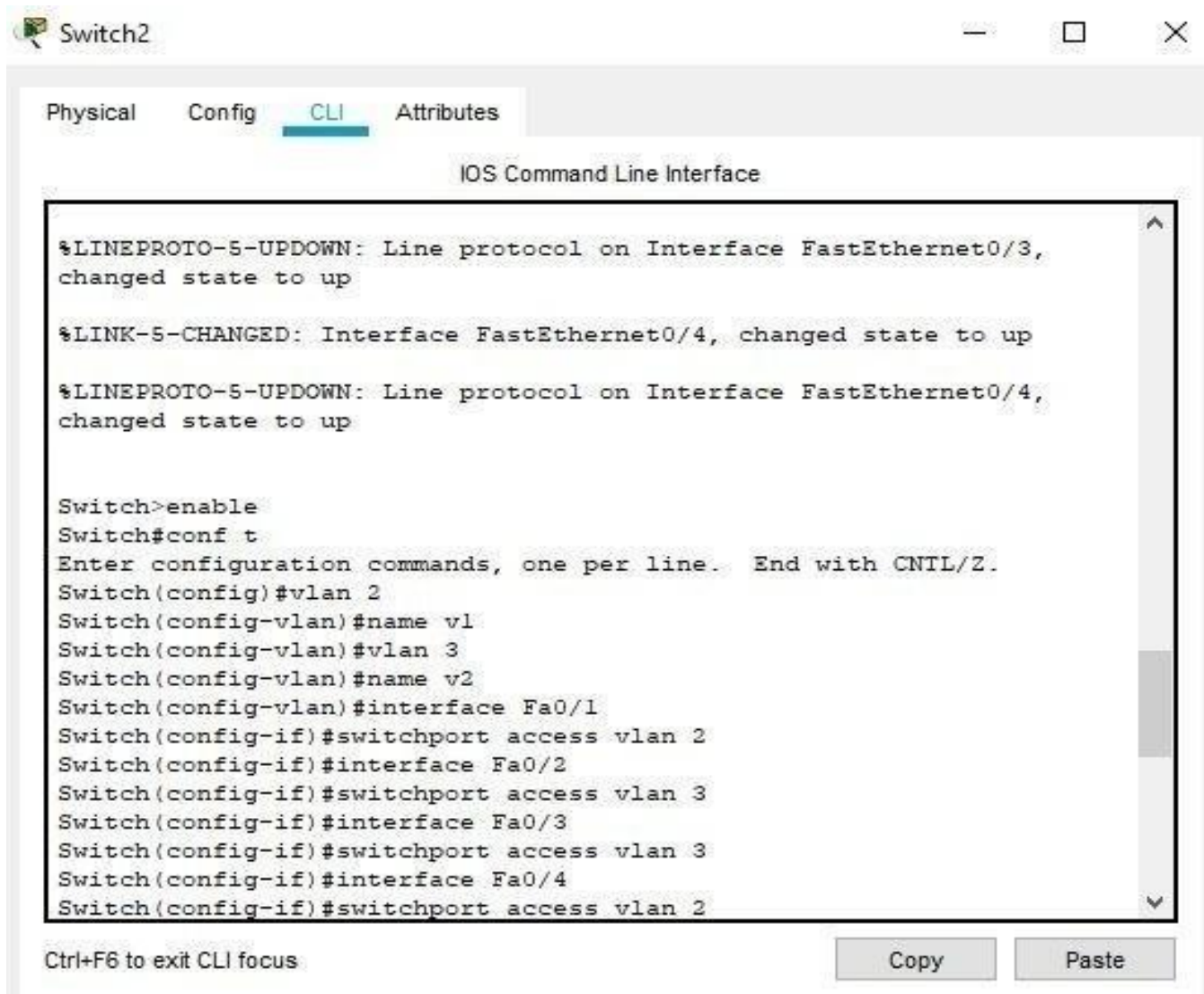
Virtual LAN (VLAN) is a concept in which we can divide the devices logically on layer 2 (data link layer). Generally, layer 3 devices divide broadcast domain but broadcast domain can be divided by switches using the concept of VLAN.

A broadcast domain is a network segment in which if a device broadcast a packet, then all the devices in the same broadcast domain will receive it. The devices in the same broadcast domain will receive all the broadcast packets but it is limited to switches only as routers don't forward out the broadcast packet. To forward out the packets to different VLAN (from one VLAN to another) or broadcast domain, inter VLAN routing is needed. Through VLAN, different small-size sub-networks are created which are comparatively easy to handle.

SIMULATION: -



Switch CLI: -

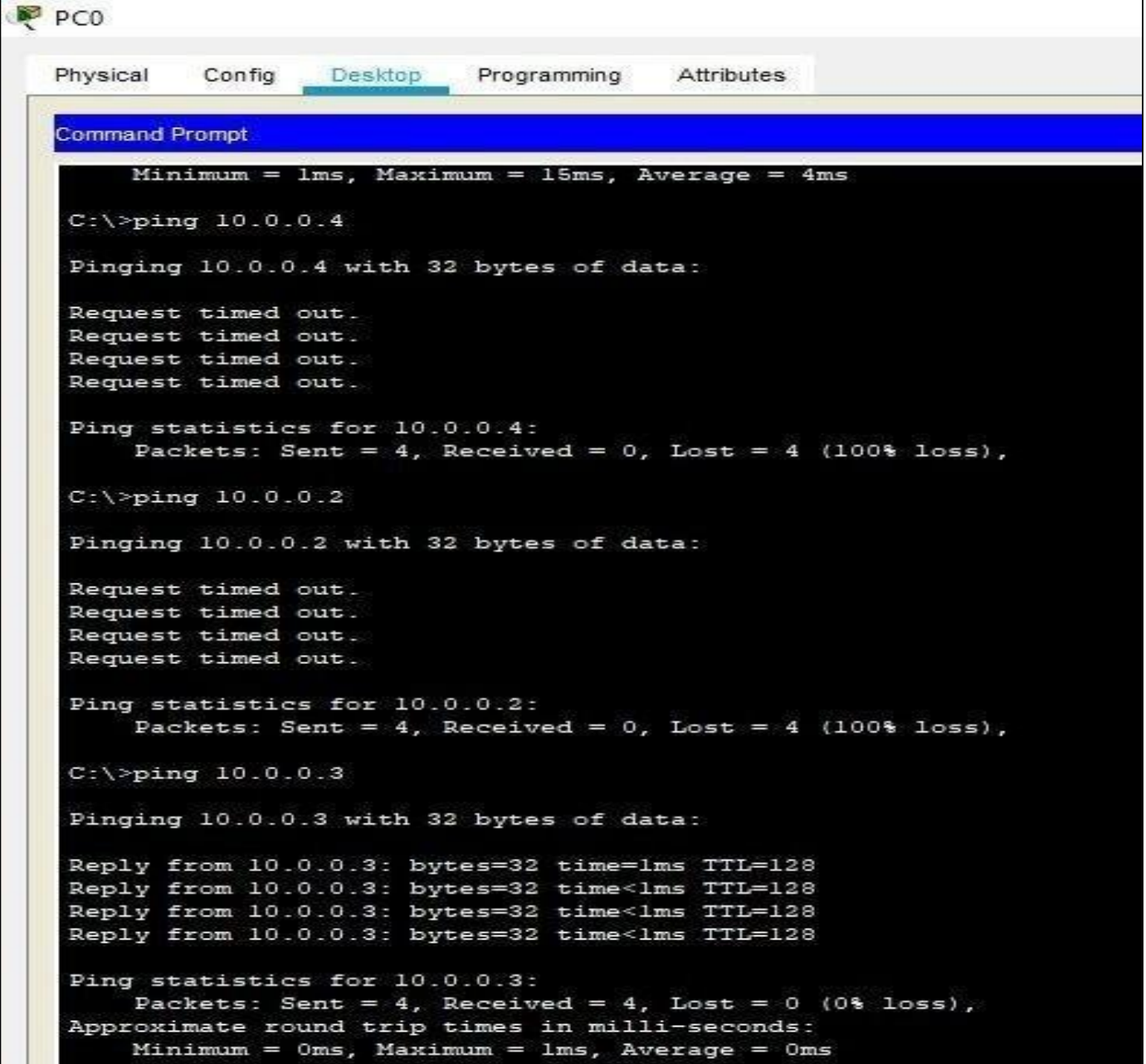


PC – 0: -

Checking whether the LAN is setup or not.

Ping command is used to check the connections.

As PC – 1 is connected to PC – 4 in a virtually established LAN. Similarly PC – 2 is connected to PC – 3 in a virtually established LAN.



The screenshot shows a virtual PC window titled 'PC0' with tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the results of three ping commands executed from the C:\ directory. The first two pings (to 10.0.0.4 and 10.0.0.2) result in 100% packet loss. The third ping (to 10.0.0.3) is successful with 0% loss.

```
Minimum = 1ms, Maximum = 15ms, Average = 4ms

C:\>ping 10.0.0.4

Pinging 10.0.0.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.0.0.3

Pinging 10.0.0.3 with 32 bytes of data:

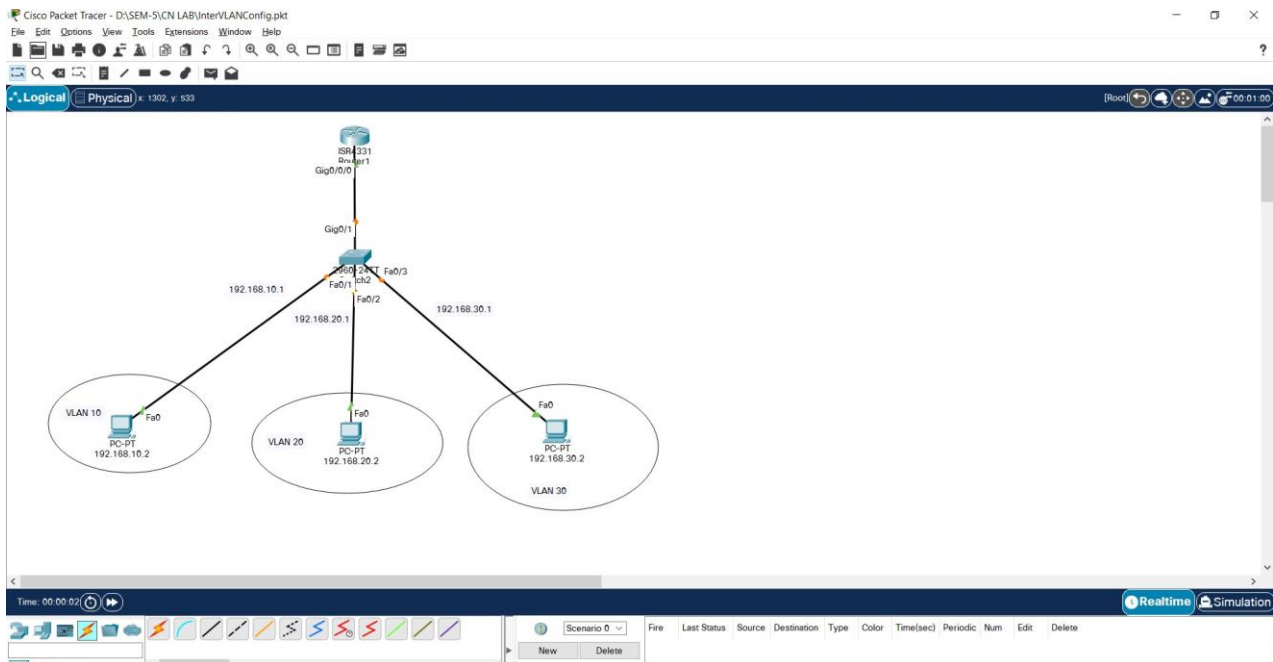
Reply from 10.0.0.3: bytes=32 time=1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Practical-10

Objective:- Design and Configuration of Inter VLAN routing using Layer 3 Switch

- Configuring 2 Switches to connect various PC's
- Requirement –
 1. 1 Router
 2. 1 switch
 3. 3 PC's



Switch Configuration

```
Switch>ENABLE
```

```
Switch#config t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch(config)#interface fa0/1
```

```
Switch(config-if)#switchport access vlan 10
```

% Access VLAN does not exist. Creating vlan 10

```
Switch(config-if)#exit
```

```
Switch(config)#vlan 10
```

```
Switch(config-vlan)#exit
```

```
Switch(config)#vlan 20
```

```
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#exit
Switch(config)#interface fa0/1
Switch(config-if)#switchport access vlan 10
Switch(config-if)#switchport mode access
Switch(config-if)#exit
Switch(config)#interface fa0/2
Switch(config-if)#switchport access vlan 20
Switch(config-if)#switchport mode access
Switch(config-if)#exit
Switch(config)#interface fa0/3
Switch(config-if)#switchport access vlan 30
Switch(config-if)#switchport mode access
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface g0/1
Switch(config-if)#no shutdown
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#showrunn
Building configuration...
```

Router Configuration

```
Router>enable
Router#config t
Router(config)#interface fa0/0
Router(config-if)#no sh
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#exit
Router(config)#interface g0/0.10
%Invalid interface type and number
Router(config)#
Router(config)#interface fa0/0.10
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed state to up
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/0.20
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20, changed state to up
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/0.30
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
% Configuring IP routing on a LAN subinterface is only allowed if that
subinterface is already configured as part of an IEEE 802.10, IEEE 802.1Q,
or ISL vLAN.
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#exit
```