

N. S. S. POLYTECHNIC COLLEGE

PANDALAM



LABORATORY RECORD

IN

20....

20....

Name.....

Class.....No.....Branch.....

Name of Examination.....

Reg: No.....

Certified that this is the bonafide record of work done

By.....

Date:

Lecturer in charge

Head of section

Examiners

INDEX

SL.NO.	NAME OF EXPERIMENT	DATE	PAGE NO.	INITIAL OF TEACHER
1	Computer network components	08/12/2023	5-7	
2	Computer network Devices	11/12/2023	8-10	
3	CABLE CRIMPING	20/12/2023	11-13	
4	Install and Configure Wired and Wireless NIC and transfer files between systems in LAN and Wireless LAN.	03/01/2024	14-15	
5	IP Address and MAC Address of NIC	03/01/2024	16-18	
6	Static and Dynamic IP Address	03/01/2024	19-20	
7	Peer to Peer Network	24/01/2024	21-22	
8	Local Area Network (LAN)	24/01/2024	23-24	
9	Basic Network Configuration Commands	24/01/2024	25	
10	Wireless Network	15/02/2024	26-28	
11	DHCP	15/02/2024	29-30	
12	ROUTING	12/02/2024	31-32	
13	Network Simulator	12/02/2024	33-34	
14	Network Configuration	28/02/2024	35-38	
15	Virtual Local Area Network (VLAN)	13/03/2024	39-42	
16	Configuring and Verifying VLANs in Cisco	13/03/2024	43-46	

N. S. S. POLYTECHNIC COLLEGE

PANDALAM

Vision

To impart quality technical education and develop skilled technicians with social commitment.

Mission

- Provide skill oriented training through institute-industry interaction to meet quality technical education.
- To strengthen academic practices in terms of faculty training.
- Enable the students to excel in their academic pursuits through life long learning.
- Inculcate the values of ethics and social responsibilities to develop as a nation builder.

N. S. S. POLYTECHNIC COLLEGE

PANDALAM

DEPARTMENT OF COMPUTER ENGINEERING

Vision

Transform young minds into socially responsible
Computer
Professionals through knowledge empowerment.

Mission

- Impart quality education.
- Provide adequate self-learning environment
- Adapt emerging technologies by industry – institute interaction.
- Extend platform for the development of personality traits.

Experiment NO: 1

Date : 08/12/2023

Computer network components

CO1: Identify and configure hardware components in a network

Aim: To familiarize and identify various networking cables and connectors.

Theory

Computer network

Computer network is a group of two or more computers that connect with each other to share a resource. Sharing of devices and resources is the purpose of computer network. You can share printers, fax machines, scanners, network connection, local drives, copiers and other resources.

In computer network technology, there are several types of networks that range from simple to complex level. However, in any case in order to connect computers with each other or to the existing network or planning to install from scratch, the required devices and rules (protocols) are mostly the same.

Cables and connectors

Cable is one way of transmission media which can transmit communication signals. The wired network typology uses special type of cable to connect computers on a network. Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

There are several kinds of cables. They are:

- Twisted Pair Cable

 - Unshielded Twisted Pair (UTP) Cable

 - Shielded Twisted Pair (STP) Cable

- Coaxial Cable
- Fiber Optic Cable

Twisted pair

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks (See figure 1).

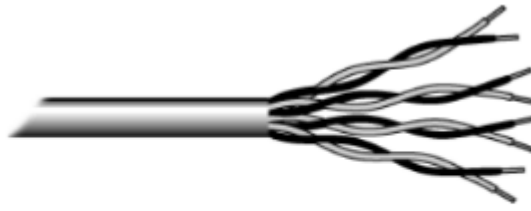


Figure 1: Unshielded twisted pair

The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated six categories of wire (additional categories are emerging).

Table 1: Categories of Unshielded Twisted Pair

Category	Speed	Use
1	1 Mbps	Voice Only (Telephone Wire)
2	4 Mbps	LocalTalk & Telephone (Rarely used)
3	16 Mbps	10BaseT Ethernet
4	20 Mbps	Token Ring (Rarely used)
5	100 Mbps (2 pair)	100BaseT Ethernet
	1000 Mbps (4 pair)	Gigabit Ethernet
5e	1,000 Mbps	Gigabit Ethernet
6	10,000 Mbps	Gigabit Ethernet

Unshielded Twisted Pair Connector:

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector (See figure 2). A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.



Figure 2: RJ-45 connector

Shielded Twisted Pair (STP) Cable

Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.). If you must place cable in environments with lots of potential interference, or if you must place cable in extremely sensitive environments that may be susceptible to the electrical current in the UTP, shielded twisted pair may be the solution. Shielded cables can also help to extend the maximum distance of the cables.

Shielded twisted pair cable is available in three different configurations:

1. Each pair of wires is individually shielded with foil.
2. There is a foil or braid shield inside the jacket covering all wires (as a group).
3. There is a shield around each individual pair, as well as around the entire group of wires (referred to as double shield twisted pair).

Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield (See figure 3). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.



Figure 3: Coaxial cable

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin.

Fiber-optic cable

It is a high-speed cable which transmits data using light beams through a glass bound fibers. Fiber-optic cable is high data transmission cable comparing to the other cable types. But the cost of fiber optics is very expensive which can only be purchased and installed on governmental level.



Result:

Various types of networking cables and connectors are identified and studied.

Experiment NO: 2

Date : 11/12/2023

Computer network Devices

CO1: Identify and configure hardware components in a network

Aim: To familiarize and identify various networking devices.

Theory

Computer network devices

Computer network devices include the major parts that are needed to install a network both at the office and home level. These hardware components include **Hub, Switch, NIC** (network interface card), **router and wireless router**.

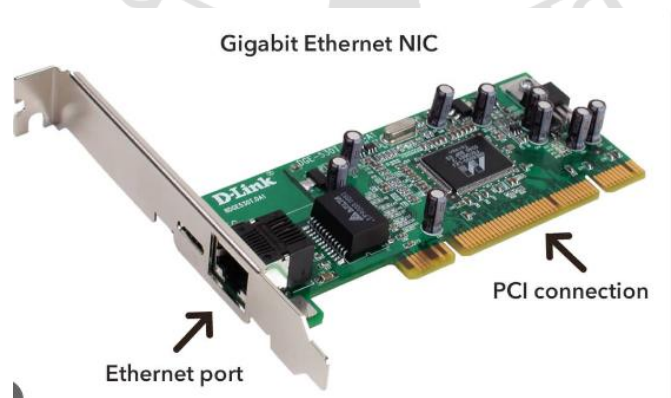
Major computer network devices

Computer network requires the following devices :-

- Network Interface Card (NIC)
- Hub
- Switches
- Router
- wireless router

1. Network Interface Card

Network adapter is a device that enables a computer to talk with other computer/network. Using unique **hardware addresses (MAC address)** encoded on the card chip, the data-link protocol employs these addresses to discover other systems on the network so that it can transfer data to the right destination.



There are **two types of network cards: wired and wireless**. The wired NIC uses cables and connectors as a medium to transfer data, whereas in the wireless card, the connection is made using Conclusion

antenna that employs radio wave technology. All modern laptop computers incorporated wireless NIC in addition to the wired adapter.

Network Card Speed

Network Interface card, one of the main computer network components, comes with different speeds, 10Mbps, 100Mbps, and 1000Mbps, so on. Recent standard **network cards built with Gigabit** (1000Mbps) connection speed. It also supports to connect slower speeds such as 10Mbps and 100Mbps. However, the speed of the card depends on your LAN speed.

For example, if you have a switch that supports up to 100Mbps, your NIC will also transfer a data with this same speed even though your computer NIC has still the capability to transfer data at 1000Mbps (1Gbps). In modern computers, network adapter is integrated with a computer motherboard. However if you want advanced and fast Ethernet card, you may buy and install on your computer using the **PCI slot** found on the motherboard (desktop) and **ExpressCard slots** on laptop .

2. Hub

Hub is a device that splits a network connection into multiple computers. It is like a distribution center. When a computer request information from a network or a specific computer, it sends the request to the hub through a cable. The hub will receive the request and transmit it to the entire network. Each computer in the network should then figure out whether the broadcast data is for them or not.



Currently Hubs are becoming obsolete and replaced by more advanced communication devices such as **Switches and Routers**.

3. Switch

Switch is a telecommunication device grouped as one of computer network components. Switch is like a Hub but built in with advanced features. It uses **physical device addresses** in each incoming messages so that it can deliver the message to the right destination or port. Like Hub, switch don't broadcast the received message to entire network, rather before sending it checks to which system or port should the message be sent. In other words switch connects the source and destination directly which increases the speed of the network. Both switch and hub have common features: Multiple RJ-45 ports, power supply and connection lights.



4. Router

When we talk about computer network components, the other device that used to connect a LAN with an internet connection is called Router. When you have two distinct networks (LANs) or want to share a single internet connection to multiple computers, we use a Router. In most cases, recent routers also include a switch which in other words can be used as a switch. You don't need to buy both switch and router, particularly if you are installing small business and home networks.

There are two types of Router: wired and wireless. The choice depends on your physical office/home setting, speed and cost.

Wired Router

A wired router connects directly to computers through wired connections. They usually have a port that connects to the modem to communicate with the internet. Another port — or ports — allows the wired router to connect to computers and other devices to distribute information.



Wireless Router

A wireless router or Wi-Fi router is a device that performs the functions of a router and also includes the functions of a wireless access point. It is used to provide access to the Internet or a private computer network. Depending on the manufacturer and model, it can function in a wired local area network, in a wireless-only LAN, or in a mixed wired and wireless network.



Result: Various network devices are identified and studied.

Experiment NO: 3

Date : 20/12/2023

CABLE CRIMPING

CO1: Identify and configure hardware components in a network

Aim:

To do the following

- a) Cable Crimping
- b) Standard Cabling
- c) Cross Cabling
- d) IO connector crimping
- e) Testing the crimped cable using a cable tester

Apparatus/Tools/Equipments/Components:

RJ-45 connector, IO Connector, Crimping Tool, Twisted pair Cable, Cable Tester.

Principle:

Standard Cabling:

1. 10BaseT and 100BaseT are most common mode of LAN. You can use UTP category-5 cable for both modes.
2. A straight cable is used to connect a computer to a hub

TIA/EIA-568 T568A termination				TIA/EIA-568 T568B termination			
Pin	Pair	Wire ^[a]	Color	Pin	Pair	Wire ^[a]	Color
1	3	tip	 white/green	1	2	tip	 white/orange
2	3	ring	 green	2	2	ring	 orange
3	2	tip	 white/orange	3	3	tip	 white/green
4	1	ring	 blue	4	1	ring	 blue
5	1	tip	 white/blue	5	1	tip	 white/blue
6	2	ring	 orange	6	3	ring	 green
7	4	tip	 white/brown	7	4	tip	 white/brown
8	4	ring	 brown	8	4	ring	 brown

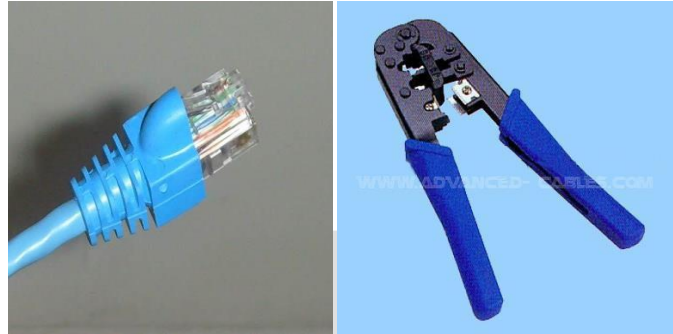
Cross Cabling:

A cross cable is used to connect 2 computers directly (with ONLY the UTP cable). It is also used then you connect 2 hubs with a normal port on both hubs.

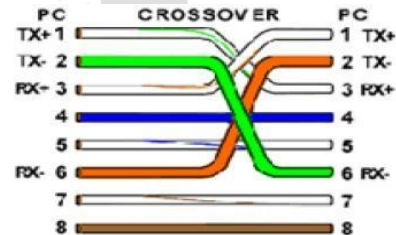
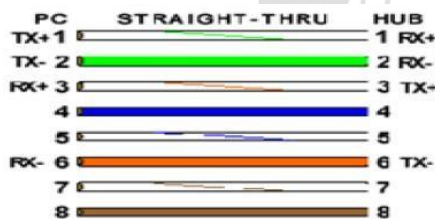
Procedure:

Cable Crimping steps:

1. Remove the outmost vinyl shield for 12mm at one end of the cable (we call this side A-side).
2. Arrange the metal wires in parallel
3. Insert the metal wires into RJ45 connector on keeping the metal wire arrangement.

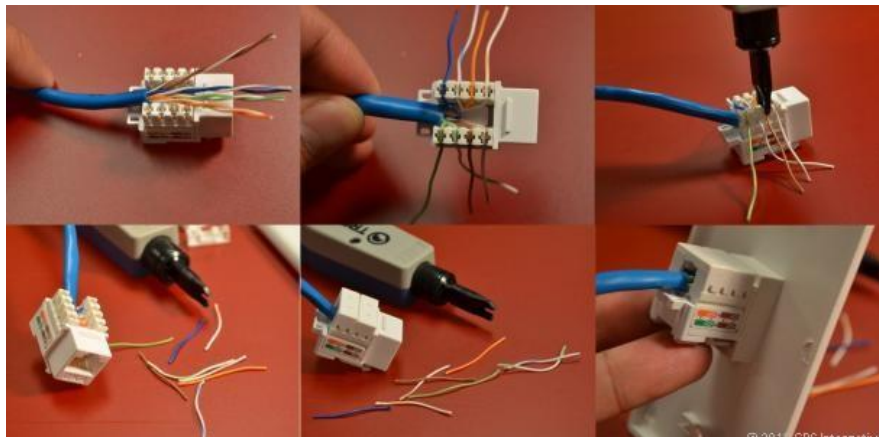


4. Set the RJ45 connector (with the cable) on the pliers, and squeeze it tightly.
5. Make the other side of the cable (we call this side B-side) in the same way.
6. After you made it, you don't need to take care of the direction of the cable.



IO connector crimping: Run the full length of Ethernet cable in place, from endpoint to endpoint, making sure to leave excess.

At one end, cut the wire to length leaving enough length to work, but not too much excess. Strip off about 2 inches of the Ethernet cable sheath.



Align each of the colored wires according to the layout of the jack. Use the punch down tool to insert each wire into the jack.

Repeat the above steps for the second RJ45 jack.

Testing the crimped cable using a cable tester:

Step 1 : Skin off the cable jacket 3.0 cm long cable stripper up to cable

Step 2: Untwist each pair and straighten each wire 190 0 1.5 cm long.

Step 3 : Cut all the wires

Step 4 : Insert the wires into the RJ45 connector right white orange left brown the pins facing up

Step 5 : Place the connector into a crimping tool, and squeeze hard so that the handle reaches its fullswing.

Step 6: Use a cable tester to test for proper continuity



Result:

Cable Crimping, Standard Cabling and Cross Cabling, IO connector crimping and testing the crimped cable using a cable tester are done successfully

Experiment NO: 4

Date : 03/01/2024

Install and Configure Wired and Wireless NIC and transfer files between systems in LAN and Wireless LAN.

CO1: Identify and configure hardware components in a network

Aim: To Install and Configure Wired and Wireless (remotely) NIC and transfer files between systems in LAN and Wireless LAN between two system in a LAN.

Principle:

NICs (Network Interface Card): Network Interface Card, or NIC is a hardware card installed in a computer so it can communicate on a network. The network adapter provides one or more ports for the network cable to connect to, and it transmits and receives data onto the network cable.

Wireless LAN card:

Every networked computer must also have a network adapter driver, which controls the network adapter. Each network adapter driver is configured to run with a certain type of network adapter.

Procedure:

Install the network card:

Disconnect all cables connected to the computer and open the case. Locate an available PCI slot (white slots) and insert the network card and secure the card with the screw that came with it. Once the adapter has been installed and secured close the computer case, connect all the cables and turn it on.

After installing the adapter driver it should be working find, now let's configure the card for use on a network.

Click on the Start button and select Settings then Control Panel. Double click on the System icon

Click on the Hardware tab.

Click on Device Manager.

You will see a list of devices installed in your computer.

If necessary, click on the + sign next to Network Adapters to expand the list.

Ensure that there is no yellow exclamation mark (!) next to the Network Adapter. This indicates a possible problem with the card or configuration.

Double click on your network driver (e.g. NE2000 Compatible). In the Device Status box you should see the message:

This Device is working correctly.

If you do not see this message or if there is no Network Adapter displayed, then your Ethernet card will

probably need configuring.

Result:

Installation and configuration of Wired and Wireless (remotely) NIC and transfer files between systems in LAN and Wireless LAN between two systems in a LAN have been done successfully.



Experiment NO: 5

Date : 03/01/2024

IP Address and MAC Address of NIC

CO2: Build Local Area Networks

Aim: To familiarise the IP address and Mac Address of NIC

Principle:

IP(Internet Protocol): It is the unique identifying number assigned to every device connected to the internet. An IP address definition is a numeric label assigned to devices that use the internet to communicate.

MAC Address: It is sometimes referred to as a hardware or physical address, is a unique, 12-character alphanumeric attribute that is used to identify individual electronic devices on a network.

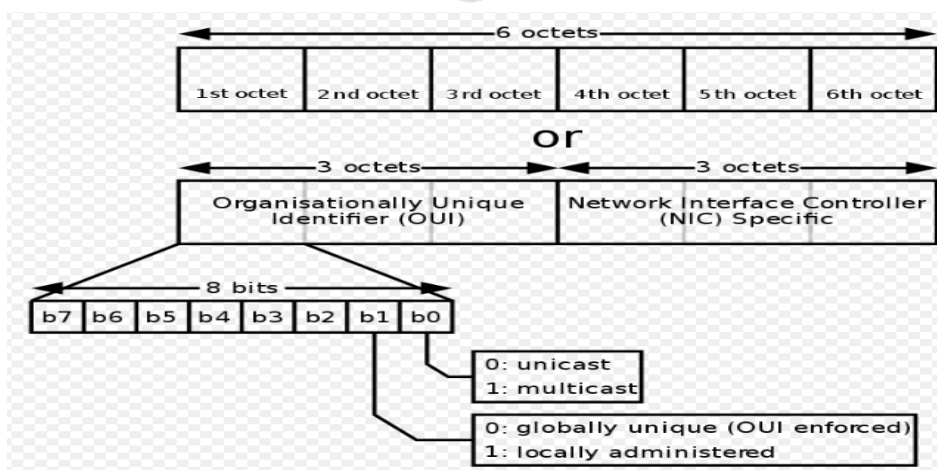
There are three possible types of communication within a Local Area Network (LAN) as well as in the Internet. – Unicast – message sent from one source to one destination. – Multicast – message sent from one source to multiple destinations (receivers). – Broadcast – message sent from one source to all the other hosts in the network.

Unless every pair of hosts in the LAN/Internet are connected directly to each other, we need to have some addressing scheme to uniquely identify the receiving machine as well as the sending machine.

Media Access Control (MAC) Addressing Scheme

The MAC (Media Access Control) Address is a physical address, assigned to the Network Interface Card (NIC). The NIC of a host is typically configured with the unicast MAC address for each of its interfaces as well as the multicast addresses to which the host has subscribed to.

IEEE assigns a block of addresses to each vendor – and allows the vendor to assign a unique value to each device – there is a 3-byte Organizationally Unique ID (OUI) . OUI identifies the equipment vendor ,a 3-byte block that identifies a particular NIC. An example of a MAC address is: 00-B0-D0-63-C2-26.



IP (Internet Protocol) Address :

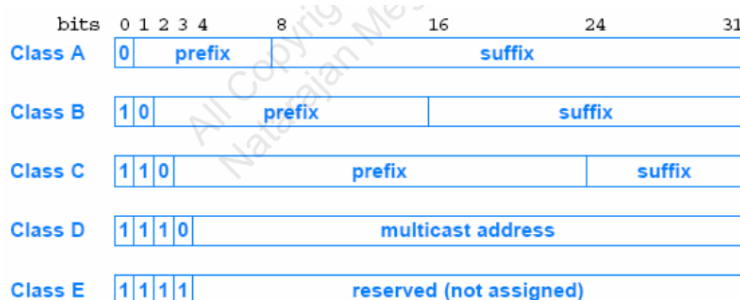
The MAC address does not change even if we move around our host to another network/LAN in the Internet. We need a logical addressing scheme that can be used to uniquely identify a machine/NIC in the Internet, depending on the network to which the machine/NIC is attached to. An IP address is a unique address that is used to identify computers or nodes on the internet.

Types of IP Address

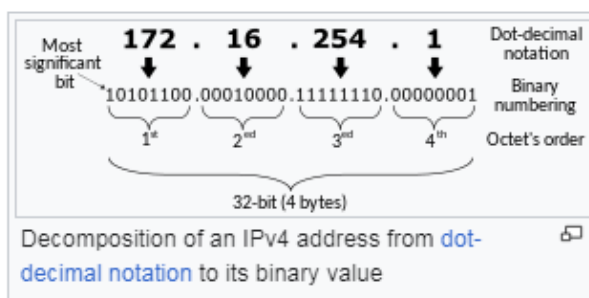
- 1. IPv4:** Internet Protocol version 4. It consists of 4 numbers separated by the dots. Each number can be from 0-255 in decimal numbers. But computers do not understand decimal numbers, they instead change them to binary numbers which are only 0 and 1. Therefore, in binary, this (0-255) range can be written as (00000000 – 11111111). Since each number N can be represented by a group of 8-digit binary digits. So, a whole IPv4 binary address can be represented by 32-bits of binary digits. In IPv4, a unique sequence of bits is assigned to a computer, so a total of (2^{32}) devices approximately = 4,294,967,296 can be assigned with IPv4.

Classes of IPv4 Address:

The first four bits of an IP address determined the class to which the address belonged



IPv4 addresses are usually represented in dot-decimal notation, consisting of four decimal numbers, each ranging from 0 to 255, separated by dots, e.g., 192.0.2.1. Each part represents a group of 8 bits (an octet) of the address.



Range of IP Addresses:

IP Class	Address Range	Maximum number of networks
Class A	1-126	126 (2^7-2)
Class B	128-191	16384
Class C	192-223	2097152
Class D	224-239	Reserve for multitasking
Class E	240-254	Reserved for Research and development

2. IPv6: But, there is a problem with the IPv4 address. With IPv4, we can connect only 4 billion devices uniquely, and apparently, there are much more devices in the world to be connected to the internet. So, gradually we are making our way to **IPv6 Address** which is a 128-bit IP address. In human-friendly form, IPv6 is written as a group of 8 hexadecimal numbers separated with colons(:). But in the computer-friendly form, it can be written as 128 bits of 0s and 1s. Since, a unique sequence of binary digits is given to computers, smartphones, and other devices to be connected to the internet. So, via IPv6 a total of (2^{128}) devices can be assigned with unique addresses which are actually more than enough for upcoming future generations.

IPv6 can be written as:

2011:0bd9:75c5:0000:0000:6b3e:0170:8394

Procedure:

Display IP Address:

Open the command prompt
Type the command: **ipconfig**

Display MAC Address:

Open the command prompt
Type the command: **ipconfig/all**

Result:

Familiarised the IP address and Mac Address of NIC.

Experiment NO: 6

Date : 03/01/2024

Static and Dynamic IP Address

CO2: Build Local Area Networks

Aim: To familiarise Static and Dynamic IP Address

Principle:

ISPs (Internet service providers) assign an IP address to each device on their network. The IP address can be static or dynamic.

Static IP Address: A static IP address is an IP address that doesn't change over time. A static IP address is a 32 bit number assigned to a computer as an address on the internet. This number is in the form of a dotted quad and is typically provided by an internet service provider (ISP). Static IP address requires you to configure your router. If you have a web server, FTP server, or other Internet resource that must have an address that cannot change, you can get a static IP address from your ISP. A static IP address is usually more expensive than a dynamic IP address, and some ISPs do not supply static IP addresses. You must configure a static IP address manually.

Dynamic IP Address: A dynamic IP address is a temporary address for devices connected to a network that continually changes over time. If you have a residential cable or DSL service, you most likely have a dynamic IP address. Internet Service Providers (ISPs) assign customers with dynamic IP addresses because they are cost effective. A dynamic IP address is an IP address that an ISP lets you use temporarily. If a dynamic address is not in use, it can be automatically assigned to a different device. Dynamic IP addresses are assigned using either DHCP (Dynamic Host Configuration Protocol) or PPPoE (Point-to-Point Protocol over Ethernet).

Procedure:

Set Static IP Address:

1. Click Start Menu > Control Panel > Network and Sharing Center or Network and Internet > Network and Sharing Center.
2. Click Change adapter settings.
3. Right-click on Wi-Fi or Local Area Connection.
4. Click Properties.
5. Select Internet Protocol Version 4 (TCP/IPv4).
6. Click Properties.
7. Select Use the following IP address.
8. Enter the IP address, Subnet mask, Default gateway, and DNS server.
9. Click OK.

Show Dynamic IP Address:

1. Right-click the Start button.
2. Type Command Prompt, then press enter.
3. Click Command Prompt.
4. Type ipconfig /all, then press enter.

Result:

Familiarised Static IP address and Dynamic IP Address.



Experiment NO: 7

Date : 24/01/2024

Peer to Peer Network

CO2: Build Local Area Networks

Aim: To establish Peer to Peer network

Principle:

All PCs must have networking hardware already installed. Examine the back of the PC for an RJ45 port (it looks like a port for a typical phone but is wider with eight contacts).

If you have more than two PCs, you will need at least one multi-port sharing device like a hub, switch, or router with enough ports to support all your PCs.

If you are only networking two PCs, all you need is one crossover cable. You do not need a hub, switch, or router.

Multi-port sharing devices that work for creating small networks:

Hubs are usually the least expensive of the devices. Hubs simply repeat the data flow out to the other lines. These work good in small networks.

Switches are like hubs but filter IP addresses to increase data flow in larger networks.

Routers become necessary when networking over 254 computers. A router can also be used to share one IP address with several other PCs.

The network link between PCs can only be as fast as the slowest device in the link. Try to use all networking devices with the same speed rating for optimal performance (this includes cables).

Try to keep hubs, switches, and routers accessible.

Some hubs, switches, and routers, require the last port be used only when the cascade port is not already in use. Do not connect a network cable for a PC into the cascade port.

Procedure:

Stepping into Peer-to-Peer:

1. Click Start, Control Panel, Network Connections.
2. Select Set up a home or small office network link under Network Tasks On the left-side.
3. The Welcome to the Network Setup Wizard screen on the Network Setup Wizard appears. Click Next.
4. The Before you continue screen appears, listing the steps that will be completed. Click the checklist for creating a network link.
5. Close the Steps for creating a home or small office network screen.
6. Click Next on the Before you continue screen.
7. connect the network interfaces click Next.
The Select a connection method screen appears. Here you will select from three connection
8. options Make your selection and click Next.

9. On the Select your Internet connection screen, select the network connection that relates to the Internet under Connections and click Next. You must make a selection or the Next button will remain grayed out.
10. The next screen, Your computer has multiple connections, is very important for both Internet connectivity and firewall issues. It's here you begin to assist the wizard by defining the "inside" network adapter (local area network) and the "wild-side" network adapter (Internet connection). Make the appropriate selection and click Next. In my case, I selected Let me choose the connections to my network
11. Because of the selection I made in, the Select the connections to bridge appears. Make the connection selection and click Next.
12. Complete the Computer description and Computer name fields on the Give this computer
13. Complete the Workgroup name field on the Name your network screen And click next.
14. Review your settings on the Ready to apply your network settings Screen and click next.
15. Click Finish after the configuration process is completed.

Result:

Peer to Peer network connection is established.

Experiment NO: 8

Date : 24/01/2024

Local Area Network (LAN)

CO2: Build Local Area Networks

Aim: To establish a local area network (LAN)

Principle:

A local area network (LAN) consists of a series of computers linked together to form a network in a circumscribed location. The computers in a LAN connect to each other via TCP/IP ethernet or Wi-Fi. A LAN is normally exclusive to an organization, such as a school, office.

Procedure:

On the host computer

On the host computer, follow these steps to share the Internet connection:

1. Log on to the host computer as Administrator or as Owner.
2. Click **Start**, and then click **Control Panel**.
3. Click Network and Internet Connections.
4. Click **Network Connections**.
5. Right-click the connection that you use to connect to the Internet. For example, if you connect to the Internet by using a modem, right-click the connection that you want under Dial-up / other network available.
6. Click **Properties**.
7. Click the **Advanced** tab.
8. Under **Internet Connection Sharing**, select the **Allow other network users to connect through this computer's Internet connection** check box.
9. If you are sharing a dial-up Internet connection, select the **Establish a dial-up connection whenever a computer on my network attempts to access the Internet** check box if you want to permit your computer to automatically connect to the Internet.
10. Click **OK**. You receive the following message:

When Internet Connection Sharing is enabled, your LAN adapter will be set to use IP address 192.168.0.1. Your computer may lose connectivity with other computers on your network. If these other computers have static IP addresses, it is a good idea to set them to obtain their IP addresses automatically. Are you sure you want to enable Internet Connection Sharing?

11. Click **Yes**.

The connection to the Internet is shared to other computers on the local area network (LAN). The network adapter that is connected to the LAN is configured with a static IP address of 192.168.0.1 and a subnet mask of 255.255.255.0

On the client computer

To connect to the Internet by using the shared connection, you must confirm the LAN adapter IP configuration, and then configure the client computer. To confirm the LAN adapter IP configuration, follow these steps:

1. Log on to the client computer as Administrator or as Owner.
2. Click **Start**, and then click **Control Panel**.
3. Click Network and Internet Connections.
4. Click **Network Connections**.
5. Right-click **Local Area Connection** and then click **Properties**.
6. Click the **General** tab, click **Internet Protocol (TCP/IP)** in the connection uses the following items list, and then click **Properties**.
7. In the **Internet Protocol (TCP/IP) Properties** dialog box, click **Obtain an IP address automatically** (if it is not already selected), and then click **OK**.
Note: You can also assign a unique static IP address in the range of 192.168.0.2 to 192.168.0.254. For example, you can assign the following static IP address, subnet mask, and default gateway:
 8. IP Address 192.168.31.202
 9. Subnet mask 255.255.255.0
 10. Default gateway 192.168.31.1
11. In the **Local Area Connection Properties** dialog box, click **OK**.
12. Quit Control Panel.

Result:

The computers are Connected in Local Area Network.

Experiment NO: 9

Date : 24/01/2024

Basic Network Configuration Commands

CO2 : Build Local Area Networks

Aim: To make use of basic network configuration commands like ping, ifconfig, traceroute etc

Procedure:

Configure Internet connection and use IPCONFIG, PING:

1. Open Command Prompt, and then type ipconfig. From the display of the ipconfig command, ensure that the network adapter for the TCP/IP configuration you are testing is not in a Media disconnected state.
2. At the command prompt, ping the loopback address by typing ping 127.0.0.1.
3. Ping the IP address of the computer.
4. Ping the IP address of the default gateway. If the ping command fails, verify that the default gateway IP address is correct and that the gateway (router) is operational.
5. Ping the IP address of a remote host (a host that is on a different subnet).
If the ping command fails, verify that the remote host IP address is correct, that the remote host is operational, and that all of the gateways (routers) between this computer and the remote host are operational.
6. Ping the IP address of the DNS server.
If the ping command fails, verify that the DNS server IP address is correct that the DNS server is operational, and that all of the gateways (routers) between this computer and the DNS server are operational.

Tracer to debug the network issues.

Tracer network:

Open Command Prompt, and type the following:

tracert host_name

Or

tracert ip_address

where host_name or ip_address is the host name or IP address, respectively, of the remote computer.

If you do not want the traceroute command to resolve and display the names of all routers in the path, use the -d parameter. This expedites the display of the path.

Result:

Thus the Configure Internet connection and use IPCONFIG, PING / Tracer to establish interconnection between systems have been done successful

Experiment NO: 10

Date : 15/02/2024

Wireless Network

CO2 : Build Local Area Networks

Aim: To study the implementation of WLAN and access point configuration.

Principle:

A wireless local area network (WLAN) is a wireless computer network that links two or more devices using wireless communication within a limited area such as a home, school, computer laboratory, or office building. This gives users the ability to move around within a local coverage area and yet still be connected to the network. Through a gateway, a WLAN can also provide a connection to the wider Internet. WLANs are based on IEEE 802.11 standards and are marketed under the Wi-Fi brand name. Wireless LANs have become popular for use in the home, due to their ease of installation and use. They are also popular in commercial properties that offer wireless access to their customers.

Architecture

Stations: - All components that can connect into a wireless medium in a network are referred to as stations (STA). All stations are equipped with wireless network interface controllers (WNICs). Wireless stations fall into two categories: Wireless Access Points, and Clients. Access Points (Aps), normally wireless routers, are base stations for the wireless network. They transmit and receive radio frequencies for wireless enabled devices to communicate with. Wireless clients can be mobile devices such as laptops, personal digital assistants, IP phones and other smartphones, or non-portable devices such as desktop computers and workstations that are equipped with a wireless network interface.

Types of wireless LANs

The IEEE 802.11 has two basic modes of operation: Infrastructure and Ad Hoc mode. In Ad Hoc mode, mobile units transmit directly peer-to-peer. In Infrastructure mode, mobile units communicate through an Access Point that serves as a bridge to other networks (such as Internet or LAN). Most Wi-Fi networks are deployed in infrastructure mode.

In infrastructure mode, a base station acts as a wireless access point hub, and nodes communicate through the hub. The hub usually, but not always, has a wired or fibre network connection, and may have permanent wireless connections to other nodes. Wireless access points are usually fixed, and provide service to their client nodes within range. Wireless clients, such as laptops, smartphones etc. connect to the access point to join the network.

Sometimes a network will have a multiple access points, with the same 'SSID' and security arrangement. In that case connecting to any access point on that network joins the client to the network. In that case, the client software will try to choose the access point to try to give the best service, such as the access point with the strongest signal.

Service set identifier (SSID)

In addition to running on different channels, multiple Wi-Fi networks can share channels. A service set is the set of all the devices associated with a particular Wi-Fi network. The service set can be local, independent, extended or mesh. Each service set has an associated identifier, the 32-byte Service Set Identifier (SSID), which identifies the particular network. The SSID is configured within the devices

that are considered part of the network, and it is transmitted in the packets. Receivers ignore wireless packets from networks with a different SSID

802.11 Network bearer standards

All the 802.11 Wi-Fi standards operate within the ISM (Industrial, Scientific and Medical) frequency bands. These are shared by a variety of other users, but no license is required for operation within these frequencies. This makes them ideal for a general system for widespread use. There are a number of bearer standards that are in common use. These are the 802.11a, 802.11b, and 802.11g standards. The 802.11n standard is the latest providing raw data rates of up to 600 Mbps.

	802.11A	802.11B	802.11G	802.11N
Date of standard approval	July 1999	July 1999	June 2003	Oct 2009
Maximum data rate (Mbps)	54	11	54	~600
Modulation	OFDM	CCK or DSSS	CCK, DSSS, or OFDM	CCK, DSSS, or OFDM
RF Band (GHz)	5	2.4	2.4	2.4 or 5
Number of spatial streams	1	1	1	1, 2, 3, or 4
Channel width (MHz) nominal	20	20	20	20, or 40

Summary of major 802.11 Wi-Fi Standards

Since wireless communication uses a more open medium for communication in comparison to wired LANs, the 802.11 designers also included encryption mechanisms: Wired Equivalent Privacy (WEP, now insecure), Wi-Fi Protected Access (WPA, WPA2), to secure wireless computer networks. Many access points will also offer Wi-Fi Protected Setup, a quick (but now insecure) method of joining a new device to an encrypted network.

Procedure:

- Step 1 : Assign a valid IP address with same network portion of Access Point's IP address to a Laptop or Computer. If the IP address and user credentials of Access Point is unknown, then restore the default settings of Access Point by factory reset. (Or use the Vendor Software to access the Access Point). Connect the AP and Computer using straight through cable.
- Step 2 : Open browser and then type the IP address of the AP in the address bar to access the Web Interface of Access Point. It may ask for user credentials.
- Step 3 : Assign proper SSID and security features for the wireless. Make necessary changes in settings as per the network requirement.
- Step 4 : Prepare the wireless network interface card in computer by installing the proper drivers according to the operating system.

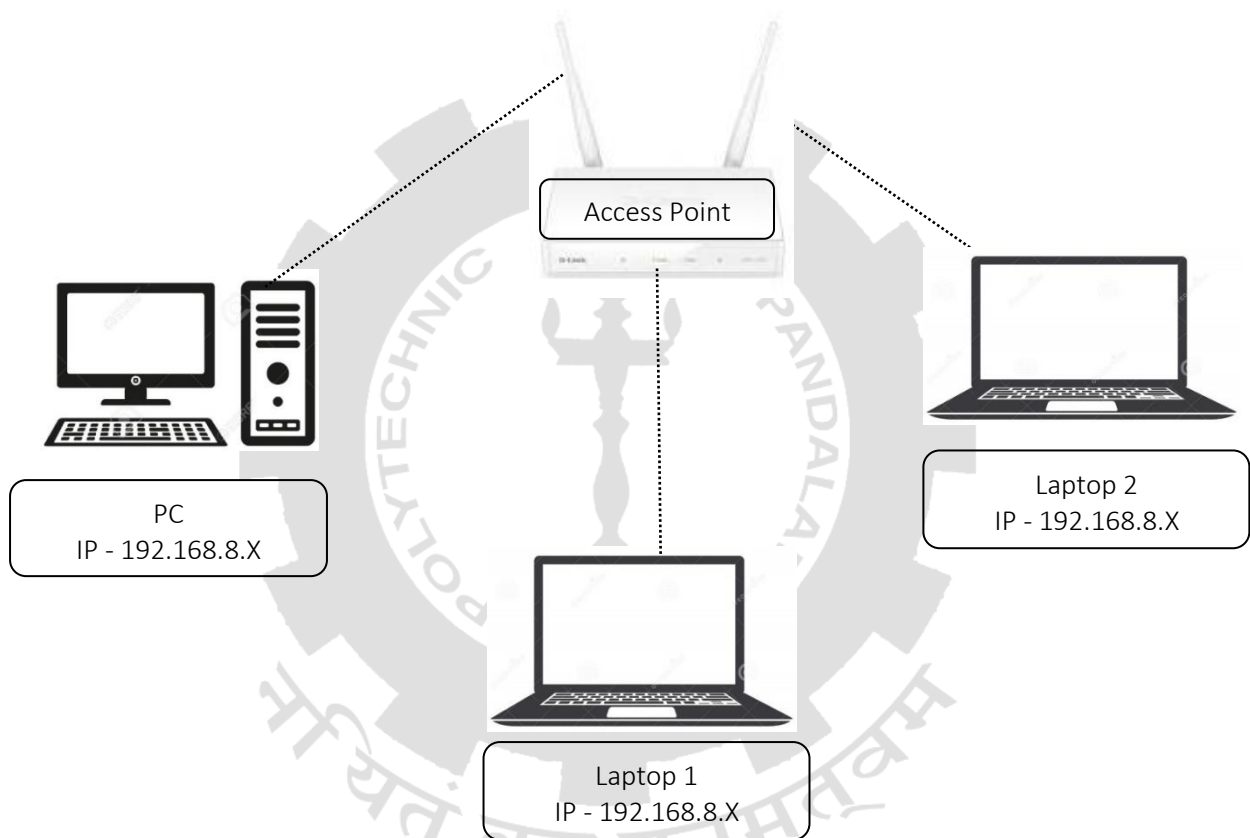
Step 5 : Assign valid Class C IPV4 addresses with same network portion to the computer and Laptops. For example 192.168.8.121 to the computer and 192.168.8.182 to the first Laptop so on.

Step 6 : Use OS utilities or WNIC vendor software to conduct a site survey to find the wireless network and connect to it. Wireless security features you made may ask for credentials and upon validation, node will hook to WLAN.

Step 7 : Ensure the connectivity using the ping command and verify the reply from the destination.

Result:

Wireless network implemented and connectivity established successfully.



Experiment NO: 11

Date : 15/02/2024

DHCP

CO3: Plan and Configure Routers.

Aim: To study the implementation of DHCP service.

Principle:

Dynamic Host Configuration Protocol (DHCP) Server is a service that automatically provides an IP address and other related configuration information such as the subnet mask, DNS server addresses and default gateway to a host in network. Dynamic Host Configuration Protocol (DHCP) is a protocol used by networked devices or clients to obtain the parameters necessary for operation in an Internet Protocol network. This protocol reduces system administration workload, allowing devices to be added to the network with little or no manual configurations. Dynamic Host Configuration Protocol is a way to administrator for network parameter assignment from a single DHCP server, or a group of DHCP servers arranged in a fault-tolerant manner. Even in small networks, Dynamic Host Configuration Protocol is useful because it can make it easy to add new machines to the local network.

As its name indicates, DHCP provides dynamic IP address assignment. What this means is that instead of having to rely on a specific IP address, a computer will be assigned one that is available from a subnet or "pool" that is assigned to the network. When DHCP assigns an IP address to a host, it actually leases the identifier to the host computer for a specific amount of time. This is called lease time of that DHCP server. The default lease is five days, but a network administrator should evaluate their own particular circumstances to determine an appropriate lease.

DHCP Terms and Definitions

Term	Definition
DHCP server	A computer running the DHCP Server service that holds information about available IP addresses and related configuration information as defined by the DHCP administrator and responds to requests from DHCP clients. That may be a server hardware, or a simple router in a small network.
DHCP client	A computer that gets its IP configuration information by using DHCP.
Scope or Pool	A range of IP addresses that are available to be leased to DHCP clients by the DHCP Server service.
Subnetting	The process of partitioning a single TCP/IP network into a number of separate network segments called subnets.
DHCP option	Configuration parameters that a DHCP server assigns to clients. Most DHCP options are predefined, based on optional parameters defined in

	Request for Comments (RFC) 2132, although extended options can be added by vendors or users.
Lease	The length of time for which a DHCP client can use a DHCP-assigned IP address configuration.
Reservation	A specific IP address within a scope permanently set aside for leased use by a specific DHCP client. Client reservations are made in the DHCP database using the DHCP snap-in and are based on a unique client device identifier for each reserved entry.
Exclusion/exclusion range	One or more IP addresses within a DHCP scope that are not allocated by the DHCP Server service. Exclusions ensure that the specified IP addresses will not be offered to clients by the DHCP server as part of the general address pool.
DHCP relay agent	Either a host or an IP router that listens for DHCP client messages being broadcast on a subnet and then forwards those DHCP messages directly to a configured DHCP server. The DHCP server sends DHCP response messages directly back to the DHCP relay agent, which then forwards them to the DHCP client. The DHCP administrator uses DHCP relay agents to centralize DHCP servers, avoiding the need for a DHCP server on each subnet.

When you connect to a network, your device is considered a client and the router is the server. In order to successfully connect to a network via DHCP, the following steps must take place.

- When a client detects it has connected to a DHCP server, it sends a DHCPDISCOVER request.
- The router either receives the request or redirects it to the appropriate DHCP server.
- If the server accepts the new device, it will send a DHCPOFFER message back to the client, which contains the client device's MAC address and the IP address being offered.
- The client returns a DHCPREQUEST message to the server, confirming it will use the IP address.
- Finally, the server responds with a DHCPACK acknowledgement message that confirms the client has been given access (or a "lease") for a certain amount of time.

Result:

DHCP server configured successfully and connects nodes to network.

Experiment NO: 12

Date : 21/02/2024

ROUTING

CO3: Plan and Configure Routers.

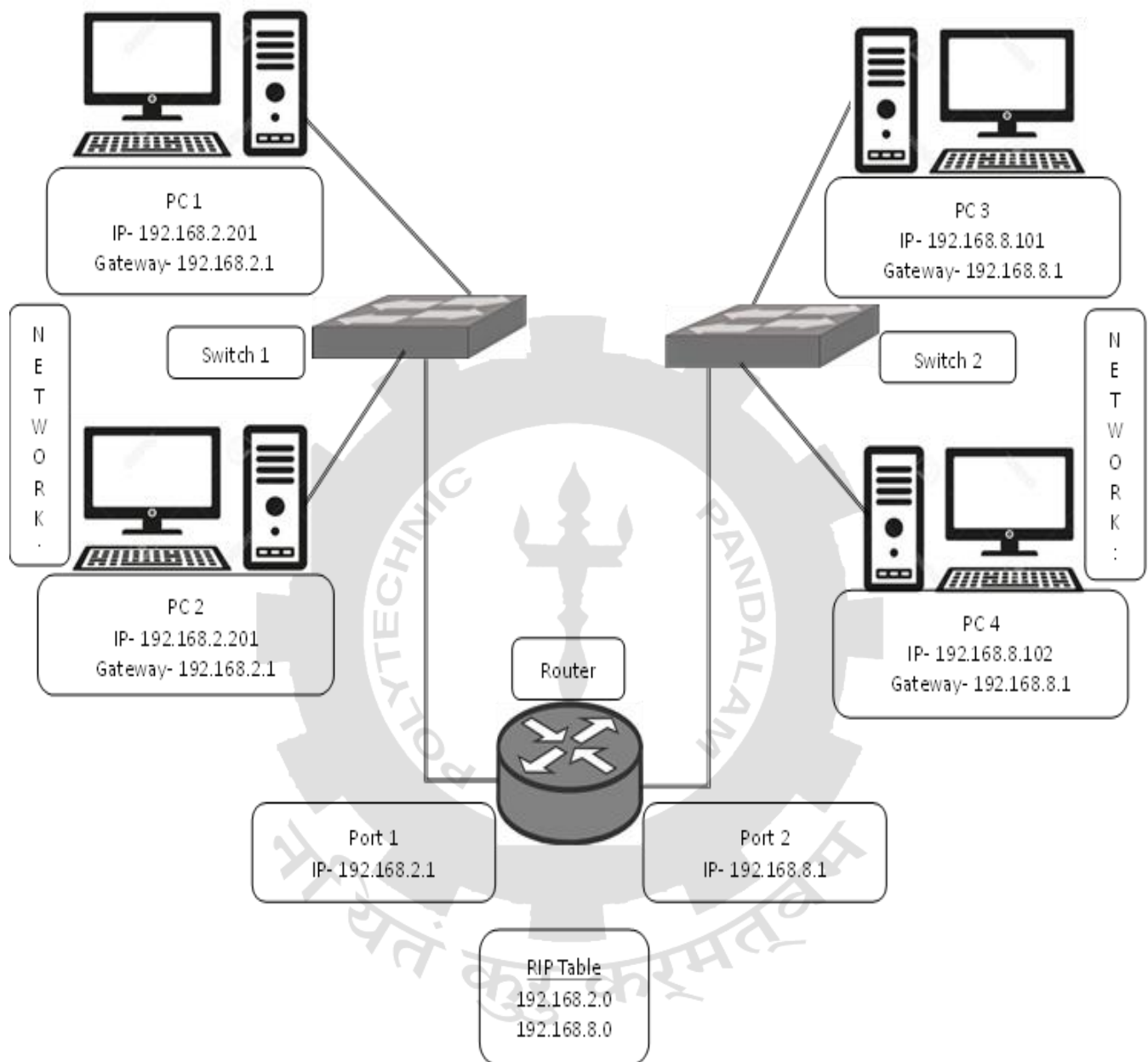
Aim: To study about the routing.

Principle:

Routing is the process of selecting a path for traffic in a network, or between or across multiple networks. Routing is usually performed by a dedicated device called a router. A router acts as a link between network, and it transmit data packets from one network to another. A routing protocol specifies how routers communicate with each other, distributing information that enables them to select routes between any two nodes on a computer network. Routing Information Protocol is a very common old routing protocol. Each RIP router maintains a routing table, which is a list of all the destinations (networks) it knows how to reach, along with the distance to that destination.

Procedure:

- Step 1 : Design the network topology. Open the Cisco Packet Tracer and create the required network by using network components like routers, switches and other devices.
- Step 2 : Complete the cabling by accessing the cable section in Packet Tracer and connect completely and correctly the cables between network in order to ensure the connectivity between the devices.
- Step 3 : Configure the IP address of the end devices such as PCs, Laptops.
- Step 4 : Configure the router by assigning the IP address to its ports and populating Routing Information Protocol (RIP) table with network address of each network.
- Step 5 : Configure the default gateway section with the address of the router port where that network is connected.
- Step 6 : Check the connectivity between networks by using ping command.



Result: Studied the concept of routing

Experiment NO: 13

Date : 21/02/2024

Network Simulator

CO3: Plan and Configure Routers.

Aim: To study about network simulator

Principle:

A network simulator is a software program that can predict the performance of a computer network or a wireless communication network. Since communication networks have become too complex for traditional analytical methods to provide an accurate understanding of system behavior, network simulators are used. In simulators, the computer network is modeled with devices, links, applications, etc., and the network performance is reported. Simulators come with support for the most popular technologies and networks in use today such as 5G, Internet of Things (IoT), Wireless LANs, mobile ad hoc networks, wireless sensor networks, vehicular ad hoc networks, cognitive radio networks, LTE.

Simulations

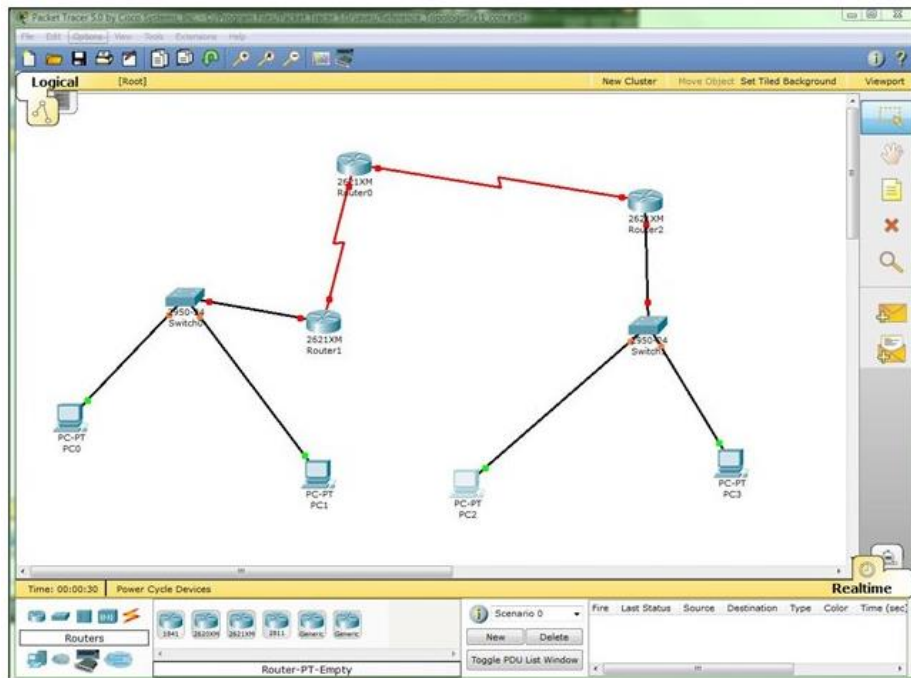
Most of the commercial simulators are GUI driven, while some network simulators are CLI driven. The network model/configuration describes the network (nodes, routers, switches, links) and the events (data transmissions, packet error, etc.). Output results would include network-level metrics, link metrics, device metrics etc. Further, drill down in terms of simulations trace files would also be available. Trace files log every packet, every event that occurred in the simulation and is used for analysis. Most network simulators use discrete event simulation, in which a list of pending "events" is stored, and those events are processed in order, with some events triggering future events—such as the event of the arrival of a packet at one node triggering the event of the arrival of that packet at a downstream node.

Packet Tracer

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

Packet Tracer allows students to design complex and large networks, which is often not feasible with physical hardware, due to costs. Packet Tracer is commonly used by NetAcad students, since it is available to them for free.[citation needed] However, due to functional limitations, it is intended by Cisco to be used only as a learning aid, not a replacement for Cisco routers and switches. The application itself only has a small number of features found within the actual hardware running a current Cisco IOS version. Thus, Packet Tracer is unsuitable for modelling production networks. It has a limited command set, meaning it is not possible to practice all of the IOS commands that might be required. Packet Tracer can be useful for understanding abstract networking concepts, such as the Enhanced Interior Gateway Routing Protocol by animating these elements in a visual form. Packet Tracer is also

Result: Understood the concept of network simulator.



Experiment NO: 14

Date : 28/02/2024

Network Configuration

CO3: Plan and Configure Routers.

Aim: Study of basic network command and Network configuration commands.

Apparatus (Software): Command Prompt And Packet Tracer.

Principle:

All commands related to Network configuration which includes how to switch to privilegemode and normal mode and how to configure router interface and how to save this configuration to flash memory or permanent memory.

This commands includes

- Configuring the Router commands
- General Commands to configure network
- Privileged Mode commands of a router
- Router Processes & Statistics
- IP Commands
- Other IP Commands e.g. show ip route etc.

Procedure:

To do this EXPERIMENT- follows these steps:

ping:

ping(8) sends an ICMP ECHO_REQUEST packet to the specified host. If the host responds, you get an ICMP packet back. Sound strange? Well, you can “ping” an IP address to see if a machine is alive. If there is no response, you know something is wrong.

Traceroute:

Tracert is a command which can show you the path a packet of information takes from your computer to one you specify. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded. In addition to this, it will tell you how long each 'hop' from router to router takes.

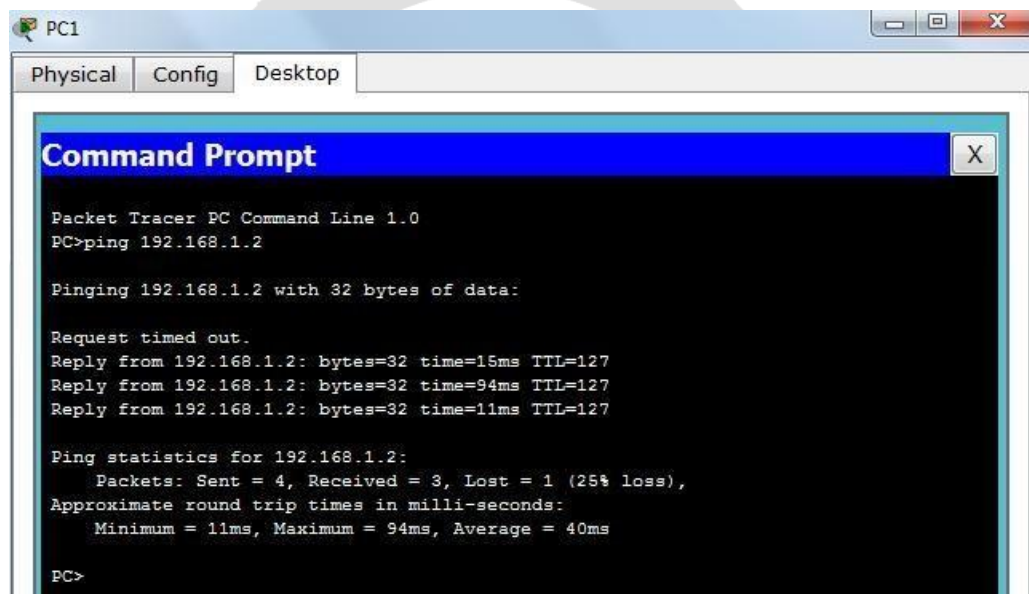
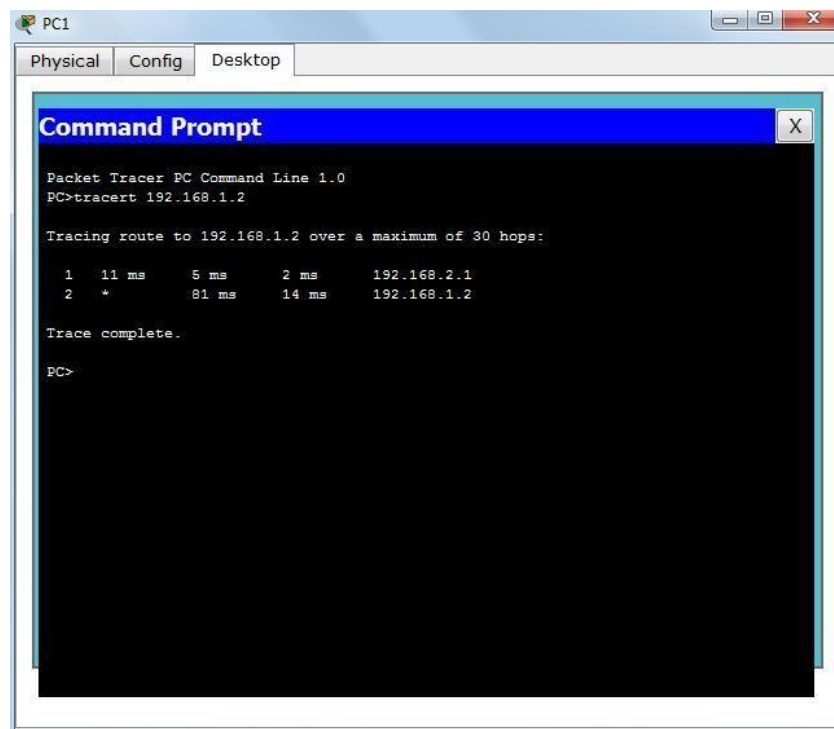
nslookup:

Displays information from Domain Name System (DNS) name servers.

NOTE :If you write the command as above it shows as default your pc's server name firstly.

pathping:

A better version of tracert that gives you statistics about packet lost and latency



Getting Help

In any command mode, you can get a list of available commands by entering a question mark (?).

Router>?

To obtain a list of commands that begin with a particular character sequence, type in those characters followed immediately by the question mark (?).

Router#co?

configure connect copy

To list keywords or arguments, enter a question mark in place of a keyword or argument. Include a space before the question mark.

Router#configure ?

memory Configure from NV memory network

Configure from a TFTP network hostterminal

Configure from the terminal

You can also abbreviate commands and keywords by entering just enough characters to make the command unique from other commands. For example, you can abbreviate the **show** command to **sh**.

Configuration Files

Any time you make changes to the router configuration, you must save the changes to memory because if you do not they will be lost if there is a system reload or power outage. There are two types of configuration files: the running (current operating) configuration and the startup configuration.

- Use the following privileged mode commands to work with configuration files. **configure terminal** – modify the running configuration manually from the terminal.
- **show running-config** – display the running configuration.
- **show startup-config** – display the startup configuration.
- **copy running-config startup-config** – copy the running configuration to the startup configuration.
- **copy startup-config running-config** – copy the startup configuration to the running configuration.
- **erase startup-config** – erase the startup configuration in NVRAM.
- **copy tftp running-config** – load a configuration file stored on a Trivial File Transfer Protocol (TFTP) server into the running configuration.
- **copy running-config tftp** – store the running configuration on a TFTP server.

IP Address Configuration

Take the following steps to configure the IP address of an interface.

Step 1: Enter privileged EXEC mode:

Router>**enable** password

Step 2: Enter the **configure terminal** command to enter global configuration mode. Router#**config terminal**

Step 3: Enter the **interface** type slot/port (for Cisco 7000 series) or **interface** type port (for Cisco 2500 series) to enter the interface configuration mode.

Example:

Router (config)#**interface ethernet 0/1**

Step 4: Enter the IP address and subnet mask of the interface using the **ip address** ipaddress subnetmask command.

Example,

Router (config-if)#**ip address 192.168.10.1 255.255.255.0**

Step 5: Exit the configuration mode by pressing Ctrl-Z Router(config-if)#**[Ctrl-Z]**

Result:

The network configuration done successfully.

Experiment NO: 15

Date : 13/03/2024

Virtual Local Area Network (VLAN)

CO4: Construct Virtual Local Area Network (VLAN)

Aim: Study the concept of Virtual Local Area network(VLAN)

Principle:

A virtual local area network (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2) In this context, virtual refers to a physical object recreated and altered by additional logic, within the local area network.

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 domains, inter Vlan routing is needed. Through VLAN, different small-size sub-networks are created which are comparatively easy to handle.

VLAN ranges:

- **VLAN 0, 4095:** These are reserved VLAN which cannot be seen or used.
- **VLAN 1:** It is the default VLAN of switches. By default, all switch ports are in VLAN. This VLAN can't be deleted or edit but can be used.
- **VLAN 2-1001:** This is a normal VLAN range. We can create, edit and delete these VLAN.
- **VLAN 1002-1005:** These are CISCO defaults for fddi and token rings. These VLAN can't be deleted.

Vlan 1006-4094: This is the extended range of Vlan.

Procedure:

Create a network in Cisco Packet Tracer with a switch and six PCs. Configure VLANs with VLAN ID 100 for students and VLAN ID 200 for faculty. Assign the first three PCs in each LAN to VLAN 100 and the remaining three PCs to VLAN 200. Test communication between VLANs to ensure isolation and connectivity.

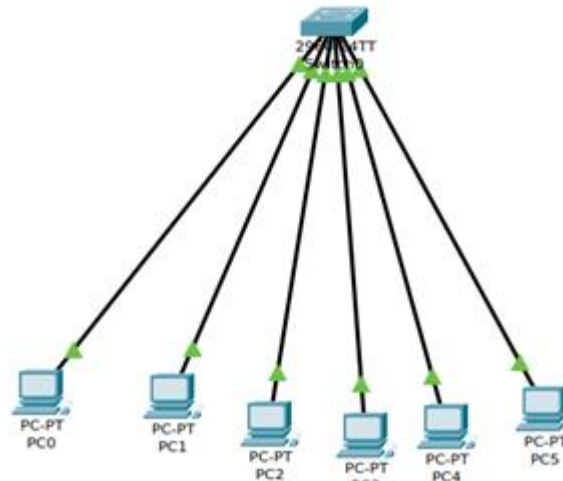
Step 1: Add a 2960-24TT Switch from the 'Switches' section onto the workspace.

Step 2: Drag and drop six PCs from the 'End Devices' section onto the workspace and assign IP addresses example:

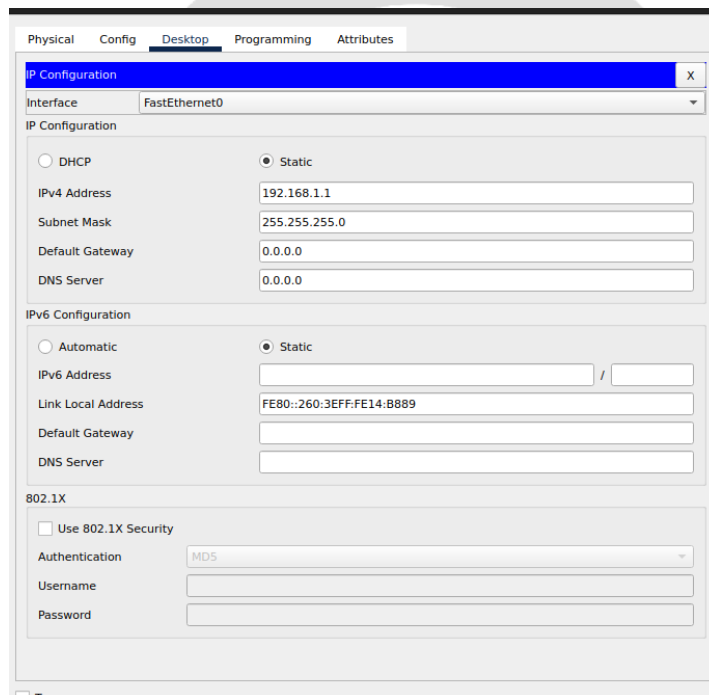
- PC1: 192.168.1.1

- PC2: 192.168.1.2

- PC3: 192.168.1.3



- PC4: 192.168.1.4
- PC5: 192.168.1.5
- PC6: 192.168.1.6



Ensure each PC has a unique IP address within the same subnet.

Step 3: Select the switch, then click on the 'Config' tab to access the Configuration view.

Step 4: Configuration in the Configuration view:

1. Click on the 'VLAN' option.
2. Click on 'Add VLAN' to create a new VLAN. Enter '100' as the VLAN ID and 'student' as the VLAN name. Click 'Apply'.
3. Repeat above step to create another VLAN with VLAN ID '200' and name it 'faculty'.

VLAN Configuration

VLAN Number	200
VLAN Name	faculty

VLAN No	VLAN Name
1	default
100	student
200	faculty
1002	fddi-default
1003	token-ring-default
1004	fddinet-default
1005	trnet-default

4. Click on 'FastEthernet0/1' port of the switch. In the 'VLAN' dropdown menu, select VLAN 100 (student).
5. Repeat step above step for ports 'FastEthernet0/2' and 'FastEthernet0/3' to assign them to VLAN 100 (student).
6. Click on 'FastEthernet0/4' port of the switch. In the 'VLAN' dropdown menu, select VLAN 200 (faculty).
7. Repeat step 4f for ports 'FastEthernet0/5' and 'FastEthernet0/6' to assign them to VLAN 200 (faculty).

FastEthernet0/1

Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input type="radio"/> Half Duplex <input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Access</div>	VLAN <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">100</div>
Tx Ring Limit	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">10</div>

8. Click 'Save' to apply the changes.

Step 6: Testing connectivity within the 'students' VLAN:

1. Open the command prompt of PC1 in the student network.
2. Ping the other PCs to ensure connectivity within the 'students' VLAN. PCs within the 'students' VLAN should respond to the pings.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Step 7: Testing isolation between VLANs:

1. Attempt to ping the PCs in the faculty network from PC1 in the student network.
2. PCs in the 'faculty' VLAN should not respond to the pings.

```
C:\>ping 192.168.10.4

Pinging 192.168.10.4 with 32 bytes of data:

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

Ping statistics for 192.168.10.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Step 8: Repeat steps 6 and 7 for a PC in the faculty network to ensure communication within its VLAN and isolation from the student VLAN.

Result: Understood the concept of Virtual Local Area Network.

Experiment NO: 16

Date : 13/03/2024

Configuring and Verifying VLANs in Cisco

CO4: Construct Virtual Local Area Network (VLAN)

Aim: To configure and verify VLANs in CISCO

Principle:

VLAN is the abbreviation for Virtual LAN, i.e. Virtual Local Area Network. This is a custom network we create from one or more existing LANs. It enables a group of devices from multiple networks (both wired and wireless) to be combined into a single Logical network. The result is a VLAN that can be administered like a physical area network. The network equipment like routers or switches must support the VLAN configurations to create a VLAN.

Procedure:

Create a network in Cisco Packet Tracer and configure VLAN in it. Here we create 2 LANs with 6 hosts each of them and in each LAN we create 2 VLANs and try to communicate between them.

Step 1: At first, we create a LAN, LAN-A with 6 hosts. To create a LAN we need one Layer 2 switch Switch0 and 6 end devices. Now we provide IP addresses to the hosts starting from 192.168.10.1 (you can provide any valid IP addresses). To provide an IP address to a host just select that host → Desktop → IP Configuration → IPv4 Addresses and provide an IP address and then ENTER, the Subnet Mask will be provided by default.

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.10.1

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::2E0:8FFF:FED5:264E

Default Gateway:

DNS Server:

802.1X

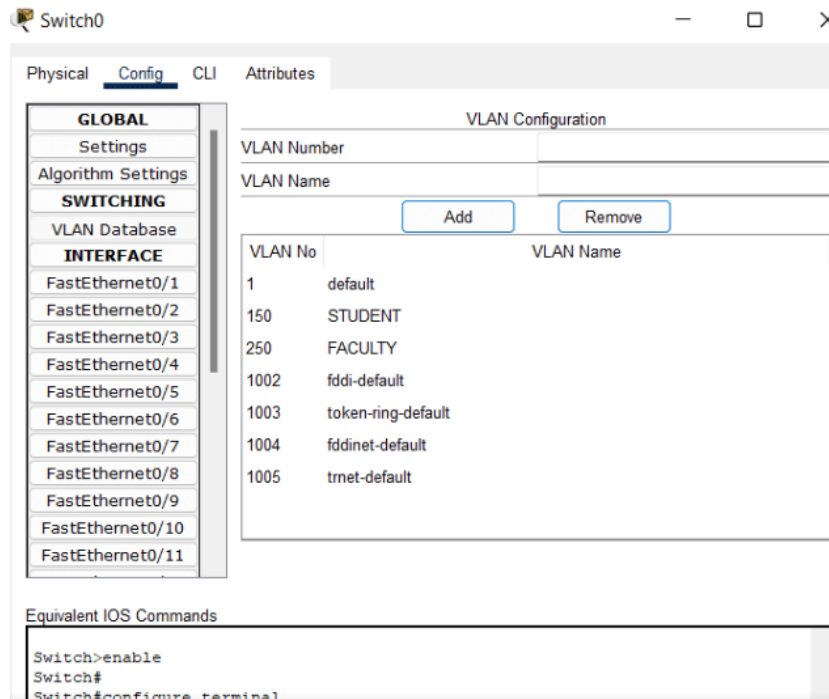
☐ Use 802.1X Security

Authentication: MD5

Username:

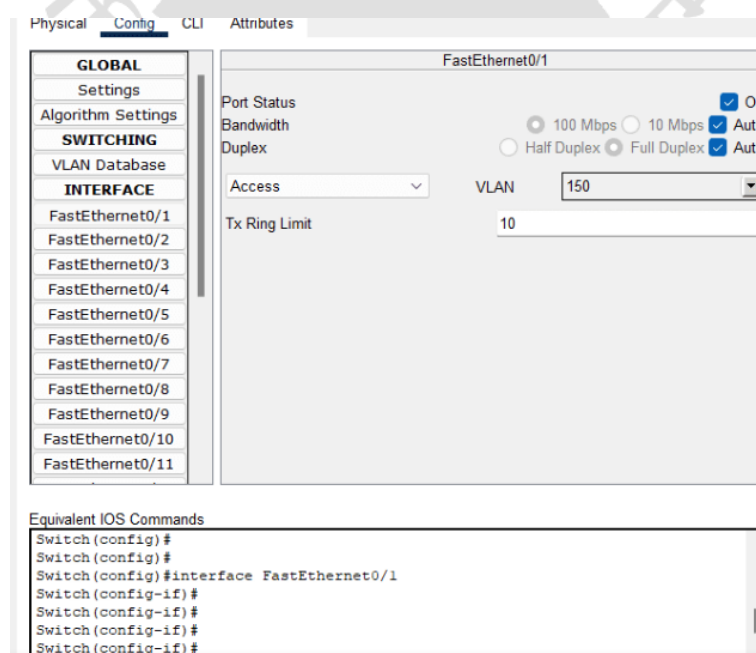
Password:

Step 2: Let us create 2 VLANs where the name of the first VLAN is VLAN-STUDENT and the second VLAN is VLAN-FACULTY. To configure VLANs we have to go to the switch Switch0 and move to Config → SWITCHING → VLAN Database. Now let us take the VLAN Number for STUDENT is 150 and for FACULTY is 250 and add these numbers to VLAN Database.



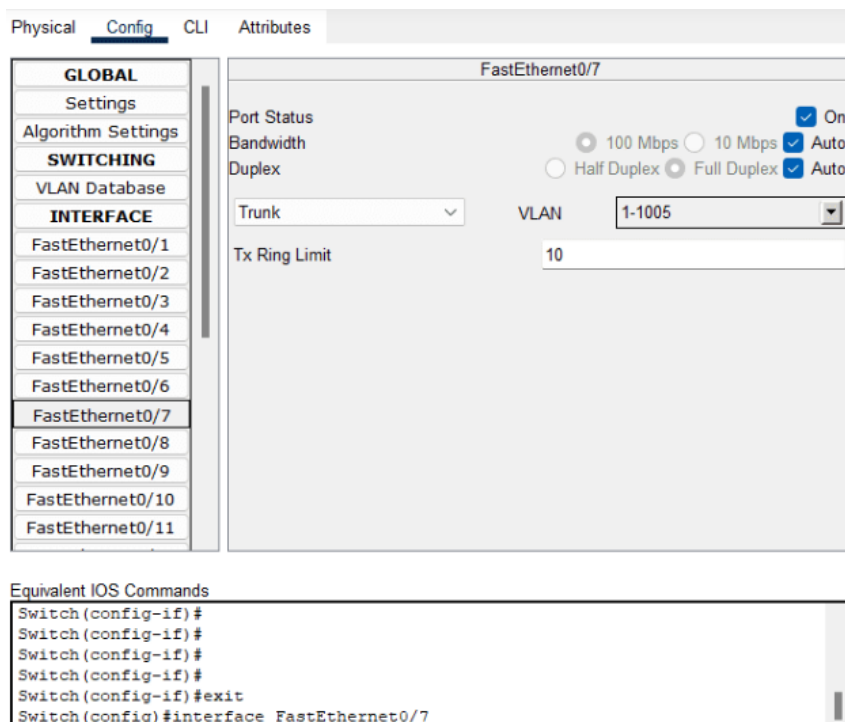
Step 3: Next we have to select the hosts under VLAN-STUDENT. Here I have put hosts with IP addresses from 192.168.10.1 to 192.168.10.3 under VLAN-STUDENT. To do so we have to select the switch Switch0 → Config → INTERFACE, here we choose FastEthernet0/1 corresponding to the host 192.168.10.1 which we consider to be in VLAN-STUDENT. Now we select the down arrow beside VLAN and select 150:STUDENT, which is for student VLAN.

Similarly, we do this same process for FastEthernet0/2 and FastEthernet0/3.

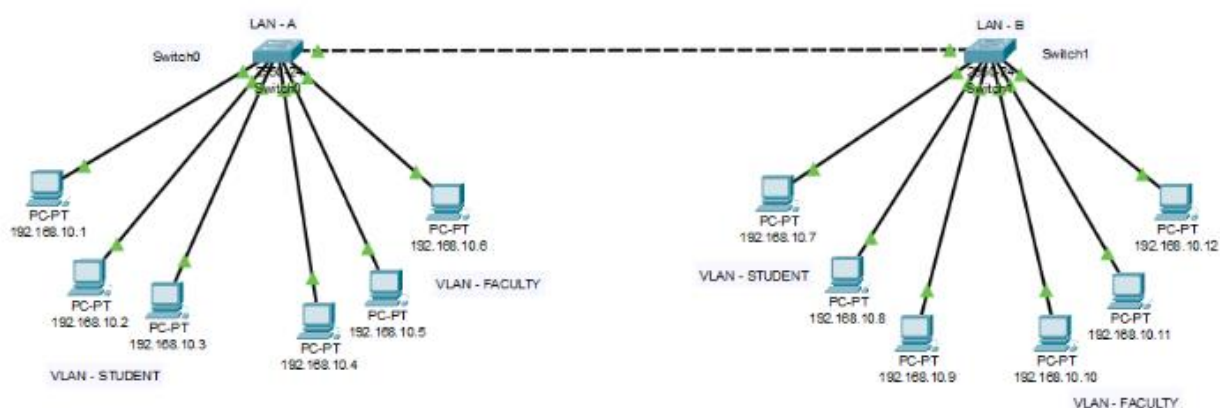


Step 4: Now we have to configure the hosts under VLAN-FACULTY. Here I have put hosts with IP addresses 192.168.10.4 to 192.168.10.6 under VLAN-FACULTY. To do so, just follow the process mentioned in Step 3, but instead of selecting the VLAN Number 150:STUDENT, select 250:FACULTY for FastEthernet0/4, FastEthernet0/5, and FastEthernet0/6.

Step 5: Lastly, just change the switch port mode from Access to Trunk for FastEthernet0/7.



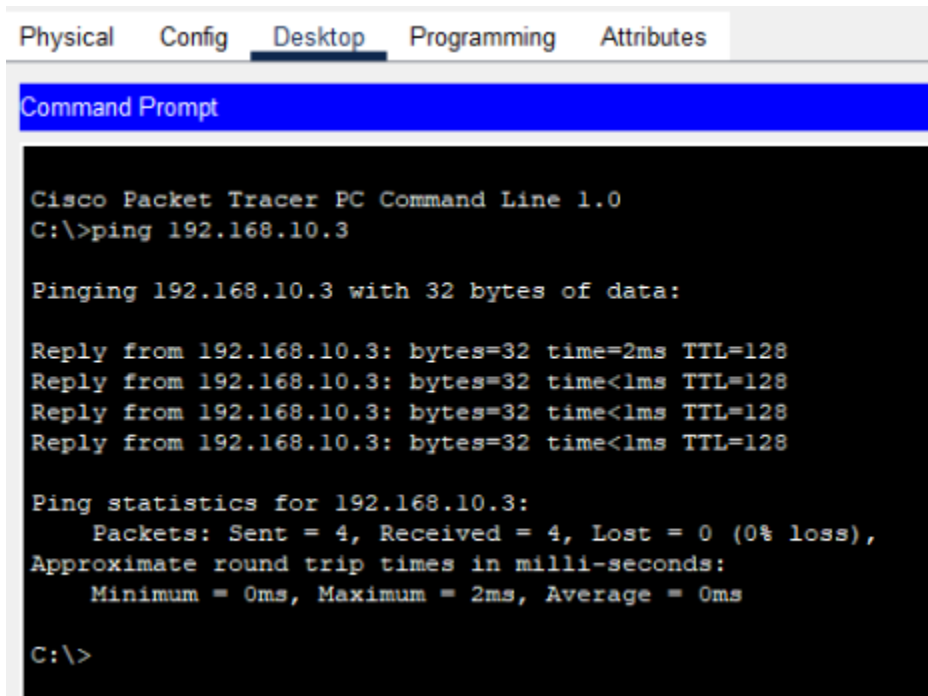
You can create LAN-B similarly by following these steps and connect LAN-A and LAN-B by using a Cross-Over cable. And your end network will look like this:



Now our VLAN configuration is ready, and we can check this by sending data packets from one host to another under LAN-A. Let us ping from 192.168.10.1 to 192.168.10.3. To do so, we have to select the host with IP 192.168.10.1 and then select Desktop → Command Prompt. Now run the following command to ping 192.168.10.3.

ping 192.168.10.3

You can get the Request timed out at first but don't worry, if you followed all the steps mentioned properly then run the command again to ping, and it'll do the job.



The screenshot shows the Cisco Packet Tracer interface with the 'Desktop' tab selected. A 'Command Prompt' window is open, displaying the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time=2ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>
```

Result: Studied to configure and verify VLANs in CISCO.